Парламентское Собрание Союза Беларуси и России
Постоянный Комитет Союзного государства
Аппарат Совета Безопасности Российской Федерации
Оперативно-аналитический центр при Президенте Республики Беларусь,
Федеральная служба по техническому и экспортному контролю Российской Федерации
Научно-исследовательский институт технической защиты информации
Межрегиональная общественная организация «Ассоциация защиты информации»

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы
XVI научно-практической конференции
17-20 мая 2011 года, г. Гродно (Республика Беларусь)

Минск
2011

УДК 004.056.5(476)(063)
ББК 32.81
К 63

Ответственный редактор
председатель программного комитета конференции,
заведующий кафедрой технологий программирования Белорусского
государственного университета, доктор технических наук,
профессор, Заслуженный деятель науки Республики Беларусь,

А.Н.Курбацкий

Комплексная защита информации: материалы XVI научно-практической конференции (17-20 мая 2011 года, г. Гродно). – Минск, 2011.– ____ с.

ISBN _____

Представлены материалы XVI научно-практической конференции «Комплексная защита информации», посвященные проблемам комплексной защиты информации и информационной безопасности. Рассматриваются нормативные правовые аспекты обеспечения информационной безопасности, вопросы создания защищенных объектов информационных технологий, защиты критически важных объектов информационно-коммуникационной инфраструктуры, криптографической и технической защиты информации, подготовки специалистов в области защиты информации.

Материалы рекомендованы к публикации программным комитетом конференции и печатаются в виде, представленном авторами.

ПРИВЕТСТВЕННЫЕ СЛОВА УЧАСТНИКАМ КОНФЕРЕНЦИИ

Участникам 16-й научно-практической конференции
«Комплексная защита информации»

Уважаемые участники и гости конференции!

От имени депутатов Палаты представителей Национального собрания Республики Беларусь и Парламентского Собрания Союза Беларуси и России, а также от себя лично сердечно приветствую вас на белорусской земле в городе Гродно.

Научно-практическая конференция «Комплексная защита информации» стала традиционной и проводится поочередно в Беларуси и России. В ней принимают участие лучшие представители науки в области защиты информации из Российской Федерации и Республики Беларусь, работники предприятий и фирм, известных в нашей стране и за ее пределами, производители и поставщики оборудования, программного обеспечения.

Сегодня во все сферы жизни активно внедряются информационные технологии. Их большие возможности и доступность должны максимально использоваться современным обществом. Вместе с тем нельзя не отметить уязвимость информационных систем от широкого спектра угроз внешнего и внутреннего характера, а также высокую вероятность наступления серьезных последствий, связанных с нарушением их функционирования. Научный анализ этих проблем и предложения по их решению – одна из важнейших задач конференции, в программу которой включены доклады по широкому спектру научных направлений.

Обсуждение организационно-правового обеспечения безопасности субъектов информационных отношений, современных методов, технологий и средств защиты информации, а также рассмотрение вопросов информационного противоборства, защиты критически важных объектов информационно-коммуникационной инфраструктуры и подготовки специалистов в области защиты информации являются актуальными, позволят выработать соответствующие практические рекомендации и послужат динамичному развитию информационных технологий в наших странах, укреплению сотрудничества и оказанию помощи друг другу в решении проблем, имеющихся в области защиты информации.

В рамках конференции Парламентским Собранием Союза Беларуси и России проводится семинар на тему «Безопасность информационного пространства Союзного государства». Депутаты Палаты представителей Национального собрания Республики Беларусь и Парламентского Собрания Союза Беларуси и России рассматривают оба мероприятия как еще одну форму нашего взаимодействия в ходе строительства Союзного государства.

Желаю вам, дорогие участники конференции, успешной и результативной работы на благо государств-участников Союзного государства.

Председатель Палаты представителей
Национального собрания
Республики Беларусь,
первый заместитель Председателя
Парламентского Собрания
Союза Беларуси и России В.П.Андрейченко

Участникам 16-й научно-практической конференции
«Комплексная защита информации»

Примите искренние поздравления по случаю открытия 16-й научно-практической конференции «Комплексная защита информации», которая является ежегодным значимым мероприятием Союзного государства. С момента проведения первой конференции в 1997 году данный форум является одним из ведущих международных мероприятий, на котором обсуждаются вопросы обеспечения информационной безопасности, защиты информационных ресурсов, создания эффективных технических и программных средств защиты информации.

Интенсивное внедрение информационных технологий во всех сферах жизнедеятельности общества привело к тому, что информационный ресурс является сегодня таким же богатством, как производственный и людской потенциал. При этом обеспечение информационной безопасности личности и государства является одним из важнейших факторов и необходимым условием, положительно влияющими на стабильное социально-политическое и экономическое развитие Беларуси, России и Союзного государства в целом.

Правительство Республики Беларусь рассматривает конференцию как общепризнанное международное мероприятие, на котором осуществляется обмен мнениями и выработка конструктивных предложений по решению теоретических, организационных, правовых и технических вопросов защиты информации. Выражаю уверенность, что запланированные к обсуждению темы, связанные с организационно-правовым обеспечением безопасности субъектов информационных отношений, современными методами и средствами защиты информации, позволят выработать предложения по решению существующих сегодня проблем информационной безопасности.

Уверен, что приоритеты развития информационных технологий, которые предстоит определить участникам конференции, позволят значительно повысить эффективность защиты информационного пространства Союзного государства Беларуси и России в современных условиях.

Желаю участникам конференции плодотворной работы и дальнейших успехов в решении задач информационной безопасности на благо наших стран и народов.

Заместитель Премьер-министра
Республики Беларусь А.Н.Калинин

Участникам 16-й научно-практической конференции
«Комплексная защита информации»

Уважаемые участники конференции!

Постоянный Комитет Союзного государства уделяет большое внимание вопросам совершенствования информационной безопасности Союзного государства и национальных систем защиты информации России и Беларуси. В июле 2007 года подписано постановление Совета Министров Союзного государства о придании этой конференции статуса ежегодной.

За 16 лет сделано немало. В 2004 году успешно завершена программа «Защита общих информационных ресурсов Беларуси и России», которая была принята еще Исполнительным Комитетом Союза Беларуси и России в 1999 году, то есть еще в прошлом тысячелетии. И это не случайно, так как вопросы связанные с построением Союзного государства пронизывает все сферы жизнедеятельности людей, а складывающаяся политическая и социально-экономическая обстановка в мире задачу информационной безопасности ставит на первый план.

Начало третьего тысячелетия человечество встретило серьезным прорывом в области освоения информационного пространства. В этой связи актуальность вопросов, связанных с защитой информации, приобретает еще большую значимость. И именно поэтому Постоянный Комитет Союзного государства ежегодно проводит эти научно-практические конференции. В ходе реализации первой программы сделано многое. Но жизнь не стоит на месте, и ее логическим продолжением являлась программа «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006-2010 годы». На заседании Совета Министров Союзного государства в марте 2011 года был принят Итоговый отчет о завершении этой программы. А на очередном заседании Совета Министров Союзного государства будет рассмотрен вопрос о Концепции проекта программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011-2015 годы.

Выражаю уверенность, что проводимое мероприятие послужит динамичному развитию информационных технологий в наших странах, укреплению сотрудничества, взаимодействия и помощи друг другу в решении проблем, встающих по мере реализации наших начинаний.

Нельзя не отметить высокую представительность научно-практической конференции. В нём принимают участие практически все заинтересованные стороны, представители руководящих государственных структур России и Беларуси, сотрудники компаний и предприятий, производители и поставщики оборудования, программного обеспечения. Также участвуют специалисты научно-исследовательских организаций, отраслевой инфраструктуры, некоммерческих структур, средств массовой информации.

Ежегодная научно-практическая конференция «Комплексная защита информации» проходит поочередно в Беларуси и России в течение 16 лет, где обсуждаются проблемы обеспечения информационной безопасности, осуществляется обмен опытом по вопросам использования информационных и коммуникационных технологий в различных сферах жизни общества и государства.

Ежегодная финансовая поддержка Постоянным Комитетом Союзного государства проведения этой конференции достаточно красноречиво говорит о том, что она признается важным элементом взаимодействия Беларуси и России в области обеспечения безопасности информационных технологий.

Организаторами конференции сформирована насыщенная и содержательная Программа. Запланировано рассмотреть важнейшие актуальные моменты и аспекты формирования общего информационного пространства России и Беларуси. Формы

совместной работы разнообразны: это и упомянутая выше научно-практическая конференция, и межгосударственный научно-практический семинар, и «круглые столы», и тематические выставки.

Перечень охватываемых вопросов можно назвать достаточно полным. Это предложения о совершенствовании законодательной и нормативно-регламентирующей базы информационного сообщества, особенности развития этой отрасли в каждой из стран – участниц Союзного государства, обсуждение вопросов криптографии, существующих проблем и путей решения вопросов стоящих в сферах защиты информации и информационной безопасности.

Полагаю, что сегодня в выступлениях участников будут высказаны конкретные предложения по совершенствованию защиты информационных ресурсов Союзного государства и их реализация в конечном итоге поможет нам эффективно решать задачи, связанные с дальнейшим построением Союзного государства.

Желаю участникам конференции успешной и результативной работы на благо государств-участников Союзного государства.

Заместитель Государственного секретаря –
член Постоянного Комитета Союзного государства Ю.М.Дубинский

Участникам 16-й научно-практической конференции
«Комплексная защита информации»

Уважаемые организаторы и участники 16-й научно-практической конференции «Комплексная защита информации»!

Прежде всего, разрешите передать Вам самые теплые пожелания успешной работы от Секретаря Совета Безопасности Российской Федерации Николая Платоновича Патрушева.

Вопросы, вынесенные на обсуждение участников конференции, так или иначе связаны с укреплением безопасности функционирования информационной инфраструктуры и развитием информационного пространства Союзного государства – Союза Беларуси и России – с усилением нашего сотрудничества в области использования потенциала современных информационных и коммуникационных технологий на благо человека, с повышением эффективности противодействия общим угрозам безопасности информационной сферы.

Мы знаем, что информационно-коммуникационные технологии являются эффективным инструментом содействия делу мира, безопасности и стабильности, укрепления демократии, социальной сплоченности граждан, надлежащего управления и верховенства права на национальном, региональном и международном уровнях. Данные технологии являются важным фактором экономического развития общества, повышения эффективности социальной политики государства, развития политической культуры граждан. Информационные технологии существенно расширяют возможности повышения эффективности государственного управления, создают новое измерение качества жизни человека.

В то же время всех нас объединяет понимание того, что для продолжения интенсивного развития информационной сферы Союзного государства необходимо обеспечить эффективное противодействие угрозам использования современных информационных технологий в целях нарушения международного мира и безопасности, совершения преступлений, подготовки и осуществления террористических актов, распространения террористической идеологии и практики разрешения противоречий общественного развития. Все мы понимаем, что добиться решительного перелома в противодействии данным угрозам еще не удалось, хотя определенные позитивные тенденции в этой области имеются.

С этой точки зрения настоящая конференция предоставляет прекрасную возможность обмена мнениями между экспертами по наиболее актуальным проблемам обеспечения информационной безопасности Союза Беларуси и Росси, по перспективным направлениям осуществления совместной деятельности по их решению.

Желаю всем участникам и гостям конференции успешной работы, плодотворных дискуссий и запоминающегося пребывания в этом замечательном белорусском городе.

Помощник Секретаря Совета Безопасности
Российской Федерации Н.В.Климашин

Участникам 16-й научно-практической конференции
«Комплексная защита информации»

Приветствую участников 16-й научно-практической конференции «Комплексная защита информации», прибывших на древнюю Гродненскую землю.

Значение защиты информации в обеспечении национальной безопасности государства и его успешного социально-экономического развития непрерывно возрастает. Эффективное функционирование системы обеспечения безопасности в информационной сфере невозможно без широкой международной координации политики в данной области. Обеспечение достижения целей Союзного государства, культурно-языковая близость, ускорение интеграционных процессов в экономической сфере и другие объективные факторы определяют важную роль взаимодействия Республики Беларусь и Российской Федерации в сфере защиты информации. Универсальный подход к анализу задач защиты информации, нацеленность на рассмотрение вопросов, имеющих высокую практическую значимость, способствовали утверждению репутации конференции «Комплексная защита информации» как важной инициативы по обеспечению безопасности Союзного государства.

Состав участников форума в текущем году подтверждает это. В ходе пленарных заседаний и «круглых столов» конференции планируется представить более 130 докладов по широкому перечню проблем обеспечения безопасности в информационной сфере. 28 докладов будут представлены на конференции сотрудниками Оперативно-аналитического центра при Президенте Республики Беларусь, являющегося головным государственным органом Республики Беларусь по технической защите информации, а также Научно-исследовательского института технической защиты информации.

Наши представители поделятся опытом деятельности по обеспечению технической защиты информации в Республике Беларусь и предложениями относительно перспектив работы в данной сфере. Мы высоко ценим предоставляемые конференцией возможности использования нашего потенциала на благо работы по укреплению безопасности Республики Беларусь и Российской Федерации в рамках Союзного государства, а также ознакомления с достижениями и идеями наших коллег.

Выражаю уверенность, что материалы 16-й научно-практической конференции «Комплексная защита информации» станут важным ресурсом для государственных органов Республики Беларусь и Российской Федерации при подготовке предложений по реализации ими своих полномочий в области обеспечения безопасности в информационной сфере.

Желаю всем участникам конференции успехов и плодотворной работы.

Начальник Оперативно-аналитического центра
при Президенте Республики Беларусь В.П.Вакульчик

Участникам 16-й научно-практической конференции
«Комплексная защита информации»

Уважаемые участники конференции, коллеги!

От имени Министерства связи и информатизации Республики Беларусь, и от себя лично приветствую участников и гостей 16-й научно-практической конференции «Комплексная защита информации» и пожелать всем плодотворной работы.

Хочу также поздравить всех участников и гостей Конференции с отмечаемым сегодня Всемирным днем электросвязи и информационного общества, который в этом году посвящен теме «Лучше жизнь с ИКТ в сельских районах».

Развитие информационного общества в Республике Беларусь сегодня является одним из национальных приоритетов Республики Беларусь. Национальная стратегия устойчивого социально-экономического развития Республики Беларусь на период до 2020 года рассматривает построение информационного общества как общенациональную задачу, требующую координации и объединения усилий государства, бизнеса и гражданского общества.

Завершившаяся в 2010 году Государственная программа информатизации «Электронная Беларусь» стимулировала внедрение информационных технологий в деятельность органов государственной власти, местных исполнительных органов, иных государственных организаций. Реализованы ведомственные проекты, направленные на развитие процессов информатизации в реальном секторе экономики, здравоохранении, образовании, культуре, торговле и других сферах жизнедеятельности общества. В период с 2008 по 2010 годы реализованы отдельные инфраструктурные компоненты построения «электронного правительства».

В августе прошлого года правительством утверждена Стратегия развития информационного общества в Республике Беларусь на период до 2015 года. Ее методологическую основу составляют документы Женевского и Тунисского саммитов по вопросам информационного общества, итоговый документ Минского, 2009 года, саммита «Соединим страны СНГ».

В реализацию Стратегии разработана и в марте текущего года утверждена Национальная программа ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011-2015 годы. Ее целью является создание условий для ускоренного развития услуг в сфере информационно-коммуникационных технологий, содействующих развитию информационного общества на инновационной основе.

Мероприятия Национальной программы в комплексе направлены на формирование и развитие государственной системы оказания электронных услуг госорганам, организациям и гражданам на базе ускоренного внедрения ИКТ в различные сферы жизни общества через формирование электронного правительства, электронного здравоохранения, электронного обучения, электронной занятости и социальной защиты населения, развитие национального контента.

Важнейшее место в Национальной программе занимает Подпрограмма «Безопасность информационно-коммуникационных технологий и цифровое доверие». Она направлена на развитие системы информационной безопасности, позволяющей минимизировать возможность злоупотребления персональной и иной конфиденциальной информацией, расширить сферу предоставления электронных услуг.

Надо отметить, что на нынешнем этапе развития информационного общества в Республики Беларусь, защита информации рассматривается как процесс регулярный, осуществляемый путем комплексного использования технических, программных средств и

организационных мероприятий на всех этапах разработки, испытаний и эксплуатации информационных систем.

Сегодняшняя конференция является важным этапом в развитии сотрудничества в области обеспечения информационной безопасности.

Выражаю надежду, что запланированные к обсуждению в рамках конференции актуальные вопросы информационной безопасности, подготовки специалистов в сфере защиты информации, современные методы и средства защиты информации, позволят выработать согласованные предложения по решению и предупреждению проблем национальной безопасности в целом.

Уверен, что профессиональный обмен мнениями в ходе работы Конференции будет способствовать ускорению и оптимизации решений по вопросам информационной безопасности в Республике Беларусь с целью совершенствования системы национальной безопасности.

Министр связи и информатизации
Республики Беларусь Н.П.Пантелей

Участникам 16-й научно-практической конференции
«Комплексная защита информации»

Уважаемый председатель Программного комитета конференции!

Уважаемые члены организационного комитета!

16 научно-практическая конференция, судя по плану её проведения, продолжает достойные традиции предыдущих конференций по проблематике комплексной защиты информации. На ней рассматриваются сложные и крайне важные вопросы защиты общих информационных ресурсов Беларуси и России, обсуждаются результаты, достигнутые в ходе выполнения совместных программ, и пути дальнейших исследований.

В 2010 году ФСТЭК России, ФСБ России и Оперативно-аналитический центр при Президенте Республики Беларусь завершили выполнение второй программы Союзного государства, государственным заказчиком-координатором которой была определена ФСТЭК России.

Сегодня мы можем отметить, что определённые в Программе 2006 2010 годов цели достигнуты, итоговый отчёт одобрен на заседании Совета Министров Союзного государства. Программа считается завершённой, проводятся мероприятия по реализации полученных результатов.

Реализация достигнутого позволит обеспечить дальнейшее совершенствование системы защиты общих информационных ресурсов Беларуси и России и на этой основе повысить защищённость информации в критически важных системах информационно-телекоммуникационной инфраструктуры Союзного государства, а также способствовать развитию высокотехнологичных методов и средств защиты информации ограниченного доступа при использовании высоких технологий её обработки.

В рамках научно-исследовательских и опытно-конструкторских работ, выполненных по заказу ФСТЭК России, разработаны и апробированы передовые технологии, не имеющие аналогов в мире, на основе которых изготовлены опытные образцы:

это средства высоконадёжной биометрической идентификации и аутентификации пользователей автоматизированных систем на основе анализа рукописных парольных фраз с возможностью анализа произвольных биометрических персонально-динамических параметров пользователей, подключённых по унифицированному интерфейсу;

это средства, обеспечивающего эффективную идентификацию пользователей автоматизированных систем на основе компьютерных речевых технологий.

Безусловно, полученные результаты имеют большую ценность и в связи с возможностью их использования при проведении работ по защите информации на национальном уровне.

Вместе с тем останавливаться на достигнутом уровне нельзя. Стремительно развиваются информационные технологии: достаточно отметить, что начинают активно внедряться GRID-технологии, так называемые облачные вычисления, суперкомпьютеры, биометрические технологии. Все это приводит к значительному расширению спектра угроз безопасности информации и непосредственно затрагивает проблематику информационной безопасности.

На основе анализа полученных результатов и в связи с дальнейшим расширением состава угроз в информационной сфере, повышением их опасности в условиях интенсивного развития информационных технологий ФСТЭК России совместно с Оперативно-аналитическим центром при Президенте Республики Беларусь и ФСБ России разработана Концепция новой программы Союзного государства «Совершенствование системы защиты

общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011-2015 годы.

Концепция одобрена Правительством Республики Беларусь, Правительством Российской Федерации и внесена на рассмотрение в Совет Министров Союзного государства.

В настоящее время завершается разработка проекта указанной программы Союзного государства.

После принятия программы предстоит большая работа по выполнению комплекса мероприятий, направленных на создание необходимых нормативно-методических и научно-технических условий для обеспечения безопасного функционирования критически важных систем информационной инфраструктуры и защиты информации ограниченного доступа на основе использования высоких технологий.

В составе наших представителей сегодня на конференции присутствуют специалисты Государственного научно-исследовательского испытательного института проблем технической защиты информации ФСТЭК России, а также других организаций, аккредитованных в области технической защиты информации не криптографическими методами.

Хотелось бы выразить уверенность, что конференция пройдет весьма плодотворно. Желаю участникам конференции успехов в решении поставленных задач, плодотворной работы в достижении целей обеспечения безопасности информации как на национальной уровне, так и в рамках Союзного государства.

Первый заместитель директора
ФСТЭК России В.Селин

А.С.ВАНЬКОВИЧ

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ГОСУДАРСТВ-УЧАСТНИКОВ И СОЮЗНОГО ГОСУДАРСТВА

Уважаемые товарищи!

Исходя из того, что концепции национальной безопасности Республики Беларусь и Российской Федерации являются методологической основой деятельности государства и совершенствования законодательства по различным направлениям обеспечения национальной безопасности, к настоящему моменту Беларусь и Россия сформировали достаточную концептуальную основу обеспечения своей национальной безопасности. Основные документы наших государств в этой сфере представлены на слайде 1.

В то же время наши государства учитывают две тенденции, сложившиеся в международной практике. Первая состоит в том, что неизбежное пересечение разнонаправленных интересов государств в международном сообществе является источником кризисов и конфликтов в различных областях межгосударственных отношений. Вторая проявляется в том, что совпадающие либо сходные интересы лежат в основе блокирования государств, образования и формирования ими межгосударственных образований. Данное положение в полной мере относится к процессу создания Союзного государства.

Необходимо отметить, что в современных условиях создание Союзного государства исходит и из практической целесообразности объединения усилий России и Беларуси в противодействии негативным факторам и последствиям глобализации мировых экономических, политических, социальных, культурных, информационных, экологических и иных процессов.

Совместными усилиями Республика Беларусь и Российская Федерация сформировали общую концептуальную базу обеспечения безопасности Союзного государства в различных областях. Перечень основных документов Союзного государства в сфере информационной безопасности показан на слайде 2.

Уважаемые коллеги!

Сегодня стала актуальной задача формирования новой концепции безопасности Союзного государства. В обоснование этого предложения считаю необходимым отметить, что Концепция безопасности Союза Беларуси и России была утверждена Решением Высшего Совета Союза Беларуси и России еще в апреле 1999 года, то есть 12 лет назад. По нашему мнению, эта Концепция выполнила свое предназначение. В то же время изменились вызовы и угрозы, совершенствовались национальные и союзная системы обеспечения безопасности и, что особенно важно, у наших государств утверждены новые концепции национальной безопасности. Эти концепции сходны по структуре, достаточно гармонизированы и унифицированы по содержанию, что является достаточной основой для того, чтобы на их основе разработать проект Концепции безопасности Союзного государства для последующего рассмотрения и утверждения Высшим Государственным Советом Союзного государства.

Товарищи!

Как председатель Комиссии Парламентского Собрания Союза Беларуси и России по безопасности, обороне и борьбе с преступностью я должен отметить, что Парламентское Собрание во взаимодействии с другими органами Союзного государства, с профильными комитетами (комиссиями) палат Федерального Собрания Российской Федерации, Национального собрания Республики Беларусь и заинтересованными министерствами и ведомствами Беларуси и России проводит согласованную работу по упреждающему

нормативно-правовому обеспечению деятельности государств-участников по вопросам безопасности информационного пространства Союзного государства.

Осуществляется мониторинг международного и национального законодательств по вопросам информационной безопасности Союзного государства. Проводится анализ действующих договоров, соглашений Республики Беларусь и Российской Федерации в сфере информационной безопасности.

Практика показывает, что нам необходимо разработать согласованный перечень нормативных правовых актов государств-участников Союзного государства в области информационной безопасности, подлежащих разработке и унификации, обеспечить их принятие (ратификацию).

В Российской Федерации в конце прошлого года принят федеральный закон «О безопасности» (представлен на слайде 3), который определяет основные принципы обеспечения безопасности в стране и, по сравнению со старой редакцией закона, принятой в 1992 году, более подробно распределяет полномочия в этой сфере между властями страны.

Согласно документу, основными принципами обеспечения безопасности является соблюдение и защита прав и свобод человека и гражданина, законность, системность и комплексность применения органами власти политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности. Законопроект провозглашает «приоритет предупредительных мер».

В новом документе более подробно прописаны полномочия главы государства, парламента, правительства, федеральных органов исполнительной власти, функции органов госвласти субъектов РФ и органов местного самоуправления в области безопасности.

Президент определяет основные направления госполитики в этой сфере, утверждает стратегию национальной безопасности РФ, другие концептуальные и доктринальные документы в области обеспечения безопасности. Глава государства формирует и возглавляет Совет безопасности РФ, устанавливает компетенцию федеральных органов исполнительной власти, которыми он руководит, в области обеспечения безопасности. Кроме того, президент в порядке, установленном законодательством, вводит на территории РФ или в отдельных ее местностях чрезвычайное положение, а также исполняет полномочия в области обеспечения режима ЧП.

Кроме того, к юрисдикции президента отнесено принятие решений о применении специальных экономических мер для обеспечения безопасности, мер по защите граждан от преступных и иных противоправных действий, по противодействию терроризму и экстремизму.

К полномочиям парламента в области безопасности отнесено рассмотрение и принятие федеральных законов по ее обеспечению. Помимо этого, Совет Федерации, как и сейчас, утверждает указы президента о введении ЧП.

Правительство, согласно закону, участвует в определении основных направлений государственной политики по безопасности, формирует федеральные целевые программы в этой области и обеспечивает их реализацию. Правительство также устанавливает компетенцию федеральных органов исполнительной власти, которыми руководит, в сфере безопасности и обеспечивает органы власти средствами и ресурсами, необходимыми для выполнения таких задач.

Помимо органов власти, граждане и общественные объединения также участвуют в реализации государственной политики по безопасности.

В законе уточнен статус Совета безопасности РФ как конституционного совещательного органа, который готовит решения президента РФ по вопросам обеспечения безопасности, организации обороны, военного строительства, оборонного производства, военно-технического сотрудничества РФ с иностранными государствами и по другим вопросам, связанным с этой областью. К основным задачам Совбеза отнесено обеспечение условий для реализации главой государства полномочий в области обеспечения

безопасности, формирование госполитики в этой сфере и контроль за ее реализацией, прогнозирование, выявление, анализ и оценка угроз безопасности, оценка военной опасности и военной угрозы, выработка мер по их нейтрализации.

Отмечу, что в Республике Беларусь нет такого общего закона. Очевидно назрела необходимость рассмотреть целесообразность разработки его проекта.

Так же, как и проанализировать комплект документов Российской Федерации в развитие своей Концепции национальной безопасности с целью рассмотреть целесообразность разработки подобных документов в Республике Беларусь.

Это Стратегия национальной безопасности Российской Федерации до 2020 года. Учитывая, что большинство присутствующих знакомо с ее содержанием, я ограничусь изложением ее структуры, которая представлена на слайде 4.

Уважаемые товарищи!

В ходе пленарных заседаний и заседаний секций с учетом их тематики представляется полезным рассмотреть Доктрину информационной безопасности Российской Федерации, которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Структура Доктрины показана на слайде 5.

Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере и служит основой для:

– формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;

– подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

– разработки целевых программ обеспечения информационной безопасности Российской Федерации.

В заключение хочу отметить, что формирование концептуальных основ защиты информационной сферы Союзного государства от современных информационных вызовов и угроз выступает как одно из приоритетных направлений обеспечения национальной безопасности государств-участников и общей безопасности Союзного государства.

Опыт участников конференции и семинара поможет выработать рекомендации для совершенствования совместной деятельности в информационной сфере и в целях обеспечения безопасности информационного пространства Союзного государства

С.Н.КАПАРИХА

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Уважаемые участники и гости конференции!

От имени Оперативно-аналитического центра при Президенте Республики Беларусь приветствую участников и гостей 16-й научно-практической конференции «Комплексная защита информации».

***

Нынешняя конференция проходит на фоне стремительных процессов внедрения информационно-коммуникационных технологий во все сферы жизнедеятельности общества, государств и экономик Беларуси и России. При этом наряду с достижениями в этой области мы сталкиваемся с новыми угрозами национальной безопасности.

Последнее время все чаще фиксируются факты компьютерных инцидентов в информационных системах республики и других стран.

В июле 2010 года с использованием вируса Stuxnet были осуществлены атаки на десятки миллионов компьютерных систем в Китае, Индии, Иране и ряде других стран. Установлено, что конечной целью создателей данной вредоносной программы являлись информационные системы Бушерской АЭС.

В течение 2009-2011 годов в Беларуси неоднократно фиксировались сбои в функционировании системы обработки безналичных расчетов банковских пластиковых карточек Банковского процессингового центра.

В конце 2010 года и апреле 2011 года зафиксированы многочисленные DDoS-атаки на сайты государственных органов республики. Причем атакам подвергаются не только государственные ресурсы, но также социальные сети и коммерческие сайты.

Сейчас широко обсуждается факт хищения из мультимедийных сетей компании Sony личных данных 77 миллионов человек, имеющих там персональные счета. Эксперты зафиксировали вторжение 27 апреля этого года, хотя, по их же мнению, хакерская атака состоялась еще 20 апреля.

В апреле этого же года в Москве был задержан злоумышленник, который путем дистанционного доступа к компьютеру бухгалтера одной из фирм получил контроль над счетами этой фирмы и похитил 5 миллионов рублей.

Атакам подвергаются и сети беспроводного доступа. Например, сейчас уже в США, в Сиэтле, полиция расследует ряд преступлений, в результате которых путем несанкционированного подключения к Wi-Fi сетям похищено более 750 тыс. долларов.

Подобного рода примеров можно привести великое множество. Как видим угрозам подвергаются самые разнообразные информационные системы: как государственные, так и коммерческие, и в самом различном исполнении. Естественно государство не может не реагировать на это.

***

Приоритетным направлением в обеспечение безопасности информационно-коммуникационных систем республики является развитие законодательства в этой сфере, как основы организации работ всех заинтересованных государственных органов, иных организаций и граждан.

Упомяну только основные акты законодательства, принятые за истекший период.

27 мая 2009 года вступили в силу ряд взаимоувязанных правовых актов, определивших порядок защиты информации в информационных системах. Это Закон Республики Беларусь «Об информации, информатизации и защите информации», а также

постановление Правительства от 26 мая 2009 г. № 675 «О некоторых вопросах защиты информации».

Одним из наиболее важных направлений в рассматриваемой сфере является защита государственных секретов. Основным законодательным актом, регулирующим правоотношения в этой области, является Закон Республики Беларусь «О государственных секретах», новая редакция которого вступила в силу 19 января 2011 года. Настоящий Закон определяет правовые основы отнесения сведений к государственным секретам, их засекречивания, рассекречивания и защиты, а также регулирует отношения, возникающие при обращении с государственными секретами, в целях обеспечения национальной безопасности Республики Беларусь. В развитие данного Закона Правительством принято постановление от 01 февраля 2011 г. № 115 «Об утверждении Положения об организации технической защиты государственных секретов».

С 21 января 2011 года в республике действует Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи». Данный нормативный правовой акт устанавливает правовые основы применения электронных документов и электронной цифровой подписи, определяет основные требования, предъявляемые к электронным документам, а также права, обязанности и ответственность участников правоотношений, возникающих в сфере обращения электронных документов и электронной цифровой подписи.

С целью повышения качества предоставляемых гражданам и юридическим лицам интернет-услуг, информации о деятельности государственных органов, иных организаций в республике принят ряд решений руководства страны. За сравнительно короткий срок достигнуты неплохие результаты.

Так, внешний интернет-шлюз за год расширился с 57 до 110 Гбит/с, количество доменных имен, зарегистрированных в зоне «by» выросло с 27263 до 40510, количество портов широкополосного подключения увеличилось с примерно 600 тыс. до 1,5 млн.

Тариф на услуги доступа к сети Интернет с гарантированной полосой пропускания при скорости потока 1 Мбит/с снизился для интернет-провайдеров с 416 долларов на конец 2009 года до 78 долларов в месяц на средину мая этого года. Также произошло снижение стоимости предоставления в пользование и техническое обслуживание абонентской линии при оказании оператором услуг доступа к сети Интернет по технологии xDSL.

9 ноября 2010 года Президент Республики Беларусь своим Указом №575 утвердил новую Концепцию национальной безопасности Республики Беларусь, которая закрепляет совокупность официальных взглядов на сущность и содержание деятельности Республики Беларусь по обеспечению национальной безопасности в современных условиях. Впервые в данном документе вводится понятие «информационная безопасность», а к числу основных национальных интересов в информационной сфере отнесено «обеспечение надежности и устойчивости функционирования критически важных объектов информатизации».

С целью формирования современных подходов к проектированию и созданию защищенных компьютерных систем, новых технологий по созданию элементной базы и средств технической защиты информации нашим Правительством утвержден ряд государственных программ, среди которых необходимо отметить:

Национальную программу ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011 – 2015 годы, которая включает подпрограмму «Безопасность информационно-коммуникационных технологий и цифровое доверие»;

Государственную научно-техническую программу «Развитие методов и средств системы комплексной защиты информации» на 2011–2015 годы.

***

Сделаны практические шаги по развитию и обеспечению безопасности информационно-коммуникационной инфраструктуры Беларуси. В соответствии с Указом Президента Республики Беларусь от 30 сентября 2010 г. № 515 Оперативно-аналитическому

центру поручено создать единую республиканскую сеть передачи данных (далее – ЕРСПД). Данная сеть объединит посредством современных высокоскоростных технологий сети передачи данных республиканских органов государственного управления, местных исполнительных и распорядительных органов, иных государственных органов и других государственных организаций, а также частных структур.

ЕРСПД станет базовой составляющей национальной информационно-коммуникационной инфраструктуры нашей страны. При этом сеть будет обеспечивать защиту от несанкционированного доступа к передаваемым по ней данным.

Указ устанавливает, что проектирование и строительство вновь создаваемых и (или) реконструируемых волоконно-оптических линий связи для организации сетей передачи данных, за исключением технологических сетей электросвязи, осуществляются при условии последующего их присоединения к ЕРСПД. Предусматривается взаимодействие сети с сетями электросвязи иностранных государств.

В первом квартале текущего года Оперативно-аналитический центр организовал проведение открытого конкурса на разработку и реализацию лучшего технического решения по построению опорной сети передачи данных для ЕРСПД.

Завершение объединения в ЕРСПД существующих сетей передачи данных государственных органов и организаций, принятие иных мер по организации и функционированию ЕРСПД должно быть завершено к 1 января 2012 года.

В соответствии с данным Указом Оперативно-аналитический центр определен независимым регулятором в сфере информационно-коммуникационных технологий (далее - ИКТ), который:

определяет стратегию развития ИКТ;

согласовывает в установленном порядке инвестиционные проекты, проекты законодательных актов, постановления Совета Министров Республики Беларусь в сфере ИКТ;

рассматривает обращения юридических лиц и индивидуальных предпринимателей по вопросам, связанным с лицензированием деятельности в области связи в части услуг передачи данных и телефонии по IP-протоколу, по их результатам вносит в Министерство связи и информатизации обязательные к исполнению решения;

принимает меры по противодействию недобросовестной конкуренции при оказании услуг передачи данных и телефонии по IP-протоколу;

регулирует тарифы на услуги электросвязи по присоединению сетей передачи данных к ЕРСПД, в том числе путем установления порядка определения и применения тарифов на услуги электросвязи по присоединению сетей передачи данных к ЕРСПД;

принимает решения, обязательные к исполнению операторами электросвязи и иными участниками рынка услуг электросвязи, по вопросам оказания услуг передачи данных и телефонии по IP-протоколу;

вносит предложения о совершенствовании законодательства в сфере ИКТ;

осуществляет иные полномочия в соответствии с законодательными актами.

Одним из приоритетных направлений государственного строительства в Республике Беларусь является курс на максимально широкое предоставление электронных государственных услуг гражданам и юридическим лицам, то есть - на реализацию проекта «Электронное правительство».

Для обеспечения идентификации и аутентификации пользователей Электронного правительства создается Государственная система управления открытыми ключами (далее - ГОСУОК). Одновременно ГОСУОК должна стать основой для организации электронного документооборота в республике с применением электронной цифровой подписи. С этой целью разрабатывается программно-аппаратная платформа удостоверяющих центров для оказания услуг по распространению открытых ключей государственным служащим и

обеспечения международного взаимодействия с использованием сертификатов открытых ключей.

Во исполнение поручения Главы государства межведомственной рабочей группой разработан проект Указа Президента Республики Беларусь «О некоторых вопросах развития информационного общества в Республике Беларусь».

Данный проект Указа направлен на обеспечение устойчивого развития информационного общества в Республике Беларусь, совершенствование государственной системы управления процессом информатизации и регулирования рынка телекоммуникационных услуг.

Документ предусматривает создание Совета по развитию информационного общества при Президенте Республики Беларусь, единого оператора межведомственных информационных систем различных ведомств - Национального центра электронных услуг, который, кроме предоставления самих услуг, будет координировать деятельность по обеспечению безопасности информационных систем государственных органов.

Вышеназванный Совет будет являться совещательным органом, создаваемым в целях совершенствования мер государственной информационной политики, содействующей развитию информационного общества в Республике Беларусь как одного из национальных приоритетов.

Основной задачей Совета является выработка решений по определению государственной информационной политики и совершенствованию механизмов ее реализации.

Совет будет осуществлять свою деятельность по следующим основным направлениям:

определение целей и задач государственной информационной политики, методов и способов ее реализации;

общая координация деятельности государственных органов и иных организаций по развитию информационного общества в Республике Беларусь;

определение мер по укреплению национальной безопасности в информационной сфере;

определение мер государственной поддержки деятельности по развитию информационного общества в Республике Беларусь;

Совет будет иметь право поручать государственным органам и иным организациям подготовку предложений по вопросам развития информационного общества в Республике Беларусь, а также привлекать для осуществления информационно-аналитических и экспертных работ научные и другие организации, а также ученых и специалистов.

Проектом Указа предусматривается утверждение Положения о независимом регуляторе в сфере информационно-коммуникационных технологий, которым, как было указано ранее, является Оперативно-аналитический центр.

***

Важнейшим фактором успеха в области развития информационных технологий является наличие высококвалифицированных кадров, способных создавать современные программные и программно-технические решения, а также обеспечивать их безопасность.

С целью поиска оптимальных путей по подготовке необходимых специалистов в республике в течение нескольких лет обсуждался национальный проект «ИТ - страна», который в конечном итоге нашел свое воплощение в подпрограмме «Развитие экспортно-ориентированной ИТ-индустрии» Национальной программы ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011–2015 годы, которая предусматривает создание условий для внедрения образовательных программ ведущих зарубежных учебных заведений в сфере ИТ-образования, крупнейших ИТ-компаний, выдающих диплом или сертификат международного образца, и организацию учебного процесса по этим программам.

Указанной подпрограммой предусмотрено создание методического центра, обеспечивающего мониторинг международного рынка учебных программ для ИТ-специальностей, исследование мировых тенденций в сфере информационных технологий и составление прогнозов, формирование списка специальностей и специализаций, определение квалификационных требований к ним и выполнение ряда иных функций.

Развивается и вузовская система подготовки и повышения квалификации кадров в сфере информационной безопасности. В течение двух последних лет организована подготовка специалистов по специальности «Компьютерная безопасность» в Гродненском государственном и Полоцком государственном университетах. Необходимо отметить, что специалистов в области защиты информации до этого готовили только столичные вузы: БГУ, БГУИР и БНТУ.

Это примечательный факт, свидетельствующий о востребованности специалистов по информационной безопасности не только в столичном регионе.

Несмотря на определенные успехи в образовательной политике, проблема нехватки высококвалифицированных специалистов остается весьма острой. Поэтому и в дальнейшем государство будет уделять пристальное внимание вопросам образования в сфере безопасности информационных технологий.

Надо отметить, что индустрия информационной безопасности формируется в значительной мере частными предприятиями, и качество их работ и услуг непосредственно влияет на состояние защищенности нашей информационной сферы. Принимая во внимание данный фактор, в нашем законодательстве введено требование к организациям-лицензиатам Оперативно-аналитического центра о необходимости наличия у них соответствующего количества специалистов со специальным образованием в сфере информационной безопасности.

На сегодняшний день работы на основании лицензий в области обеспечения информационной безопасности в республике выполняют 134 организации. Фактически лицензиатами являются все крупнейшие в стране разработчики, проектировщики, производители и интеграторы в области информационных технологий.

Для контроля за качеством поставляемых в республику средств защиты информации создана система сертификации и государственной экспертизы по требованиям безопасности информации. Руководящим органом государственной экспертизы и сертификации в данной области является Оперативно-аналитический центр, а непосредственно испытания осуществляют 13 аккредитованных совместно с Госстандартом испытательных лабораторий.

***

Безусловно, перечисленные в докладе принимаемые в нашей стране меры по обеспечению информационной безопасности не являются раз и навсегда застывшей материей. Область, в которой мы с вами трудимся, отличается исключительно высоким динамизмом и требует постоянного адекватного реагирования на вновь возникающие угрозы, а в идеале, - упреждающих воздействий по обеспечению безопасности нашего общего кибернетического пространства.

Убежден, что на конференции мы услышим интересные выступления, и будет рождено много плодотворных идей, которые будут способствовать обеспечению информационной безопасности Беларуси и России.

Удачной вам работы.

Благодарю за внимание!

РАЗДЕЛ 1
НОРМАТИВНЫЕ И ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.В.ВОЙТОВ

ЗАЩИТА ИНФОРМАЦИИ – ВАЖНАЯ СОСТАВЛЯЮЩАЯ НАУЧНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ПОДДЕРЖКИ ИННОВАЦИОННОГО РАЗВИТИЯ СТРАНЫ

В настоящее время остро назрела необходимость обеспечения функционирования государственной системы защиты информации. Созданные в последние годы организационные структуры, принятые национальные законодательные акты, действующая нормативная, методологическая и материально-техническая базы еще не в полной мере решают основополагающую задачу в данной области – обеспечение безопасности Республики Беларусь в информационной сфере, являющейся составной частью национальной безопасности.

За последние годы в республике реализуется комплекс мер по совершенствованию обеспечения информационной безопасности. Вместе с тем анализ состояния безопасности информационно-вычислительных систем различных государственных органов, организаций и предприятий республики показывает, что ее уровень не в полной мере соответствует современным потребностям. Отставание отечественных информационных технологий вынуждает государственные органы при создании информационно-вычислительных систем идти по пути закупок средств вычислительной техники, а также программного обеспечения импортного производства, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации.

В связи с расширением сфер применения систем обработки и распространения информации наблюдается рост количества случаев несанкционированного использования, модификации и уничтожения информации. Угрозы вычислительному и информационному ресурсам не могут быть выявлены, локализованы и ликвидированы внедрением в информационные системы отдельных аппаратных, программных средств и организационных мероприятий. Все средства и мероприятия должны быть объединены в систему защиты. Защиту информации следует рассматривать как регулярный процесс, осуществляемый путем комплексного использования технических, программных средств и организационных мероприятий на всех этапах разработки, испытаний и эксплуатации информационных систем. Требования по защите, предъявляемые к информационной системе, должны рассматриваться как часть общих функциональных требований к ней.

Научно-техническое обеспечение развития информатизации в республике в рамках программы «Электронная Беларусь» в 2006 – 2010 годах и подготовка Стратегии развития информационного общества в Республике Беларусь на период до 2015 года (утверждена постановлением Совета Министров Республики Беларусь от 09.08.2010 № 1174) осуществлялись на основе Государственной комплексной целевой научно-технической программы «Информационные технологии» (государственный заказчик – НАН Беларуси). Данная программа была направлена на создание новых интеллектуальных информационных технологий и систем, разработку моделей, математических методов и программно-

аппаратных средств для повышения конкурентоспособности продукции и развития социальной сферы страны.

Государственная комплексная целевая научно-техническая программа «Информационные технологии» представляла собой комплекс из государственной комплексной программы научных исследований «Научные основы информационных технологий и систем (Инфотех)» и двух государственных научно-технических программ «Информационные технологии» и «Защита информации», взаимодополняющих друг друга в рамках приоритетного направления научной и научно-технической деятельности «Информационные и телекоммуникационные технологии».

Направленностью Государственной комплексной целевой научно-технической программы «Информационные технологии» являлось научное и научно-техническое обеспечение государственных программ:

– государственная программа информатизации Республики Беларусь на 2003-2005 годы и на перспективу до 2010 года «Электронная Беларусь»;

– государственная научно-техническая программа «Разработка и внедрение современных техники, средств и технологий для государственной системы предупреждения и ликвидации чрезвычайных ситуаций и гражданской обороны» (ГНТП «Защита от чрезвычайных ситуаций»);

– государственная научно-техническая программа «Разработать и внедрить в промышленности технологии информационной поддержки жизненного цикла продукции (ГНТП «CALS-технологии»);

– государственная программа вооружения на 2006-2015 гг.;

– научно-технические программы Союзного Государства – «Развитие и внедрение в государствах-участниках Союзного государства наукоёмких компьютерных технологий на базе мультипроцессорных вычислительных систем» («Триада»); «Разработка базовых элементов, технологий создания и применения орбитальных и наземных средств многофункциональной космической системы» («Космос-НТ»); «Разработка и использование программно-аппаратных средств ГРИД-технологий и перспективных высокопроизводительных (суперкомпьютерных) вычислительных систем семейства «СКИФ»» («СКИФ–ГРИД»); «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006–2010 годы»; «Разработка нанотехнологий создания материалов, устройств и систем космической техники и их адаптация к другим отраслям техники и массовому производству» («Нанотехнология-СГ»);

– государственная программа «Научное сопровождение развития атомной энергетики в Республике Беларусь на 2009 – 2010 годы и на период до 2020 года».

В настоящее время информационно-коммуникационные технологии также входят в число приоритетных направлений научно-технической деятельности в Беларуси, утвержденных Указом Президента Республики Беларусь от 22 июля 2010 г. №378 ”Об утверждении приоритетных направлений научно-технической деятельности в Республике Беларусь на 2011 – 2015 годы“.

Концепцией Государственной программы инновационного развития Республики Беларусь на 2011–2015 годы, одобренной Президиумом Совета Министров Республики Беларусь (протокол заседания от 21 апреля 2010 г. № 11), среди важнейших направлений инновационного развития отраслей и регионов определены:

– построение современной телекоммуникационной инфраструктуры;

– создание и обеспечение функционирования государственной системы оказания электронных услуг;

– формирование и развитие в республике услуг в сфере информационно-коммуникационных технологий, соответствующих мировому уровню.

В ходе реализации Национальной программы ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011 – 2015 годы предполагается

применение современных решений в области технологий, отнесенных Концепцией Государственной программы инновационного развития Республики Беларусь на 2011 – 2015 годы к критическим, а именно:

– обработки и передачи информации, формирования и хранения государственных информационных ресурсов;

– создания и обеспечения функционирования государственной системы предоставления информационных услуг;

– функционирования интегрированных систем автоматизации деловых и административных процедур, электронного документооборота;

– функционирования технических и аппаратно-программных систем и средств защиты информации и контроля ее защищенности;

– развития государственной системы научно-технической информации (образовательных, медицинских, библиотечных, музейных интернет-ресурсов).

Достигнутые результаты и положительный опыт реализации Государственной комплексной целевой научно-технической программы «Информационные технологии» положены в основу формирования государственной комплексной целевой научно-технической программы «Информационные и космические технологии» на 2011-2015 годы (постановление Совета Министров Республики Беларусь от 01.02.2011 № 116). Государственный заказчик – координатор НАН Беларуси.

Государственная комплексная целевая научно-техническая программа «Информационные и космические технологии» направлена на инновационно-структурное обновление экономики, стимулирование разработки и реализации эффективных инновационных и инвестиционных проектов и на повышение уровня конкурентоспособности экономики на основе структурной перестройки, технико-технологического перевооружения и реструктуризации производства. Программа является научно-техническим обеспечением Концепции национальной безопасности Республики Беларусь, Национальной программы исследования и использования космического пространства в мирных целях на 2008-2012 годы, Национальной программы ускоренного развития услуг в сфере информационно-коммуникационных технологий и Программы деятельности Правительства на 2011 – 2015 годы.

Основной целью данной программы в части информатизации является научное и научно-техническое обеспечение перехода информационно-коммуникационных технологий в одну из ведущих отраслей экономики, противодействие использованию потенциала ИКТ в целях угрозы национальным интересам Республики Беларусь, а также получения посредством информационных технологий возможности использования космических технологий в повседневной деятельности при принятии коммерческих и управленческих решений в сельском, лесном, водном хозяйстве и мелиорации, предотвращении и ликвидации последствий чрезвычайных ситуаций, разведке недр и обновлении топографических карт.

Государственная комплексная целевая научно-техническая программа «Информационные и космические технологии» представляет собой комплекс из государственной комплексной программы научных исследований, государственной программы научных исследований и четырех государственных научно-технических программ, взаимодополняющих друг друга в рамках приоритетного направления научной и научно-технической деятельности «Информационно-коммуникационные, авиационные и космические технологии». В состав Государственной комплексной целевой научно-технической программы включены шесть самостоятельных программ: государственная программа научных исследований «Информатика и космос», государственная программа прикладных научных исследований «Космические исследования», государственные научно-технические программы «Информационные технологии», «CALS-ERP-технологии», «Защита информации-2» и «Космические системы и технологии».

Государственная научно-техническая программа «Развитие методов и средств системы комплексной защиты информации» (ГНТП «Защита информации-2») на 2011-2015 гг. направлена в первую очередь на реализацию Концепции национальной безопасности Республики Беларусь.

К числу приоритетных направлений обеспечения безопасности Республики Беларусь в информационной сфере данной Концепцией отнесены следующие направления:

– разработка и внедрение современных методов и средств защиты информационных технологий, прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;

– осуществление государственного контроля за разработкой, созданием, развитием и использованием средств защиты информации;

– обеспечение правовых и организационных условий предупреждения, выявления, пресечения преступлений в информационной сфере.

Обеспечение технологической независимости Республики Беларусь в важнейших областях информатизации, телекоммуникации и связи, управлении технологическими процессами и производством, транспорте, энергетике и т.д. позволит определить стратегическую задачу создания основы для информационной безопасности государства. При этом приоритетным является научно-техническое направление по созданию специализированной вычислительной техники, разработки современных методов и средств защиты информации, используемых в системах управления экологически опасными и экономически важными производствами, в энергетике, транспорте, органах государственного управления. Данное научно-техническое направление является сложным и многогранным, что обуславливает необходимость его решения в рамках Программы « Защита информации».

Дальнейшее совершенствование государственной (национальной) системы защиты информации должно быть направлено прежде всего на комплексное решение проблемы обеспечения ИБ с целью обеспечения современного уровня защиты инфраструктуры страны, уменьшения технологической зависимости в сфере ИТ и повышения степени доверия к продукции ИТ иностранных фирм-поставщиков, включая автоматизированные линии и системы управлением промышленными и производственными процессами. Решение данной проблемы может быть осуществлено в рамках программы путем проведения фундаментально-поисковых, научно-исследовательских и опытно-конструкторских работ.

Основными целями Программы являются:

– создание научно-технических условий для создания системы защиты информации государственных информационных систем и информационных систем, содержащих информацию, распространение и (или) предоставление которой ограничено;

– создание научно-технических условий для эффективного обеспечения безопасности информации на действующих и разрабатываемых критически важных объектах инфраструктуры страны, автоматизированных систем управления технологическими процессами и производством;

– создание условий для развития эффективных высокопроизводительных методов и средств защиты информации.

Таким образом, развитие в республике данного направления позволит создать базис для обеспечения информационной безопасности страны и свести к минимуму возможность злоупотребления персональной и иной конфиденциальной информацией, расширить сферу использования электронного документооборота, обеспечить возможность ведения электронной торговли, предоставления электронных услуг, широкомасштабного внедрения систем электронных платежей.

М.А.ВУС, Р.М.ЮСУПОВ

ПЕРЕЧИТЫВАЯ ЗАНОВО…

I. Концептуальным проблемам информационной безопасности в Союзе России и Беларуси была посвящена научно-практическая конференция, проведенная в Санкт-Петербурге в 2000 году. На конференции поднимались вопросы гармонизации законодательства в рамках Союзного государства, отмечалась необходимость организации проведения совместных исследований учеными и специалистами двух суверенных государств, в частности, исследований по унификации правовых тезауросов и классификаторов. Материалы и рекомендации этой представительной конференции и сегодня - десятилетие спустя - не потеряли своей актуальности. Размещенные в сети Интернет, на сайте **www.proinfo.narod.ru** они содержат в себе конструктивный посыл. В итоговом документе конференции отмечалось, что «*информационное пространство России и Беларуси требует единых подходов в защите от внешней информационной агрессии*», в связи с этим подчеркивалась необходимость разработки Конвенции информационной безопасности для Союза Беларуси и России. В рекомендациях конференции обращалось внимание на необходимость «*обеспечить включение в индикаторы оценки состояния информационной безопасности угрозы мировоззренческим факторам формирования личности и жизнесберегающим ресурсам развития общества*». Сказанное не потеряло своей актуальности и сегодня [1].

II. К концу XX века развитие новых информационных и телекоммуникационных технологий, являясь естественным и необходимым условием экономического и научно-технического прогресса, породило целый комплекс негативных последствий связанных, прежде всего, с появлением реальной возможности использования этих технологий в преступных, в том числе террористических и военных целях. На стыке проблем военной безопасности и противодействия новым видам преступности в сфере высоких технологий возникла проблема международной информационной безопасности.

Угрозы использования информационно-коммуникационных технологий в преступных, террористических и военно-политических целях, несовместимых с обеспечением международной безопасности, могут реализовываться как в гражданской, так и в военной сферах и привести к тяжелым политическим и социально-экономическим последствиям в отдельных странах, регионах и в мире в целом, к дестабилизации общественной жизни целых государств. Все это вывело задачи защиты информации и противодействия распространению информационного оружия на уровень глобальной проблемы безопасности.

За прошедшее десятилетие проблемы информационной безопасности неизмеримо обострились. Угрозы информационно-технологического характера стали сегодня серьезным вызовом международной безопасности. На сегодня в мире уже фактически сложился новый вид организованной преступности, специализирующийся на преодолении (взломе) защиты компьютерных систем, хищении секретов и денежных средств, а известные события сентября 2001 г. стерли грань между криминальной и военно-политической составляющей обеспечения международной информационной безопасности.

Всемирная федерация ученых поставила угрозу международной информационной безопасности на первое место в списке угроз человечеству в XXI веке. Объективно возникла потребность в международно-правовом регулировании мировых процессов гражданской и военной информатизации. Назрел вопрос разработки на международном уровне нормативно-правовых актов регулирующих трансграничный информационный обмен, обеспечивающих защиту национальных информационных ресурсов, минимизирующих негативное информационное воздействие на массовое сознание, запрещающих использование информационно-кибернетических технологий во враждебных (деструктивных, агрессивных)

целях против согласованных категорий объектов (критических объектов и технологий). В этой связи следует отметить, что в Окинавской Хартии глобального информационного общества, подписанной в 2000 году «восьмеркой» ведущих государств, закреплены лишь вопросы целостности информационных сетей и пресечения преступлений в компьютерной сфере и фактически проигнорирована военно-политическая составляющая проблемы международной информационной безопасности.

Российская Федерация и Республика Беларусь являются членами Организации Объединенных Наций, в рамках которой на протяжении последнего десятилетия инициируются процессы поиска путей укрепления международной информационной безопасности. В рамках ООН неоднократно было озвучено предложение России (при поддержке Беларуси, Бразилии, Китая и ряда других стран) о необходимости исследования военно-политической составляющей угрозы международной информационной безопасности. Единственной страной, голосовавшей против, оказались США. Национальная политика США ориентирована на объединение (связывание) мирового сообщества глобальным кибернетическим пространством, которое - в силу технологического лидерства - подконтрольно американскому правительству и регулируется международно-правовыми нормами, не предусматривающими не только никакой ответственности за проведение политически мотивированных кибернетических атак, но даже не упоминающих об их существовании в принципе [2].

Стремятся вычленить из общего контекста проблемы обеспечения международной информационной безопасности вопросы исключительно киберпреступности и кибертерроризма, США выступают не только против выработки юридически обязывающих документов в области международной информационной безопасности, но даже «отказываются от работы по формированию терминологического глоссария по проблематике международной информационной безопасности в любой его форме». Международное сотрудничество апологетам информационных войн видится «преимущественно в форме распространения западного опыта, методик и технических средств по обеспечению защиты информационных и телекоммуникационных систем и сетей, что в свою очередь, может предоставлять им возможности обеспечивать для себя транспарентность и контроль информационного пространства других государств и содействовать своей инфоэкспансии» [3].

Необходимость обеспечения международной информационной безопасности и безопасности сетей, предотвращения злоупотребления информационными ресурсами и технологиями в преступных и террористических целях нашла свое отражение, в частности, в итоговом документе тунисского саммита Всемирной встречи на высшем уровне по вопросам информационного общества (2005 г.). Там же была подчеркнута необходимость общего понимания участниками построения глобального информационного общества вопросов безопасности Интернет и сотрудничества в этой сфере. Примечательно, что на очередном Форуме Всемирного саммита по информационному обществу, который пройдет сегодня в Женеве под эгидой Международного союза электросвязи (16-20 мая 2011 г.), будут рассмотрены такие вопросы как право на общение, социальные сети как средство развития и кибербезопасность.

III. Значительные и конкретные шаги по укреплению коллективной безопасности государств, входящих в эти структуры, предпринимают в настоящее время Содружество Независимых Государств (СНГ) и Организация Договора о коллективной безопасности (ОДКБ). Советом глав государств СНГ утверждена Концепция сотрудничества в сфере обеспечения информационной безопасности и Комплексный план мероприятий по её реализации. Планом работы Экспертного совета Межпарламентской Ассамблеи СНГ предусмотрена разработка проекта Рекомендаций по совершенствованию и гармонизации национального законодательства государств-участников СНГ в сфере обеспечения информационной безопасности. Очевидно, что одним из направлений на пути гармонизации

законодательств должна стать проработка вопросов полноты и совместимости терминологии, правовых дефиниций.

Решением Совета коллективной безопасности ОДКБ принята Программа совместных действий по формированию системы информационной безопасности государств – членов ОДКБ и утверждено Положение о сотрудничестве государств – членов ОДКБ в сфере информационной безопасности. В программу деятельности Парламентской Ассамблеи ОДКБ (по инициативе Парламента Республики Беларусь) включены, в том числе, разработка единого понятийного аппарата в области информационной безопасности и разработка рекомендаций по сближению и гармонизации национального законодательства государств-членов ОДКБ в сфере информационной безопасности. В инициативном плане сотрудничество на этом направлении налаживают сегодня Санкт-Петербургский Институт информатики и автоматизации РАН, Институт государства и права РАН и Институт национальной безопасности Республики Беларусь.

Государства Шанхайской организации сотрудничества (ШОС), выступившие союзниками в продвижении идеи обеспечения международной информационной безопасности, подготовили и подписали 16 июня 2009 г. в Екатеринбурге межправительственное соглашение о сотрудничестве в области обеспечения международной информационной безопасности, ставшее первым в международной практике документом направленным на ограничение всего комплекса угроз международной информационной безопасности включая их военно-политические, криминальные и террористические аспекты. Важным элементом этого Соглашения являются включенные в него согласованные, выработанные группой экспертов «Перечень основных понятий в области международной информационной безопасности» и «Перечень основных видов угроз в области международной информационной безопасности, их источников и признаков». В числе основных видов угроз указано, в частности, распространение информации, наносящей вред общественно-политической, социально-экономической, духовной и культурной среде других государств. Это Соглашение открыто для присоединения любого государства, разделяющего его цели и принципы. [4]

Трансграничный характер информационных технологий, современных вызовов и угроз диктует необходимость дополнения национальных усилий по обеспечению информационной безопасности совместными действиями на двустороннем, региональном и международном уровнях. Представляется, что в формате Межпарламентской Ассамблеи СНГ и Парламентской Ассамблеи ОДКБ Россия и Беларусь могли бы совместно выступить инициаторами, если не присоединения к самому Соглашению, то как минимум, инкорпорирования (дополнения) в ныне действующие концептуальные документы СНГ и ОДКБ понятийного аппарата из Соглашения ШОС о сотрудничестве в области международной информационной безопасности. Принимая во внимание имеющиеся программы совместных действий по формированию системы информационной безопасности, а также тот факт, что целый ряд государств являются одновременно членами СНГ, ШОС и ОДКБ, такое предложение видится конструктивным и вполне реалистичным.

Литература

1. См. информационный ресурс открытого доступа: http://www.proinfo.narod.ru

2. Международная информационная безопасность: дипломатия мира / Сборник материалов под общ. ред. д-ра воен. наук, проф. С.А. Комова. – М, 2009.

3. Там же, стр. 156.

4. Указ. источник, стр. 232-240.

А.В.ГЛЕВИЧ, Ю.В.ЗЕМЦОВ, П.Е.КОВАЛЕЦ

СЕМЕЙСТВО СТАНДАРТОВ «СИСТЕМЫ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ»

Человеческая деятельность, направленная на достижение упорядочения в определённой области – стандартизация – осуществляется уже очень давно и помогает достичь экономии всех видов ресурсов, технической и информационной совместимости, а также взаимозаменяемости продукции и многого другого. В частности, стандартизация в области информационной безопасности (ИБ) позволяет установить оптимальный уровень упорядочения и унификации, подтвердить соответствие информационных систем предъявляемым к ИБ требованиям. Для профессионалов – это экономия времени на поиск эффективных и зарекомендовавших себя решений, а для потребителя – гарантия получения результата ожидаемого качества.

Одним из основных стандартов в области контроля качества является стандарт международной организации по стандартизации ISO 9001:2008 «Системы менеджмента качества – Требования». Не вдаваясь в подробности, отметим, что он основан на методологии «Планирование – Выполнение – Проверка – Действие» (ПВПД –PDCA). Этот стандарт очень активно применяется по всему миру. Также стоит отметить, что в Беларуси 2010 год был «Годом качества», в связи с чем количество организаций, прошедших сертификацию согласно стандарту ISO 9001, значительно возросло.

Вышесказанное дает нам повод подробнее рассмотреть одно достаточно востребованное в области ИБ семейство международных стандартов – ISO/IEC 27000. Оно также базируется на методологии PDCA и, как указано в стандарте ISO/IEC 27001(подробнее он описан далее), система управления, сертифицированная согласно ISO 9001, также может удовлетворить требования семейства ISO/IEC 27000. Таким образом, сертификация согласно ISO/IEC 27001 для организаций, уже внедривших систему управления согласно ISO 9001, не вызовет сложностей и даже может оказаться простой формальностью.

Взаимосвязь стандартов семейства ISO/IEC 27000

Семейство стандартов «Информационные технологии – Технологии безопасности – Системы управления защитой информации» (далее – СУЗИ) состоит из взаимосвязанных и дополняющих друг друга стандартов, которые либо уже изданы, либо находятся в разработке. Одни стандарты описывают требования к СУЗИ (ISO/IEC 27001) и требования к организациям по сертификации (ISO/IEC 27006), которые удостоверяют соответствие стандарту ISO/IEC 27001. Другие дают представление о различных аспектах внедрения СУЗИ, акцентируя внимание на процессе управления и указаниях по регулированию, а также предоставляют руководства, специфичные для конкретных областей (например, для телекоммуникаций). Взаимосвязь между стандартами семейства СУЗИ проиллюстрирована на рисунке 1.

Семейство стандартов СУЗИ взаимосвязано со многими другими стандартами ISO и ISO/IEC. Далее предоставлено описание и классификация стандартов данного семейства.

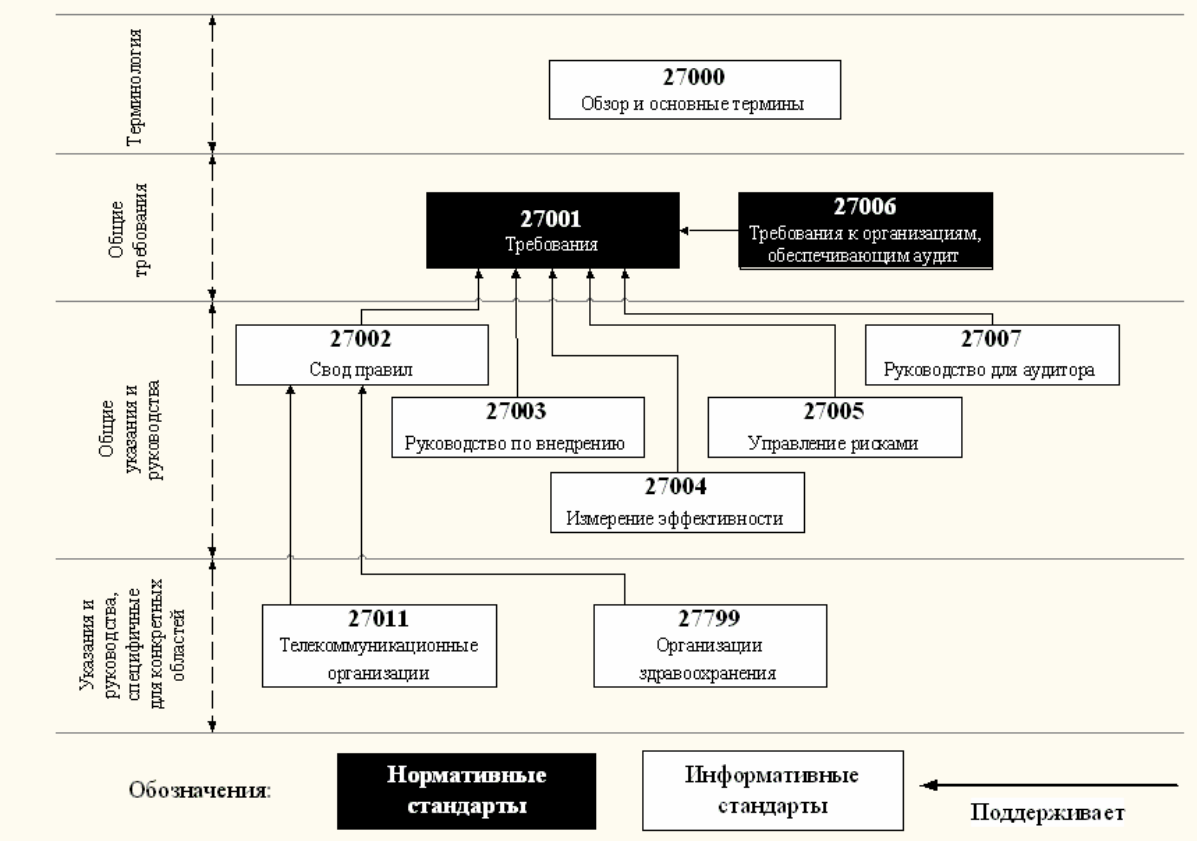


Рисунок 1 - Взаимосвязь стандартов семейства ISO 27000

Вводные стандарты

Вводный стандарт ISO/IEC 27000 «Определения и основные принципы» описывает основные принципы систем управления защитой информации и определяет соответствующие термины. Данный стандарт разработан как введение во все семейство ISO/IEC 27000. Лицам, которые только знакомятся с данным семейством, он будет полезен тем, что содержит основные понятия и разъясняет базовые принципы. А тем, кто уже имел дело с некоторыми стандартами данной серии – тем, что позволяет составить целостную картину семейства стандартов ISO/IEC 27000 и оценить преимущества от внедрения и сертификации систем на базе этих стандартов. Также здесь перечислены критические факторы, необходимые для успешного функционирования СУЗИ, и эффект от ее внедрения.

Стандарты, устанавливающие требования

Стандарт ISO/IEC 27001 «Требования» определяет нормативные требования к развитию и функционированию СУЗИ, включая ряд необходимых средств контроля и уменьшения рисков, связанных с информационными активами, которые организация стремится защитить с помощью приведения СУЗИ в действие. Для выполнения требований в качестве части процесса функционирования СУЗИ должны быть выбраны цели и средства управления контролем из Приложения А (ISO/IEC 27001), которые непосредственно получены из ISO/IEC 27002 пункты 5 – 15 и соответствуют перечисленным в них целям и средствам. Данный стандарт является базовым для всего семейства ISO/IEC 27000, так как определяет основные требования, выполнение которых необходимо для любой системы управления защитой информации (что также видно из рисунка 1). Несмотря на то, что эти требования должны выполняться полностью для соответствия стандарту, выбор технических средств и решений не регламентируется, что дает определенную свободу и гибкость в построении СУЗИ. Существуют аналоги данного стандарта: российский стандарт ГОСТ Р ИСО МЭК 27001-2006 и белорусский предстандарт СТБ П ISO/IEC 27001-2008,

которые в точности перечисляют все требования, определенные в ISO/IEC 27001, и между собой отличаются лишь терминологией. И хотя более точные моменты присутствуют и в ГОСТ, и в СТБ, хотелось бы, чтобы не было расхождений в русскоязычной терминологии данной области. Яркий пример этому – название семейства «Системы менеджмента информационной безопасности» в российском и «Системы управления защитой информации» в белорусском варианте. Будем здесь и далее придерживаться белорусского варианта терминологии.

Стандарты, содержащие общие указания

Стандарт ISO/IEC 27002(в прошлом ISO/IEC 17799) «Свод правил по управлению защитой информации» дает представление о реализации средств управления защитой информации. А именно, пункты 5 – 15 данного стандарта предоставляют конкретные советы и руководство по реализации СУЗИ лучшими методами, в дополнение к средствам управления, указанным в пунктах А.5 – А.15 ISO/IEC 27001.

Стандарт ISO/IEC 27003 «Руководство по внедрению системы управления защитой информации» предоставляет процессно-ориентированный подход к реализации СУЗИ в соответствии с ISO/IEC 27001.

Стандарт ISO/IEC 27005 «Управление рисками защиты информации» предоставляет рекомендации по реализации процессно-ориентированного подхода к управлению рисками, чтобы способствовать выполнению требований ISO/IEC 27001 по управлению рисками информационной безопасности.

Другие стандарты семейства ISO/IEC 27000

В данный момент разрабатываются или уже изданы некоторые другие стандарты, расширяющие область применения семейства и затрагивающие различные аспекты защиты информации. Например, стандарт ISO 27008 предоставит руководство по аудиту СУЗИ относительно средств управления безопасностью. В отличие от ISO 27007, он будет сосредоточен на самой СУЗИ, а не на определенных средствах управления. Документ предоставит руководство о том, как проверить или подтвердить степень практического внедрения средств управления безопасностью. Разрабатываемый стандарт ISO 27033 будет составным стандартом, целью которого будет предоставление детализированного руководства по аспектам безопасности управления и использования сетей информационной системы. Большая часть его основана на существующем стандарте ISO 18028. Первая часть ISO/IEC 27033-1:2009 «Основные концепции управления сетевой безопасностью», была издана в 2009 году и описывает понятия, связанные с безопасностью сети, а также предоставляет руководство управления ею.

Преимущества и особенности сертификации

Отметим основные преимущества внедрения СУЗИ согласно ISO/IEC 27000 и сертификации на соответствие стандарту ISO/IEC 27001:2005.

Для организаций, в целом, можно выделить следующие преимущества:

- повышение управляемости и надежности работы ИТ-инфраструктуры;
- повышение защищенности ключевых бизнес-процессов;
- повышение доверия к организации со стороны контрагентов.

Для структурных подразделений организаций, таких, как подразделения информационных технологий и службы безопасности, ISO/IEC 27000 дает следующие преимущества:

- систематизация процессов обеспечения ИБ;
- расстановка приоритетов в сфере ИБ;
- управление ИБ в рамках единой корпоративной политики.

При всей очевидной полезности внедрения СУЗИ согласно ISO/IEC 27000, нельзя не отметить следующие особенности сертификации на соответствие стандарту ISO/IEC 27001:2005:

– сертификация требует существенных затрат трудовых и материальных ресурсов, которые могли бы быть направлены на совершенствование СЗИ;

– непропорциональность затрат на сертификацию масштабу организации, что осложняет малым предприятиям ее прохождение;

– возможное временное нарушение ранее работающей структуры из-за внедрения новых элементов, необходимых для сертификации.

Подводя итог, в очередной раз заметим, что сертификация не призвана предоставлять самый легкий и дешевый способ защиты от угроз ИБ. Однако не существует более действенного способа повысить степень доверия к ИТ-инфраструктуре организации, чем сертификация на соответствие нормам современных стандартов, в том числе и стандартов серии ISO/IEC 27000.

А.Н.ГОРБАЧ

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ОБЩИХ ИНФОРМАЦИОННЫХ РЕСУРСОВ БЕЛАРУСИ И РОССИИ. СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

Интенсивное развитие современных информационных технологий, все более широкое их использование во всех сферах государственной и общественной деятельности обуславливает возрастание актуальности задачи постоянного совершенствования системы защиты общих информационных ресурсов Беларуси и России.

В настоящее время наступил период, который позволяет серьезно и взвешенно оценить состояние нашего взаимодействия в сфере защиты информации в рамках Союзного государства и определить перспективы дальнейших совместных действий соответствующих властных структур Российской Федерации и Республики Беларусь, а также организаций и конкретных профессиональных специалистов государств-участников в этой области.

В декабре 2010 года завершено выполнение мероприятий программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006-2010 годы». Итоговый отчет по программе рассмотрен и принят на заседании Совета Министров Союзного государства 15 марта текущего года.

В процессе выполнения программы были получены следующие основные результаты:

во-первых, разработаны ряд нормативных правовых актов и руководящих документов, которые предполагается использовать для взаимодействия органов государственного управления различного уровня. Наиболее важными из них являются основополагающие концептуальные документы, определяющие организационную основу системы защиты совместных информационных ресурсов Союзного государства, в том числе регламентирующих деятельность по обеспечению безопасности информации на критически важных объектах информационно-телекоммуникационной инфраструктуры Союзного государства и контроля эффективности этих мероприятий.

Реализация разработанных документов позволит:

обеспечить согласованную деятельность национальных органов по обеспечению безопасности информации на критически важных объектах информационно-телекоммуникационной инфраструктуры Союзного государства;

сформировать гармонизированную нормативную и методическую базу в области защиты информации государств-участников, что является важным условием для развития

национальных промышленных технологий создания информационных систем в защищенном исполнении, взаимного признания каждой из сторон сертификатов на средства и системы защиты информации, обеспечения их совместной разработки и производства и расширения рынков сбыта;

развить методологию обоснования требований к перспективным средствам и системам защиты информации, основанным на современных информационных технологиях. Разработать с использованием этой методологии ряд программных и аппаратно-программных средств и систем защиты информации, а также контроля защищенности информационных ресурсов и информационно-телекоммуникационных систем;

совершенствовать нормативно-методические документы по проведению комплексной аттестации объектов информатизации по требованиям безопасности информации, сертификации средств защиты информации и контроля состояния защиты информации;

во-вторых, разработано ряд высокоэффективных систем и средств защиты информации, по своим техническим характеристикам и эффективности применения на сегодняшний день не имеющих аналогов. Указанные средства предназначены для использования при создании систем защиты информации государственных информационных систем, обеспечения защиты объектов информатизации, а также осуществления контроля эффективности систем защиты информации. При этом реализованы перспективные технологии защиты совместных информационных ресурсов Союзного государства от утечки и воздействия по техническим каналам, от компьютерных атак и вирусов, от несанкционированного доступа, в том числе на основе криптографических методов.

Все разработанные изделия по своим технико-экономическим характеристикам соответствуют современному мировому уровню технологического развития средств защиты информации. Использование созданных средств позволит повысить уровень защиты информации национальных и союзных органов управления.

Внедрение результатов, полученных в ходе выполнения мероприятий Программы, будет осуществлено в соответствии с Планом реализации, который разработан государственным заказчиком–координатором совместно с государственными заказчиками Программы по результатам рассмотрения Советом Министров Союзного государства итогового отчета о выполнении Программы.

Реализация указанных результатов позволит обеспечить дальнейшее совершенствование системы защиты общих информационных ресурсов Беларуси и России и на этой основе повысить защищённость информации в критически важных системах информационно-телекоммуникационной инфраструктуры Союзного государства, а также способствовать развитию эффективных высокотехнологичных методов и средств защиты информации.

Безусловно, полученные результаты имеют большую ценность в связи с возможностью их использования при проведении работ по защите информации на национальном уровне.

Эффект от реализации результатов программы заключается:

в обеспечении конфиденциальности, целостности и доступности информации, циркулирующей в информационных системах и информационно-телекоммуникационных сетях Союзного государства;

в предотвращении (снижении риска) нарушений функционирования критически важных систем информационно-телекоммуникационной инфраструктуры Союзного государства и связанных с этими нарушениями экономических, экологических и социальных последствий;

в развитии производства конкурентоспособных технических, программно-аппаратных и программных средств защиты информации;

в экономии финансовых средств за счет разработки единых для государств-участников Союзного государства нормативных и методических документов, средств

защиты информации по отношению к собственным затратам Российской Федерации и Республики Беларусь.

Таким образом, полученные в период с 2000 по 2010 годы результаты позволили создать основные условия для формирования и совершенствования системы защиты информации Союзного государства, предотвращения ущерба от реализации информационных угроз общим информационным ресурсам, производства конкурентоспособных средств защиты информации.

Однако останавливаться на достигнутом будет неправильно. В условиях сохраняющегося в мире противостояния и соперничества государств, высокого уровня организованной преступности и терроризма, развития способов и средств технической разведки, несанкционированного доступа к информации в информационных системах, несанкционированного воздействия на нее эффективная защита общих информационных ресурсов Союзного государства является одной из основ обеспечения его безопасности. Решение этой проблемы связано с дальнейшим объединением научно-технического и экономического потенциала Российской Федерации и Республики Беларусь, использованием имеющихся в их арсенале и разработкой новых наиболее эффективных подходов, способов и средств защиты информации, а также с преодолением правовых, организационных, нормативно-методических и технических противоречий.

Поэтому уже сегодня актуальной задачей для нас является формирование новой программы Союзного государства в области защиты информации. С целью решения указанной проблемы Федеральной службой по техническому и экспортному контролю Российской Федерации и Оперативно-аналитическим центром при Президенте Республики Беларусь организована разработка Концепции программы Союзного государства по проведению совместных фундаментально-поисковых, научно-исследовательских и опытно-конструкторских работ в области защиты информации ”Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий“ на 2011-2015 годы, которая установленным порядком одобрена Правительствами Беларуси и России и представлена на рассмотрение Совета Министров Союзного государства.

Концепцией предусматривается выполнить в рамках новой программы следующие мероприятия.

1. Проработать вопросы создания перспективных средств и способов защиты информации при реализации наукоемких технологий ее обработки, таких как Grid - технологии и технологии беспроводной передачи данных.

2. Проработать вопросы технической реализации перспективных средств защиты информации, разрабатываемых на основе таких высоких технологий, как:

архитектурная реализация доверенных сред и, в первую очередь, для распределенных вычислительных систем, взаимодействующих с использованием сетей связи общего пользования;

разграничение доступа к программным и техническим средствам на основе высоконадежной биометрии, использующей нейросетевые методы обработки биометрической информации;

создание интегрированных систем обеспечения защиты информации на объектах информатизации и мониторинга защищаемых объектов на основе бесконтактных способов оперативного сбора и ввода данных (например, способа радиочастотной идентификации).

3. Провести анализ и оценку реальной защищенности критически важных систем информационной инфраструктуры, обеспечивающих деятельность органов Союзного государства, разработать методологические и организационные основы оценки защищенности создаваемых продуктов информационных технологий (например, пластиковых карт, различного рода носителей идентификационной информации) от угроз безопасности информации.

4. Проработать пути создания соответствующих требованиям безопасности информации аппаратных и программно-аппаратных компонентов в критически важных системах информационной инфраструктуры Союзного государства, в том числе с применением высоких технологий.

5. Подготовить нормативное, алгоритмическое и программное обеспечение инфраструктуры открытых ключей на информационном пространстве Союзного государства.

6. Проработать вопросы формирования системы стандартов, устанавливающих единую терминологию в области защиты общих информационных ресурсов Беларуси и России, технологию проведения работ по их защите, методы обоснования требований к объектам и средствам защиты.

7. Разработать учебные пособия для подготовки специалистов в области обеспечения безопасности информации в критически важных системах информационной инфраструктуры и технической защиты информации на объектах информатизации Союзного государства в рамках дополнительного профессионального образования с учетом современных образовательных технологий.

Программу планируется осуществить в течение пяти лет с 2011 по 2015 годы. Сроки реализации Программы обусловлены планируемым объемом работ по решению проблемы создания единого научно-технического обеспечения защиты общих информационных ресурсов Беларуси и России от угроз безопасности информации с учетом необходимости и логической последовательности решения взаимосвязанных задач Программы. Рассмотрение проекта программы запланировано в текущем году на сентябрьском заседании Совета Министров Союзного государства.

Таким образом, на сегодняшний день совместно с коллегами из Российской Федерации мы наметили перспективу дальнейшего сотрудничества по решению задач, связанных с совершенствованием системы защиты общих информационных ресурсов Беларуси и России.

М.Л.ДАНИЛКОВИЧ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В настоящее время организации хранят и обрабатывают данные о сотрудниках, клиентах, партнерах, поставщиках и других физических лицах. Утечка, потеря или несанкционированное изменение персональных данных (ПД) приводит к невосполнимому ущербу, а порой и к полной остановке деятельности организации, а также нарушает права и свободы граждан.

Целью обеспечения безопасности персональных данных при их обработке в информационных системах ПД (ИСПД) является предотвращение или существенное затруднение неправомерного использования ПД, накапливаемых, сохраняемых и обрабатываемых с использованием автоматизированных информационных систем, а также обеспечение нейтрализации последствий деструктивных воздействий и восстановления нормального функционирования ИСПД.

Основными задачами обеспечения безопасности ПД являются:

а) в стратегическом плане – создание организационных и технических условий для обеспечения безопасности ПД на основе формирования совокупности правовых документов и разработки единой методологии организации и ведения работ по обеспечению безопасности ПД, реализуемой через систему организационно-распорядительных и специальных нормативных документов;

б) в тактическом плане – всестороннее обеспечение проведения работ по обеспечению безопасности ПД на основе разработки типовых методов обеспечения безопасности ПД, совершенствования технического оснащения ИСПД, развития систем лицензирования, сертификации и аттестации;

в) в техническом плане – разработка специализированных средств обеспечения безопасности ПД на основе единого подхода к обоснованию требований, согласования технических решений и разработки методик применения средств для решения типовых задач обеспечения безопасности ПД.

Для решения проблемы защиты ПД в Республике Беларусь необходимо разработать и ввести в действие ряд законопроектов и технических нормативных правовых актов, которые позволят:

– определить категории и перечень ПД;

– урегулировать правовые вопросы обработки ПД;

– классифицировать информационные системы ПД;

– определить требования по защите ПД;

– спроектировать систему защиты ПД;

– провести оценку соответствия ИСПД предъявляемым требованиям;

– организовать контроль соблюдения использования средств защиты информации в ИСПД.

К особенностям информационного элемента ИСПД можно отнести следующее:

– повышенная опасность (как для субъекта ПД, так и для общества и государства в целом) угроз, реализующихся путем несанкционированной модификации ПД, в том числе за счет подмены идентификатора ПД при неизменном содержании или содержания ПД при неизменном идентификаторе;

– в рамках одной ИСПД могут храниться, накапливаться и обрабатываться ПД различной степени важности (относящиеся к различным категориям), причем в процессе обработки категория ПД может изменяться;

– ущерб, возникающий при нарушении целостности, доступности, достоверности и конфиденциальности ПД, может носить как непосредственный (ущерб, наносимый собственнику ПД), так и опосредованный (ущерб, наносимый оператору ИСПД, обществу или государству) характер;

– отдельные ПД могут относиться к информации, содержащей государственную тайну, что предопределяет необходимость обеспечения их безопасности в соответствии с законодательством в области защиты государственной тайны;

– для систем, используемых органами власти и управления более высоких уровней, общей тенденцией является понижение степени персонализации ПД за счет агрегирования данных в процессе их обработки.

ИСПД можно классифицировать по следующим признакам:

– категория обрабатываемых в информационной системе ПД;

– объем обрабатываемых ПД (количество субъектов ПД, данные которых обрабатываются в информационной системе);

– заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;

– структура информационной системы;

– наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;

– режим обработки ПД;

– разграничение прав доступа пользователей информационной системы;

– местонахождение технических средств информационной системы.

Для формирования требований по защите ПД необходимо определить угрозы, которые могут быть реализованы в ИСПД и представляют опасность для ПД.

Классифицировать основные угрозы безопасности ПД при их обработке в ИСПД можно следующим образом:

– по видам неправомерных действий:

– хищение, копирование или распространение информации без непосредственного воздействия на ее содержание;

– модификация содержания информации вплоть до полного ее уничтожения;

– воздействие на программные или аппаратные средства ИСПД, приводящее к блокированию или уничтожению информации;

– по видам каналов, с использованием которых реализуются неправомерные действия:

– технические каналы утечки информации;

– каналы НСД с целью получения информации;

– каналы НСД с целью модификации информации;

– каналы, использующие технические средства создания помех функционированию ИСПД;

– каналы, использующие специальные программно-математические воздействия.

Основными нормативными документами в интересах обеспечения безопасности ПД могут служить следующие:

– положение о методах и способах защиты информации в ИСПД;

– базовая модель угроз безопасности ПД при их обработке в ИСПД;

– методика определения актуальных угроз безопасности ПД при их обработке в ИСПД.

Обеспечение безопасности ПД позволит решить одну из важнейших проблем и потребностей современного общества - защита прав человека в условиях вовлечения его в процессы информационного взаимодействия в том числе, право на защиту личной (персональной) информации в процессах автоматизированной обработки информации.

Литература

1. Марков А.С., Никулин М.Ю., Цирлов В.Л. Сертификация средств защиты персональных данных: революция или эволюция? - «Защита информации. Инсайд». - 2008.- №5.

2. Сухинин Б.М. Проблемные вопросы защиты персональных данных – Тез.докладов XI Международной конференции РусКрипто'2009. – Москва, 2-5 апреля 2009 г.

3. Левиев Д.О. Практический опыт защиты персональных данных в кредитно-финансовых организациях – Тез. докладов V Международной специализированная выставка-конференция Infosecurity Russia 2008, - Москва, 7–9 октября 2008 г.

Е.А.ДОЦЕНКО

ПОЛИТИКА БЕЗОПАСНОСТИ КАК ЭФФЕКТИВНОЕ СРЕДСТВО ЗАЩИТЫ

Введение

С каждым днем информационная безопасность приобретает все более значимый характер. Многие организации несут убытки, связанные с нарушением информационной безопасности. Мало кто может дать определение рисков информационной безопасности и соответственно полноценно управлять ими. Выражение убытков может иметь различный вид: утрата конфиденциальности информации, потеря времени на расследование инцидентов, значительные денежные суммы в случаях мошенничества в финансовой сфере и т.п.

В то же время, не редки случаи вкладывания значительных средств в обеспечение и поддержку информационной безопасности организации. Приобретаются дорогостоящие средства защиты. Но все это не приводит к положительным результатам. Эти средства бессмысленны без адекватного конфигурирования и управления. Те, кто это понимает, нанимают в свой штат высококвалифицированных специалистов. Но и это не приводит к достижению желаемого уровня информационной безопасности. Так происходит из-за отсутствия единой системы (модели) информационной безопасности организации, которая могла бы все процессы обеспечения информационной безопасности объединить в одно целое. Не стоит применять фрагментарный подход к решению проблем информационной безопасности. Это неизбежно приведет к неокупаемости затраченных инвестиций.

Адекватный уровень информационной безопасности в организации может быть обеспечен только на основе комплексного подхода, предполагающего планомерное использование как технических, так и организационных мер защиты на единой концептуальной основе.

Из всего этого напрашивается вывод, что каждое действие, направленное на обеспечение информационной безопасности организации, должно быть четко определено конкретными правилами. Совокупность таких правил называется политикой.

Определение

В современной практике обеспечения информационной безопасности термин «политика безопасности» может употребляться как в широком, так и в узком смысле слова. В широком смысле, политика безопасности определяется как система документированных управленческих решений по обеспечению информационной безопасности организации (далее – Политика). В узком смысле под политикой безопасности обычно понимают локальный нормативный документ, определяющий требования безопасности, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения информационной безопасности. Таким образом, Политика состоит из локальных политик.

Существует два подхода описания Политики:

– создание единого документа с красивым названием «Политика безопасности»;

– создание набора конкретных документов, рассматривающих отдельные вопросы обеспечения информационной безопасности организации.

Оба подхода имеют право на жизнь. Второй подход хорош тем, что малейшие изменения в какой-либо из политик не требуют пересмотра всех в целом. Изменения касаются только одного документа и не затрагивают остальных аспектов обеспечения безопасности информационных ресурсов. Не требуется пересмотра огромного документа в целом. С учетом того, что обычно его визирует руководство организации, любые коррективы подчас приводят к длительному ожиданию подписи.

Очень часто рядом с политиками безопасности идет концепция безопасности. Как правило, такой документ рассчитан на не специалистов по защите информации и лишь отражает внимание руководства организации к данной проблеме, не вдаваясь в технические детали. Как показывает опыт, в ней содержатся общепринятые положения по информационной безопасности. В принципе, наличие этого документа спорно. Все будет зависеть от его содержания и желания руководства организации иметь такой документ.

Идеальным вариантом будет создание документа «Политика информационной безопасности» (или концепции) со ссылками в нем на конкретные политики (в узком смысле). Следует понимать, концепция – это не описание способа реализации. В ней нельзя «привязываться» к конкретным техническим решениям, продуктам и производителям. Иначе изменение политической ситуации в организации, уход с рынка какого-либо из вендоров и т. п. приведет к необходимости изменения концепции, а этого происходить не должно.

Содержание

Концепция должна содержать систему взглядов на достаточно высоком уровне. Цели и задачи в области информационной безопасности, никаких инструкций, нормативов, описания продуктов, имен ответственных и т.п. Описывает общий подход к информационной безопасности без специфичных деталей.

Типичное содержание политик имеет следующий вид:

«Термины и определения»;

«Введение» (обычно отсутствует);

«Цель». Описывает цели создания данного документа;

«Область применения». Описывает объекты или субъекты, которые должны выполнять требования данной политики;

«Требования». Описывает сами требования;

«Ответственность». Описывает наказание за нарушение указанных в предыдущем разделе требований;

«История изменений».

Политики должны описывать требования, начиная от парольной защиты и межсетевого экранирования, заканчивая использованием портативных мобильных устройств и аутсорсинга.

Разработка и внедрение

Разработка Политики – длительный и трудоемкий процесс, требующий высокого профессионализма, отличного знания нормативной базы в области информационной безопасности. Этот процесс обычно занимает многие месяцы и не всегда завершается успешно.

Внедрение Политики практически всегда связано с созданием некоторых неудобств для сотрудников организации и снижением производительности бизнес-процессов. Влияние мер информационной безопасности на бизнес-процессы необходимо минимизировать. Для того чтобы понять, какое влияние политика будет оказывать на работу организации, следует привлекать к разработке этого документа представителей бизнес-подразделений, служб технической поддержки и всех, кого это непосредственно коснется.

Чтобы правильно выполнять требования Политики, необходимо сначала ознакомить с ней всех сотрудников организации и постоянно их обучать путем проведения семинаров, презентаций, индивидуальных разъяснений.

Жизненный цикл Политики

Политика – не статичный документ или, точнее, набор документов. Они тоже должны пересматриваться. Но не в результате смены программной платформы или имени ответственного за безопасность отдельного сегмента информационной системы организации, а под влиянием таких факторов, как изменение технологии обработки информации, появление новых бизнес-процессов и т.п.

Для успешного управления информационной безопасностью должны циклически по порядку выполняться следующие действия:

– аудит безопасности;

– разработка;

– внедрение;

– контроль;

– пересмотр и корректировка.

Первые версии документов обычно не в полной мере отвечают потребностям организации. Скорее всего, после наблюдения за процессом внедрения Политики и оценки эффективности ее применения потребуется осуществить ряд доработок. В дополнение к этому, используемые технологии и организация бизнес-процессов непрерывно изменяются,

что приводит к необходимости корректировать существующие подходы к обеспечению информационной безопасности. В большинстве случаев периодический пересмотр Политики является нормой.

Заключение

Без Политики любая деятельность по обеспечению информационной безопасности будет малоэффективной. Системный подход позволит взять всю ситуацию под контроль, что, в свою очередь, и является залогом успешной защиты информационных ресурсов.

Для разработки эффективной Политики, помимо профессионального опыта, знания нормативной базы в области информационной безопасности, необходимо также учитывать основные факторы, влияющие на эффективность Политики, и следовать основным принципам разработки политик, к числу которых относятся: минимизация влияния на производительность труда, непрерывность обучения, контроль и реагирование на нарушения безопасности, поддержка руководства организации и постоянное совершенствование.

Ю.И.ИВАНЧЕНКО

ПРОБЛЕМЫ ОЦЕНКИ СООТВЕТСТВИЯ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

В докладе представлен краткий анализ нормативных правовых актов РБ касающихся обеспечения ИБ и оценки соответствия объектов ИТ требованиям по ИБ.

В настоящих тезисах представлены положения нормативных правовых актов Республики Беларусь, которые, по мнению автора, являются проблемными и требуют обсуждения на профессиональном уровне.

Ключевым нормативным правовым актом в рассматриваемой области является Закон Республики Беларусь «Об оценке соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации». Он определяет терминологию, правовые и организационные основы оценки соответствия объектов оценки требованиям **только технических** нормативных правовых актов.

Оценка соответствия определяется как деятельность по определению соответствия объектов оценки соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации. К техническим нормативным правовым актам в области технического нормирования и стандартизации относятся [2]:

технические регламенты;

технические кодексы;

стандарты, в том числе государственные стандарты, стандарты организаций;

технические условия.

Цели оценки соответствия определены в статье 5 [1] и включают:

– обеспечение защиты жизни, здоровья и наследственности человека, имущества и охрану окружающей среды;

– повышение конкурентоспособности продукции (работ, услуг);

– обеспечение энерго- и ресурсосбережения;

– создание благоприятных условий для обеспечения свободного перемещения продукции на внутреннем и внешнем рынках, а также для участия в международном экономическом, научно-техническом сотрудничестве и международной торговле.

Виды оценки соответствия установлены в статье 7 [1] и включают всего 2 вида: аккредитацию и подтверждение соответствия. Подтверждение соответствия (статья 25) может носить обязательный или добровольный характер. Обязательное подтверждение

соответствия осуществляется в форме обязательной сертификации и декларирования соответствия. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации.

Объекты оценки соответствия по каждому виду оценки определены в статье 8 [1]:

– *при аккредитации* это компетентность юридического лица в выполнении работ по подтверждению соответствия или проведении испытаний объектов оценки соответствия.

– *при подтверждении соответствия это*:

продукция и процессы ее разработки, производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации;

выполнение работ и оказание услуг;

системы управления качеством;

системы управления окружающей средой;

системы управления безопасностью продукции;

системы управления охраной труда;

профессиональная компетентность персонала в выполнении определенных работ (оказании определенных услуг);

иные объекты, в отношении которых установлены требования технических нормативных правовых актов. К техническим нормативным правовым актам в области технического нормирования и стандартизации, на соответствие требованиям которых осуществляется оценка соответствия, относятся технические регламенты и государственные стандарты Республики Беларусь.

В тоже время закон Республики Беларусь «О техническом нормировании и стандартизации» к объектам технического нормирования, объектам стандартизации относит только продукцию, процессы ее разработки, производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации или оказание услуг.

В законе «Об информации, информатизации и защите информации» введены 2 понятия – аттестация и государственная экспертиза в следующем контексте (без определений).

«Информация, распространение и (или) предоставление которой ограничено, а также информация, содержащаяся в государственных информационных системах, должны обрабатываться в информационных системах с применением системы защиты информации, **аттестованной** в порядке, установленном Советом Министров Республики Беларусь».

«Для создания системы защиты информации используются средства защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам **государственной экспертизы**, порядок проведения которой определяется Советом Министров Республики Беларусь». Т.о. по букве закона оба этих понятия остаются за рамками **Национальной системы подтверждения соответствия**.

Что такое система защиты информации в законе не уточняется, но определены меры по защите информации, которые, по-видимому, должны быть реализованы в упомянутой системе.

К правовым мерам по защите информации отнесены заключаемые **обладателем** информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.

К организационным мерам по защите информации отнесены меры обеспечения особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

К техническим (программно-техническим) мерам по защите информации отнесены меры по использованию средств защиты информации, в том числе криптографических, а также систем контроля доступа и регистрации фактов доступа к информации.

Положением о порядке аттестации **систем защиты информации** [3] аттестация определяется как комплекс организационно-технических мероприятий, в результате которых **подтверждается соответствие** системы защиты информации требованиям нормативных правовых актов в области защиты информации, в том числе технических нормативных правовых актов, и оформляется аттестатом соответствия. Система защиты информации определена как совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, функционирующих по правилам, установленным соответствующими нормативными правовыми актами в области защиты информации, в том числе техническими нормативными правовыми актами. Таким образом, Положение расширяет установленный законом [1] перечень форм подтверждения соответствия.

Указом Президента Республики Беларусь «О лицензировании отдельных видов деятельности» от 01.09.2010 №450 в дополнение к существовавшим видам деятельности, на осуществление которых требуются специальные разрешения (лицензии) введены еще два: аттестация объектов информатизации и аттестация информационных систем, но не систем защиты информации.

В Положении содержится исчерпывающий перечень того, что в себя включает оценка системы защиты информации:

анализ организационной структуры информационной системы, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения системы защиты информации, разработанной документации и ее соответствия требованиям нормативных правовых актов в области защиты информации (!?), в том числе технических нормативных правовых актов.

проверку правильности отнесения информационной системы к классу типовых объектов информатизации, выбора и применения средств защиты информации;

рассмотрение и анализ результатов испытаний средств защиты информации и системы защиты информации;

проверку уровня подготовки кадров и распределения ответственности персонала за организацию и обеспечение выполнения требований по защите информации;

оценку системы защиты информации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

оформление протоколов испытаний (оценки) и заключения по результатам проверок.

В перечне исходных данных из 21 позиции, в частности, указаны документы, устанавливающие отнесение информационной системы к классу типовых объектов информатизации согласно СТБ 34.101.30-2007 и Задание по безопасности на информационную систему (вопрос разработки Задания по безопасности на информационную систему (даже как совокупность банков данных, информационных технологий и комплексов программно-технических средств) заслуживает отдельного обсуждения). Сам стандарт определяет объекты информатизации как средства электронной вычислительной техники (автоматизированные системы различного уровня и назначения вычислительные сети и центры, автономные стационарные и персональные электронные вычислительные машины, а также копировально-множительные средства, в которых для обработки информации применяются цифровые методы) вместе с программным обеспечением, которые используются для обработки информации. Встает вопрос о корректности и применимости СТБ 34.101.30 при проведении аттестации. Оценка же системы защиты информации на соответствие Заданию по безопасности на информационную систему видимо предполагается

в процессе «проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации».

Положение игнорирует СТБ П ИСО 27001, содержащий требования именно к системам, и политику безопасности, хотя «Положение о порядке защиты информации …» требует разработки (актуализации) политики информационной безопасности.

В сложившихся условиях остается без ответа вопрос: с какой целью проводится оценка соответствия и аттестация, в частности, что же должно быть оценено и на соответствие чему?

В заключение, по-видимому, риторический вопрос – когда же мы придем к взаимному признанию результатов оценки соответствия в области информационных технологий хотя бы в рамках союза России и Белоруссии?

Литература

1. Закон Республики Беларусь «Об оценке соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации».

2. Закон Республики Беларусь «О техническом нормировании и стандартизации».

3. Постановление Совета Министров Республики Беларусь 26 мая 2009, №675 О некоторых вопросах защиты информации.

Н.А.КАРПОВИЧ

ЗАЩИТА ИНФОРМАЦИИ В КОНТЕКСТЕ РЕАЛИЗАЦИИ ЭКОЛОГИЧЕСКОЙ ФУНКЦИИ ГОСУДАРСТВА

С учетом формирования таких реалий сегодняшнего дня, как единого в глобальном масштабе информационного пространства, феноменов информационной безопасности и информационного (сетевого) общества неизмеримо возросла значимость деятельности государства в информационной сфере – фундаментального онтологического объекта его воздействия. Информация во всех ее проявлениях является важнейшим фактором эффективности государственной власти, в том числе по реализации экологической функции государства. Суть информационной деятельности А.Н.Васенина рассматривает как «обусловленное потребностями социально-политического развития комплексное направление деятельности государственного механизма по обеспечению граждан, их объединений, в целом общества и государства актуальной в конкретный временной период публично значимой информацией посредством ее производства, распространения и контроля в законодательно установленных формах» [1, с. 7]. Информационный срез функциональной деятельности государства А.Н.Васенина, Ю.Г.Просвирнин, Э.В.Талапина, С.И.Нефедов и другие авторы выделяют в отдельное, самостоятельное направление – информационную функцию государства. Однако информационная деятельность, на наш взгляд, это не самостоятельное направление, а лишь способ, средство осуществления всех других его функций, причем в современных условиях, один из важнейших. Разумеется, сказанное не исключает применения терминов «информационная функция», «функция информирования», и др. Однако, очевидно, что в данном случае критерием выделения таких категорий является не сфера жизнедеятельности общества – экология, экономика, политика, культура, и пр., а фактически способ осуществления деятельности, в частности, органов государства в названных сферах, т.е. функция как метод. Это, кратко говоря, иной ряд функций.

Комплекс мер по обеспечению права граждан на экологическую информацию как неотъемлемая составляющая экологической функции государства базируется на положениях ст. 34 Конституции Республики Беларусь, согласно которой гражданам гарантируется право

на получение, хранение и распространение полной, достоверной и своевременной информации о состоянии окружающей среды. 30 октября 2001 года для Республики Беларусь вступила в силу Конвенция о доступе к информации, участии общественности в процессе принятия решений и доступе к правосудию по вопросам, касающимся окружающей среды" (г. Орхус 25 июня 1998 г.), которая предусматривает широкий доступ к экологической информации общественности, в том числе ее участия в процессе принятия решений и доступа к правосудию по соответствующим вопросам.

На этой правовой основе предоставление и распространение экологической информации зафиксировано ст. 7 Закона Республики Беларусь «Об охране окружающей среды» в качестве одного из основных направлений государственной политики.

Феномен «экологическая информация» включает поиск, производство, получение, передачу, сбор, обработку, накопление, хранение, распространение и (или) предоставление информации о состоянии окружающей среды, воздействиях на нее и мерах по ее охране, о воздействиях окружающей среды на человека, состав которой определяется законодательными актами и международными договорами Республики Беларусь, пользование этой информацией и ее защиту, применение информационных технологий в объеме, требуемом целями и задачами реализации экологической функции государства. Накопление экологической информации осуществляется посредством проведения соответствующих экологических мероприятий: учета в области охраны окружающей среды, ведения кадастров природных ресурсов, мониторинга, формирования и ведения государственного фонда данных о состоянии окружающей среды и воздействиях на нее, предоставления и распространения сведений, включенных в реестры экологической информации указанного фонда данных и др. Распространение экологической информации осуществляется ее обладателями посредством ее доведения до сведения государственных органов и организаций, иных юридических лиц и граждан через размещение в печатных изданиях, других средствах массовой информации, на своих официальных сайтах в глобальной компьютерной сети Интернет или иными общедоступными способами. Экологическая информация также предоставляется ее обладателями посредством ее передачи государственным органам, иным юридическим лицам и гражданам в силу обязанностей, возложенных на обладателей такой информации законодательством, или на основании договора о предоставлении специализированной экологической информации.

Указанные мероприятия осуществляются как в целом, так и во всех подсистемах функционирования названного феномена во всех его проявлениях – на горизонтальном и вертикальном срезах управления, на центральном, региональном и местном уровнях, в государственном и в общественном аспектах и пр. Полагаем, что они в конечном итоге имеют не только эколого-информационное значение, но и являются необходимой предпосылкой целенаправленного эффективного регулирования государством широкого круга идеологических, социальных, предупредительных, экономических и иных процессов. Поэтому отсутствие экологической информации, либо ее неполнота, несвоевременность, недостоверность, на наш взгляд, может рассматриваться как потенциальная угроза национальной безопасности в целом.

Защита экологической информации с целью сохранения приданных ей характеристик организуется собственником или оператором информационной системы, содержащей такую информацию, либо обладателем информации, если она не содержится в информационных системах. С точки зрения обеспечения защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере как основного содержания информационной безопасности, зафиксированного в Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, важна последовательная реализация правовых, организационных и технических мер по защите экологической информации с целью придания ей характеристик целостности (неизменности), конфиденциальности,

доступности и сохранности. Среди таких мер можно назвать создание и развитие общегосударственных и местных систем экологической информации, обеспечение их совместимости и взаимодействия в едином глобальном информационном пространстве, формирование и защита эколого-информационных ресурсов, включающих статистические данные об экологическом положении в Республике Беларусь, обеспечение единства государственных стандартов в экологической сфере, их соответствия международным рекомендациям и требованиям, поддержка иных проектов информатизации в экологической сфере и т. д.

Отметим, что отдельные виды экологической информации требуют и специфических мер по ее защите. Так, защита экологической информации может осуществляться на основании ст. 74-2 Закона «Об охране окружающей среды» посредством ограничения доступа к ней: экологическая информация не подлежит предоставлению или распространению, если она отнесена к государственным секретам, либо если ее разглашение приведет к нарушению правил осуществления правосудия, производства предварительного расследования, ведения административного процесса, либо если разглашение информации причинит вред окружающей среде или создаст угрозу его причинения, а также в других случаях, предусмотренных законодательными актами, международными договорами Республики Беларусь в интересах национальной безопасности, защиты прав и свобод граждан, прав юридических лиц.

Вместе с тем, Конституция и иное законодательство Республики Беларусь исходят из презумпции широкой доступности экологической информации. Так, противозаконным является ограничение доступа к экологической информации о состоянии окружающей среды или причиненном ей вреде; о выбросах загрязняющих веществ в атмосферный воздух и сбросах сточных вод в водные объекты с превышением нормативов в области охраны окружающей среды или в отсутствие таких нормативов, если их установление требуется законодательством Республики Беларусь; о сбросах в водный объект химических и иных веществ, их смесей, предметов или отходов; о внесении химических и иных веществ в землю (почву), приведшем к ухудшению ее качества или качества подземных вод; об ионизирующем и электромагнитном излучении, шумовом или ином физическом воздействии с превышением нормативов в области охраны окружающей среды или в отсутствие таких нормативов, если их установление требуется законодательством Республики Беларусь.

Такая информация может достаточно подробно характеризовать внутреннюю ситуацию в стране в целом и является объектом внутренних и внешних источников угроз национальной безопасности в информационной сфере, актуальных для белорусского государства в силу отмеченных Концепцией национальной безопасности Республики Беларусь открытости и уязвимости ее информационного пространства от внешнего воздействия, активного развития технологий манипулирования информацией; попыток несанкционированного доступа извне к информационным ресурсам Беларуси, приводящие к причинению ущерба ее национальным интересам, в том числе в экологической сфере и др. Поэтому в отношении экологической информации общего назначения, предназначенной для общего пользования и распространяемой либо безвозмездно предоставляемой, а также специализированной экологической информации актуальной является разработка специальной системы мероприятий, основанной на общих принципах обеспечения национальной безопасности: законности, соблюдения конституционных прав и свобод человека; гуманизма и социальной справедливости; гласности; соблюдения баланса интересов личности, общества и государства, их взаимной ответственности и др. по нейтрализации вышеназванных источников угроз.

Такие мероприятия могут включать совершенствование механизмов реализации прав субъектов на получение, хранение, пользование и распоряжение экологической информацией, в том числе с использованием информационно-коммуникационных технологий. Учитывая всеобщую значимость экологической информации, возможную

масштабность негативных последствий недобросовестного пользования ею, помимо гарантий доступа к эколого-информационным ресурсам, формирующимся преимущественно за счет средств государственного бюджета, в законодательстве должен быть закреплены и обязанности субъекта получения эколого-информационных услуг, в том числе касающиеся условий правомерного пользования предоставленной информацией.

Защита информации – это и ее адекватное донесение до потребителей, что во многом обеспечивается минимизацией числа посредников передачи такой информации. Поэтому важным является повышение качества, объема и конкурентоспособности национального контента, его продвижению во внешнее информационное пространство с целью позиционирования Республики Беларусь на основе использования формируемой ею информации как экологически ориентированного государства.

Литература

1. Васенина, А.Н. Информационная функция современного российского государства: автореф. дис. ... канд. юрид. наук: 12.00.01 / А.Н.Васенина; Нижегор. акад. МВД России. – Н.Новгород, 2007. – 36 с.

В.Ф.КАРТЕЛЬ

ОСНОВНЫЕ НАПРАВЛЕНИЯ ЗАЩИТЫ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

В настоящее время жизнь общества характеризуется динамичным развитием современных информационных технологий. Системы и средства вычислительной техники и современные телекоммуникационные сети являются неотъемлемой частью нашей жизни и одним из главных факторов, влияющим на все сферы жизни и развития общества.

Сегодня информация является таким же богатством страны, как производственные и людские ресурсы. В современном мире, все больше тяготеющему к глобализации и взаимопроникновению экономик, основанному на обмене новейшими научными и технологическими достижениями, проблемы информационной безопасности приобретают особую актуальность.

От успешного решения вопросов безопасности и уровня защищенности информационной среды в сфере государственного управления, в различных отраслях промышленности, на транспорте, в сфере торговли и на финансовом рынке во многом зависит конкурентоспособность белорусского государства и благополучие граждан.

Вместе с тем нельзя не отметить уязвимость информационных систем от широкого спектра угроз внешнего и внутреннего характера, а также высокую вероятность наступления серьезных негативных последствий, связанных с нарушением их функционирования.

Стремительное развитие информационных технологий и широкое использование глобальных сетей в последнее десятилетие привели к тому, что объекты национальной критической информационной инфраструктуры становятся целями преступных действий, «мишенями» для противоправных посягательств террористических и криминальных групп, использующих глобальные сети в своих преступных намерениях.

Высокая сложность и одновременно уязвимость информационно-телекоммуникационных инфраструктур (ИТИ), являющихся основой национального и мирового информационных пространств, а также фундаментальная зависимость от их стабильного функционирования других инфраструктур государства приводят к возникновению принципиально новых угроз. Эти угрозы связаны, прежде всего, с потенциальной возможностью организации широкого спектра кибернетических атак на критически важные компьютерные системы этих инфраструктур в деструктивных целях.

Особая озабоченность в этом плане возникает в связи с разработкой, применением и распространением информационного оружия, в результате чего становятся возможны «информационные войны» и «кибернетический терроризм», основой которых является осуществление электронных, радиочастотных и компьютерных атак на критически важные объекты национальных ИТИ, обеспечивающих управление в жизненно важных сферах деятельности, обеспечивающих национальную безопасность страны.

Эти атаки имеют целью не только нанесение ущерба экономике страны. Их успешная реализация может привести к срыву задач государственного управления, в сфере обороны и управления войсками, оказанию психологического давления и возникновению паники среди населения и др.

Мировая и отечественная статистика реализованных угроз в отношении объектов ИТИ, уязвимость современных информационно-телекоммуникационных систем управления к кибернетическим атакам, тяжесть последствий таких атак, растущая технологическая оснащенность нападающих требуют принятия решительных мер по защите критических систем ИТИ.

Не менее актуальной остается и задача защиты критических инфраструктур от стихийных бедствий и катаклизмов, ошибок персонала.

С учетом указанных обстоятельств основополагающая роль в решении проблемы защиты национальных критических инфраструктур и их критически важных объектов информатизации (автоматизированных систем управления ими) принадлежит государству.

В Республике Беларусь сегодня эта роль закреплена в Концепции национальной безопасности, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. N 575. В ней впервые обеспечение надежности и устойчивости функционирования критически важных объектов информатизации (далее – КВОИ) отнесено к основным национальным интересам в информационной сфере, а нарушение функционирования КВОИ – к основным потенциальным либо реально существующим угрозам национальной безопасности. Несовершенство системы обеспечения безопасности КВОИ признается существенной внутренней угрозой национальной безопасности.

В этой связи приоритетным направлением нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в данной сфере.

Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность [1].

Решение задач, поставленных в Концепции национальной безопасности, требует разработки четко обоснованной стратегии защиты КВОИ, действенных механизмов ее реализации, создания организационной системы защиты КВОИ важнейших инфраструктур и кибернетического пространства страны в целом, разработки методов и средств, обеспечивающих адекватную защиту и оценку степени защищенности КВОИ, в первую очередь, для инфраструктур, критически важных для национальной безопасности.

Разработка принципиальных направлений стратегии защиты КВОИ отраслевых инфраструктур, как совокупности политических, организационных, технических, методических и иных мероприятий, требует существенной проработки вопросов обеспечения их безопасности в масштабе государства, создания современной системы управления защитой и контроля безопасности КВОИ.

В рамках этой проблемы необходимо решить следующие основные задачи:

1) определить общие требования по обеспечению безопасной эксплуатации и надежного функционирования КВОИ и разработать систему классификации КВОИ по уровням безопасности;

2) разработать методику расчета показателей защищенности КВОИ и уровня технической защиты информации от угроз различного вида, включающую анализ угроз их безопасности, оценку риска нарушения безопасности КВОИ жизненно важных инфраструктур в сфере государственного управления, кредитно-финансовой, транспортной, энергетики, чрезвычайных служб, жизнеобеспечения населения и других;

3) разработать методику оценки технической защиты информации и безопасного функционирования КВОИ;

4) разработать систему государственного регулирования и управления в области функционирования и обеспечения безопасности КВОИ, в том числе установить порядок отнесения объектов информатизации к критически важным, организации функционирования и обеспечения безопасности критически важных объектов информатизации, создать Государственный реестр КВОИ.

Важно отметить, что одной из составляющих выработки предлагаемых направлений явились результаты, полученные в ходе выполнения белорусскими и российскими специалистами в рамках программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006–2010 годы» ряда научно-исследовательских работ по проблематике безопасности критически важных систем информационно-телекоммуникационной инфраструктуры Союзного государства.

Аналогичные исследования и связанные с ними разработки проводятся в США, Канаде, странах Европы, Австралии, Китае и др. Выделяются критически важные для национальной безопасности инфраструктуры, анализируются угрозы КВОИ и возможные меры по повышению их безопасности. КВОИ регистрируются в государственных перечнях; организуется государственный контроль их безопасности; разрабатываются планы защиты КВОИ; ведутся научные исследования и разработки по повышению живучести КВОИ в условиях враждебной среды за счет введения новых, упреждающих атаки и обеспечивающих быстрое восстановление механизмов защиты; разрабатываются законодательные акты, регламентирующие обязанности всех субъектов по защите национальных кибернетических пространств, и нормативные технические акты, устанавливающие повышенные требования к обеспечению безопасности КВОИ.

В частности, защита кибернетических аспектов критических инфраструктур являлась целью стратегических документов, принятых Европейской комиссией и Государствами-членами ЕС в 2009 году. К ним относятся – Европейская программа защиты критических инфраструктур (European Programme for Critical Infrastructure Protection – EPCIP), Специальные стратегии по защите информационной инфраструктуры – CIIP, Защита критической энергетической инфраструктуры – CEIP.

Наиболее значимыми с точки зрения информационной, сетевой и Интернет безопасности является «Защита Европы от широкомасштабных атак и разрушений» (март 2009 года) и Заключение Конференции министров Европейского союза по защите критической информационной инфраструктуры (Таллин, 27-28 апреля 2009 г.), которые выдвинули на главное место необходимость поддерживать координацию между государствами – членами, содействие обмену надежными и имеющими большой практическое значение данными, касающимися инцидентов безопасности, и разработку совместных планов во внештатных ситуациях [2].

Особо широко работы по защите критических инфраструктур ведутся в США. Еще 7 января 2000 г. Президентом США был подписан "Национальный план защиты информационных систем". Общее руководство ходом работ в рамках данного плана возлагалось на Федеральный координационный совет по проблемам безопасности информационной инфраструктуры. План содержит 10 самостоятельных программ,

объединенных общей целью и связанных с решением задач в сфере определения критических сегментов и уязвимых сторон национальной информационной инфраструктуры, обучения и переподготовки специалистов, проведения НИОКР, внедрения технических средств защиты, принятия новых законов, соблюдения гражданских прав и свобод. При этом подчеркивается необходимость консолидации усилий правительства, федеральных ведомств и частного сектора в защите национальных информационных ресурсов как важнейшего условия достижения поставленной цели. План строит оборону киберпространства, опираясь на новые стандарты безопасности, многоуровневые технологии обеспечения безопасности, новые исследования и обученных людей. Разработана Стратегия защиты кибернетического пространства страны. В 2007 году разработан Закон о повышении безопасности Америки, включающий разделы 1101 «Защита критической инфраструктуры» и 1102 «Оценка риска и доклад». Закон обязывает ежегодно оценивать уязвимости и риски нарушения безопасности критических инфраструктур и активов по секторам, составлять ежегодные доклады Комитету национальной безопасности и Сенату о состоянии критической инфраструктуры, важной для национальной безопасности. Доклад должен включать мероприятия и контрмеры, предлагаемые, рекомендуемые или предписываемые Министром на основании этих оценок [3].

Таким образом, можно констатировать, что основные направления организации защиты отечественных критических инфраструктур, отраженные в Концепции национальной безопасности Республики Беларусь, документах по ее реализации, государственных программах, соответствуют современным международным подходам и позволят не только оценить степень защищенности КВОИ жизненно важных инфраструктур, повысить их стойкость к внутренним и внешним угрозам, но и обеспечить государственный контроль их безопасности, консолидировать усилия государственных органов, иных организаций, граждан Республики Беларусь, повысить эффективность их деятельности по обеспечению национальной безопасности Республики Беларусь, защите ее национальных интересов в информационном пространстве.

Литература

1. Об утверждении Концепции национальной безопасности Республики Беларусь: Указ Президента Респ. Беларусь, 9 нояб. 2010 г., N 575 // Нац. реестр правовых актов Респ. Беларусь. – 2010. – N 276. – 1/12080.

2. JOINT RESEARCH CENTRE - Work Programme 2010. Action n° 31008 – SCNI – Protection and Security of Critical Networked Infrastructures.

3. Improving America's Security Act of 2007.

В.Ф.КАРТЕЛЬ, В.В.ЮРКЕВИЧ

ОСНОВНЫЕ ИТОГИ ПРОГРАММЫ СОЮЗНОГО ГОСУДАРСТВА «СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ОБЩИХ ИНФОРМАЦИОННЫХ РЕСУРСОВ БЕЛАРУСИ И РОССИИ НА 2006–2010 ГОДЫ»

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, которая превращается в системообразующий фактор нашей жизни и активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности, как России, так и Беларуси. Безопасность Союзного государства существенным образом зависит от уровня безопасности ее информационной составляющей.

Республика Беларусь и Российская Федерация располагают значительными совместными информационными ресурсами, которые представляют собой систему организационно, методически и технологически взаимоувязанных национальных информационных ресурсов, создаваемых каждым государством на собственные средства, в своих собственных интересах и в интересах обмена данными между государствами-участниками, в том числе на условиях совместного использования, а также информационными ресурсами, создаваемыми на средства и в интересах Союзного государства. Обеспечение их надежного функционирования, сохранности и целостности является одной из первоочередных задач в деятельности Союзного государства.

Для решения вопросов по созданию эффективной системы защиты общих информационных ресурсов Беларуси и России был выполнен ряд мероприятий в рамках программ Союзного государства.

В период с 2000 по 2004 годы выполнялись работы по программе «Защита общих информационных ресурсов Беларуси и России», утвержденной Постановлением Исполнительного Комитета Союза Беларуси и России от 8 сентября 1999 г. №27, направленной на решение задач по обеспечению безопасности информационного пространства Союзного государства, и государств – участников договора от 8 декабря 1999 г.

На основе достигнутых результатов, полученных в ходе реализации этой программы, была разработана и утверждена постановлением Совета Министров Союзного государства от 26 сентября 2006 года № 32 программа Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006–2010 годы», которая явилась логическим продолжением программы «Защита общих информационных ресурсов Беларуси и России».

Работы по программе «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006–2010 годы» выполнялись в период с 2006 по 2010 годы.

Государственным заказчиком-координатором Программы была определена Федеральная служба по техническому и экспортному контролю России (ФСТЭК России).

Государственным заказчиком программы от Российской Федерации определена Федеральная служба безопасности Российской Федерации (ФСБ России), а от Республики Беларусь - Оперативно-аналитический центр при Президенте Республики Беларусь.

Головным исполнителем от Российской Федерации был определен Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России (ГНИИ ПТЗИ ФСТЭК России), а от Республики Беларусь Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации».

В выполнении заданий Программы от Республики Беларусь и Российской Федерации принимали участие ведущие научно-исследовательские институты и организации, имеющие большой опыт разработки сложных автоматизированных систем, средств защиты информации, разработки нормативных и правовых документов по защите информации.

Наиболее важными целями и направлениями работ Программы являлись:

1. Создание нормативно-методических и научно-технических условий для формирования и совершенствования системы защиты совместных информационных ресурсов и информационно-телекоммуникационной инфраструктуры Союзного государства от информационных угроз.

2. Создание нормативно-методических и научно-технических условий для эффективного обеспечения безопасности информации на действующих и разрабатываемых критически важных объектах информационно-телекоммуникационной инфраструктуры Союзного государства.

3. Создание условий для развития эффективных высокотехнологичных методов и средств защиты совместных информационных ресурсов и информационно-телекоммуникационной инфраструктуры Союзного государства.

В интересах достижения этих целей белорусской стороной было выполнено 16 программных мероприятий. В результате их реализации получены следующие результаты:

разработана обоснованная система межгосударственных стандартов в области обеспечения безопасности информации на критически важных объектах информационно-телекоммуникационной инфраструктуры Союзного государства *(НИР «Стандарт-ОБИ». Исполнитель задания - Государственное учреждение образования «Институт Национальной безопасности Республики Беларусь»)*;

исследованы методические подходы оценки утечки видеоинформации по техническому каналу, обусловленному модуляцией гармоник сигнала строчной развертки информативным видеосигналом и методы выявления технического канала утечки видеоинформации *(НИР «Поиск-БР». Исполнитель задания – Гомельский филиал Научно-производственного республиканского унитарного предприятия «Научно-исследовательский институт технической защиты информации»)*;

проведен анализ существующих принципов организации защищенных архивов электронных документов, определен и обоснован перечень требований к форматам и структуре данных, составляющих электронный документ защищенного архива, к обязательным реквизитам электронного документа защищенного архива и формам его представления, к созданию электронной копии документа на бумажном носителе, к правилам сертификации, распространения и отзыва открытых ключей проверки электронной цифровой подписи электронных документов защищенного архива, к защите электронных документов защищенного архива *(НИР «Архив ЭД Защита». Исполнитель задания – Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»)*;

исследован и проведен анализ международного опыта построения средств анализа и контроля эффективности защиты распределенных информационных ресурсов (РИР) от воздействия компьютерных атак, существующих показателей защищенности, подлежащих проверке при контроле эффективности защиты РИР от компьютерных атак, существующих метрик оценки показателей защищенности *(НИР «Контроль-БР». Исполнитель задания – Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»)*;

проведены исследования существующих видов и алгоритмов проведения враждебного информационного воздействия (ВИВ) на объекты информационных технологий (ИТ). Исследованы принципы построения систем обнаружения, прогнозирования ВИВ, принципы построения принятия решений по противодействию ВИВ, разработаны методические рекомендации по организации противодействия враждебному информационному воздействию *(НИР «Отражение». Исполнитель задания – Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»)*;

проведен анализ подходов к оценке важности систем критически важных объектов (КВО) информационно-телекоммуникационной инфраструктуры Союзного государства, сформулированы принципы отнесения объектов информатизации к категории ключевых *(НИР «Список-БР». Исполнитель задания – Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»)*;

проведены исследования по организации мониторинга состояния обеспечения безопасности информации на критически важных трансграничных системах информационно-телекоммуникационной инфраструктуры Союзного государства, по проведению контроля на критически важных объектах информационно-телекоммуникационной инфраструктуры, по информационному обмену между национальными органами контроля *(НИР «Мониторинг-БР». Исполнитель задания –*

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»);

проведены обоснование и конкретизация показателей качества профилей защиты, заданий по безопасности и объектов информационных технологий, а также критериев принятия решений о степени пригодности (непригодности) документов для разработки объектов информационной технологий и соответствия объектов информационных технологий заданию по безопасности *(НИР «Сабит». Исполнитель задания – Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», соисполнитель - Объединенный институт проблем информатики НАН Беларуси)*;

проведен анализ теоретических основ, используемых при разработке квантово-оптических криптографических линий связи, разработаны методы и техника измерения свойств квантовых битов на основе одиночных фотонов. Создан экспериментальный макет системы квантового распределения ключа для квантовых криптографических систем *(НИР «Квант». Исполнитель задания – Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», соисполнитель – Государственное научное учреждение «Институт физики им. Б.И.Степанова НАН Беларуси»).*

В ходе выполнения научно-исследовательских работ разработан ряд проектов нормативно-методических и руководящих документов, которые планируется подготовить в установленном порядке к утверждению в органах Союзного государства. Кроме того, созданы экспериментальные образцы защищенного электронного архива электронных документов, программного комплекса системы автоматизированного анализа и оценки безопасности объектов информационных технологий на этапах проектирования и модернизации, автоматизированной информационно-справочной системы «Каталог-БР». На основе проведенных исследований экспериментальных образцов планируется дальнейшее проведение опытно-конструкторских работ.

В результате опытно-конструкторских работ, выполненных в рамках программных мероприятий, изготовлены опытные образцы:

переносного автоматизированного программно-аппаратного комплекса по проведению специальных исследований технических средств обработки информации в расширенном диапазоне частот и контроля защищенности помещений от утечки информации по акустическим и виброакустическим каналам *(ОКР «Филин». Исполнитель задания – Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», соисполнители – учреждение образования «Полоцкий государственный университет» и Гомельский филиал Научно-производственного республиканского унитарного предприятия «Научно-исследовательский институт технической защиты информации»)*;

аппаратуры считывания радиочастотных идентификаторов *(ОКР «Мираж». Исполнитель задания – Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»)*;

средства контроля эффективности защиты распределенных информационных ресурсов от воздействия компьютерных атак (сканер «Контролер» *(ОКР «Контролер-БР». Исполнитель задания – Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»)*;

специализированного носителя информации на базе перепрограммируемого записывающего устройства для средств криптографической защиты информации *(ОКР «Носитель». Исполнитель задания – Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»)*.

Разработанные опытные образцы обеспечивают потребительские и технические характеристики и по своим функциональным возможностям не уступают зарубежным

аналогам. Использование разработанных технических средств позволит повысить уровень защиты информации при снижении финансовых затрат.

В настоящее время проводится взаимный обмен полученными результатами работ между Российской Федерацией и Республикой Беларусь.

В результате реализации программных мероприятий созданы необходимые правовые, организационные и научно-технические условия для обеспечения эффективной защиты информационных ресурсов и информационно-телекоммуникационной инфраструктуры Союзного государства.

В целом результаты программы позволяют реализовать первоочередные задачи Союзного государства, изложенные в Договоре о создании Союзного государства:

обеспечение функционирования взаимоувязанных систем связи и телекоммуникаций;

ведение единых банков данных;

формирование единого научного, технологического и информационного пространства;

обеспечение безопасности единого информационного пространства.

В настоящее время в интересах дальнейшего совершенствования организации и мер защиты совместных информационных ресурсов Беларуси и России, повышения эффективности национальных систем защиты информации, действующих в интересах Союзного государства, Оперативно-аналитическим центром при Президенте Республики Беларусь совместно с ФСТЭК России проводятся работы по разработке новой программы Союзного государства в данной области с реализацией в 2011-2015 гг.

И.А.КАРТУН

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБЪЕКТОВ

В настоящее время с развитием компьютеризации информация о частной жизни физического лица и персональные данные (далее – персональные данные) переводятся в электронный вид, а организации стали активно обмениваться данной информацией по роду своей деятельности. В связи с этим остро встает вопрос защиты персональных данных, как определенной категории информации, имеющей немаловажное значение для каждого гражданина.

Рассмотрим вопросы законодательства, касающиеся персональных данных и их защиты.

Закон Республики Беларусь «О регистре населения» вводит понятие «персональные данные» и говорит об обязательной их защите только в рамках созданного регистра населения – государственной централизованной автоматизированной информационной системы, основу которой составляет база персональных данных граждан Республики Беларусь, а также иностранных граждан и лиц без гражданства, постоянно проживающих в Республике Беларусь. Целью создания регистра населения является объединение государственных информационных ресурсов учета физических лиц и формирование единого информационного пространства республики для удовлетворения информационных потребностей государственных органов, юридических и физических лиц.

Что касается получения информации из регистра, согласно Закону все организации условно делятся на две группы. К первой группе принадлежат организации, для которых использование персональных данных из регистра необходимо для выполнения задач, входящих в компетенцию этих организаций, определенную законодательством Республики Беларусь. Таким организациям данные будут предоставляться бесплатно по договору о

регулярном предоставлении данных. Организация – получатель информации из регистра будет иметь свой идентификационный код (ключ авторизации, электронная цифровая подпись), который будет включаться во все информационные сообщения данной организации. А регистр населения с помощью системы распознавания ключей автоматически определяет, что и в каком объеме можно выдавать организации - получателю и что от нее получать.

Второй группе организаций – тем, для которых использование персональных данных из регистра не является необходимым условием выполнения их задач, будут предоставляться только обезличенные персональные данные и только на платной основе.

Граждане смогут получать персональные данные из регистра в отношении себя, тех физических лиц, законными представителями которых они являются, и - с письменного согласия – персональные данные других физических лиц, законными представителями которых они не являются.

Закон Республики Беларусь «О регистре населения» также содержит положения, направленные на защиту персональных данных, содержащихся в регистре. Законом предусмотрено, что порядок защиты персональных данных, содержащихся в регистре, определяется распорядителем регистра и, в случае ненадлежащего выполнения этой функции, он будет нести ответственность, предусмотренную законодательными актами за ненадлежащее выполнение своих функций. На защиту персональных данных направлены также положения Закона о необходимости использования для ведения регистра компьютерных программ и технических средств, сертифицированных в установленном законодательством порядке.

Вышедшее позднее Постановление Совета Министров Республики Беларусь от 10 сентября 2009 г. № 1178 «Об утверждении положений о порядке защиты персональных данных переписи населения Республики Беларусь и порядке предоставления итоговых данных переписи населения Республики Беларусь» подобно Закону Республики Беларусь «О регистре населения» определяет порядок защиты и предоставления итоговых данных переписи населения Республики Беларусь. Персональные данные по переписи населения являются конфиденциальными, не подлежат разглашению и используются только в статистических целях. Конфиденциальность персональных данных и их неразглашение гарантируется данным законом. Стоит отметить, забегая вперед, что система защиты информации системы переписи населения была аттестована, что немаловажно.

Закон Республики Беларусь «Об информации, информатизации и защите информации» определяет персональные данные как информацию, распространение и (или) предоставление которой ограничено, а также говорит о защите персональных данных, содержащихся в информационных системах. Данный нормативно-правовой акт, в отличие от двух предыдущих, распространяет свое влияние на все персональные данные без привязки к конкретной информационной системе, в которой они обрабатываются. Однако именно данный закон заставляет задуматься над реальностью выполнения требований по защите персональных данных.

Приведем некоторые постулаты Закона Республики Беларусь «Об информации, информатизации и защите информации»:

«Никто не вправе требовать от физического лица предоставления информации о его частной жизни и персональных данных, включая сведения, составляющие личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, касающиеся состояния его здоровья, либо получать такую информацию иным образом помимо воли данного физического лица, кроме случаев, установленных законодательными актами Республики Беларусь»;

«Распространяемая и (или) предоставляемая информация должна содержать достоверные сведения о ее обладателе, а также о лице, распространяющем и (или)

предоставляющем информацию, в форме и объеме, достаточных для идентификации таких лиц»;

«Защита информации организуется: в отношении информации, распространение и (или) предоставление которой ограничено, – собственником или оператором информационной системы, содержащей такую информацию, либо обладателем информации, если такая информация не содержится в информационных системах»;

«Меры по защите персональных данных от разглашения должны быть приняты с момента, когда персональные данные были предоставлены физическим лицом, к которому они относятся, другому лицу либо когда предоставление персональных данных осуществляется в соответствии с законодательными актами Республики Беларусь".

Мы видим необходимость иметь для обработки персональных данных согласие на нее однозначно идентифицированных субъектов.

Рассмотрим для примера процедуру бронирования билетов на железной дороге через Интернет. Пользователь, заполняет на сайте определенные поля, внося туда свои персональные данные, автоматически согласившись с их распространением. Как может владелец интернет-сайта доказать согласие на обработку персональных данных покупателя? Сославшись на то, что тот сам заполнил необходимые поля при бронировании билета и тем самым выразил косвенное согласие на их обработку? А если это персональные данные не покупателя, а какого-то другого человека, которые покупатель посчитал нужным использовать при оформлении заказа? Вполне может быть, что сведения, указанные при заказе, вообще не являются чьими-то персональными данными, а вымышлены.

Проблема в том, что во всемирной сети нет идентификации личности. За исключением случаев использования сертификатов цифровой подписи, доказать, что действия в сети выполняет именно тот человек, за которого он себя выдает, невозможно. В данной статье невозможно рассмотреть все особенности ее применения, отметим лишь, что большой проблемой является проверка сертификатов многочисленных, самостоятельно функционирующих удостоверяющих центров и возможность получения сертификата на ник (псевдоним) пользователя в зарубежных удостоверяющих центрах (используются штатные возможности операционной системы – https). Выходом могло бы являться, например, обязательно требование использования владельцем информационной системы сертифицированных в Республике Беларусь криптографических решений, однако владелец информационной системы попросту не сможет установить подобное программное обеспечение обычным людям на их персональные компьютеры. Тогда кто будет нести ответственность за компрометацию персональных данных?

Проблемы появляются и при контролировании подлинности и правомерности размещения персональных данных в аккаунтах пользователей социальных сетей. Очевидно, что размещение персональных данных в социальных сетях, их изменение без согласия субъекта может привести к негативным последствиям для этого самого субъекта.

Подобные вопросы, скорее всего, со временем решатся, однако очевидно одно – для защиты персональных данных должны использоваться системы защиты информации, аттестованные в установленном законодательством порядке, что даст гарантию конфиденциальности, целостности и доступности персональных данных.

В.В.КОМИСАРЕНКО

РЕГУЛИРОВАНИЕ ТЕХНОЛОГИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

В 1976 году Уитфилдом Диффи и Мартином Хеллманом было впервые предложено понятие «электронная цифровая подпись» (далее – ЭЦП). В тот момент они всего лишь предполагали, что схемы ЭЦП могут существовать. В 1977 году Рональд Ривест, Ади Шамир и Леонард Адлеман разработали криптографический алгоритм RSA, который можно было использовать для создания ЭЦП.

В настоящее время ЭЦП получила очень широкое распространение. ЭЦП прошла путь от математической идеи до технологии, которая включает в себя совокупность процедур, методов, программных, программно-технических и технических средств, относящихся к практическому применению ЭЦП.

Законодательство в сфере регулирования ЭЦП постоянно совершенствуется. В целях гармонизации законодательства государств Комиссия Организации Объединенных Наций по праву международной торговли (UNCITRAL) 12 июня 1996 года приняла типовой Закон об электронной торговле. Этот Закон был призван облегчить использование средств связи и хранения информации.

В России в сфере ЭЦП действует федеральный Закон от 10 января 2002г. №1-ФЗ «Об электронной цифровой подписи». Третье чтение прошел новый законопроект «Об электронной подписи».

В Республике Беларусь правовые основы использования ЭЦП заложены в пункте 2 статьи 161 Гражданского кодекса Республики Беларусь о письменной форме сделки. В этом пункте установлено, что использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи допускается в случаях и порядке, предусмотренных законодательством или соглашением сторон. 28 декабря 2009 года принят Закон «Об электронном документе и электронной цифровой подписи», который вступил в силу в декабре 2010 года. В данном Законе определяются условия, при которых электронный документ с ЭЦП приравнивается к документу на бумажном носителе, подписанному собственноручно, и имеет одинаковую с ним юридическую силу. В соответствии с Законом государственное регулирование в сфере обращения электронных документов и электронной цифровой подписи осуществляется Президентом Республики Беларусь, Советом Министров Республики Беларусь, Национальным банком Республики Беларусь, Оперативно-аналитическим центром при Президенте Республики Беларусь, органами и учреждениями Государственной архивной службы Республики Беларусь, иными государственными органами и другими государственными организациями в пределах их компетенции и в порядке, предусмотренном этим Законом и иными актами законодательства Республики Беларусь.

Государственное регулирование в сфере технологии ЭЦП включает в себя:

– формирование и проведение единой государственной политики в сфере применения ЭЦП;

– утверждение государственных программ и обеспечение их реализации;

– создание и развитие системы требований к элементам технологии ЭЦП (разработка и утверждение нормативных правовых актов в области технического нормирования и стандартизации);

– регулирование отношений в сфере функционирования Государственной системы управления открытыми ключами (далее – ГосСУОК);

– подтверждение соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации или заявленным показателям;

– регулирование деятельности субъектов отношений в области технологии ЭЦП;

– контроль за деятельностью субъектов отношений по применению ЭЦП.

Формирование единой государственной политики в сфере применения ЭЦП включает в себя решение концептуальных вопросов в данной сфере, определение принципов применения технологии ЭЦП, формулировку основных целей применения ЭЦП и постановку первоочередных задач.

Большую роль в процессах внедрения ЭЦП на практике играют государственные программы, в рамках реализации проектов которых ставятся задачи по применению ЭЦП для обеспечения подлинности электронных документов, обрабатываемых в автоматизированных системах и информационных системах документационного обеспечения управления.

Создание и развитие системы требований к элементам технологии ЭЦП осуществляется в соответствии с Законом «О техническом нормировании и стандартизации». Основными объектами технического нормирования и стандартизации в сфере технологии ЭЦП являются:

– алгоритмы (процедуры) выработки и проверки ЭЦП и их параметры;

– форматы данных (сертификатов открытых ключей проверки подписи, списков отозванных сертификатов, значений ЭЦП, подписанных сообщений, хранения и защиты личных ключей и другие);

– прикладные интерфейсы средств ЭЦП;

– средства ЭЦП, включая средства управления ключами ЭЦП, программные и программно-технические средства автоматизации регистрационных и удостоверяющих центров, средства для создания копий электронных документов на бумажном носителе, активы указанных средств.

Национальный банк Республики Беларусь разрабатывает и утверждает планы развития ГосСУОК, осуществляет иное регулирование отношений в сфере ее функционирования. В целях реализации положений Закона «Об электронном документе и электронной цифровой подписи».

Координация деятельности органов государственного управления в направлении развития ГосСУОК осуществляется в рамках Межведомственного координационного совета. В состав совета вошли представители Национального банка Республики Беларусь, Аппарата Совета Министров Республики Беларусь, Министерства связи и информатизации Республики Беларусь, Министерства по налогам и сборам Республики Беларусь, Министерства юстиции Республики Беларусь, Министерства труда и социальной защиты Республики Беларусь, Государственного таможенного комитета Республики Беларусь, Национального статистического комитета Республики Беларусь, Оперативно-аналитического центра при Президенте Республики Беларусь, государственного учреждения «Главное хозяйственное управление» Управления делами Президента Республики Беларусь, государственного учреждения «Белорусский научно-исследовательский центр электронной документации», Белорусского государственного университета.

Сертификация средств ЭЦП осуществляется в соответствии с положениями Закона «Об оценке соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации». Органом по сертификации средств ЭЦП является Оперативно-аналитический центр при Президенте Республики Беларусь. Постановлением Совета Министров Республики Беларусь №675 утвержден порядок проведения государственной экспертизы средств защиты информации (в том числе и средств ЭЦП). Экспертиза продукции проводится Оперативно-аналитическим центром при Президенте Республики Беларусь. Экспертиза средств ЭЦП проводится в случае их единичного производства, либо в случае, когда необходимо проверить реализацию требований, которые техническими нормативными правовыми актами не установлены. В последнем случае экспертиза проводится на соответствие заявленным показателям

(характеристикам), содержащимся в документации изготовителя. При этом номенклатура показателей согласовывается с органом государственной экспертизы.

Указом Президента Республики Беларусь от 1 сентября 2010 г. №450 утверждено Положение о лицензировании отдельных видов деятельности. В Положении установлены составляющие работы и услуги деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи, на осуществление которых требуются специальные разрешения (лицензии). В соответствии с Указом выдачу лицензий на право осуществления деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи, осуществляет Оперативно-аналитический центр при Президенте Республики Беларусь.

Анализируя установленные Положением о лицензировании отдельных видов деятельности, составляющие работы и услуги по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи, можно установить, что в сфере технологии ЭЦП лицензированию подлежат следующие работы и услуги:

– разработка, производство, реализация, монтаж, наладка, сервисное обслуживание (либо выборка из указанного перечня работ) средств ЭЦП;

– проведение испытаний средств ЭЦП по требованиям безопасности информации;

– удостоверение формы внешнего представления электронного документа на бумажном носителе;

– оказание услуг по распространению открытых ключей проверки подписи.

Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 4 марта 20011 г. №18 утверждено Положение о порядке применения средств криптографической защиты информации в системах защиты информации. Положение определяет порядок применения средств криптографической защиты информации, к которым относятся и средства ЭЦП, в системах защиты информации государственных информационных систем, а также информационных систем, содержащих информацию, распространение и (или) предоставление которой ограничено.

Реализация совокупности приведенных мер по регулированию технологии ЭЦП позволит обеспечить высокий уровень безопасности при ее практическом использовании.

И.И.ЛИВШИЦ

СОВРЕМЕННАЯ ПРАКТИКА ПРОВЕДЕНИЯ АУДИТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Предметная область

Система менеджмента информационной безопасности (СМИБ) - одна из нескольких «высокотехнологичных» систем менеджмента, привлекающая внимание специалистов в последнее время. Интерес к СМИБ возник не случайно, т.к. менеджмент современных предприятий пришел (ценой практики известных инцидентов ИБ) к пониманию проблемы защиты своих активов через определенные процедуры.

Предметную область СМИБ четко формулирует стандарт ISO/IEC 27001:2005 (п. 3.7): **система менеджмента информационной безопасности (СМИБ)** *[information security management system] [ISMS] - часть общей системы менеджмента, основанная на управлении бизнес-рисками для создания внедрения, эксплуатации, мониторинга, анализа, поддержания и улучшения ИБ.*

Понимание, что СМИБ – задача многомерная, требующая участия различных подразделений в организации, установления тонкого баланса затрат «***угроза – атака – оценка – защита***», в настоящее время встречается не так часто. СМИБ, как современный инструмент менеджмента, может быть исключительно эффективен в ситуациях, когда бизнес адекватно понимает и обоснованно принимает определенные, точно оцененные риски и способен оперативно управлять своими бизнес-процессами даже в условиях негативного изменения ситуации.

Нормативная база (критерии аудита)

Нормативная база СМИБ будет рассматриваться в данной публикации в «расширительном толковании» - и как критерии аудита (в точном соответствии с термином «критерии аудита»), и как справочная (дополнительная) информация, необходимая для создания и, в большей степени, для постоянного улучшения СМИБ.

Базовым или сертифицирующим стандартом является только ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования». Требования аудитов СМИБ четко и однозначно «прописаны» в разделе 6 стандарта ISO/IEC 27001:2005. Очевидно, что инструмент внутреннего аудита является эффективным и позволяет, что весьма важно, решать вопросы оперативно и «не выносить сор из избы».

Ситуации аудитов ИБ

Важно рассмотреть проблему ИБ в аспекте безопасности бизнес-процессов. Для компактности изложения остановимся на 3-х примерах:

А.8.3.3 Удаление прав доступа – Права доступа всех служащих, подрядчиков и пользователей третьей стороны к информации и средствам обработки информации должны быть удалены по истечении срока их найма, действия договора или соглашения, или скорректированы после изменения.

В одной из крупнейших ИТ-компаний России аудиторами был задан вопрос: «Каким образом выполняются требования п. А.8.3.3?». С разрешения Представителя руководства организации был проанализирован ряд учетных записей сотрудников, прекративших работу за последние 6 мес. Выяснилось, что при увольнении учетные записи не блокировались, а просто передавались новым сотрудникам. Более того, часть настроек («профили» пользователей) никак не корректировались после второй и даже третьей смены «владельца», например, для роли «бухгалтер» были открыты права доступа к системам маркетинга (CRM) и финансовой отчетности.

А.9.2.7 Вынос имущества – Оборудование, информация или ПО не могут быть вынесены из помещения организации без соответствующего разрешения.

Проблема выноса имущества и контроля этого процесса известна достаточно давно. На одном из аудитов с разрешения руководителя службы безопасности предприняли попытку выноса большой коробки за пределы бизнес-центра. Но не через проходную «в лоб» – так было неинтересно, а через задние ворота корпоративной парковки … Ворота были открыты, и аудитор в костюме с галстуком без помех вынес большую коробку (для целей эксперимента, пустую).

А.10.7.2 Утилизация носителей информации – Носители информации, когда в них больше нет необходимости, должны надежно и безопасно утилизироваться, используя формальные процедуры.

К проблеме утилизации носителей информации необходимо относиться со всей серьезностью, т.к. все утечки информации, как правило, выполняются именно через «отчуждаемые» носители.

Добавленная стоимость аудитов ИБ

Как было показано выше, известна статистика оценки целей сертификации систем менеджмента для различных организаций: 40% для целей получения красивого сертификата (*не хуже чем у других…),* 40% для целей выполнения внешних требований (*тендеры…)* и только 20% для выполнения поставленных целей высшего руководства (владельцев). СМИБ не является исключением этой статистики и необходимо обсудить, какую пользу или «***добавленную стоимость аудитов ИБ***» может принести организации. Проблема обеспечения ИБ находится в фокусе внимания менеджмента по ряду причин, среди которых: постоянные изменения в действующем законодательстве, активное развитие информационных технологий, глобальная интеграция экономических (в т.ч. кризисных) процессов, агрессивная конкурентная среда. Рассмотрим несколько отраслевых примеров «***добавленной стоимости аудитов ИБ***».

Пример 1. Применение стандарта ISO/IEC 27001:2005 для отрасли машиностроения.

В июне 2010 г. группой аудиторов проводился аудит СМИБ на одном из крупнейших машиностроительных предприятий России. Во вторник в одном из подразделений департамента управления персоналом аудитор зафиксировал несоответствие, касающееся защиты записей организации. Формулировка несоответствия (незначительно измененная) такова: *«В группе кадрового делопроизводства (департамент управления персоналом) отсутствует формальный процесс санкционирования предоставления персональных данных сотрудников при передаче отчетов в пенсионный фонд, что противоречит требованиям действующего Федерального закона XXX».*

В пятницу при проверке юридического департамента аудиторы попросили информацию о проверках, которые проводились регуляторами за последний год. Среди нескольких отчетов было предоставлено предписание по устранению в срок до мая 2010 г. ряда нарушений, в т.ч. и нарушений по порядку защиты данных, выявленных в том самом подразделении департамента управления персоналом 3 днями ранее…

Пример 2. Применение стандарта ISO/IEC 27001:2005 для отрасли здравоохранения (фрагмент)

Пункт ISO/IEC 27001: 2005	**Требование ISO/IEC 27001:2005**	**Рекомендуемые меры (средства) защиты**
4.2.1 a)	Определить область применения и границы СМИБ в терминах характеристик бизнеса, организации, ее местоположения, активов и технологий, включая подробности и обоснование любых исключений из области применения.	A.5.1.1 «Документ политики ИБ» A.5.1.2 «Анализ политики ИБ» A.7.1.1. «Реестр активов» A.7.1.2 «Владение активами» A.8.2.1. «Ответственность руководства»

Заключение

Внедрение и сертификация СМИБ в соответствии с требованиями ISO/IEC 27001:2005 предоставляет организации комплекс преимуществ:

– независимое подтверждение факта, что в организации должным образом выявлены, оценены и системным образом управляются риски, т.е. соответствующие процедуры ИБ разработаны, внедрены, постоянно анализируются и улучшаются компетентным и ответственным персоналом;

– доказательство соблюдения действующего законодательства и нормативных актов в области ИБ;

– доказательство стремления высшего руководства организации к обеспечению ИБ в требуемом объеме для всей организации в соответствии с установленными требованиями;

– доказательство создания адекватной и актуальной модели рисков в организации;

– демонстрация определенного уровня ИБ для обеспечения конфиденциальности информации клиентов и партнеров организации;

– демонстрация проведения регулярных аудитов ИБ, оценки результативности и постоянных улучшений СМИБ.

Практика аудитов ИБ, как обязательная документированная процедура международного стандарта ISO/IEC 27001:2005, призвана обеспечить снижения рисков, уровня последствий и реального ущерба от инцидентов ИБ, а также снижения операционных издержек и исключения «перекрестного» финансирования в рамках единой СМИБ.

Н.Д.МИКУЛИЧ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ. АКТУАЛЬНЫЕ ВОПРОСЫ

В современных условиях полноценную защиту информации можно обеспечить только с применением криптографических методов защиты информации. Современная криптография как наука основывается на совокупности фундаментальных понятий и фактов математики, физики, теории информации и сложности вычислений. Несмотря на традиционную ее сложность, многие теоретические достижения криптографии сейчас широко используются.

Они обеспечивают решение основных задач информационной безопасности: конфиденциальность, целостность, подлинность, аутентификация как пользовательской и служебной информации при хранении и передаче по каналам связи.

Это достигается:

– шифрованием данных, баз данных;

– шифрованием всего информационного трафика и отдельных сообщений;

– криптографической аутентификацией устанавливающих связь объектов информационного взаимодействия;

– защитой несущего данные трафика средствами имитозащиты и электронно-цифровой подписи для обеспечения целостности и достоверности передаваемой информации;

– применением криптографических стойких проверочных кодов для контроля целостности данных, программного обеспечения;

– применением электронно-цифровой подписи для обеспечения юридической значимости электронных документов.

Криптографические протоколы также являются одним из важнейших средств решения задач информационной безопасности в сетях передачи данных. Их применение обусловлено использованием обширных механизмов межсетевого взаимодействия. Большинство криптографических протоколов в своей основе используют криптографические алгоритмы (блочного шифрования, ЭЦП, хэш-функции).

К 2000 году в Республике Беларусь была создана нормативно-правовая база, обеспечивающая создание и развитие отечественных средств криптографической защиты информации (СКЗИ), заложены основы использования электронной цифровой подписи (ЭЦП) и организации юридически значимого электронного документооборота в корпоративных информационных системах субъектов хозяйствования.

С принятием 28 декабря 2009 года Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи» актуальной задачей является формирование единой государственной политики в сфере применения ЭЦП, построение государственной системы управления открытыми ключами (ГосСУОК) электронной цифровой подписи и внедрение ЭЦП в систему межведомственного электронного документооборота Республики Беларусь.

В условиях стремительно развивающегося рынка электронных услуг и электронной торговли первоочередными задачами для республики являются вопросы цифрового доверия, создание системы идентификации для физических и юридических лиц.

Для юридических и физических лиц должны быть созданы доступные в ценовом и техническом аспекте механизмы и средства, обеспечивающие идентификацию и аутентификацию пользователей, конфиденциальность и целостность сообщений в системах и сетях общего пользования. Это позволит расширить сферу использования электронного документооборота, обеспечит возможность ведения электронной торговли, предоставления электронных услуг организациям и гражданам, широкомасштабного внедрения систем электронных платежей.

Для этого необходимо:

совершенствовать нормативную правовую базу для обеспечения правовых условий использования ЭЦП;

унифицировать элементы информационно-технологических систем, обеспечивающие использование ЭЦП;

обеспечить совместимость различных программно-технических решений, функционирующих в настоящее время, с создаваемой ГосСУОК;

обеспечить взаимодействие существующих и создаваемых удостоверяющих центров (УЦ), оказывающих услуги в электронном документообороте, в том числе банковской сфере.

дополнить существующую нормативно-правовую базу необходимыми нормативными правовыми актами (далее – НПА) и техническими нормативными правовыми актами (далее – ТНПА) регламентирующими функционирование ГосСУОК.

Основные из нормативных правовых и технических нормативных правовых актов, регламентирующих функционирование ГосСУОК:

Положение об удостоверяющем центре ГосСУОК;

Положение о регистрационном центре ГосСУОК;

Общие требования к удостоверяющему центру и правила его функционирования в ГосСУОК;

Общие требования к регистрационному центру и правила его функционирования в ГосСУОК;

Политика применения сертификатов в ГосСУОК;

Регламент корневого удостоверяющего центра ГосСУОК;

Регламент Подчиненного удостоверяющего центра ГосСУОК;

Государственный стандарт Республики Беларусь СТБ П 34.101.xxx-2010 «Информационные технологии. Взаимосвязь открытых систем. Правила присвоения значений компонентов идентификаторов объектов информационных технологий».

Кроме того, дорабатываются действующие технические нормативные правовые акты Республики Беларусь, регламентирующие деятельность в сфере защиты информации с использованием криптографических методов:

«Информационные технологии. Синтаксис запроса на получение сертификата»;

«Информационные технологии. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»;

«Информационные технологии. Защита информации. Форматы параметров криптографических алгоритмов»;

«Информационные технологии. Электронные цифровые подписи и инфраструктуры (ЭЦПИ). Требования к политике удостоверяющих центров, выдающих квалифицированные сертификаты»;

«Информационные технологии. Инфраструктура открытых ключей Интернет X.509. Онлайн-протокол статуса сертификата (OCSP)»;

«Банковские технологии. Процедуры выработки псевдослучайных данных с использованием секретного параметра»;

«Банковские технологии. Формат карточки открытого ключа».

В Республике Беларусь продолжается формирование семейства базовых криптографических алгоритмов.

Алгоритмы шифрования.

Утвержден и вводится в действие СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности». Стандарт определяет семейство криптографических алгоритмов шифрования и контроля целостности, которые используются для защиты информации при ее хранении, передаче и обработке. Стандарт применяется при разработке средств криптографической защиты информации. Основные характеристики: длина блока -128 бит, длина ключа- 128,192, 256 бит, длина имитовставки – до 64 бит. Шифрование может выполняться в одном из шести режимов: простой замены, сцепления блоков, гаммирования с обратной связью, счетчика, одновременного шифрования и имитозащиты данных, одновременного шифрования и имитозащиты ключа.

Функции хэширования.

В СТБ 34.101.31-2011 определен алгоритм хэширования для вычисления хэш-значений – двоичных слов фиксированной длины, которые определяются по сообщению без использования ключа и служат для контроля целостности сообщения и представления сообщения в сжатой форме. Длина хэш-значения – до 256 бит.

Системы ЭЦП.

Разработан и проходит нормоконтроль проект стандарта «Алгоритмы выработки и проверки электронной цифровой подписи на основе эллиптических кривых». Стандарт устанавливает алгоритмы выработки и проверки ЭЦП, генерации и проверки параметров эллиптической кривой, генерации и проверки личных и открытых ключей подписи, а также вспомогательные алгоритмы транспорта ключа и генерации псевдослучайных чисел. В нем описываются алгоритмы электронной цифровой подписи, в которых используются вычисления в группе точек эллиптической кривой над конечным простым полем. Стандарт призван заменить СТБ 1176.2-99. Переход от алгоритмов СТБ 1176.2-99 к алгоритмам стандарта позволит уменьшить время выработки и проверки ЭЦП, сократить длины параметров и ключей при сохранении уровня криптографической стойкости. Он также как и СТБ 1176.2-99 базируется на схеме ЭЦП Шнора.

Приказом начальника ОАЦ от 04.03.2011г. утверждено Положение о порядке применения средств криптографической защиты информации в системах защиты информации.

Положение определяет порядок применения средств криптографической защиты информации (далее – СКЗИ) в системах защиты информации государственных информационных систем, а также информационных систем, содержащих информацию, распространение и (или) предоставление которой ограничено. В приложении приведен перечень технических нормативных правовых актов и документов, в которых определены

требования к СКЗИ и на соответствие которым осуществляется сертификация, государственная экспертиза СКЗИ.

А.А.ОБУХОВИЧ

О ПОРЯДКЕ АТТЕСТАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В Республике Беларусь аттестация систем защиты информации по существу только начинает внедряться в практику создания и применения информационных систем.

Первый опыт выполнения работ по аттестации выявил ряд проблем, основными из которых являются:

– недостаточность и несогласованность нормативных правовых актов в области защиты информации, в том числе и технических нормативных правовых актов;

– отсутствие методического обеспечения проведения аттестации;

– слабая специальная подготовка кадров, обеспечивающих выполнение требований по защите информации, как при разработке, так и при эксплуатации информационных систем.

Недостаточность и несогласованность нормативных правовых актов в области защиты информации, в том числе и технических нормативных правовых актов (ТНПА) выражается в следующем:

– система стандартов, регламентирующая порядок разработки и постановки продукции на производство, по которой проводятся ОКР по созданию государственных информационных систем, не предусматривает выполнение необходимых работ, связанных с обеспечением защиты информации, а именно: разработка и оценка в испытательных лабораториях заданий по безопасности, проведение аттестации подсистемы защиты информации. При этом ни ЕСКД и ЕСПД не предусмотрена разработка сопутствующих документов: функциональная спецификация, отчет по оценке уязвимостей, отчет по доказательству соответствия: проект верхнего уровня - функциональная спецификация – реализация;

– отсутствуют ТНПА, содержащие функциональные требования безопасности (например, пакеты функциональных требований безопасности) для информационных систем, относящихся к различным классам по СТБ 34.101.30;

– нет документов, содержащих критерии для обоснования и выбора УГО по СТБ 34.101.3.

Приведенные несоответствия проявляются уже на стадии разработки и согласования технических заданий на разработку (модернизацию) информационных систем. На этой стадии заказчик, ссылаясь на неурегулированность этих вопросов в законодательстве и ТНПА, пытается «сэкономить» на перечне работ и перечне документации (исключить их из ТЗ), выдвигая в тоже время необоснованные (иной раз завышенные) функциональные и гарантийные требования безопасности. Так прослеживается желание заказчика устанавливать в задании по безопасности УГО 2 или расширенный УГО 2 в то время как практически этот уровень могут обеспечить только предприятия-разработчики, имеющие сертификат соответствия их систем менеджмента качества требованиям стандарта ИСО 9001.

На этапе ввода систем в эксплуатацию несоответствие проявляется при выборе момента начала проведения аттестации:

– с одной стороны, в предоставляемых с заявкой на аттестацию исходных данных заявитель должен выдать исполнителю протоколы функциональных требований безопасности стадии подсистемы защиты информации;

– с другой стороны, по ГОСТ 34.601-90 приемочные испытания являются завершающей стадией разработки, после которой осуществляется только ввод информационной системы в постоянную эксплуатацию.

Отсутствие должного методического обеспечения проведения аттестации выражается в следующем:

– отсутствие типовых методик проведения аттестации для подсистем защиты информации, относящихся к различным классам по СТБ 34.101.30;

– нет документов, содержащих требования (рекомендации) по формированию перечня практических проверок на объектах системы и к используемым для этих целей инструментальным средствам;

– документально не определена легитимность использования средств защиты, срок действия сертификатов соответствия на которые истек, хотя они были закуплены и внедрены в период действия указанных сертификатов.

Особую озабоченность вызывает то, что действующее положение о порядке аттестации систем защиты информации ориентировано на узкий класс информационных систем и не учитывает особенности распределенных межведомственных информационных систем, насчитывающих сотни или тысячи относящихся к различным ведомствам абонентов. Эти системы имеют следующие особенности:

– различные по перечню, уровню и детализации требования к защите информации в ведомственных сегментах системы (даже по отношению к одинаковой информации);

– различные по условиям размещения технических средств и по наличию подготовленного персонала условия эксплуатации на объектах системы;

– использование действующей технической инфраструктуры (комплексы средств автоматизации, ЛВС и ведомственные системы связи) для нужд внедряемой информационной системы.

Проведение аттестации таких систем строго по действующему положению потребует огромных финансовых затрат, значительно превышающих затраты на создание самой системы, и растянется на неопределенный срок.

Приведенные выше обстоятельства требуют безотлагательного пересмотра и совершенствования как «Положения о порядке защиты информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено», так и «Положения о порядке аттестации систем защиты информации».

В первом документе предлагается более подробно изложить:

– состав и содержание работ (с перечнем документов, утверждаемых по их окончании) по разработке и оценке подсистем защиты информации;

– права, обязанности и ответственность заказчика разработки (модернизации) информационной системы, владельцев используемых системой информационных ресурсов, разработчика системы и специализированных организаций (испытательных лабораторий, организаций, проводящих работы по аттестации).

Во втором документе целесообразно учесть указанные выше особенности распределенных межведомственных информационных систем.

Для методического обеспечения проведения аттестации систем защиты информации целесообразно разработать СТБ П «Правила проведения аттестации систем защиты информации государственных информационных систем», содержащего правила принятия решении по оценке достаточности применяемых средств и организационных мер защиты в информационных системах, относящихся к различным классам по СТБ 34.101.30.

П.А.ОРЛОВ, Н.В.РУЧАНОВА

СИТУАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Принятие эффективных управленческих решений, оперативность и качество их реализации напрямую зависят от возможностей информационно-аналитического обеспечения лиц, принимающих такие решения. Появление в мире новых рисков, вызовов и угроз, обострение глобальных проблем человечества, несовершенство существующей архитектуры безопасности с одной стороны, и экспоненциально возрастающие объемы информационных потоков с другой, требуют новых подходов к созданию информационно-аналитических систем для органов государственного управления.

Основные приоритеты в области обеспечения безопасности и устойчивого развития утверждены в Концепции национальной безопасности Беларуси, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 года №575. В Концепции впервые описана совокупность официальных взглядов на сущность и содержание деятельности Республики Беларусь по обеспечению баланса интересов личности, общества, государства и их защите от внутренних и внешних угроз.

Документ дает четкое представление о количестве и сложности взаимосвязей внутренних и внешних угроз, подлежащих учету и мониторингу в целях обеспечения политической, экономической, научно-технологической, социальной, демографической, информационной, военной, экологической и, как совокупности перечисленных: национальной безопасности белорусского государства и защиты стратегических национальных интересов (Рис. 1).

Рисунок 1. Национальные стратегические интересы Республики Беларусь и угрозы национальной безопасности

Одной из основных задач обеспечения национальной безопасности выступает создание системы обеспечения национальной безопасности и организация ее эффективного функционирования.

Организационный и материально-технический потенциал сил обеспечения национальной безопасности совместно с развитыми оперативными информационно-аналитическими ресурсами должен решать задачи как оперативного, так и стратегического управления, а именно:

– сбор, обработку и анализ информации (мониторинг) о развитии ситуации (обстановки) в соответствующих сферах обеспечения национальной безопасности;

– оценка ситуации, выявление узлов возникновения внутренних и внешних угроз;

– формализация признаков угрозы национальной безопасности;

– оценка степени влияния потенциальных внешних и внутренних угроз на национальную безопасность (моделирование влияния возможных угроз);

– прогнозирование развития событий и возможных негативных последствий (при невмешательстве или различных степенях участия);

– выработку предложений по совершенствованию оперативного реагирования на вызовы и угрозы национальной безопасности.

Мониторинг индикаторов состояния национальной безопасности потребует агрегации информации из разнородных информационных источников, которые необходимо структурировать и анализировать. Важнейшим инструментом, обеспечивающим интеграцию и эффективное использование организационного потенциала, являются система ситуационно-аналитических центров органов государственного управления (САЦ). Основное назначение САЦ – это обеспечение эффективной консолидации, целенаправленное использование и применение современных методов обработки информации, как для оперативного управления и мониторинга, так и для решения задач долгосрочного планирования, моделирования и анализа глобальных факторов и показателей развития Республики Беларусь.

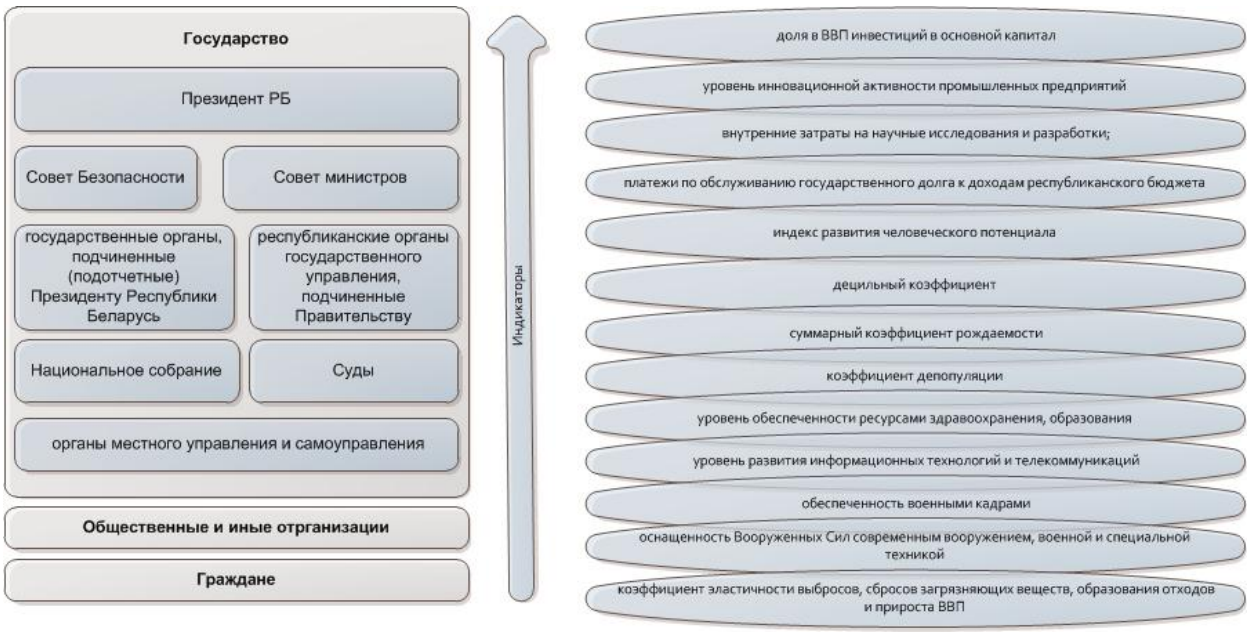


Рисунок 2. Система обеспечения национальной безопасности и показатели состояния национальной безопасности

Создание САЦ предполагает разработку специализированного программного обеспечения и наличие соответствующего технического оборудования. Одним из возможных архитектурных подходов может являться построение программной составляющей САЦ на базе типовых решений «ПРОГНОЗ».

Внедрение решений «ПРОГНОЗ» при создании ситуационно-аналитического центра позволяет решить следующие задачи:

– создание единой схемы информационного взаимодействия для эффективного принятия управленческих решений на основании анализа информационных потоков и интеграции информационных ресурсов;

– объединение источников информации в единое хранилище данных с унифицированным алгоритмом доступа к данным и обработки информации;

– обеспечение регулярного и бесперебойного сбора и аккумулирования оперативных данных на основе интеграции различных информационных систем, их обработку и наглядное представление для поддержки принятия своевременных и обоснованных управленческих решений;

– автоматизация процесса проведения аналитической работы: сбор информации, выделение предметной области анализа, анализ информации с применением современных технологий выделения знания, поддержка принятия решения:

– обеспечение интуитивно-понятного отображения наиболее важной информации для оперативного принятия решений в кризисных ситуациях (визуализация графов связей субъектов, отображение информации на картах, диаграммы, графики, аналитические справки, оперативная отчетность, регламентная отчетность и т.д.);

– оценка текущей ситуационной картины, прогноз развития ситуаций и событий на основе моделирования по комплексу разнородных данных (сценарное моделирование, имитационное моделирование, вычисление тренда, экономическое моделирование и т.д.);

– использование экспертных суждений и критериев для автоматизированного анализа слабо-структурируемой информации в ходе решения управленческих задач, связанных с необходимостью выбора оптимального варианта при наличии нескольких альтернатив.

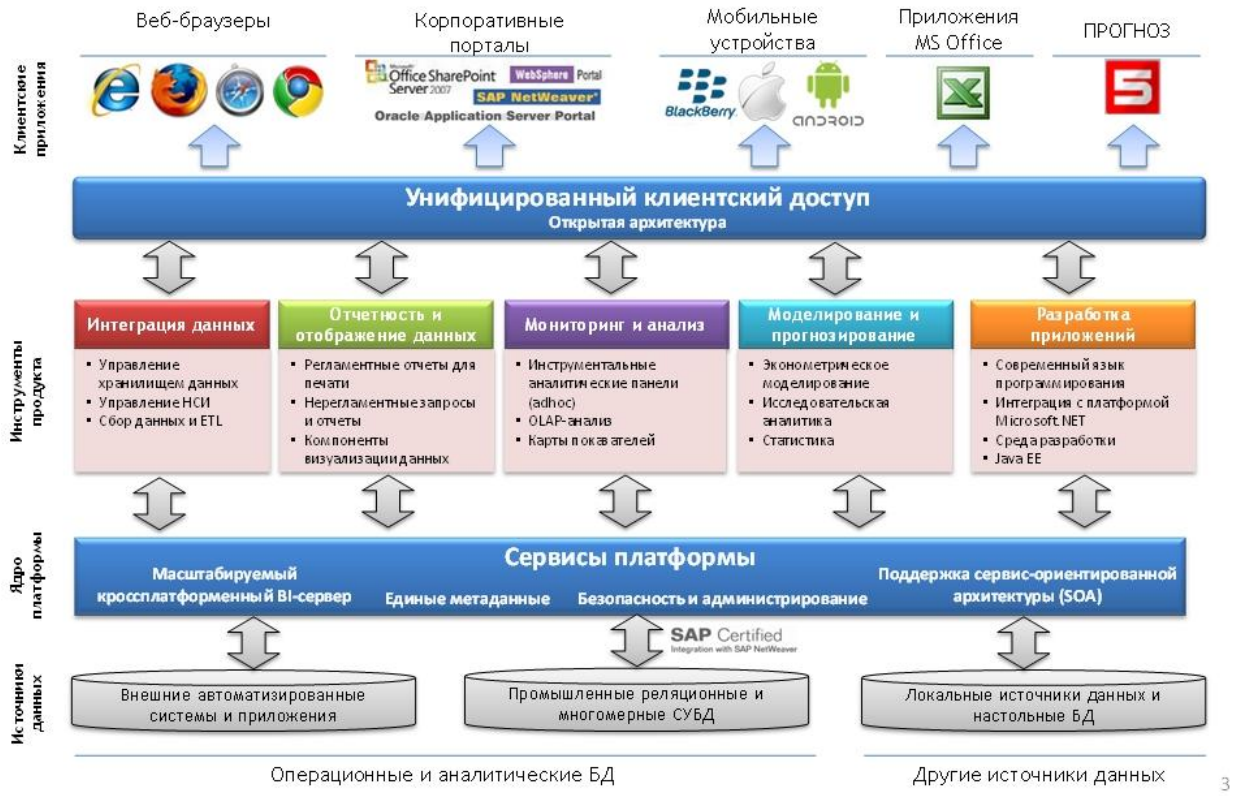


Рисунок 3. Модульная структура аналитического комплекса "ПРОГНОЗ"

САЦ, построенный на безе решений «ПРОГНОЗ» позволит производить эффективное моделирование, прогнозирование развития ситуации и динамично подготавливать материалы для принятия управленческих решений на нескольких уровнях: руководители, аналитики, эксперты.

Применение мобильных решений, интегрированных с информационной системой САЦ, позволит руководителям высшего уровня иметь в личной распоряжении информационно-аналитический инструмент в любой момент времени в любой географической точке.

Е.О.ТИТОВА

«ЗОЛОТОЕ ПРАВИЛО» НАКОПЛЕНИЯ ДЛЯ СЛУЧАЯ ДОГОНЯЮЩЕГО ТИПА РОСТА НОВОЙ ЭКОНОМИКИ В УСЛОВИЯХ ИНТЕГРАЦИИ И ЕГО ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Краеугольным камнем системы государственного регулирования экономики является определение оптимальных темпов экономического роста. Для своего решения эта задача требует нахождения оптимальной нормы накопления. Для Союзного государства важнейшими задачами являются: ликвидировать научно-техническое отставание, приблизить уровень и качество жизни к стандартам высокоразвитых стран, перейти на новое качество экономического роста, построить информационное общество.

«Догоняющий» тип экономического роста – это такое развитие, когда выбираются ключевые показатели, которых надо достичь в сопоставлении со странами-эталонами. Для их достижения выстраиваются прочие целевые показатели и вся система госрегулирования экономики в целом. «Догоняющий» тип экономического роста известен в литературе, как неравномерный, искусственно ускоренный, чрезмерно зарегулированный, применяющий агрессивные экспортные стратегии и методы привлечения инвестиций, но быстро переходящий в либеральную модель развития по мере достижения экономических и других успехов.

Современные макроэкономические модели почти исключительно выстроены под лидирующий тип роста, и странам с «догоняющим» типом приходится подстраивать их под свою специфику, постоянно сталкиваясь с разными несоответствиями. Недостатком современных макроэкономических моделей является и то, что они не позволяют отслеживать переход к новому качеству экономического роста, которое можно кратко охарактеризовать как информационно-инновационно-экологическое. Так, в модели В.Леонтьева затраты на экологические работы показываются с отрицательным знаком, как уменьшение ВВП. Классические модели не позволяют отделить «просто» капиталовложения от инвестиций в инновации, а их экономический смысл резко различается.

Существуют многосекторные модификации моделей экономического роста, однако они не позволяют отследить влияние сектора науки и инноваций на макроэкономическую динамику и оптимизировать пропорции накопления по секторам, особенно в секторе науки. Упрощенно рассматриваются проблемы расходов бюджета и вообще не затрагиваются проблемы экономической безопасности.

Преимущества интеграции в современных моделях роста вообще не учитываются, они изучаются в моделях внешнеэкономической деятельности, а он с каждым годом проявляется все больше. И, наконец, традиционные модели накопления и роста почти не уделяют внимания максимизации некоторых критериальных показателей и вариантности расчетов, поскольку в период их разработки этого не позволяла техническая база тогдашних ЭВМ. В результате решение сводится к тривиальным констатациям, что оптимальная пропорция накопления равна соотношению производительности капитала в разных секторах, и что точку экстремума, или максимального темпа экономического роста, можно найти путем дифференцирования некоторой функции. Однако оптимум находится в другой точке, если в качестве критерия выбрана цель «догнать в кратчайшие сроки».

Таким образом, накопилась «критическая масса» недостатков, которая требует коренного пересмотра самой постановки проблемы оптимальной пропорции накопления и максимального темпа экономического роста.

Совмещение классической модели экономического роста с его «догоняющей» разновидностью, притом в условиях интеграции и создания новой экономики, представляет собой новую постановку задачи, требующую для своего решения не только принципиально новых теоретических подходов, но и более мощных вычислительных средств, чем те, которые традиционно используются для расчета темпов экономического роста. Поэтому построение модели «догоняющего» роста новой экономики в условиях интеграции представляет собой актуальную научно-практическую задачу.

Изучение модели «чистого» накопления, без ограничений по равновесию, трудовым ресурсам и прибыльности, показывает, что пропорция накопления, дающая максимальный темп экономического роста, зависит только от выбранного горизонта планирования, а не от производительности факторов. Поведение максимума функции опровергает еще одно утверждение классиков: о том, что оптимальный темп накопления представляет собой стационарную траекторию. На самом деле задача динамического программирования, которая позволяет выйти на экстремум, дает результаты, большие, чем решение в стационарных стратегиях, однако требует огромных вычислительных мощностей. Требуется перебрать факториальное число вариантов.

Модель «золотого правила» накопления Р.Солоу сформулирована таким образом, чтобы обеспечить равновесие, или равенство спроса и предложения на всех видах рынков. На самом деле, чем выше темпы, тем больше факторов нестабильности экономики. Поэтому требования стабильности играют в теории экономической динамики роль тормоза. Ограничения, принятые Робертом Солоу, вполне оправданны для экономики, которая обладает всеми признаками «лидирующего» типа экономического роста. Однако для «догоняющих» экономик эти допущения должны быть заменены другими.

После установления самых общих, «чистых» свойств «золотого правила», устраним нереальные допущения, принятые в простейшей модели. Для этого придется ввести в модель динамику основных производственных фондов, рабочей силы, сектор безопасности, науки и др. Главное же, вместо склонности к потреблению и к сбережению придется ввести параметры деления первого подразделения на производство средств производства для нескольких секторов, и только после этого искать максимум темпов экономического роста.

Данная модель имеет целью служить исходным пунктом для построения многоотраслевой динамической модели оптимизации пропорций накопления и темпов экономического роста в условиях новой экономики «догоняющего» типа. Такая, практически значимая модель потребует расчета колоссального множества вариантов, но позволит оптимизировать затраты на высокие устойчивые темпы экономического роста и ликвидации технической отсталости.

Для практического создания такой модели потребуется вычислительная мощность, способная производить операции не просто с большим количеством переменных, а со всеми возможными сочетаниями возможных политик накопления для всех секторов. Перед системой защиты информации станет комплексная задача обеспечения бесперебойных поставок данных на сервер, хранения информации во время проведения вариантных расчетов, обеспечения безопасного обращения к программному обеспечению модели и, по мере необходимости, периодического обновления программного обеспечения.

Нужна ли нам интеграция? Есть ли методика расчета экономической эффективности расходов на информатизацию системы государственного регулирования экономики Союзного государства? Можно изучить два варианта оптимального накопления и максимального темпа роста. Первый – раздельно для Беларуси и для России. Второй – вместе для двух стран, как если бы были полностью сняты все барьеры для свободного передвижения людей, идей, товаров и капиталов, и существовала объединенная система

государственного регулирования экономики Союзного государства, пользующаяся одними и теми же вычислительными мощностями, программным обеспечением и статистическими данными для решения крупных общих задач. Как показывают расчеты, второй максимум значительно больше первого, и это – показатель того, насколько эффективна, с точки зрения прироста ВВП, интеграция систем государственного регулирования экономики Беларуси и России.

А.А.ТЕПЛЯКОВ, А.В.ОРЛОВ

ПОДХОД К ВЫДЕЛЕНИЮ И ИДЕНТИФИКАЦИИ УГРОЗ

Наряду с определением ценности информационных ресурсов и их уязвимости, выявление угроз является составляющей процесса определения рисков и последующей выработки мер системы защиты информации.

Упрощенная (относительно приведенной в СТБ 34.101.1–2004) схема построения систем защиты информации приведена на Рис. 1.

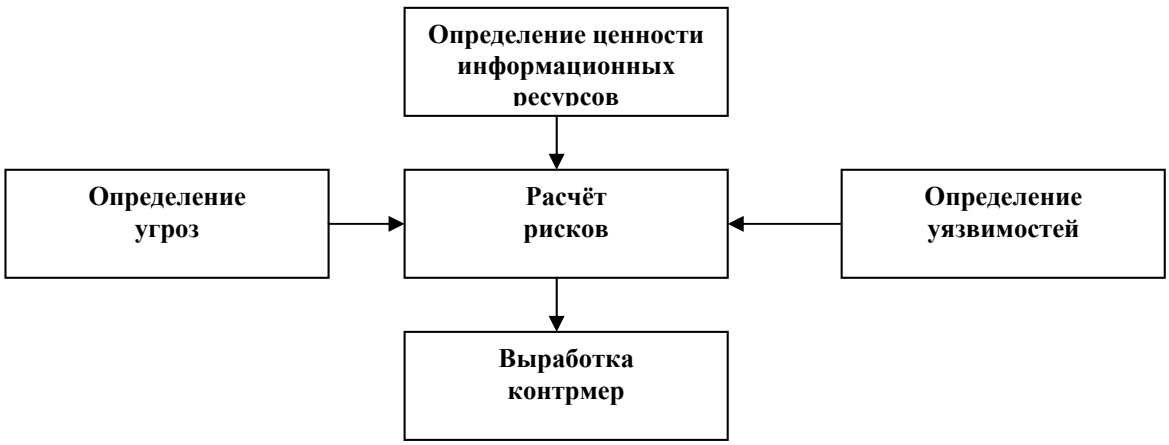


Рис. 1

Под угрозой, в частности [1], понимается «потенциальная причина инцидента, который может нанести ущерб системе или организации». Как следует из определения, угрозу представляют только те «причины» (а реально – действия), которые способны нанести ущерб. В свою очередь, проявление подобного рода действий только потенциально возможно, но не предопределено. Другими словами, угрозы необходимо идентифицировать, а их возможное появление – отслеживать.

Для идентификации угроз [2], они должны быть описаны в понятиях: источник угроз (нарушитель), атака и актив, который подвергается атакам. В свою очередь, «источники угроз» описывается в понятиях: квалификация, используемый ресурс и мотивация, а «атаки» – в понятиях: методы атак, используемые уязвимые места и возможности для атаки.

Как известно, идентификация напрямую связана с классификацией, предусматривающей деление объема понятия по признакам, отмеченным в содержании понятия. Угрозы принято делить на внешние и внутренние, реальные и потенциальные, в зависимости от величины возможного ущерба и т.д. На практике может быть использован любой вариант деления, так как всякая классификация предопределена тем кругом задач или тем набором целей, которые в настоящий момент существуют и требуют решения.

В свою очередь, раскрывая содержание данного выше определения угроз, их можно рассматривать, как составляющую степени ценности информационного ресурса для его

собственника и предпринимаемых кем-то действий, связанных с попыткой завладеть (уничтожение, искажение тоже связано с владением, пусть и временным) этим ресурсом или его частью.

То есть, классификацию имеет смысл проводить по двум признакам: во-первых, с точки зрения значимости для удовлетворения информационных потребностей для достижения целеполагания в самой организации; во-вторых, с точки зрения потенциального интереса к ней со стороны сторонних потребителей.

Предлагаемый подход к классификации, кроме того, напрямую связывает приведенные выше, определяемые в [2], действия по идентификации угроз.

Что касается отслеживания угроз, то, по нашему мнению, здесь возможен, в частности, следующий подход. Угроза, как действие (а чаще – последовательность действий - атака) имеет ряд неустранимых элементов. К ним относятся: цель; объект; субъект; время; место и результат. Ряд таких же, обязательных элементов содержит и деятельность: цель; объект; субъект; метод; последовательность действий; используемые средства и результат.

Сведя элементы деятельности и действия в таблицу (Таблица 1), и, заполняя её, например, результатами расследования инцидентов, можно отслеживать и определять степень значимости той или иной угрозы.

Таблица 1

ДС/Д-ть	Цель	Объект	Субъект	Метод	Последовательность ДС	Средства	Результат
Цель							
Объект							
Субъект							
Время							
Место							
Результат							

Такой подход к отслеживанию угроз позволяет также проводить ещё один этап их дифференциации, что, в свою очередь, способствует более обоснованной выработке контрмер [3] и их целенаправленному применению.

Литература

1. ГОСТ Р ИСО/МЭК 13335-1 – 2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

2. СТБ 34.101.1 – 2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт. Минск.

3. Орлов, А.В., Тепляков, А.А. Об одном из аспектов организации защиты информационных ресурсов. Материалы XV Международной конференции 1-4 июня 2010 г., Иркутск. М: 2010, с.149-154.

С.П.ФИЯСЬ

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СВЕТЕ КОНЦЕПЦИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Необходимость активизации процесса поступательного формирования Республики Беларусь как сильного и процветающего государства невозможно рассматривать вне контекста развития новых общемировых тенденций. Уровень развития информационного пространства общества определяющим образом влияет на процесс функционирования государственных институтов, экономику, обороноспособность, во многом определяет вопросы внешней и внутренней политики. Нетрудно сделать вывод о том, что наличие и состояние информационного пространства общества в современных условиях приобретает роль нового государственнообразующего признака. Таким образом, нельзя не согласиться с тем, что обустроенность информационного пространства является необходимым условием и для развития Республики Беларусь. Быстрое совершенствование процессов информатизации, проникновение информации во все сферы жизненно важных интересов личности, общества и государства повлекли помимо несомненных преимуществ появление ряда специфических проблем. Одной из таких проблем стала необходимость обеспечения информационной безопасности.

В утвержденной Указом Президента Республики Беларусь 09.11.2010 №575 Концепции национальной безопасности Республики Беларусь подчеркивается, что Республика Беларусь реализует модель социально ориентированной рыночной экономики, которая доказала свою жизнеспособность. На ее основе достигнуты высокие темпы роста ВВП и уровня жизни белорусского народа, в целом обеспечена экономическая безопасность. Происходящие в настоящее время процессы преобразования в политической жизни и экономике Республики Беларусь оказывают непосредственное влияние на состояние информационной безопасности, и как следствие - на состояние национальной безопасности Республики Беларусь.

Концепция отмечает, что информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств. Усиливается роль и влияние средств массовой информации и глобальных коммуникационных механизмов на экономическую, политическую и социальную ситуацию. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Происходит эволюция информационного противоборства как новой самостоятельной стратегической формы глобальной конкуренции. Распространяется практика целенаправленного информационного давления, наносящего существенный ущерб национальным интересам.

Согласно Концепции национальной безопасности под информационной безопасностью определено состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Основными национальными интересами в информационной сфере являются:

реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;

формирование и поступательное развитие информационного общества;

равноправное участие Республики Беларусь в мировых информационных отношениях;

преобразование информационной индустрии в экспортно-ориентированный сектор экономики;

эффективное информационное обеспечение государственной политики;

обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

Концепцией дается характеристика состояния национальной безопасности в информационной сфере:

Последовательно реализуются демократические принципы свободы слова, права граждан на получение информации и ее использование. Государство создает необходимые условия для развития средств массовой информации и национального сегмента глобальной сети Интернет. Во все сферы жизнедеятельности общества активно внедряются современные информационно-коммуникационные технологии.

Сохраняется отставание от ведущих стран мира по уровню информатизации. В условиях открытости информационного пространства страны и конкуренции со стороны иностранного информационного продукта недостаточными остаются качество и популярность белорусского национального контента.

Важно понять, от кого следует защищаться, кто может являться источником угроз, каковы технические возможности и возможные действия потенциального нарушителя? Используемые злоумышленниками методы и средства проведения атак на информационные системы становятся все более изощренными, и оказать достойный отпор их действиям можно, только обладая специальными знаниями.

В этой связи опыт США, страны с одной из наиболее развитой в мире информационной инфраструктурой представляется весьма интересным и поучительным с точки зрения анализа тенденций, связанных с обеспечением информационной безопасности национальной инфраструктуры.

Уже в феврале 2003 г. был подписан основополагающий документ, который называется «Национальная стратегия. Безопасное киберпространство». Вышеназванный документ призван скоординировать усилия правительства и частного бизнеса по обеспечению информационной безопасности США. В рамках данной стратегии ежегодно составляется план защиты критически важных информационных систем. Национальная стратегия по защите киберпространства нацеливает правительство на сотрудничество с частным сектором в сфере создания системы экстренного реагирования на кибератаки и снижения степени уязвимости государства к таким угрозам.

Классическая модель информационной безопасности основывалась на автономности и локальности ресурсов информационной системы, а ее постановка заключалась, образно говоря, в трех НЕ: не допустить, не пропустить, не упустить. Соответственно и сама концепция защиты информационных ресурсов строилась по этим же принципам, когда главными задачами обеспечения информационной безопасности являлись: ограничение круга пользователей, создание системы доступа по паролям и разграничение информации по категориям.

Зарубежные публикации последних лет показывают, что возможности злоупотреблений информацией, передаваемой по каналам связи, развивались и совершенствовались не менее интенсивно, чем средства их предупреждения. В этом случае для защиты информации требуется не просто разработка частных механизмов защиты, а организация комплекса мер, то есть использование специальных средств, методов и мероприятий с целью предотвращения потери информации.

Мир подошел к той черте, когда границы между государствами перестали быть непреодолимыми барьерами не только для бизнеса и торговли, науки и образования, отдыха и развлечений, но и для терроризма, преступности, в том числе в сфере высоких технологий. Остроту межгосударственного информационного противоборства можно наблюдать в оборонной сфере, высшей формой которой являются информационные войны. Элементы такой войны уже имели место в локальных военных конфликтах на Ближнем Востоке и на Балканах. Так, войскам НАТО удалось вывести из строя систему противовоздушной обороны Ирака с помощью информационного оружия.

Новые условия геополитической обстановки проявляются в нашей стране через такие важные атрибуты как международная экономическая интеграция, свобода перемещения граждан и контактов между ними, свободный поток информации и идей, «открытость» сторон. Наряду с положительными аспектами реализации принципов «открытости», значительное превосходство США и их союзников перед странами СНГ в техническом оснащении спецслужб позволяет им получить уникальные возможности по добыванию разведывательной информации.

О серьезности данной проблемы можно судить по факту того, что лозунгом текущей эпохи всеми признается лозунг «Кто владеет информацией - тот владеет миром». Существование таких структур как АНБ (Агентство национальной безопасности США) и ШПС (Штаб правительственной связи Великобритании) и им подобным является бесспорным доказательством большой заинтересованности в информации других государств и на удовлетворение потребности в ценных сведениях тратятся большие средства.

По данным из открытых источников информации в структуре «АНБ»: в 6 раз больше сотрудников, чем в ЦРУ. Занимается электронной разведкой 4120 мощных центров прослушивания, размещенных на многочисленных военных базах в Германии, Турции, Японии и других странах. Они имеют возможность собирать и анализировать почти повсеместно радиограммы, телефонные переговоры. Могут перехватывать идущие по радиорелейным и спутниковым каналам связи, электронные сигналы любого типа, включая излучения систем сигнализации в квартирах и противоугонных устройств автомобилей.

Известная американская разведывательная система «Эшелон» перехватывает все, что существует в электромагнитном виде и обеспечивает тотальный контроль электронных средств коммуникаций. Создаваемая США система «Magic Lantern» позволяет тайно внедрять в компьютеры подозреваемых программы слежения, засылая их через Интернет при помощи вирусов.

Концепция определяет основные потенциальные либо реально существующие угрозы национальной безопасности в информационной сфере:

деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;

нарушение функционирования критически важных объектов информатизации;

недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;

снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента;

утрата либо разглашение сведений, составляющих охраняемую законодательством тайну и способных причинить ущерб национальной безопасности.

Концепция разделяет источники угроз на внутренние и внешние.

В информационной сфере внутренними источниками угроз национальной безопасности являются:

распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;

зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;

несоответствие качества национального контента мировому уровню;

недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;

рост преступности с использованием информационно-коммуникационных технологий;

недостаточная эффективность информационного обеспечения государственной политики;

несовершенство системы обеспечения безопасности критически важных объектов информатизации.

Внешними источниками угроз в информационной сфере национальной безопасности являются:

открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;

доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;

информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;

нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;

развитие технологий манипулирования информацией;

препятствование распространению национального контента Республики Беларусь за рубежом;

широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;

попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

Основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере.

В информационной сфере с целью нейтрализации **внутренних источников угроз** национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом, важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Нейтрализации ряда внутренних источников угроз национальной безопасности способствует информационное обеспечение государственной политики, которое заключается

в доведении до граждан Республики Беларусь и внешней аудитории объективной информации о государственном курсе во всех сферах жизнедеятельности общества, официальной позиции по общественно значимым событиям внутри страны и за рубежом, о деятельности государственных органов. Составной частью информационного обеспечения государственной политики выступает информационное противоборство, представляющее собой комплексное использование информационных, технических и иных методов, способов и средств для воздействия на информационную сферу с целью достижения политических, экономических и иных задач либо защиты собственного информационного пространства.

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

Важнейшей задачей сегодня является организация скоординированной деятельности республиканских органов государственного управления по обеспечению безопасности информационной среды белорусского общества, разработка стратегии обеспечения информационной безопасности Беларуси

Поэтому важным моментом в организации системы ее эффективной защиты является создание организаций координирования, которые бы состояли как из правительственных, так и общественных организаций, с привлечением коммерческих структур, осуществляющими деятельность в ключевых секторах национальной критической инфраструктуры. Тесная взаимосвязь между государственным и частным сектором страны является неотъемлемым условием национальной безопасности. Это взаимодействие должно подразумевать: исследование проблемы и осведомленность об угрозе национальной критической инфраструктуре; фокусирование внимания спецслужб и производителей программного обеспечения и компьютерной техники на безопасности и защищенности продукции; своевременное и быстрое реагирование на инциденты, связанные с повреждением работы систем; наличие системы каналов формального и неформального обмена информацией об угрозе компьютерной преступности и кибертерроризма.

В.В.ХИЛЮТА

ХИЩЕНИЕ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ В ЗАРУБЕЖНОМ УГОЛОВНОМ ПРАВЕ

Вторая половина XX века с бурным развитием информационных технологий принесла с собой качественный скачек: информация превратилась в один из главных элементов национального богатства. Совершенствование компьютерных технологий все более приближает нас к тому времени, когда значительная доля информационных ресурсов будет содержаться в технических средствах. Пожалуй, сегодня практически нет ни одной сферы человеческой деятельности, в которой бы не использовались компьютеры, позволяющие создавать, накапливать, хранить, обрабатывать и передавать огромные объемы информации. Создание электронно-вычислительной техники большой производительности, ее широкое внедрение в экономическую, социальную и управленческую деятельность, привело к повышению значимости информации и информационных ресурсов.

В то же время, динамичное внедрение новейших электронных систем и коммуникационных средств в различные сферы деятельности современного общества привело не только к развитию положительных тенденций и явлений, но и выявило целый ряд

проблем негативного характера. Всевозможные явления всеобщей криминализации сопровождаются массой негативных тенденций, связанных со злоупотреблениями возможностями компьютерной техники. Новые технологии порождают и новые преступления. Многочисленные факты выявления и установления закономерностей механизмов развития новых видов преступлений, связанных с использованием средств компьютерной техники и информационных технологий, показывают, что сама компьютерная техника может быть как предметом преступного посягательства, так и инструментом совершения преступления.

Условно, подобного рода противоправные деяния можно разбить на несколько групп: а) преступления, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации как таковых (такие действия рассматриваются как посягательства на собственность и квалифицируются по статьям гл. 24 УК РБ); б) преступления, направленные на получение несанкционированного доступа к компьютерной информации, ее модификации, связанные с неправомерным завладением компьютерной информацией, разработкой, использованием либо распространением вредоносных программ и т.д. (такие действия рассматриваются как преступления против информационной безопасности и квалифицируются по статьям гл. 31 УК РБ); в) преступления, в которых компьютеры и другие средства компьютерной техники используются в качестве средства совершения корыстного преступления, и умысел виновного лица направлен на завладение чужим имуществом путем изменения информации либо путем введения в компьютерную систему ложной информации [1]. (такие действия рассматриваются как хищение путем использования компьютерной техники и квалифицируются по ст. 212 УК РБ).

Применительно к последней группе противоправных деяний, в законодательстве ряда зарубежных государств, специально выделяются составы преступлений, охраняющие имущественные отношения от преступных посягательств, совершаемых с использованием компьютера.

Так, уголовное законодательство *США,* посвященное борьбе с компьютерными преступлениями, отличается своеобразием и постоянным обновлением. Основной закон США, касающийся компьютерных преступлений был сформулирован в 1986 г. «О мошенничестве и злоупотреблениях, связанных с компьютерами», а впоследствии состав «мошенничества с использованием компьютеров» вошел в Свод законов США. В параграфе 1030 (а) (4) Свода Законов США мошенничество с использованием компьютера определяется как доступ, осуществляемый с мошенническими намерениями, и использование компьютера с целью получения чего бы то ни было ценного посредством мошенничества, включая незаконное использование машинного времени (т.е. бесплатное использование компьютерных сетей и серверов) стоимостью более 5 тыс. долларов США в течение года, т.е. без оплаты использования компьютерных сетей и серверов [2].

В *Великобритании* ответственность за компьютерные преступления установлена в статутах, принятых Парламентом. К основным актам, устанавливающим ответственность за компьютерные преступления можно отнести: Закон о злоупотреблениях компьютерами 1990 г., Закон о телекоммуникациях (обмане) 1997 г., Закон о защите данных 1998 г., Закон об электронных коммуникациях 2000 г. и др. Однако из перечня основных компьютерных преступлений специально не выделяется состав «компьютерного мошенничества», связанного с посягательством на чужое имущество.

---

[1] Гончаров, Д. Квалификация хищений, совершаемых с помощью компьютеров / Д.Гончаров // Законность. – 2001. – № 11. – С. 31.

[2] См.: Степанов-Егиянц, В. Ответственность за компьютерные преступления / В.Степанов-Егиянц // Законность. – 2005. – № 12. – С. 51.

Среди законодательных актов *Японии,* регулирующих правоотношения в сфере информационных технологий, следует назвать Уголовный кодекс и Закон «О несанкционированном проникновении в компьютерные сети» 2000 г. Согласно ст. 246-2 УК *Японии* за компьютерное мошенничество наказывается «любое лицо, изготавливающее фальшивые электромагнитные записи, свидетельствующие о приобретении, изменении или потере имущественных прав, путем внесения в компьютер, используемый в деловых операциях иным лицом, ложных сведений или команд либо пускающее фальшивые электромагнитные записи в обращение в ходе деловых операций другого лица, и получающее от этого незаконный доход либо способствующее получению незаконного дохода третьим лицом». В соответствии с Законом «О незаконном проникновении в компьютерные сети» особо следует выделить такое правонарушение, как незаконное (несанкционированное) проникновение в компьютерные системы и информационные сети с целью кражи, порчи информации, ее использования с целью извлечения дохода и причинение ущерба законным владельцам сетей, систем и информационных баз данных [1].

Ответственность за компьютерное мошенничество согласно параграфу 263 а УК *ФРГ* подлежит лицо, которое «действуя с намерением получить для себя или третьего лица имущественную выгоду, причиняет вред имуществу другого лица, воздействуя на результат обработки данных путем неправильного создания программ, использования неправильных или неполных данных, путем неправомочного использования данных или иного неправомочного воздействия на процесс обработки данных». В данном случае компьютер используется как орудие совершения преступления, поскольку указанные в § 263 а УК ФРГ формы реализации объективной стороны выступают именно в качестве способов достижения корыстной цели [2]. Таким образом, немецкий законодатель четко разграничил два вида мошенничества: традиционное и компьютерное.

Уголовный кодекс *Франции* включает различные составы большого числа компьютерных преступлений: посягательства на деятельность по обработке данных автоматизированных систем; посягательства, связанные с использованием карточек и обработкой данных на ЭВМ; незаконные действия, совершаемые с компьютерной информацией в ущерб интересам государства и т.д. Однако специально УК Франции не выделяет состав, посвященный охране имущественных отношений, посягательства на которые осуществляются с использованием компьютерной техники [3]. В то же время нормы французского УК защищают сами информационные системы и их программное обеспечение как объекты собственности.

В соответствии со ст. 287 УК *Республики Польша* имущественным преступлением признаются действия лица, которое «с целью получения имущественной выгоды или причинения другому лицу вреда, не имея на то права, влияет на автоматизированное преобразование, собирание или передачу информации или изменяет, удаляет либо вводит новую запись на компьютерный носитель информации» [4]. Под имущественной выгодой в уголовном праве Польши рассматривается выгода, приобретаемая лицом для 1) себя, 2) другого физического или юридического лица, 3) организационной единицы без образования юридического лица, 4) группы лиц, осуществляющей организованную преступную деятельность.

---

[1] Степанов-Егиянц, В. Ответственность за компьютерные преступления / В.Степанов-Егиянц // Законность. – 2005. – № 12. – С. 49–51.

[2] См.: Орловская, Н.А. Зарубежный опыт противодействия компьютерной преступности (проблемы криминализации и наказуемости) / Н.А.Орловская // Сборник научных трудов международной конференции «Информационные технологии и безопасность». Выпуск № 1. – Киев, 2003. – С. 110–118.

[3] См.: Мазуров, В.А. Компьютерные преступления: классификация и способы противодействия / В.А.Мазуров. – М., 2002. – С. 11.

[4] Уголовный кодекс Республики Польша / Под общ. ред. Н.Ф.Кузнецовой. – Минск, 1998. – С. 98.

Согласно ч. 3 ст. 190 УК *Украины* (Мошенничество) в отдельный квалифицирующий признак выделено мошенничество, совершенное путем незаконных операций с использованием электронно-вычислительной техники. В основе данного преступления лежит обман или злоупотребление доверием, при этом указанное квалифицирующее мошенничество обстоятельство образуют лишь операции, осуществление которых без использования электронно-вычислительной техники является невозможным (осуществление электронных платежей, операций с безналичными средствами и т.д.) [1].

В *Российской Федерации* в УК отсутствует специальная норма, предусматривающая ответственность за совершение «компьютерного хищения» и правоприменительная практика исходит из того, что хищения, совершаемые с использованием компьютерной техники в ряде случаев рассматриваются либо как мошенничество, либо как кража по признаку незаконного проникновения в помещение, либо в иное хранилище. Кроме этого такого рода противоправные действия дополнительно влекут уголовную ответственность по ст. 272 УК РФ [2].

Таким образом, можно сказать, что развитие уголовного законодательства ряда государств в обозначенном нами вопросе, происходит в двух направлениях: а) применяется более широкое толкование традиционных норм о преступлениях против собственности и их правоприменение происходит по аналогии применительно к хищениям, совершаемых с помощью компьютеров (Россия, Испания, Латвия); б) применяются специальные нормы о компьютерных хищениях либо выделенные квалифицирующие обстоятельства в общих нормах о преступлениях против собственности (Нидерланды, Узбекистан). Более того, общемировая тенденция свидетельствует также о том, что около 70 % всех преступлений, совершаемых в информационной сфере составляет группа деяний, в которых компьютеры и другие средства электронной техники используются в качестве средства совершения корыстного преступления (хищения) и умысел виновного лица направлен на завладение чужим имуществом путем изменения информации либо путем введения в компьютерную систему ложной информации.

Ю.С.ХАРИН

О РЕЗУЛЬТАТАХ И ПЕРСПЕКТИВНЫХ НАУЧНЫХ НАПРАВЛЕНИЯХ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

XXI век принес человечеству новые направления глобализации, одно из которых порождено стремительным развитием информационных технологий и ведет к созданию и массовому освоению информационного пространства. В современном обществе информация все более становится высокоценным ресурсом либо товаром, который необходимо тщательно защищать при хранении, обработке и передаче.

Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую

---

[1] См.: Научно-практический комментарий Уголовного кодекса Украины от 5 апреля 2001 года / Под ред. Н.И.Мельника, Н.И.Хавронюка. – Киев, 2002. – С. 516.

[2] См.: Бражник, С.Д. Проблемы совершенствования норм об ответственности за преступления, связанные с компьютерной техникой / С.Д.Бражник // Налоговые и иные экономические преступления: Сб. науч. статей. Вып. 2, Ярославль, 2000. – С. 80; Клепицкий, И. Мошенничество и правонарушения гражданско-правового характера / И.Клепицкий // Законность. – 1995. – № 7. – С. 42; Борунов, О.Е. Проблемы квалификации хищения денежных средств со счетов банка с использованием средств компьютерной техники / О.Е.Борунов // Российский судья. – 2004. – № 6. – С. 28; Гончаров, Д. Квалификация хищений, совершаемых с помощью компьютеров / Д.Гончаров // Законность. – 2001. – № 11. – С. 32.

информацию. На современном уровне развития науки и техники защита информации осуществляется четырьмя способами: криптографическая защита информации (КЗИ); защита от побочных электромагнитных излучений и наводок (ПЭМИН); защита от несанкционированного доступа (НСД); организационно-правовые методы.

Основным способом, обеспечивающим гарантированную надежность, является криптографический способ [1, 2]. Он базируется на новой науке – криптологии, объединяющей криптографию и криптоанализ.

Второй способ защиты информации включает комплекс методов подавления побочных электромагнитных излучений и наводок, неизбежно порождаемых узлами компьютеров, мониторами, любыми электронными устройствами, кабелями и т.д.

Третий способ защиты информации основывается на использовании паролей, смарт-карт, е-токенов и более сложных методов для защиты компьютеров и компьютерных сетей от проникновения несанкционированного пользователя.

Четвертый способ – организационно-правовая защита информации обеспечивается нормативно-законодательными актами, представляющими собой иерархическую систему от Конституции РБ до функциональных обязанностей и контракта отдельного конкретного исполнителя, определяющих перечень сведений, подлежащих охране, и меры ответственности за их разглашение.

В настоящее время в мировом сообществе защита информации является самостоятельной научно-технической отраслью: имеются научно-исследовательские институты, центры и лаборатории, занимающиеся разработкой моделей, методов и алгоритмов защиты информации; функционируют десятки тысяч фирм, компаний, производящих программные и аппаратные средства и системы защиты информации [1, 2]. В Республике Беларусь отдельные задачи разработки методов, алгоритмов и программных средств защиты информации решались в Белгосуниверситете с 1976 г., однако интенсивные работы развернулись лишь с 1995 г., когда был создан Государственный центр безопасности информации при Президенте Республики Беларусь и сформирована ГНТП «Защита информации». Значимым событием явилось создание в 2000 г. по Постановлению Совета Министров Республики Беларусь учреждения БГУ «Национальный научно-исследовательский центр прикладных проблем математики и информатики» для координации НИОКР в области криптографической защиты информации, преобразованного в 2008 г. в НИИ прикладных проблем математики и информатики (НИИ ППМИ).

Достижения и перспективные научные направления в области КЗИ

Развитие криптологии стимулирует развитие математики и информатики. Имея это в виду, ректор МГУ академик В.А. Садовничий отметил, что «криптология все более становится источником развития математики и информатики на современном этапе».

I. Построение (генерация) случайных и псевдослучайных последовательностей и их вероятностно-статистический анализ (тестирование). Генераторы случайных и псевдослучайных последовательностей (ПСП) – неотъемлемые элементы современных средств криптографической защиты информации. Составная часть проблемы генерации РРСП - оценка «качества генерируемой последовательности». Для этого используются семейства статистических тестов, называемые «батареями тестов». В настоящее время известны «батарея тестов Д. Кнута», «батарея тестов Дж. Марсальи», «батарея тестов Национального института стандартов США» и некоторые другие. Недостатки существующих «батарей тестов»: 1) многие известные тесты проверяют лишь одно из вероятностных свойств, характеризующих случайную последовательность; 2) многие из известных тестов построены «эвристически» и не фиксируют семейство альтернатив H_1; 3) многие тесты не имеют оценок мощности; 4) при включении нескольких тестов в батарею не удается оптимизировать «составной» тест.

Актуальной проблемой является разработка адекватных моделей для описания отклонений H_1 от модели РРСП и построение методов и алгоритмов для обнаружения оценивания таких отклонений. В связи с этим в Белгосуниверситете разрабатывается теория статистического анализа случайных последовательностей с конечным пространством состояний, дискретным временем и «длинной» памятью . В рамках этой теории наряду с известными моделями (цепь Маркова порядка *s*, дискретная авторегрессия DAR(*s*) порядка *s* над полем GF(p), MTD – модель Рафтери, цепь Маркова переменного порядка) разработаны и используются новые модели (цепь Маркова *s*-го порядка с *r* частичными связями ЦМ(*s*,*r*) [3, 4], INAR – временные ряды).

Разработаны также методы статистического тестирования генераторов на основе теории множественной проверки гипотез [5].

II. Разработка национального криптоалгоритма и «линейки» криптографических примитивов.

Нелинейность криптографических преобразований обеспечивают так называемые S-блоки (блоки подстановки, узлы замены) $f(\cdot): V_n \to V_n$, где V_n – *n*-мерное векторное пространство над полем Галуа $\mathrm{F}_2 = \{0,1\}$, которые отвечают за нелинейную зависимость между прообразами и ключами криптопреобразований. Для эффективного построения S-блоков развита теория бент-функций и разработан метод построения экспоненциальных S-блоков. На базе этих результатов разработан национальный блочный криптографический алгоритм BelT [6]. Спецификации криптосистемы BelT, а также алгоритмов шифрования, выработки имитовставки и хэширования на ее основе оформлены в виде стандарта Республики Беларусь «Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности», который вступает в действие в 2011 г.

III. Методы стеганографии. Стеганография (от греч. steganos – прикрытый) – новое направление криптологии, имеющее целью сокрытие (hiding) сообщения в потоке передаваемой информации [1,2]. Стеганография применяется для скрытой маркировки цифровых данных с помощью «цифровых водяных знаков» (watermaking) с целью защиты электронных произведений (книг, музыки, видео) от пиратского копирования. Стеганография требует развития разделов математики, связанных с вэйвлетами, случайными полями, случайными множествами [7].

IV. Методы разделения секрета («secret sharing»). При создании Инфраструктуры Открытых Ключей, решении задач обеспечения сетевой безопасности часто возникает следующая задача разделения секрета . Пусть имеется некоторый «секрет», представимый двоичным вектором $s \in V_n$. Надо разделить этот секрет между *n* участниками так, чтобы восстановить этот секрет могли лишь *k* или более участников, собрав свои «частичные секреты» ($k<n$). В [8] предложен новый метод решения обобщенной задачи разделения секрета в кольце многочленов над конечным полем F_q.

V. Разработка стандартов в области КЗИ. Важнейшей проблемой внедрения информационных технологий защиты информации в электронном документообороте Республики Беларусь является согласованность (стандартизация) используемых средств криптографической защиты информации и правил (протоколов) их использования. В связи с достаточно высокой наукоемкостью стандартов в этой области, их разработка невозможна без привлечения ученых в области криптологии. В НИИ ППМИ разработаны следующие нормативные документы:

– СТБ П 34.101-27 «Информационные технологии и безопасность. Профиль защиты программных средств криптографической защиты информации»;

– СТБ П 34.101-31 «Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности»;

– РД РБ «Банковские технологии. Общие требования к средствам электронной цифровой подписи»;

– РД РБ «Банковские технологии. Процедура выработки псевдослучайных данных с использованием секретного параметра».

VI. Система сертификационных испытаний. Важнейшей проблемой внедрения информационных технологий защиты информации является организация сертификационных испытаний средств КЗИ. На базе НИИ ППМИ с 2001 года функционирует Испытательная лаборатория для выполнения следующих работ:

1) проведение сертификационных испытаний средств КЗИ на соответствие требованиям действующих в Республике Беларусь стандартов СТБ 1176.2 на процедуры выработки и проверки электронной цифровой подписи, СТБ 1176.1 на функцию хэширования, ГОСТ 28147 на алгоритм шифрования;

2) проведение отдельных экспертиз средств КЗИ.

С 2001 г. проведено более 50 испытаний программных и аппаратно-программных средств КЗИ по заказу банковских организаций, государственных предприятий, фирм.

Перечислим кратко еще ряд перспективных направлений научных исследований в области КЗИ.

VII. Разработка стойких функций хэширования.

VIII. Разработка систем электронной цифровой подписи.

IX. Разработка криптосистем с открытым ключом.

X. Разработка «систем доказательства с нулевым знанием».

Перспективные научные направления в области защиты информации от ПЭМИН

Несмотря на то, что защита от ПЭМИН традиционно относится к так называемой технической защите информации, в этом направлении возникает множество задач, требующих применения современных методов математической физики, математического моделирования, теории электромагнитных полей . Отметим следующие актуальные задачи [9].

I. Разработка математических моделей электромагнитных полей, порождаемых электронными устройствами.

II. Разработка методов расчета электромагнитных экранов.

Перспективные научные направления в области защиты от НСД

В области защиты от НСД выделяются два уровня: локальный и сетевой. Перечислим основные научные проблемы, имея в виду оба этих уровня.

I. Разработка методов биометрической аутентификации пользователя.

II. Разработка методов разграничения доступа к объектам ОС.

III. Разработка методов обеспечения безопасности в корпоративных информационных сетях.

IV. Разработка методов построения межсетевых экранов.

V. Разработка протоколов защищенных каналов, включая защиту беспроводных сетей.

VI. Разработка методов защиты от вредоносных программ и спама.

VII. Разработка методов обнаружения, распознавания и предотвращения вторжений.

Достижения и проблемы подготовки кадров и повышения квалификации в области защиты информации

Как всякое новое направление науки и техники, защита информации требует подготовки соответствующих кадров. В связи с этим, в Республике Беларусь открыты следующие специальности и специализации (уровни «Специалист» и «Магистр»):

– математическое и программное обеспечение криптографии и анализа данных (БГУ);

– компьютерная безопасность (БГУ, ГрГУ, ПГУ);

– защита информации в телекоммуникационных системах (БГУИР).

С 2000 г. действует ВАК-овская специальность:

05.13.19 – Методы защиты информации, информационная безопасность (физ.-мат., техн. науки).

По Постановлению Совмина РБ в 2005 г. на базе БГУ создана Республиканская система повышения квалификации и переподготовки кадров в области информационной безопасности.

Литература

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос-АРВ, 2001, 478 с.

2. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. – М.: Новое знание, 2003, 383 с.

3. Харин Ю.С. Цепи Маркова с r-частичными связями и их ста-тистическое оценивание. – Докл.НАН Беларуси, 2004, т. 48, № 1, с. 40-44.

4. Харин Ю.С., Петлицкий А.И. Цепь Маркова s-порядка с r-частичными связями и статистические выводы о ее параметрах. – Дискретная математика, 2007, т. 12, вып. 2, с. 109-130.

5. Костевич А.Л., Никитина И.С. Уточнение процедуры Бонферрони множественной проверки гипотез. – Обозрение прикладной и промышленной математики, 2009, т. 16, вып. 3, ст. 436-448.

6. Агиевич С.В., Галинский В.А., Микулич Н.Д., Харин Ю.С. Об одном алгоритме блочного шифрования. – Управление защитой информации, т.6, № 4, 2002, с.407-412.

7. Харин Ю.С., Абрамович М.С. Стеганографические методы защиты информации: обзор. – Упр. защитой информации, т. 13, № 1, 2009, с.58-66.

8. Galibus T., Matveev G., Shenets N. Some structural and security properties of the modular secret sharing. – SYNASC′08, IEEE Comp. Soc. Press: CPS, California, 2009, p. 197-200.

9. Ерофеенко В.Т., Пулко Ю.В. Расчет защитных электромагнитных экранов с поверхностными токами: Комплексная защита информации. – Мн.: НИИ ТЗИ, 2009 – с. 90-91.

В.Б.ЩЕРБАКОВ, Ю.К.ЯЗОВ, С.А.ГОЛОВИН

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ ВТОРОЙ СОВМЕСТНОЙ ПРОГРАММЫ "ЗАЩИТА ОБЩИХ ИНФОРМАЦИОННЫХ РЕСУРСОВ БЕЛАРУСИ И РОССИИ" И НАПРАВЛЕНИЯ ДАЛЬНЕЙШИХ РАБОТ

Завершена вторая программа Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006-2010 годы» (далее – Программа), которая выполнялась в соответствии с постановлением Совета Министров Союзного государства от 26 сентября 2006 г. № 32.

Государственным заказчиком – координатором Программы являлась Федеральная служба по техническому и экспортному контролю (ФСТЭК России), кроме того, государственным заказчиком от Российской Федерации была Федеральная служба безопасности Российской Федерации (ФСБ России).

Головным исполнителем Программы со стороны России было Федеральное государственное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ГНИИИ ПТЗИ ФСТЭК России), а исполнителями - 15 организаций.

Выполнение Программы как комплекса научно-исследовательских и опытно-конструкторский работ стало логичным продолжением исследований по первой Программе, которая была завершена в 2004 г. В отличие от первой программы здесь усилия были сосредоточены на создании нормативно-методических и научно-технических условий для эффективного обеспечения безопасности информации на действующих и разрабатываемых критически важных объектах информационно-телекоммуникационной инфраструктуры Союзного государства. Вместе с тем были продолжены работы, направленные и на формирование и совершенствование системы защиты совместных информационных ресурсов и развитие эффективных высокотехнологичных методов и средств защиты информации.

Основными целями Программы являлись:

1. Создание нормативно-методических и научно-технических условий для формирования и совершенствования системы защиты совместных информационных ресурсов и информационно-телекоммуникационной инфраструктуры Союзного государства от информационных угроз.
2. Создание нормативно-методических и научно-технических условий для эффективного обеспечения безопасности информации на действующих и разрабатываемых критически важных объектах информационно-телекоммуникационной инфраструктуры Союзного государства.
3. Создание условий для развития эффективных высокотехнологичных методов и средств защиты совместных информационных ресурсов и информационно-телекоммуникационной инфраструктуры Союзного государства.

В ходе выполнения Программы решались задачи, в первую очередь, по разработке системы руководящих документов, регламентирующих деятельность по обеспечению безопасности информации на критически важных объектах информационно-телекоммуникационной инфраструктуры Союзного государства и контроля эффективности этих мероприятий, а также по разработке информационно-технических систем такого контроля. Наряду с этим в развитие первой Программы решались задачи совершенствования системы нормативных и методических документов по обеспечению защиты совместных информационных ресурсов от информационных угроз, а также по разработке перспективных технологий защиты совместных информационных ресурсов Союзного государства от утечки по техническим каналам и от несанкционированного доступа.

Для выполнения поставленных задач было организовано выполнение 46 научно-исследовательских и опытно-конструкторских работ (НИОКР), из них российской стороной - 30 НИОКР.

В результате выполнения указанных работ получены результаты, которые связаны как с разработкой целого ряда новых концептуальных, нормативных, методических и информационных документов, так и созданием новых технических решений.

В части, касающейся документов, следует подчеркнуть, что в рамках первой и второй Программы было подготовлено около ста документов по обеспечению деятельности в области защиты информации, а в ходе выполнения завершившейся второй Программы - 42 таких документа, в том числе:

1. Документы, касающиеся ведения данных о совместных информационных ресурсах, такие как:

– Классификатор государственных информационных систем и критически важных систем информационно-телекоммуникационной инфраструктуры (КВСИИ) Союзного государства;

– Перечень государственных информационных систем Союзного государства;

– Перечень существующих и перспективных критически важных систем информационной инфраструктуры Союзного государства.

2. Концептуальные документы, определяющие развитие системы взглядов в области защиты информации и, особенно, в части, касающейся обеспечения безопасности информации в КВСИИ Союзного государства, такие как:

– Концепция организации работ по ОБИ в КВСИИ Союзного государства;

– Основы межгосударственного нормативного регулирования ОБИ в КВСИИ Союзного государства;

– Концепция осуществления совместного контроля состояния ОБИ в КВСИИ Союзного государства.

3. Документы, определяющие нормы и требования по выполнению отдельных работ, а также методы и методики контроля их выполнения, такие как:

– Сборник нормативных и методических документов по сертификационным испытаниям по требованиям безопасности информации средств вычислительной техники (СВТ), подключаемых к информационным сетям общего пользования (СОП), и используемых при этом технических средств защиты конфиденциальной информации от утечки за счет побочных электромагнитных излучений и наводок;

– Руководство по организации и проведению работ по ОБИ и контролю на объектах КВСИИ Союзного государства;

– Положение по проведению межгосударственных экспертиз безопасности информации в КВСИИ Союзного государства;

– Положение по защите навигационной информации в критически важных системах информационной инфраструктуры Союзного государства;

– Методика аттестации объектов информатизации Союзного государства по требованиям безопасности информации при наличии в их составе СВТ, подключаемых к СОП;

– Рекомендации по защите речевой информации от утечки за счет побочных электромагнитных излучений средств вычислительной техники в диапазоне 10 кГц – 1,8 ГГц, а также за счет высокочастотного облучения по электромагнитному полю;

– Методические рекомендации по выявлению угроз деструктивных информационных воздействий на информацию в критически важных системах информационно-телекоммуникационной инфраструктуры и т.д.

Особо хочется отметить разработку двух межгосударственных стандартов, касающихся биометрической аутентификации. Суть в том, что в этих стандартах впервые решаются вопросы нормативного регулирования создания средств так называемой «высоконадежной» биометрии.

Проблемам развития биометрических методов аутентификации в настоящее время уделяется значительное внимание во многих странах. Российские исследователи предлагают использовать нейросетевые преобразователи «биометрия-код», исследователи США и Канады идут по пути использования преобразователей, построенных с использованием нечеткой логики. Рано или поздно эта проблема будет решена мировым сообществом и тогда возникнет другая проблема: оценки стойкости защиты биометрических данных конкретного человека после их размещения в нейросетевом или нечетком контейнере.

Для таких контейнеров и разработаны указанные, а также ряд других связанных с ними российских стандартов, опираясь на которые можно оценить стойкость защиты

биометрических данных применительно к атакам подбора. В этом отношении данные разработки относятся к безусловно лидирующим в мире. Мы опережаем западные страны как минимум на 5-7 лет.

В результате сегодня можно утверждать, что совместными усилиями организаций России и Беларуси практически создана система первоочередных документов Союзного государства в этой области.

В части, касающейся новых технических решений в области защиты совместных информационных ресурсов, в ходе выполнения Программы, разработаны:

территориально-распределенная система информационной поддержки мониторинга активности компьютерных вирусов в информационных системах Союзного государства (ФСБ России);

перспективные технологии защиты совместных информационных ресурсов Союзного государства от утечки и воздействия по техническим каналам, от несанкционированного доступа, от компьютерных атак и вирусов, а также защиты на основе криптографических методов (в том числе, с использованием методов квантовой криптографии);

информационно-справочная система по моделям угроз безопасности информации КВСИИ Союзного государства и электронная база данных с документами Союзного государства в области ТЗИ и ОБИ в КВСИИ.

В результате российской стороной получено и зарегистрировано в установленном российским законодательством порядке 47 результатов интеллектуальной деятельности (включая те, которые реализованы в проектах более 40 организационно-распорядительных, нормативных и методических документов, в 7 опытных образцах средств защиты информации и в 2 программных изделиях).

На новые технические решения в области защиты информации оформлены 2 патента на изобретения и 4 патента находятся в стадии оформления.

Внедрение разработанных в Программе организационно-распорядительных, нормативных и методических документов будет осуществлено путем их утверждения Советом Министров Союзного государства или по его поручению Постоянным Комитетом Союзного государства.

Кроме этого, предлагается использовать полученные в рамках Программы результаты в интересах России и Беларуси при разработке и введении в действие национальных нормативных и методических документов в области обеспечения безопасности информации.

Внедрение разработанных в ходе выполнения Программы средств защиты информации будет осуществлено путем организации их серийного производства в России и Беларуси.

Использование разработанных информационно-справочных систем позволит существенно повысить эффективность служебной деятельности руководителей и специалистов, работающих в сфере обеспечения информационной безопасности Союзного государства и государств-участников.

Внедрение результатов, полученных в ходе выполнения мероприятий Программы, будет осуществляться в соответствии с Планом по реализации результатов Программы, разработанным государственным заказчиком–координатором совместно с государственными заказчиками с учетом результатов рассмотрения Итогового отчета о выполнении Программы Советом Министров Союзного государства.

Разработанные в рамках Программы изделия планируются к постановке на производство в зависимости от потребности в 2011 – 2012 годах. По всем разработанным изделиям определены предприятия-изготовители.

Таким образом, из всего вышеизложенного следует, что цели Программы достигнуты в полном объеме.

Реализация результатов выполнения Программы позволит обеспечить дальнейшее совершенствование системы защиты общих информационных ресурсов Беларуси и России и

на этой основе повысить защищенность информации в КВСИИ Союзного государства, а также способствовать развитию эффективных высокотехнологичных методов и средств защиты информации.

Эффект от реализации результатов программы Союзного государства будет заключаться:

в обеспечении конфиденциальности, целостности и доступности информации, циркулирующей в информационных системах и информационно-телекоммуникационных сетях Союзного государства;

в предотвращении (снижении риска) нарушений функционирования критически важных систем информационно-телекоммуникационной инфраструктуры Союзного государства и связанных с этими нарушениями негативных экономических, экологических и социальных последствий;

в развитии производства конкурентоспособных технических, программно-аппаратных и программных средств защиты информации;

в экономии финансовых средств за счет разработки единых для Союзного государства нормативных и методических документов и средств защиты информации по отношению к затратам Российской Федерации и Республики Беларусь, если бы они такую разработку осуществляли самостоятельно без Программы (каждый вложенный в Программу российский рубль обеспечит не менее 1,5-2 российских рублей экономии финансовых средств).

Касаясь перспектив дальнейшего совершенствования защиты общих информационных ресурсов Беларуси и России, необходимо отметить следующее.

В условиях интенсивного развития информационных технологий, связанного с решением все более сложных и масштабных задач во всех сферах деятельности государства и общества, возрастает открытость государства и общества, и соответственно этому растёт опасность угроз безопасности информации, связанных с деятельностью иностранных специальных служб, преступных сообществ и отдельных лиц в таких сферах, как государственное управление, банковская деятельность, эксплуатация критически важных систем информационной инфраструктуры, обработка персональных данных.

В этой связи одним из основных направлений деятельности в области информационной безопасности Союзного государства является обеспечение предупреждения и нейтрализации угроз безопасности информации в условиях интенсивного развития высоких информационных технологий, все более широкого их использования во всех сферах государственной и общественной деятельности. К таким технологиям относятся так называемые GRID-технологии и облачные вычисления, технологии высоконадежной биометрии, которые несомненно нуждаются в дальнейшем развитии, технологии дистанционного обучения специалистов в области защиты информации и т.д.

Требуют анализа и принятия соответствующих мер по их нейтрализации стремительно возрастающие угрозы нарушения конфиденциальности информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты), в том числе, персональных данных граждан Беларуси и России.

Продолжает оставаться острой проблема обеспечения безопасности информации в критически важных системах информационной инфраструктуры Союзного государства от деструктивных информационных воздействий, растёт опасность нарушения их функционирования за счет внедрения программно-аппаратных закладок, воздействий на информацию, передаваемую по каналам связи, использования средств "электромагнитного терроризма", в связи с чем необходим совместный поиск эффективных программных и программно-аппаратных решений этой проблемы.

Изложенное подтверждает актуальность проблемы постоянного совершенствования единого научно-технического обеспечения защиты общих информационных ресурсов Беларуси и России, решение которой будет продолжаться в рамках новой программы Союзного государства на 2011-2015 годы.

РАЗДЕЛ 2
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В СЕТИ ИНТЕРНЕТ

М.С.АБЛАМЕЙКО

АНАЛИЗ ЗАКОНОДАТЕЛЬСТВ ПО ЗАЩИТЕ ОТ КИБЕРПРЕСТУПЛЕНИЙ В РОССИИ И БЕЛАРУСИ И МЕРЫ ПО ИХ ГАРМОНИЗАЦИИ

Введение

Преступные проявления в сфере высоких технологий, так называемая киберпреступность, стали оказывать все большее влияние на работу национальных компьютерных сетей. Человечество постепенно перемещается в эпоху кибервойн (войн в киберпространстве), которые по своим последствиям могут быть не менее разрушительными, чем обычные войны.

В России и Беларуси постоянно растет число киберпреступлений. Так, в Беларуси произошел рост преступлений против информационной безопасности с 119 в 2003 году до 1614 в 2008-м. В частности в 2004 году в РБ было зарегистрировано более 130 преступлений против информационной безопасности, в 2006 – 272, в 2007 – 996 преступлений, а в 2008 году киберпреступность возросла на 62 % – 1614 преступлений [1] .В Беларуси за 2010 год зафиксировано более двух тысяч киберпреступлений

Законодательства двух стран (России и Беларуси) в этой сфере несколько отличаются друг от друга. Однако, для принятия совместных мер желательно чтобы они были максимально близки. Также важно, чтобы национальное законодательство России и Беларуси в данном вопросе соответствовало международным нормам и стандартам.

Законодательство и действия Российской Федерации по борьбе с киберпреступностью

На сегодняшний день законы РФ предусматривают уголовную ответственность за преступления в сфере компьютерной информации, что отражено в главе 28 Уголовного кодекса РФ, который состоит из трех статей [2]:

– Статья 272. Неправомерный доступ к компьютерной информации (Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети);

– Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ (Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами);

– Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред).

В настоящее время эти статьи нельзя назвать совершенными, приняты они были в 1996 году. Прошло15 лет и ситуация поменялась. Придуманы многочисленные способы обхода закона. Зачастую органы внутренних дел ограничены несовершенным законодательством, и чисто формально хакеры, которые наносят немалый вред, признаются невиновными.

Российская Федерация является очень активной по предупреждению киберугроз на международном уровне. В 1998 году Россия представила Резолюцию ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», определив основные понятия неавторизованных вторжений в компьютерные сети, и предложив международные принципы защиты от кибернападений [3]. В 1999 году Резолюция включила военные угрозы, проистекающие от информационных и телекоммуникационных технологий. Эти резолюции регулярно одобряются Генеральной Ассамблеей ООН, а США регулярно голосуют против них.

Российское министерство внутренних дел ежегодно проводит мероприятия под условным названием "Сеть" уже на протяжении десяти лет. Только в в 2008 году в ходе такой операции была приостановлена деятельность 610 деструктивных Internet-ресурсов, возбуждено 270 уголовных дел, выявлено 325 преступлений.

Законодательство и действия Республики Беларусь по борьбе с киберпреступностью

За последние 10 лет в Республике Беларусь принималось немало серьезных мер по защите собственных компьютерных сетей от кибератак. В Министерстве внутренних дел Республики Беларусь создано и функционирует специальное подразделение по борьбе с киберпреступностью (по противодействию преступлений в сфере высоких технологий). В Уголовном кодексе Республики Беларусь в разделе XII «Преступления против информационной безопасности», глава 31 «Преступления против информационной безопасности», в статье 349 «Несанкционированный доступ к компьютерной информации» говорится о следующем [4]:

1. Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), повлекший по неосторожности оборудования либо причинение иного существенного вреда, – (абзац 1 части 1 статьи 349 в ред. Закона Республики Беларусь от 22.07.2003 № 227-З) наказывается штрафом или арестом на срок до шести месяцев.

2. Несанкционированный доступ к компьютерной информации, совершенный из корыстной или личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, (абзац 1 части 2 статьи 349 в ред. Закона Республики Беларусь от 22.07.2003 № 227-З) наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

3. Несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризированной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

Министерство внутренних дел Беларуси активно участвует в выработке международных механизмов по предотвращению киберпреступности. Делегация МВД в марте 2009 года приняла участие в Вене в рабочем совещании ОБСЕ по всеобъемлющему подходу к повышению кибербезопасности. Особый акцент при этом был сделан на

необходимость присоединения государств к Конвенции Совета Европы по кибербезопасности, подписание которой позволит выйти на более качественный уровень взаимодействия [5].

В Республике Беларусь до сих пор не отмечалось каких-либо массированных нападений на компьютерные сети. Одним из самых больших событий, нарушивших стабильность работы компьютерных сетей, стал в 2009 году сбой в работе сети Национального Процессингового Центра, который привел к отказу от обслуживания большого количества банкоматов. Это произошло из-за вируса, однако учитывая размер происшествия и его последствия, Правительство Беларуси поручило Министерству связи и информатизации совместно с заинтересованными разработать перечень мер, по предотвращению сбоев на компьютерные сети. Такой объемный документ был разработан и утвержден летом 2009 года Первым заместителем Премьер-министра Республики Беларусь.

Мероприятия стран СНГ и Союзного государства

Государства СНГ и Союзное государство предпринимают совместные шаги по защите от киберугроз. Так, в июне 1999 года была принята концепция информационной безопасности государств СНГ, и в списке источников угроз этой безопасности первым пунктом названа «государственная политика ряда зарубежных стран, направленная на осуществление глобального мониторинга политических, экономических, военных, экологических и других процессов в целях получения односторонних преимуществ».

В Соглашении о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, дается следующее определение преступлению в сфере компьютерной информации - "уголовно наказуемое деяние, предметом которого является компьютерная информация" .

В последние годы на заседаниях Организации Договора Коллективной Безопасности (ОДКБ) регулярно стали рассматриваться вопросы, касающиеся кибербезопасности. Одним их последних мероприятий стало проведение 15.04.2009 года на территории стран-членов Организации Договора о коллективной безопасности широкомасштабной операции «Прокси» по противодействию киберкриминалу. Эта кампания направлена на выявление и пресечение в национальных сегментах Интернета информационных ресурсов криминального характера.

В декабре 1999 года была одобрена программа действий России и Беларуси по реализации положений договора о создании Союзного государства. В разделе о совместной деятельности спецслужб появился пункт: «Осуществляются мероприятия против негативного информационного воздействия на государственные органы, общественные организации и население Союзного государства, а также пресекаются любые попытки противоправной разведывательной деятельности специальных служб и организаций третьих стран…» [6].

Выполняются совместные программы Союзного государства в сфере информационной безопасности. Одним из крупнейших форумов, где регулярно происходит обмен мнениями, является ежегодная научно-техническая конференция Союзного государства «Комплексная защита информации». Уже 10 лет издается российско-белорусский научно-практический журнал «Управление защитой информации», в Беларуси издается сборник статей «Проблемы правовой информатизации».

Предложения по гармонизации и развитию законодательств по защите от киберпреступлений

Из проведенного анализа можно сделать вывод, что существующие законодательства двух стран не предусматривали кибернападений на такие жизненно важные структуры стран, какими стали компьютерные сети и не могут напрямую быть использованы применительно к появившимся новым вызовам 21-го века. Очевидно, что настала чрезвычайная

необходимость для разработки новых правовых механизмов защиты от массированных кибератак.

Также можно сделать вывод, что используемые термины «преступления в сфере компьютерной информации» (РФ) и «преступления против информационной безопасности» (РБ) является достаточно узкими. Так, в них сложно включить широко распространенные атаки на Интернет-сайты. Их предметом является не компьютерная информация, а сам сайт, а целью - парализация его работы. Например, при атаке на систему Интернет-банкинга кредитная организация, которой принадлежит система, понесет значительные убытки из-за непроведенных банковских операций. В то время как сами «атакующие» никакой выгоды не получат – часто такие атаки осуществляются из хулиганских побуждений.

Т.е. вопрос о терминологии в сфере компьютерных преступлений продолжает оставаться открытым. Между тем это принципиальный вопрос, поскольку в зависимости от применяемой терминологии соответствующий институт будет наполняться различным содержанием.

Наверное, надо расширить предусмотренный в главе 31 УК РБ и главе 28 УК РФ перечень составов преступлений и использовать в наименовании термин киберпреступления. Его можно заменить на более русский термин «преступления в сфере безопасности обращения компьютерной информации». Данная формулировка также соответствует традиционным представлениям об объекте посягательства, как сфере социальных отношений, и выводит нас из чисто технической в общественную плоскость. Таким образом, если бы перечень составов главы 28 УК РФ и главы 31 УК РБ расширился, то использование термина киберпреступления было бы оправданным.

Одной из наиболее продвинутых в плане описания уголовной ответственности за киберпреступления является законодательство США. В последнее время наблюдается тенденция к сближению и унификации мер, применяемых к хакерам на территории разных стран. Россия и Беларусь пока недостаточно активно участвуют в этом процессе, но в Европе и странах СНГ, например, уже давно существует единая «Рекомендация № R 89 (9) Комитета Министров стран-членов Совета Европы относительно преступлений, связанных с компьютерами».

Учитывая все возрастающую опасность киберугроз, нашим странам необходимо предпринять решительные совместные шаги по развитию и гармонизации законодательств, недопущению кибернападений и правовой оценке их последствий.

Литература

1. http://www.bybanner.com/article/9084.html

2. Уголовный кодекс Российской Федерации от от 13.06.1996 N 63-ФЗ (принят ГД ФС РФ 24.05.1996)

3. http://www.mid.ru/bl.nsf/6f92c64e92f7ee83c3256def0051fa16/ a5222e2fbc01cb804325699c003c110e?OpenDocument

4. Уголовный кодекс Республики Беларусь. Принят Палатой представителей 2 июня 1999 года. Одобрен Советом Республики 24 июня 1999 года:. – Минск: Амалфея, 2006. – С.230-231.

5. http://mvd.gov.by/modules.php?name=News&file=article&sid=5808

6. Кибер террор: оценка уровня угрозы http://www.agentura.ru/equipment/psih/ info/conferencepole/soldatov/

С.В.АБЛАМЕЙКО, С.М.БРАТЧЕНЯ, Н.И.КАЛОША, В.Ю.ЛИПЕНЬ

ПРЕДОСТАВЛЕНИЕ УСЛУГ ПО ПРОВЕДЕНИЮ ЭЛЕКТОРАЛЬНЫХ МЕРОПРИЯТИЙ С ИСПОЛЬЗОВАНИЕМ ВНЕШНЕЙ СИСТЕМЫ «ГАРАНТ» И СЕТИ ИНТЕРНЕТ

В своей публикации [1] авторы ознакомили участников конференции «КЗИ» с разработками в сфере электоральных технологий, которые были ориентированы на использование размещаемых на избирательных участках комплексов электронного голосования (ЭГ), явившихся развитием разработок для системы ЭГ «Сайлау» для Республики Казахстан. В ходе НИР «Инфотех-62» в ОИПИ НАН Беларуси был разработан программный комплекс поддержки макетов Веб-портала системы мониторинга электоральных мероприятий «Гарант» и программно-технических средств комплекса участка, обеспечивающих регистрацию избирателей и голосование, а также обнародование списков зарегистрированных избирателей и комплектов проверочных кодов.

Бурное развитие Интернет и устройств Интернет-доступа (в особенности мобильных) создает условия для перехода напрямую к Интернет-голосованию без дорогостоящего переоснащение избирательных участков. Участвуя на протяжение последних четырех лет в зарубежных конференциях по тематике E-Governance, E-Participation, E-Voting [2], авторы видят, что на проблематике Интернет-голосования концентрируются значительные усилия ИТ-специалистов, включая и российских коллег. Рассматривая проблему сбора персонализированных данных более широко, можно говорить о переходе к чисто электронной реализации таких трудоемких мероприятий, как переписи населения, опросы, централизованное тестирование знаний, выборы и референдумы различных уровней, плебисциты, «праймериз», сбор подписей в поддержку кандидатов, партий или важных решений. При этом могут использоваться сотни тысяч взаимодействующих с Веб-центрами компьютеров, которые будут находиться в пунктах коллективного доступа (центрах обслуживания населения), в Интернет-кафе, в стационарных и подвижных (на автомобилях) почтовых отделениях, исполкомах, школах, вузах, а также и в личном пользовании респондентов.

Использование при выполнении вышеуказанных видов работ традиционных бумажных технологий сопряжено с неоправданно высокими затратами времени и расходами финансовых и людских ресурсов. Внедрение дешевых и оперативных ИКТ сбора и обработки персонализированных данных, изначально формируемых в электронном виде, дает возможность резко снизить подобные затраты. Так, например, при проведении последней переписи населения в Литве сведения о миллионе жителей были сразу сформированы в электронном виде по данным регистров и электронным ответам граждан. Действительно, переход к более дешевому сбору данных в электронном виде мог бы позволить более часто проводить мероприятия рассматриваемого типа, посвящая их решению широкого круга жизненных проблем. Это помогло бы создать базу для развития местного самоуправления и повышения социальной активности граждан.

Как указано в [3], многие руководители партии «Единая Россия» являются сторонниками скорейшего перехода именно на Интернет-голосование, что позволит, по их мнению, снизить затраты на оснащение участков системами КОИБ и КЭГ, которые всё равно простаивают в периоды между выборами. При переходе на сетевое голосование по сравнению с традиционными бумажными технологиями могут быть резко снижены расходы на оплату труда большого числа служащих, привлекаемых к работе в участковых комиссиях и в качестве наблюдателей. В публикациях российских коллег в качестве причин недоверия к итогам выборов или игнорирования участия в них частью избирателей отмечается отсутствие возможности наглядно показать избирателю, что его голос зачтен в актив именно тому кандидату, партии, ответу на вопрос референдума, которые он предпочел и отметил в

бюллетене. По нашему мнению это обусловлено тем, что при опускании бюллетеня в урну происходит «деперсонализация» индивидуальных результатов голосования, и далее система оперирует только с проинтегрированными на уровне избирательного участка локальными результатами. Интересно, что и при реализации Интернет-голосования, например, в Эстонии с использованием имеющихся у всех граждан ID-карт, которые позволяют избирателю аутентифицировать себя по сети и заверять свой ответ с помощью электронной цифровой подписи (ЭЦП), также до конца не реализован принцип «end-to-end», поскольку «деперсонализация» сохраняемого на сервере в течение нескольких дней заверенного результата всё же происходит в момент отделения ЭЦП от результата при его суммировании с целью подведения итогов мероприятия. Обнародуемые итоги содержат только просуммированные результаты.

Судя по результатам опросов, до 60% населения Эстонии считает, что хранение на сервере голоса, заверенного личной ЭЦП, создает лазейки для нарушения анонимности волеизъявления. Существование подобных недостатков формирует у части электората недоверие к институту выборов и дает поводы оппозиционной стороне оправдывать проигрыши на выборах, трактуя их, как результат вмешательства местных администраций или компьютерных специалистов, обслуживающих систему ЭГ.

При разработке системы «Гарант» авторы анализировали также результаты эксплуатации систем ЭГ в Швейцарии, апробации системы в Австрии [4] и в ряде других стран. Авторы считают, что их разработка базируется на оригинальном подходе и использует ряд собственных технологий, позволяющих устранить или снизить влияние недостатков известных систем Интернет-голосования. Система «Гарант» была задумана как один из сервисов системы предоставления государственных информационных услуг. Она должна предоставлять электоральные услуги территориям (организациям), проводящим мероприятия, выполняя при этом роль «третьей доверенной стороны». Для оформления заказа потребитель должен ввести средствами Веб-портала электронные списки избирателей и объектов кастинга, а также сведения о мероприятии. С процедурами заказа и сопровождения мероприятия можно ознакомиться на Веб-портале: http://e-vote.basnet.by/. В презентации на примере действующего макета Веб-портала демонстрируется применение оригинального подхода к формированию защищенных логинов и паролей, используемых для «скрытной» персонализации и верификации результатов, а также для регулирования доступа к исполнению on-line процедур в сети. Технология «скрытной» персонализации, впервые предложенная и апробированная авторами в системе ЭГ «Сайлау», в нынешнем варианте Веб-реализации дает избирателю возможность установить, каким образом в итоговых результатах выборов (референдума) было зарегистрировано его участие (неучастие), а также скрытно проверить, в актив какому кандидату, партии, ответу на вопрос референдума был зачтен его голос. Схема связей системы «Гарант» с субъектами мероприятия показана на рис.1.

Важной особенностью предложенной системы является механизм аутентификации, использующий персональные данные избирателя и SID (криптографические коды), передаваемые избирателям перед выборами по предъявлении ими паспорта. Каждый SID генерируется по алгоритму $SID_i = EID_i \oplus F_{crypt}\ (EID_i,\ K,\ R_i)$, где EID_i — уникальный открытый номер избирателя, $\oplus$ — оператор конкатенации, а F_{crypt} — безопасная криптографическая функция, имеющая аргументы EID_i, секретный ключ K и случайно выбранное секретное R_i, хранимое в доступной лишь криптосерверу базе данных. Функция F_{crypt} действует таким образом, что генерация валидных SID требует знания не только открытых данных и секретного ключа K, но и случайных чисел R_i. Злоумышленнику потребовался бы доступ к базе данных, в которой они хранятся. Секретный ключ и база данных могут быть сделаны открытыми после завершения голосования для проведения аудита удаленными сетевыми наблюдателями. Любому избирателю, сохранившему выданный при регистрации логин и пароль доступа к серверу голосования, доступен

механизм верификации отданного им голоса. Проверка возможна и путем обмена SMS-сообщениями.

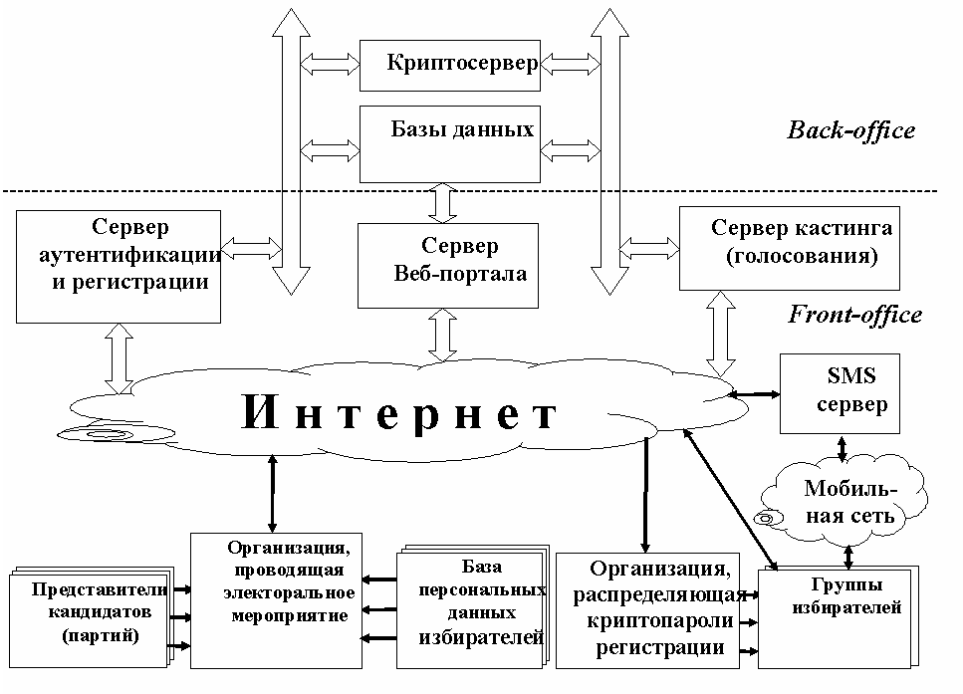


Рис.1. Схема взаимодействия системы «Гарант» с субъектами электорального мероприятия

Апробация предложенных технологий может быть проведена посредством натурных демонстраций на выставках с участием посетителей в качестве голосующих, а также рекламного предоставления услуг по удаленному мониторингу неофициальных мероприятий, проводимых отечественными или зарубежными учебными заведениями, корпорациями, органами местного самоуправления и партиями.

Авторы приглашают ИТ-экспертов и профильных руководителей к всестороннему обсуждению предложенных идей и подходов для формирования идеи совместного проекта электронной системы проведения репрезентативных и электоральных мероприятий (в рамках ЕЭП) с использованием практических наработок специалистов России, Казахстана и Беларуси. Реализация совместного проекта потенциально более экономична, чем разработка трех автономных национальных систем.

В силу того, что государственных границ в сети Интернет не существует, зоной предоставления электоральных услуг системы могли бы стать и конфликтные африканские или азиатские страны. Подобные предложения сформулированы авторами в докладах, поданных на зарубежные конференции. Реализуются русскоязычная и англоязычная версии Веб-портала системы «Гарант».

Литература

1. Абламейко С.В. О Проекте экспериментальной системы предоставления государственных информационных услуг / С.В.Абламейко, В.Ю.Липень, Д.В.Липень // Комплексная защита информации: материалы 14-ой Междунар. науч. практ. конф., Могилев, 19-22 мая 2009 г. / – Могилев, 2009. – С. 301-302.

2. Ablameyko, S. Organizing and monitoring election events with «The Guarantor» / S. Ablameyko [V.Lipen, N.Kalosha] // EDEM, 2010. – Conference on Electronic Democracy 2010 : proc. of EDEM 2010. – Krems, 2010. – P. 299–310.

3. http://www.ng.ru/politics/2010-11-16/3_electrodemocracy.html

4. R. Krimmer, A. Ehringfeld, M. Traxl, The Use of E-Voting in the Austrian Federation of Students Elections, The 4th International Conference on electronic voting, 2010, Bregenz, Austria.

О.В.КАЗАРИН, А.А.САЛЬНИКОВ, Р.А.ШАРЯПОВ, В.В.ЯЩЕНКО

СУЩЕСТВУЮЩИЕ И НОВЫЕ АКТОРЫ КИБЕРКОНФЛИКТОВ

1. Введение

Целью данной работы является исследование *конфликтов в киберпространстве* (*киберконфликтов*) и, главным образом, тех из них, которые связаны с использования современных информационных технологий *во враждебных и преступных целях*. Поэтому в дальнейшем будут рассматриваться такие явления как кибервойны, кибертерроризм, киберпреступления и, следовательно, можно говорить о таких акторах киберконфликтов, как *киберпреступники*, *кибертеррористы*, *акторы, ответственные за ведение кибервойн, кибероперацийнаступательного и оборонительного характера* [1].

В то же время, на наш взгляд, в последнее время оформляются (продолжают оформляться) как вполне самостоятельные акторы *противоборства* (*противостояния*)*в киберпространстве* такие образования, как «*сетевая гвардия*» (*NetGuard*), «*сетевое ополчение*» (*NetHomeGuard* или *NetMilitia*), *неправительственные сетевые структуры* (*NetNGO* [2]), «*сетевой спецназ*» (*NetSpecialForces*), действия которых имеют свою внутреннюю логику, свою мотивацию и цели [1].

Если действия акторов, связанных с ведением кибервойн (как, правило, государственных акторов, но не только, не обязательно), а также киберпреступников, кибертеррористов являются предметом достаточно длительных по времени и объемных по масштабу исследований различного рода, то изучение действий вышеуказанных акторов только начинают «свое плавание в исследовательском море». Хотя до конца еще не совсем понятно, следует ли их вообще выделять в отдельный пул акторов, действующих на «сетевом поле» киберпространства?

2. Новые акторы киберконфликтов

Проиллюстрируем роль, место и мотивацию новых акторов, действующих в киберпространстве (см. рис. 1). Приведенные на этом рисунке акторы расположены в порядке усиления их влияния на различные элементы киберпространства как с точки зрения киберзащиты, так и кибернападения.

Если упрощенно, – *обычные пользователи, администраторы, провайдеры* и т.п., как правило, не оказывают намеренного негативного влияния на различные элементы киберпространства, не участвуют в киберконфликтах (это акторы, которые либо законно предоставляют ресурсы киберпространства, либо законно их потребляют). *Незлонамеренные хакеры*, как правило, ненамеренно участвуют в киберконфликтах из-за азарта, озорства (баловства), любопытства, «спортивного» интереса (пари, спора) и т.п. *Злонамеренные хакеры* намеренно участвуют в киберконфликтах по многим причинам: из-за мести, зависти, корысти, злобы и т.п. *Сетевые комбатанты* оказывают влияние на состояния киберпространства со «своими» целями и «своей» мотивацией. *Киберпреступники* участвуют в киберконфликтах (их создают) в криминальных целях, а *кибертеррористы* – в террористических. *Подразделения правительственных и неправительственных организаций, участвующих в кибероперациях*, оказывают влияние на состояние

---

[1] А также всевозможных миротворческих информационных операций, операций по принуждению к миру в киберпространстве (если такое возможно) и т.п.

[2] Non-governmentorganizations.Сюдатакжеможно отнести различные частные компании, например, частные военные компании - MilitaryPrivacyCompanies (MPC).

киберпространства, в основном, в военно-политических целях. И, наконец, *кибервойска* оказывают комплексное направленное влияние на состояние киберпространства исключительно в интересах государства.

Уровень воздействия новых акторов – их еще будем далее называть *сетевые комбатанты* – на состояние и характеристики киберпространства различен, как различны условия и операционные среды, в которых они действуют (см. рис. 2).

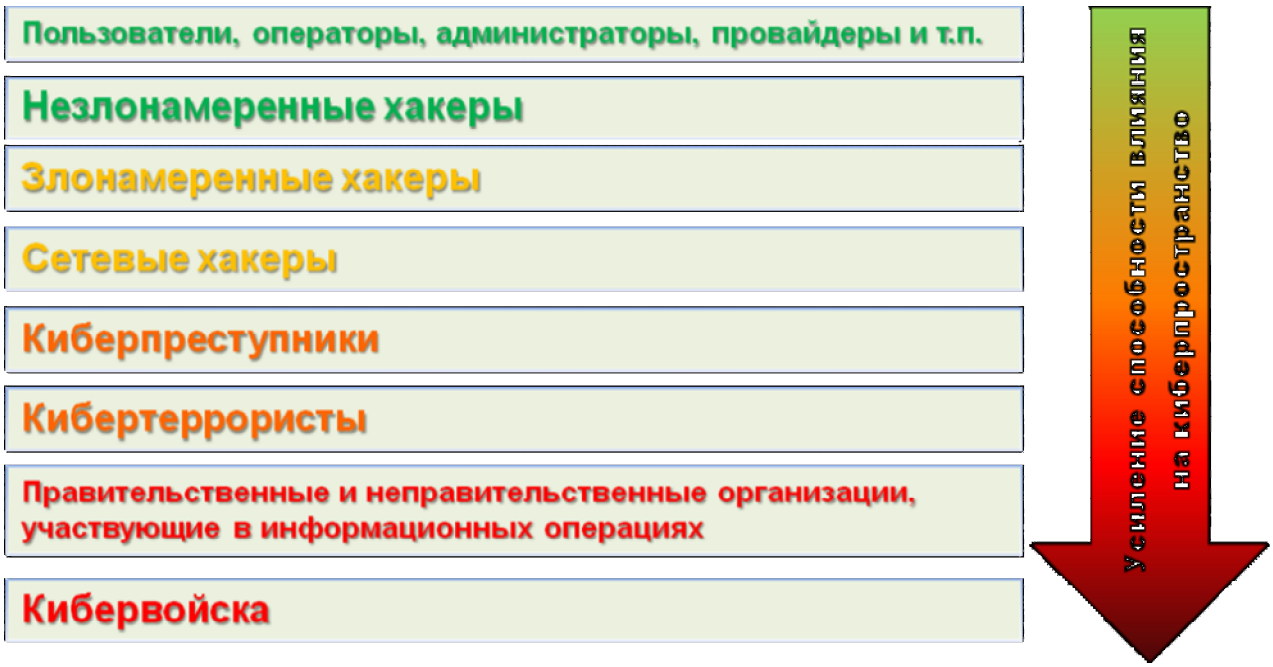


Рис. 1. Акторы и степень их влияния на киберпространство

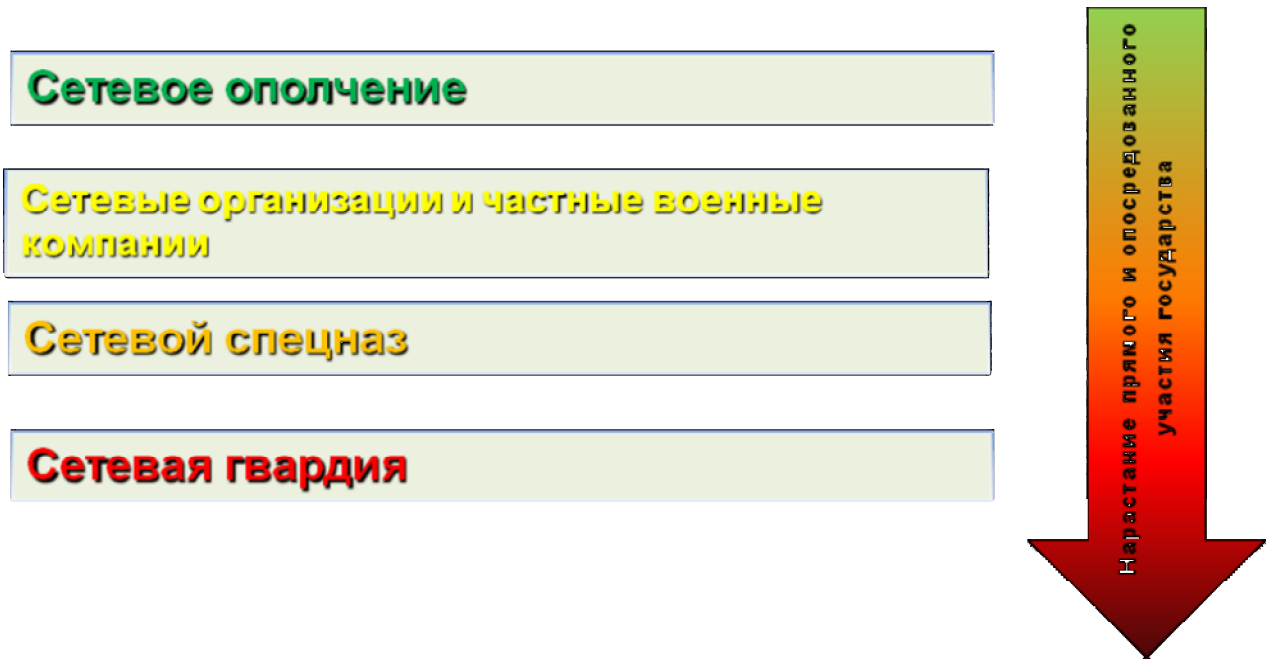


Рис. 2. Новые акторы и участие государства

«Простые» *сетевые ополченцы* действуют часто самостоятельно на свой страх и риск, считая, как правило, что все их поступки совершаются во имя истины и установления справедливого миропорядка. Финансовая сторона дела их мало интересует. Часто в их

действиях присутствуют обычные азарт, озорство, ребячество и т.п. Сетевые ополченцы ведут свои «бои», как правило, скоординированно, их атаки – являются массированными, сетецентрическими. Это достигается за счет умелого, интенсивного интернет-взаимодействия, придуманного еще хакерским сообществом.

Для других акторов (например, *сетевых частных военных компаний*) информационные операции – это хорошо налаженный бизнес, где игра идет по своим сугубо прагматичным правилам. Их работа должна хорошо оплачиваться, заказчик, по большому счету, может быть любым, лишь бы «хорошо платил», а моральная сторона дела их часто мало интересует.

Для *сетевого спецназа* – информационные операции, как и для многих других «силовиков», информационные операции – это, прежде всего, профессиональное отношение к делу, обыденное и качественное выполнение приказа.

Другое дело – *сетевая гвардия*. Здесь речь идет о таких сторонах человеческой природы, как патриотизм, любовь к родине, острое чувство несправедливости. Финансовая сторона дела – вторична. Главное – противостоять потенциальному «киберврагу», отстоять свою национальную «кибернезависимость».

В целом, мотивация деятельности некоторых новых акторов киберконфликтов еще недостаточно изучена. Предмет и объекты исследования – *новы*, а характер исследований – *явно междисциплинарный*. Это – политология и социология, психология и философия, естествознание и компьютерные науки. На наш взгляд, здесь – огромное поле деятельности для специалистов во многих областях знаний.

3. Заключение

Само по себе изучение различных действующих лиц, их коалиций в киберпространстве интересно и полезно с точки зрения исследования киберконфликтов. Но, вряд ли, это может являться самоцелью. Более или менее четкое *определение государственных и негосударственных акторов киберконфликтов* и *характера их возможных действий может позволить*:

– устанавливать различный уровень угроз для объектов критических инфраструктур и, соответственно, адекватный уровень и масштаб превентивных и/или ответных действий;

– устанавливать ответственность государственных структур за действия государственных и негосударственных [1] акторов, действующих в его (условном) секторе киберпространства;

– устанавливать ответственность государственных структур за «попадание в руки» киберпреступников и кибертеррористов «продвинутых» информационных технологий;

– подготавливать и осуществлять международные мероприятия при определении источников кибератак, в том числе при эскалации и деэскалации трансграничных киберконфликтов;

– прогнозировать развитие киберконфликтов между определенными акторами и их коалициями, с участием третьих сторон;

– приступить к пониманию более сложных и глубоких проблем, связанных с управлением киберконфликтами [2], не только с технической (технологической), но и с политической, социальной, психологической, международной и (даже) культурологической точек зрения;

– и многое-многое другое.

И в этом смысле, конечно, нужны международные научные контакты, общение, обмен мнениями, общеплановые и целевые дискуссии в данных областях знаний.

---

[1] Если это возможно.

[2] А, если такое понимание «уже пришло», - к разработке практических решений.

Литература

1. Казарин О.В., Сальников А.А., Шаряпов Р.А., Ященко В.В. Новые акторы и безопасность в киберпространстве// Вестник Московского университета. Серия «Политические науки». – 2010. – №2. – С.71-84; №3. – С.90-103.

А.Н.КУРБАЦКИЙ

НЕКОТОРЫЕ АСПЕКТЫ БЕЗОПАСНОГО ОСВОЕНИЯ И ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Лет пятнадцать назад, когда начиналась формироваться предметная область нашей конференции, проблема защиты информации, представлялась, связанной в основном с государством. Затем эта тема стала все более актуальной для бизнеса, и вот сейчас защита информации стала актуальной для личности, практически для каждого человека.

Последнее десятилетие стало популярным понятие информационного общества. Многие государства разработали или разрабатывают стратегии, концепции построения информационного общества.

Одним из важнейших результатов формирования информационного общества стало развитие глобального информационного пространства, в котором развернулась острая борьба за достижение информационного превосходства.

С одной стороны мировое сообщество строит единое информационное пространство или в более узком смысле киберпространство. С другой стороны, многие уже возводят защищенные границы для себя в этом «общем» пространстве. Например, в США, помимо Агентства национальной безопасности, созданы киберкомандования в Пентагоне, практически во всех родах войск. Те же тенденции наблюдаются в Великобритании, Франции, Германии, Китае, Индии, России и т.д.

Если говорить о последствиях построения информационного общества и единого информационного пространства, то всегда нужно иметь ввиду следующие соображения. Тот, кто опережает в развитии информационно-коммуникационных технологий (ИКТ), практически всегда будет находиться в большем выигрыше и в плане построения информационного общества и эффективного использования для себя единого информационного пространства. Проблема в том, что мы всегда должны играть по правилам, установленным не нами, и использовать уже известные стандарты. Но дело в том, что когда ИКТ становятся стандартами, они уже практически не являются инновационными, так как разработка и принятие стандартов – это годы. Пока мы разбираемся со стандартами, конкуренты уже работают действительно с новыми ИКТ. Поэтому нужно очень четко представлять последствия внедрения новых для нас ИКТ. Нужен постоянный стратегический анализ последствий внедрения ключевых ИКТ, как один из основных факторов обеспечения безопасности государства и общества.

Среди пользователей глобальных информационных систем особо нужно выделить молодое поколение. Его представители, с одной стороны, еще активно формируются в личность, становятся активными членами общества, с другой стороны, могут в массовом порядке активно воздействовать на государство. Раньше эти процессы были гораздо более медленными, и главное – детерминированными и управляемыми как со стороны государства, так и, во многих случаях, со стороны общества. Сейчас же этот детерминизм и управляемость быстро разрушаются, и, в итоге, государство и общество сталкиваются с большими трудностями, которые при определенных условиях могут стать катастрофическими. В существенной степени такими ускорителями возможностей молодого поколения явились глобальные сети, Интернет. Всегда ли этот процесс ускорения позитивен

– большой вопрос. Более ранняя активизация требует получения опыта принятия решений на основе получаемой информации, большей ответственности за последствия принятых решений – а этого опыта как раз и не хватает. Общество и государство оказались практически не готовы к таким процессам.

Последствия сегодняшних упущений в образовании и воспитании могут проявиться гораздо раньше, чем мы думаем.

Практически мы пока не имеем массового формирования молодежной культуры на основе применения информационных и коммуникационных технологий, которая способствовала бы применению в реальной жизни знаний и навыков, полученных молодежью в виртуальной среде.

Особый интерес представляют социальные сети, которые могут быть своего рода надстройкой над государством и возможно станут сильным информационным механизмом модернизации общества, государства, что собственно уже и подтверждается, в частности, событиями в арабском мире.

Впервые громко заявив о себе в начале 2000-х годов, сейчас социальные сети переживают настоящий бум. Сегодня социальные сети обзавелись целым рядом возможностей, выводящих их на принципиально новый уровень.

В социальных сетях накапливается огромное количество информации, которая может использоваться по-разному, и часто непрогнозированно для тех, кто ее размещает в сети. Например, молодежь, размещая сейчас любую информацию о себе, своих родителях, своих друзьях в социальных сетях, обычно не задумывается, что через десять-пятнадцать лет эта информация может помешать карьере, бизнесу, личной жизни и т.п., как себе, так и своим близким и друзьям.

Проблема молодого поколения и виртуального мира крайне актуальна, поскольку время смены поколений очень скоротечно, и мы часто ошибаемся в оценках тех или иных общественных явлений из-за недооценки скоротечности и запаздываем в своих перспективных прогнозах.

Общество само не слишком заботится о своей безопасности и постоянно формирует предпосылки для угроз информационной безопасности. В частности, общество должно контролировать свою виртуализацию. Иначе негативные черты виртуализации будут только быстро нарастать. Как в процессе воспитания – семья отходит на второй план, школа отходит на второй план, их реально начинает заменять практически не контролируемый обществом виртуальный мир.

К сожалению, государства решают текущие задачи своей безопасности, бизнес-структуры решают проблемы прибыли, но мало кто заботится о проблемах общества в целом. Ни одна из международных структур (НАТО, ШОС, ОДКБ) не решают проблемы экспертизы и прогнозирования влияния ИКТ на информационную безопасность общества.

Понятно, что задачи и цели у этих международных организаций свои, но их экспертно-аналитический потенциал неплохо было бы использовать и для более широких целей.

Влияние ИКТ сейчас таково, что если заранее его не прогнозировать, то последствия от их массового внедрения могут быть весьма плачевными, как с сетевыми, виртуальными играми, которые по сути вышли из под контроля. А новые технологии, в частности, мобильные, лишь усугубляют проблему.

Сегодня было бы интересно вообще рассматривать ИКТ, в первую очередь, как социогуманитарные технологии.

Функциональность новой ИКТ, как правило, гораздо более очевидна, чем ее влияние на информационную безопасность. Часто функциональность лежит на поверхности, интуитивно понятна и поэтому сразу же включается маховик раскручивания потребительских свойств, основанных на функциональности, извлечения из этого прибыли, а

какие последствия могут быть у такой массовой бизнес-раскрутки мало кто на этом этапе задумывается.

Появились новые ИКТ – появляются новые проблемы в информационном пространстве, появляются новые возможности для киберконфликтов, кибертерроризма, киберпреступности.

При этом нельзя сказать, что и мирового сообщества нет опыта прогнозирования и контроля над новыми технологиями.

Если разработчики новых ИКТ будут понимать, что существует последующая экспертиза, то они, можно надеяться, будут более ответственно относиться к своей продукции.

Нужно формировать ответственность (социальную ответственность) бизнеса за свою ИКТ-продукцию.

Можно привести пример с лекарствами, продуктами питания. Прежде чем лекарство начинают массово производить, идет его экспертиза, опытная апробация и т.д. Часто нужны годы, чтобы лекарство запустить в серию. А ведь с некоторыми ИКТ проблемы могут быть не меньшие.

Или взять определенный опыт международного агентства по атомной энергии (МАГАТЭ). МАГАТЭ – это ведущий мировой форум научно-технического сотрудничества в области мирного использования ядерных технологий, созданный в рамках Организации Объединенных Наций в 1957 году в качестве самостоятельной организации.

Процесс построения информационного общества и связанное с этим развитие сектора информационно-коммуникационных технологий предполагает развитие экспертного сообщества. Здесь можно пойти по пути развития в экспертное сообщество добровольного объединения ИТ-специалистов. Одной из лучших мировых практик в данной области является институт инженеров по электротехнике и радиоэлектронике – IEEE (Institute of Electrical and Electronics Engineers) – международная некоммерческая ассоциация специалистов в области техники, мировой лидер в области разработки стандартов по радиоэлектронике и электротехнике. Интересен опыт международной федерации ученых, в первую очередь, в сфере информационной безопасности (World Federation of Scientists PMP on Information Security).

Известно, что любое серьезное решение требует серьезной экспертной оценки. Поэтому важно как формировать экспертные сообщества, так и эффективно организовывать работу коллективов экспертов. Сегодня все больше распространяется распределенная (сетевая) форма работы коллектива экспертов. Я не вижу большой разницы в технологическом плане том, как работают эксперты, например передовых ситуационно-аналитических центров и могут работать эксперты нашего сообщества.

А.Н.КУРБАЦКИЙ

О ПРАВИЛАХ ПОВЕДЕНИЯ В ИНТЕРНЕТЕ

Мы практически свыклись с лидирующей ролью Америки в различных геополитических, стратегических инициативах. Но я хочу привести пример, когда за счет методичной, целенаправленной, последовательной работы можно опережать и инициативных американцев. Ученые и эксперты, в первую очередь Московского государственного университета, в течение десяти лет последовательно занимались комплексными проблемами информационной безопасности. Ими активно поднимался и исследовался вопрос обеспечения безопасности в информационном пространстве, в частности, в Интернете. Вначале эта тема обсуждалась на общегородском семинаре,

проводимом в МГУ в начале 2000-х годов. Затем, после создания института проблем информационной безопасности МГУ в 2005 году, эта тема стала одной из основных исследовательских тем института. Вскоре появились партнеры для совместных исследований из университета Нью-Йорка. А в 2007 году по инициативе института проблем информационной безопасности МГУ в Гармише-Партенкирхене был проведен первый международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму». С тех пор он проводится ежегодно и остается практически единственным в мире регулярным международным мероприятием, где комплексно рассматриваются вопросы информационной безопасности. Среди более чем 150 участников – ученые, дипломаты, предприниматели, представители государственных структур Австрии, Беларуси, Болгарии, Германии, Израиля, Индии, Канады, Китая, России, США и Японии, а также ООН, НАТО, ОБСЕ, Европейского центра по изучению вопросов безопасности имени Дж. Маршалла, Европарламента. Позитивным фактором является формирование такой дискуссионной площадки представителями ведущего российского университета не на территории России, а в центре Западной Европы – одно соседство Европейского центра по изучению вопросов безопасности имени Дж. Маршалла чего стоит.

В центре внимания форума – поиск путей к глобальному сотрудничеству в борьбе с информационными угрозами, комплексные проблемы безопасности в информационном пространстве.

А 12 апреля 2010 г. по инициативе российской стороны был сделан еще один перспективный шаг – представители девяти стран – Беларуси, Болгарии, Германии, Израиля, Индии, Китая, России, США, Японии подписали в Гармиш-Партенкирхене (Германия) Декларацию о создании Международного исследовательского Консорциума информационной безопасности. В Декларации отмечается постоянно возрастающая опасность угроз в сфере международной информационной безопасности и выражается желание участников объединить свои научные и экспертные потенциалы для изучения этих угроз и путей их предотвращения. Цель Консорциума – осуществление совместной научной деятельности; его членами могут быть организации, работающие в области информационной безопасности. Консорциум содействует координации исследований по этой тематике, проводимых его участниками, формированию перечня приоритетных направлений таких исследований, развитию тематических грантовых программ, публикациям и проведению конференций, в первую очередь, под эгидой ООН. Организация открыта для приема новых членов, ее руководящим органом является Координационный совет, в который входят представители всех участников Консорциума.

С 23 по 29 апреля 2011 года в Гармише-Партенкирхене проводились пятый международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму» и заседание Консорциума. Основным результатом форума и заседания Консорциума, после долгой дискуссии, было принятие предложения о разработке свода универсальных правил поведения в мировом информационном пространстве.

По сути эта идея была центральной в видеообращении ректора МГУ академика Садовничего В.А. «За безопасное освоение киберпространства». В частности, он отметил, что созданная за последние десятилетия разветвленная система инфраструктур (киберпространство) предоставляет новые возможности для реализации все более изощренных угроз личности, обществу и государству, приобретающих комплексный, транснациональный характер. И далее в видеообращении следовало предложение о принятии на уровне ООН документа, закрепляющего фундаментальные принципы деятельности в киберпространстве и обеспечения безопасности этой деятельности.

В ходе дискуссии на открытом заседании Координационного совета Консорциума и было принято предложение о разработке универсальных правил поведения в информационном пространстве (или более узко – в Интернете).

Интересна оценка этого предложения Рафаэлем Перлом, главой отдела по борьбе с терроризмом ОБСЕ:

«Если не создать правил поведения, интернет со временем превратится в "Дикий Запад" – небезопасную, хаотичную среду, в которой вольготно чувствовать себя смогут только преступники. В этом смысле Россия, предложившая составить свод правил пользования мировым информационным пространством, попала прямо в точку. Платформой для обсуждения такого кодекса поведения могла бы стать Организация по безопасности и сотрудничеству в Европе (ОБСЕ). Ведь ООН, к которой апеллирует Россия, и ОБСЕ в этом плане друг друга не исключают. ООН устанавливает глобальные стандарты, ОБСЕ воплощает их на региональном уровне. При этом было бы наивно полагать, что, если удастся разработать и принять правила поведения в интернете, то все их сразу начнут придерживаться. Так обычно происходит со всеми правилами. И это не отменяет того факта, что в некоторых сферах государство и общество обоюдно заинтересованы в регулировании. Ведь сегодня фактически все, что мы делаем, зависит от киберпространства. От еды, которая попадает к нам на стол из других стран через сложную логистическую цепочку, до нашего собственного передвижения по миру. Механизмы управления государством, национальная безопасность и мировая экономика – все это немыслимо без интернета, а потому уязвимо». Один из ведущих мировых экспертов в области кибербезопасности, глава канадской компании SecDev Group, специализирующейся на сетевой безопасности, Рафал Рогозинский, рассказал, что может помешать России добиться принятия универсальных правил поведения в информационном пространстве. Он отметил, что это «очень хорошая идея. Сейчас интернет не регулируется на уровне государств, но проблемы в области безопасности у всех стран общие. Информационная сфера, как, скажем, и авиация, нуждается в каких-то правилах. Хотя киберпространство, конечно, отличается от других пространств. Здесь нужен очень деликатный дипломатический подход. Российская инициатива очень хорошая. Пройдет ли она (учитывая интересы США, Европы и других основных игроков в этой сфере)? Увидим».

В ходе дискуссии в итоге практически ушли от использования терминов «управление Интернетом (регулирование Интернета)» в контексте обеспечения информационной безопасности, что всегда несколько раздражало американских экспертов и перешли к активному использованию термина «правила поведения».

Можно считать это существенным шагом вперед для экспертного сообщества. Уже то, что все согласились с необходимостью разработки правил поведения в Интернете имеет важное значение для обеспечения безопасности информационного пространства.

Понятно, что правила разработать мало, нужны механизмы их соблюдения. Здесь часто приводят аналогию с правилами дорожного движения. Правила, конечно, можно не соблюдать, но каковы будут последствия несоблюдения. К сожалению, надеяться на массовое сознательное соблюдение правил не приходится, даже если все массово правила и выучат. Только знание последствий несоблюдения правил, может удержать многих в рамках соблюдения правил. Нужна массовая разъяснительная работа. Одним из необходимых условий соблюдения правил, является идентификация личности в информационном пространстве (в Интернете).

Западные эксперты часто в дискуссиях о целесообразности введения идентификации в Интернете, ссылаются на то, что это приведет к нарушению свободы личности, свободы слова.

Однако можно привести целый ряд примеров, когда уже сейчас практически осуществляется идентификация в информационном пространстве:

Сетевые игры и виртуальные миры.

Радиочастотные метки (RFID).

Хранение и анализ информации при переходе национальных границ.

Космический мониторинг. Информационные хранилища геоинформационных систем.

Видеонаблюдение.

Электронные медицинские карты.

Клиентские карты магазинов, супермаркетов, гостиниц, различных сервисов.

Последние представляют собой инициативы бизнеса. Основная суть – идентифицировался – получаешь скидки, льготы, бонусы и т.п.

Аналогично может поступать и государство. Идентифицируйся и упрощается взаимодействие с государством. Например, обеспечивается более эффективное для пользователя общение в рамках электронного правительства. Поэтому не нужна жесткая, обязательная схема идентификации всех в информационном пространстве. Все можно сделать в мягкой форме, используя, привлекательность бонусов, льгот и т.п. Параллельно может происходить массовая разъяснительная работа о целесообразности идентификации в информационном пространстве для обеспечения информационной безопасности личности и общества.

Если говорить о безопасности в Интернете, то важны, конечно, и технические, и технологические решения. Но самое важное – это образовательные и просветительские аспекты обеспечения безопасности. Лет двадцать-двадцать пять назад, когда в нашу жизнь активно внедрялись персональные компьютеры, появился массовый образовательный процесс – ликвидация компьютерной безграмотности. Сейчас же, использование ИКТ в нашей жизни таково, что пришло время говорить о ликвидации безграмотности в области информационной безопасности. И начинать этот массовый процесс нужно с детских садов, школ, семьи.

А.Н.ЛЕПЕХИН

ПРАВОВЫЕ МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ И ФЕНОМЕН СОЦИАЛЬНЫХ СЕТЕЙ

Современный этап развития общественных отношений характеризуется существенным преобразованием информационной сферы. Появление и постоянное совершенствование сетей и технологий передачи данных диалектически обусловили и возникновение новых способов коммуникации в современном обществе. Нисколько не оспаривая преимущества современных информационных технологий, мы должны понимать, что их развитие наносит определенный отпечаток на модель развития общества в целом и его членов в частности. Поскольку изменение привычного понимания границ общения (как территориальных так и нравственных) безусловно отразилось на индивидах современного общества.

Не в даваясь в полемику по поводу целей и причин создания информационных ресурсов, предоставляющих услуги виртуального общения и знакомства (условно предлагаем их называть социальными сетями), следует учитывать, что несмотря на их преимущества в удовлетворении потребностей членов общества в общении, он сам (человек), в принципе, не защищен в правовом плане при использовании таких социальных сетей.

Анализируя современное законодательство Республики Беларусь в части определения нормативных актов регламентирующих вопросы защиты информации, мы приходим к выводу, что одним из таких основополагающих нормативных правовых актов является Закон Республики Беларусь «Об информации, информатизации и защите информации» от

10.11.2008 г. В котором наряду с рядом прогрессивных положений, касающихся правового закрепления информационных отношений, по нашему мнению, остались не рассмотренными несколько проблемных вопросов. И, в первую очередь, это касается сферы действия этого закона.

Так, в ст.2 Закона Республики Беларусь «Об информации, информатизации и защите информации» определяется круг общественных отношений, который регулируется нормами данного закона, возникающих при:

– поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также пользовании информацией;

– создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов;

– организации и обеспечении защиты информации.

Вместе с тем, по нашему мнению, требует серьезной законодательной проработки вопрос о действии нормативных правовых актов Республики Беларусь, регулирующих отношения в информационной сфере, в пространстве. Очевидно, что Республика Беларусь, как суверенное государство осуществляет реализацию власти, в том числе и законодательной, на своей территории. Но глобальные информационные сети имеют несколько иную физическую природу (если не привязываться только к физическому расположению серверов хостинга). Поэтому определение сферы действия норм национального информационного права в пространстве является важной научной и прикладной задачей. С одной стороны, можно воспользоваться принципом аналогии права и применять нормы уголовного и административного права для определения сферы действия иного нормативного правового акта, с другой, такой подход сопряжен с рядом правовых проблем.

Как уже отмечалось, что развитие социальных сетей связано с определенными правовыми проблемами и коллизиями. Так, в соответствии со ст.29 Закона Республики Беларусь «Об информации, информатизации и защите информации» к правовым мерам по защите информации относят заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.

Вместе с тем, анализ порядка использования большинства информационных ресурсов, предоставляющих возможности виртуального общения и знакомства (социальных сетей) показал, что при регистрации (создании учтенной записи) пользователя на таком информационном ресурсе, никаких соглашений с пользователями о порядке пользования этим ресурсом и его информацией не существует. Более того, физически хостинг находится, как правило, за пределами Республики Беларусь, и соответственно возникают вопросы: «Нормами права, какой страны будут регулироваться возникающие спорные правоотношения, а в ряде случаев и разрешаться вопросы ответственности? Противоправные действия совершены с территории Республики Беларусь в отношении иностранного гражданина, в государстве которого такие действия не являются противоправными и наоборот?» И, как показывают последние тенденции, пользование социальными сетями в ряде случаев сопряжено с противоправными действиями, начиная от размещения фейковых (подложных) анкет с реальными фотографиями граждан и заканчивая совершением мошеннических действий от имени пользователя и распространения детской порнографии.

Таким образом, на данном примере мы постарались показать ту значимость, которую представляют социальные сети на современном этапе, и те правовые проблемы, которые еще предстоит решить как мировому сообществу, так и нашему белорусскому государству.

Е.Н.ЛИВАК, А.М.КАДАН

МЕДИЦИНСКИЙ СУБРЕГИСТР НАСЕЛЕНИЯ: УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ

Введение

Для решения задач формирования баз данных медицинских клинических показателей и анализа накопленной в них информации в настоящее время в Республике Беларусь применяются *разрозненные* информационные системы, связанные, как правило, с отдельными областями медицины либо функционирующими в рамках одного (нескольких) учреждений здравоохранения (структурных подразделений).

В таких системах невозможно решение задач интеграции и совместное использование данных различными медицинскими учреждениями и различных медицинских направлений. Проведенный авторами анализ информационных систем, используемых в медицинских учреждениях РБ, показывает, что они не используют технологии многомерного представления данных, допускающие оперативный и интеллектуальный анализ, что не позволяет осуществлять поиск неочевидных закономерностей и фактов, которые могли бы открыть новые возможности в профилактике и лечении целого ряда заболеваний и, в первую очередь, наследственных (онкологических).

Группой специалистов (С.Э. Савицкий, Е.Н. Ливак, А.М. Кадан) предложено создание Медицинского субрегистра населения Гродненской области – автоматизированной информационно-аналитической системы (далее – АИАС МСНГрО), основанной на *едином* электронном хранилище медицинских данных населения Гродненской области и обеспечивающей организацию (сбор, хранение), защиту и анализ медицинской информации, поиск неочевидных зависимостей и закономерностей в данных. Философия авторов – отказ от систем замкнутых ресурсов.

Основное назначение АИАС МСНГрО – интегрировать данные разрозненных баз медицинских данных; обеспечить возможность доступа, совместной обработки и анализа данных различных медицинских учреждений и направлений лечащим врачам и сотрудникам сферы управления здравоохранением; предоставить оперативный доступ к медицинской информации о пациенте в случае чрезвычайных ситуаций службам «быстрого реагирования» (скорой помощи, МЧС и другим); обеспечить доступ пациентов к персональным электронным медицинским записям (электронной истории болезни, результатам медицинских обследований и лечения); обеспечить возможность оперативного и интеллектуального анализа медицинских данных для решения задач (в том числе научных) клинической медицинской практики.

Разработка АИАС МСНГрО выполняется специалистами Гродненской областной клинической больницы, Управления здравоохранения Гродненского облисполкома и силами преподавателей и сотрудников кафедры системного программирования и компьютерной безопасности Гродненского государственного университета имени Янки Купалы.

Обеспечение безопасности – важнейшее требование к АИАС МСНГрО

Важнейшим требованием, предъявляемым к обеспечению функционирования АИАС МСНГрО, является обеспечение безопасности информационных ресурсов и поддерживающей инфраструктуры. И, прежде всего, обеспечение конфиденциальности, целостности и доступности хранимых и обрабатываемых медицинских данных.

Система должна обеспечивать законное использование персональных медицинских данных, очевидно являющихся конфиденциальной информацией. Проблема баз медицинских данных – в противоречивости организации доступа к ним (свободный/закрытый). С одной стороны, медицинские работники должны знать историю болезни пациента, результаты предыдущих обследований и лечения, сам пациент также

должен владеть информацией о своем здоровье. С другой стороны, «медицинская информация рассказывает о пациенте без прикрас: генетическая предрасположенность к болезням, аборты и репродуктивное здоровье, эмоциональное и психическое здоровье, злоупотребление наркотиками, сексуальные реакции, болезни, переданные половым путем, ВИЧ-статус, физические отклонения… После того как личная медицинская информация обнародована, людей могут беспокоить, угрожать им…» [1, с. 69]. Таким образом, в системе должен быть обеспечен контроль доступа к данным в соответствии с отношением пользователей системы к запрашиваемым данным и/или должностными обязанностями сотрудников медицинских учреждений.

Очевидно, что в системе должны быть недопустимы незаконная модификация и удаление данных (как случайное, так и умышленное с целью нанесения ущерба).

Проблемы конфиденциальности и целостности данных взаимосвязаны. Злоумышленник, незаконно получивший доступ к информации, может изменить ее. Обеспечение конфиденциальности данных помогает предотвратить их раскрытие и незаконную модификацию/удаление. Нарушение целостности данных может повлечь за собой нарушение работоспособности системы на время восстановления информации из резервных копий. Кроме того, нарушение целостности может остаться незамеченным и привести к принятию решений на основе недостоверной информации.

Управление защитой информации в АИАС МСНГрО

Управление безопасностью в системе МСНГрО не ограничивается только обеспечением защиты информации от нелегального раскрытия, использования и модификации – удовлетворением перечисленным выше требованиям к обеспечению конфиденциальности, целостности и доступности медицинских данных системы и управлением доступа к данным. Управление защитой информации в системе предусматривает также аудит событий, происходящих в системе, и действий пользователей, а также реализацию комплекса мероприятий по обеспечению невозможности обмана, в том числе, возможность определить автора и происхождение отдельных записей – аналог подписи на традиционном бумажном документе.

В целом, технологии безопасности, лежащие в основе организации защищенного хранения и обмена конфиденциальной медицинской информацией в АИАС МСНГрО, можно подразделить на следующие технологические группы:

– конфиденциальность персональных медицинских данных,

– целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения),

– доступность всех ресурсов (обеспечение уверенности в том, что законный пользователь за приемлемое время получит доступ к запрашиваемому ресурсу),

– управление доступом к ресурсам (идентификация, аутентификация, авторизация),

– невозможность обмана (идентификация авторства, невозможность отрицания акта по выполнению действий в системе),

– аудит (отслеживание ответственности за процессы).

Управление доступом включает три технологические группы: идентификацию, аутентификацию, авторизацию.

Заметим, что идентификация в системе помимо идентификации пользователей включает также идентификацию объектов (ресурсов) системы. Аутентификация - это процесс проверки одним объектом (доверенным) подлинности другого (доверителя). В качестве объектов-доверителей в системе выступают не только пользователи, но и серверы, клиенты и другие ресурсы системы. Доверенными объектами являются система в целом, базы данных, файлы, принтеры, кубы данных, элементы многомерной модели и т.п.

Подлинность пользователя устанавливается на основе ключевого сравнения. Для первоначального этапа эксплуатации системы («промышленная отладка») в качестве

эталонных идентификаторов (удостоверений) в системе приняты имена и пароли пользователей. Такое решение обосновано, с одной стороны, экономической целесообразностью; с другой стороны, учетом того, что предъявляемые к системе требования не подразумевают сверхвысокую степень конфиденциальности хранимых и обрабатываемых данных (сверхсекретные данные), и поэтому мощность механизма защиты, основанного на эталонном (ключевом) сравнении, на первом этапе является приемлемой. Развитие системы безопасности МСНГрО предполагает использование технологий, исключающих запоминание пользователем «секретной» информации, например, применение электронных ключей и/или, как минимум, хранение идентификационных кодов на внешнем носителе.

Объектами авторизации в системе являются пользователи, группы пользователей, серверы распределенной системы сбора информации. В процессе авторизации пользователя устанавливаются его права по отношению к ресурсам (данные, с которыми разрешено работать; операции, которые разрешено выполнять).

Целью аудита является сбор информации об удачных и неудачных попытках доступа к объектам, применении привилегий и других, важных с точки зрения безопасности, действиях и протоколирование этих событий для дальнейшего анализа.

Невозможность отрицания акта выполнения действий представляет собой комплекс мероприятий по обеспечению доказательства того, что то или иное действие действительно было выполнено. Такой комплекс мероприятий позволит предотвратить отказ доверителя от совершенных действий. Невозможность отрицания акта выполнения действий в системе обеспечивается проведением аутентификации, авторизации, аудита и целостности данных. Кроме того, доверитель извещается о том, что за действие, которое он собирается предпринять, он несет ответственность.

Управление защитой информации в системе МСНГрО осуществляется с помощью технологий, представленных в таблице.

Технологическая группа	Технологии
Конфиденциальность	Криптографическая защита Защищенные протоколы (SSL/TLS, IPSec)
Идентификация – субъектов – объектов (ресурсов)	Ключевое сравнение Стеганографическая защита Цифровые сертификаты Электронные ключи
Аутентификация – пользователей – ресурсов	Базовая аутентификация PIN-аутентификация Электронные ключи ЭЦП Цифровые сертификаты Защищенные протоколы (SSL/TLS)
Авторизация	Ролевой механизм Списки контроля доступа Привилегии. Разрешения. Защищенные протоколы (SSL/TLS, IPSec)
Целостность	ЭЦП Функции хэширования Защищенные протоколы (SSL/TLS, IPSec)
Аудит	Регистрационные журналы
Невозможность обмана	Стеганографическая защита Электронная цифровая подпись Журналирование

Литература

1. Шнайер, Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. — СПб.: Питер, 2003. — 386 с.

А.А.МАТВЕЕВ

АСПЕКТЫ УПРАВЛЕНИЕ ИНТЕРНЕТОМ

Сегодня информационные технологии гармонично интегрировались в жизнь общества и государства. Их использование является фоновым процессом, обеспечивающим все сферы жизни человека.

Интернет де-факто стал не только технологической основой информационных инфраструктур, но и фактором их развития, выполнения этими инфраструктурами функций информационного обеспечения экономической, социальной, политической и духовной сфер жизни общества, сферы государственного управления, обеспечения обороноспособности страны и безопасности государства. Однако совершенствование технологий приводит не только к укреплению индустриального общества, но и к появлению новых, ранее неизвестных источников опасности для него. Экономика и обороноспособность ведущих государств мира все в большей степени зависят от нормального функционирования глобальных компьютерных сетей.

Сегодня, все более очевидным становятся потенциальные возможности использования информационно-коммуникационных технологий с целью нарушения работоспособности информационных систем и информационных сетей критически важных объектов инфраструктуры общества и государства.

События последних лет (атаки на информационные системы различных государств, в том числе критически важные объекты инфраструктуры; информационные войны; утечки и распространение закрытой информации; сетевой шпионаж; локальные киберконфликты и интернет-терроризм) показали, что данные угрозы из потенциальных превратились в реальные и начинают оказывать непосредственное воздействие на национальные интересы государств.

Противодействие угрозам безопасному использованию сети Интернет, безусловно, относится к функциям государственной власти. Поэтому так важно понимание аспектов связанных с управлением Интернетом.

Управление интернетом – это не заранее регламентированный процесс, которым занимается какая-то международная организация, специализированная организация в системе ООН или неправительственная организация, подобная ICANN, чья задача – распределение доменного (адресного) пространства. Само словосочетание «управление Интернетом» не совсем привычно для большинства интернет-пользователей. Тем не менее, вопрос о регулировании сети Интернет возник еще в конце XX века и уже тогда вызвал бурное общественное обсуждение. Сегодня под управлением Интернетом понимают набор общих принципов, норм и правил, которые регулируют эволюцию и использование Интернета и помогают правительствам, бизнесу и гражданскому обществу договариваться между собой по этим вопросам. Управление Интернетом, как в мировом, так и в национальном, и региональном масштабах предполагает участие в этом процессе всех заинтересованных сторон, т.к. у каждой группы специалистов имеются собственные профессиональные взгляды и подходы в этой области. Специалисты в области телекоммуникаций во главу угла ставят развитие технологической инфраструктуры, программисты – разработку различных стандартов, языков и приложений, специалисты по коммуникациям делают акцент на упрощении обмена информацией. Политики основное внимание уделяют вопросам перспектив развития общества, связанных с развитием Интернета, и угрозам – таким, как безопасность Интернета или защита детей.

Что можно отметить в качестве приоритетных задач для регулирования интернета? Сегодня проблемы, изначально бывшие центральными в сфере управления Интернетом (вопросы функционирования ICANN), постепенно утрачивают свое значение. На их место приходят такие вопросы, как сетевая нейтральность, сближение различных технологий (например, телефонии, телевидения и Интернета), проблемы социальных сетей. Мне бы хотелось отметить три группы приоритетных вопросов, решение которых необходимо не только для обеспечения устойчивости развития, но и для оптимальности использования интернет-технологий.

Первая из них – это доступ и доступность (access и accessibility), причем речь идет о доступности и в плане технологическом, и в плане экономическом (доступная цена), и в плане обеспечения свободы информации, равного доступа к ресурсам, в плане преодоления информационного неравенства.

Вторая задача – это безопасность использования интернета. Как и в любом новом явлении, в бурном развитии интернета есть как позитивные, так и негативные стороны. К сожалению, очень часто на первый план выходит негатив: мошенничество, порнография, возможность совершения разнообразных правонарушений. Необходимо, видимо, прямо сейчас (что, собственно, уже и происходит) уделить пристальное внимание в нашем взаимодействии на уровне государства, гражданского общества и бизнеса именно этому аспекту, то есть недопущению использования интернета в антиобщественных целях.

И, наконец, третья задача связана с таким важным вопросом, как интернационализация интернета. Интернет первоначально зародился на территории Соединенных Штатов и когда-то был практически стопроцентно англоязычным. Сейчас ситуация резко меняется. Именно с помощью интернационализации можно использовать преимущества, которые дают интернет-технологии в каждой конкретной стране, в том числе и в нашей. Речь идет о создании многоязычных ресурсов (информационный контент), что активно и происходит на наших глазах. Значит, вопрос многоязычного контента – вопрос международного участия в управлении интернетом.

Управление Интернетом должно сохранить существующую функциональность и надежность Интернета и вместе с тем оставаться достаточно гибким для внесения изменений в интересах расширения технических возможностей и повышения легитимности. Это возможно только при комплексном подходе, включающем технические, правовые, социальные и экономические аспекты. В процессе трансформации системы управления Интернетом важно не потерять то позитивное, что свойственно существующей системе управления. Эта система за сравнительно небольшой срок – около 20 лет – позволила добиться превращения сети в глобальную информационную инфраструктуру, содействовала становлению новых отраслей экономической деятельности, революционному изменению технологий информационного взаимодействия граждан, их общения с государством, становлению принципиально нового механизма распространения массовой информации, изменению технологий социального единения людей, повышению роли и значения общественных организаций, транспорентности власти и, соответственно, усилению ее зависимости от общества.

Проблема совершенствования системы управления Интернетом не имеет легких решений, но эти решения во многом определят потенциал дальнейшего развития сети Интернет на стратегическую перспективу.

Литература

1. Курбалийя Й. Управление Интернетом / *Координационный центр национального домена сети Интернет* - М.: Москва.-2010.

2. Окинавская Хартия глобального информационного общества // Дипломатический вестник.– 2000. – № 8.

А.В.ТЕСЛЮК

ЗАЩИЩЕННЫЙ ХОСТИНГ. ТЕОРИЯ И ПРАКТИКА ЕГО ПОСТРОЕНИЯ ДЛЯ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ОРГАНИЗАЦИЙ, ИСПОЛЬЗУЮЩИХ В СВОЕЙ ДЕЯТЕЛЬНОСТИ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННЫЕ СЕКРЕТЫ

Информационное общество – современный этап развития цивилизации с доминирующей ролью знаний и информации, воздействием информационно-коммуникационных технологий на все сферы человеческой деятельности и общество в целом.

Развитие информационного общества является одним из национальных приоритетов республики и рассматривается как общенациональная задача, требующая объединения усилий государства, бизнеса и гражданского общества. При этом информационно-коммуникационным технологиям отводится роль необходимого инструмента социально-экономического прогресса, одного из ключевых факторов инновационного развития экономики.

В настоящее время в республике завершилось формирование основ информационного общества. Заложена правовая основа информатизации. Успешно развивается национальная информационно-коммуникационная инфраструктура, позволяющая оказывать новые телекоммуникационные и информационные услуги на основе технологий широкополосного доступа. На протяжении последних 15 лет в результате выполнения государственных программ разработан ряд общегосударственных и ведомственных информационных систем, создана национальная система формирования и регистрации информационных ресурсов. Значительная часть республиканских органов государственного управления, облисполкомов и большинство райисполкомов представлены в сети Интернет.

Современные Интернет технологии предоставляют широкие возможности обществу и государству. Одним из возможных способов использования Интернет технологий является создание и использование сайтов в сети Интернет. Такая деятельность связана с рисками различного рода, в том числе и рисками нарушения информационной безопасности. Нарушение информационной безопасности может произойти как по причине активных действий нарушителя, так и по причине пассивного бездействия лица, не предпринимающего адекватных мер к обеспечению информационной безопасности, в результате чего собственнику интернет-сайта или иному физическому или юридическому лицу, обществу в целом или государству может быть причинен серьезный ущерб. Сложность обеспечения адекватных мер информационной безопасности определяется быстрым развитием Интернет технологий и появлением новых видов угроз. В связи с этим особое значение приобретают вопросы информационной безопасности интернет-сайтов государственных органов и организаций, так как они в свое время являются лицом страны.

Противодействие угрозам безопасному использованию сети Интернет, безусловно, относится к функциям государственной власти.

Так в соответствии с пунктом 13 Указа Президента Республики Беларусь от 1 февраля 2010 г. №60 «О мерах по совершенствованию использования национального сегмента сети Интернет» специально уполномоченным государственным органом в сфере безопасности использования национального сегмента сети Интернет определен Оперативно-аналитический центр при Президенте Республики Беларусь.

В соответствии с пунктом 7 вышеназванного Указа Президента Республики Беларусь государственным органам и организациям, использующим в своей деятельности сведения,

составляющие государственные секреты, интернет-услуги оказываются поставщиками интернет-услуг, определяемыми ОАЦ по согласованию с Президентом Республики Беларусь.

В соответствии с Положением о порядке определения поставщиков интернет-услуг, уполномоченных оказывать интернет-услуги государственным органам и организациям, использующим в своей деятельности сведения, составляющие государственные секреты, утвержденным приказом ОАЦ от 2 августа 2010 г. № 60, в августе была проведена оценка соответствия возможностей обратившихся в ОАЦ поставщиков интернет-услуг.

Проект перечня уполномоченных поставщиков интернет-услуг был внесен на согласование Президенту Республика Беларусь и после согласования утвержден приказом ОАЦ от 17 декабря 2010 №92.

Уполномоченные поставщики интернет-услуг при оказании интернет-услуг обеспечивают защиту информации указанных государственных органов и организаций.

Вопросы защиты информации в государственных органах и организациях не так просты для реализации в комплексе, однако введение дополнительных мер защиты со стороны уполномоченных поставщиков интернет-услуг значительно снижает риски нарушения информационной безопасности в информационных системах государственных органов и организаций.

Г.И.ШЕРСТНЁВА

О СПЕЦИФИКЕ «ИНФОРМАЦИОННОГО ОРУЖИЯ»

В современных условиях расширились возможности использования информационно-коммуникационных технологий (ИКТ) в целях, несовместимых с задачами поддержания международной стабильности и безопасности, соблюдения принципов отказа от применения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека.

Особые опасения в этом плане вызывают разработка, применение и распространение так называемого «информационного оружия», в результате которых становятся возможны информационные войны, способные вызвать разрушительные мировые катастрофы.

Специфика «информационного оружия» заключается в том, что при враждебном использовании ИКТ речь не идет о применении оружия в его традиционном понимании, поскольку ИКТ в основном являются гражданскими технологиями или технологиями двойного назначения. Тем не менее, последствия их враждебного использования могут быть сопоставимы по своим масштабам с ущербом от применения «классического» оружия и даже оружия массового уничтожения. Информоружие не знает географических расстояний, оно подрывает традиционное понятие государственных границ, делая их технологически проницаемыми. Его применение носит обезличенный характер и позволяет замаскировать разрушительную по своим масштабам информационную операцию, проведенную государством, под киберпреступление, например, в виде нападения хакера, или акт кибертерроризма, реализованный международными террористами. Одновременно трудно определить государство, осуществившее информационную атаку, поскольку агрессия может реализовываться с территории третьих стран.

Особую опасность представляет разработка специалистами по информационной войне вопросов целенаправленного воздействия и преобразования сознания всего населения страны-противника или его отдельной части, например Вооруженных Сил, а не сознания отдельного индивидуума.

В качестве такой комплексной формы воздействия на народ и государство в целом рассматривается оружие «поражения сознания» или так называемое «консциентальное оружие». Достаточно полно этот вид оружия и последствия его применения для России

рассмотрены в сборнике под общей редакцией доктора психологических наук Ю.В. Громыко (см. «Кому будет принадлежать консциентальное оружие в 21 веке?, М., «Россия - 2010»,1997г.

По мнению авторов данного труда, основная функция такого оружия состоит в том, чтобы разложить и уничтожить народ данной страны, чтобы он перестал существовать как народ, разбившись на индивидов-граждан всего мира или на какие-то другие аморфные группы. То есть, впервые сознание населения страны и военнослужащих ее армии превращается в отдельный четко выделяемый предмет воздействия и преобразования со стороны противника.

Специфика применения информационного оружия основана на сочетании ИТ - технологий и приемов воздействия на психику человека. В изучении такого информационно-психологического воздействия представляют интерес исследования в уже весьма обширной междисциплинарной области, лежащей на границе безопасности и психологии. Как показывает анализ, в этой области происходит интересный и содержательный диалог между психологами и специалистами по безопасности. Что же в этом взаимодействии важного и чем оно так интересно?

Например, при взгляде на проблему в макромасштабе можно отметить, что чрезмерная реакция общества на угрозы терроризма основана на неправильной оценке рисков и чувстве неопределенности, имеющем глубокие психологические корни. Для ситуации в США, в частности, исследователи подсчитали, что если даже принимать во внимание резкий всплеск – все жертвы атак 9/11,то от рук международных террористов американцы гибнут не чаще, чем от удара молнии. Или в автомобильных авариях из-за случайного столкновения с животными. Или от аллергической реакции на арахис. Или, наконец, жертв террора лишь немногим больше, чем несчастных, утонувших в ванне.

Переводя общие наблюдения на микроуровень повседневной жизни, специалисты отмечают, что подобного рода заблуждения успешно используются злоумышленниками. Многие из реальных атак на информационные и физические системы эксплуатируют психологию в большей степени, нежели технологии. Формулируя чуть иначе, все больше и больше преступлений включают в себя элементарный или изощренный обман. По мере того как технологии безопасности становятся все лучше и совершеннее, зачастую куда легче оказывается вводить в заблуждение людей, чем взламывать компьютеры или отключать сигнализацию в зданиях.

В 2002 году известный специалист по криптографии и компьютерной безопасности Брюс Шнайер написал книгу «Beyond Fear» («Без страха. Здравые рассуждения о безопасности в переменчивом мире») (см. Psychology and Security Resource Page (www.cl.cam.ac.uk/~rja14/psysec.html).

Явно под впечатлением от тех серьезных перемен, что произошли в западном мире и, особенно в США после событий 11 сентября 2001 года американец Шнайер доказывал свою «непопулярную» и крайне непатриотичную по тем временам позицию, обратим внимание на один из важнейших психологических факторов – страх, с помощью которого тогдашняя госадминистрация получила от общества практически все желаемые полномочия и уступки.

Фактор страха как был, так и остается одним из важнейших инструментов при манипуляциях человеческим сознанием, будь то в политике, бизнесе или в подаче новостей средствами массовой информации.

Понятно, что тема страхов человеческих имеет самое непосредственное отношение и к теме «психология и безопасность».

Одна из причин, по которой современные люди боятся так много и часто, заключается в том, что доминировать в их жизни стали состязающиеся группы продавцов страха, каждая из которых имеет свои собственные интересы, однако все они подкрепляют свои заявления и продают товары через страх. Политики и средства массовой информации, бизнес-корпорации и организации по защите окружающей среды, представители здравоохранения и

разнообразные группы «защиты прав» непрерывно предупреждают обывателей о появлениях все новых и новых напастей, коих непременно следует бояться.

Психологические реакции испуга, исподволь взращиваемые в людях, проявляются в самых обычных житейских ситуациях.

Хрестоматийным примером злоупотреблений и спекуляций на страхах человеческих в области ИТ стала так называемая «проблема 2000», которую старательно расписывали как предвестника глобальной техногенной катастрофы. Масштабы этой международно скоординированной акции и миллиарды выделенных под нее долларов беспрецедентны для эпохи компьютеров. Лишь немногие ИТ-эксперты находили смелость поставить под сомнение всю эту чрезмерную активность с раздуванием угроз.

Таким образом, исследования людей, занимающихся разработкой практичных систем защиты и разнообразных протоколов обеспечения безопасности, с одной стороны, и специалистов из таких областей, как социальная психология, эволюционная биология и поведенческая экономика,– с другой, все больше становятся одной из активных точек контакта между компьютингом и психологией. Опыт же свидетельствует, что подобный обмен всегда был крайне полезен для обеих дисциплин.

И еще один аспект применения информационного оружия.

Максимальный эффект от применения оружия «поражения сознания», в отличие от эффектов действия других форм информационно-психологического воздействия, достигается в условиях формального мира и так называемых локальных войн и конфликтов, Это обусловлено тем, что в данных условиях большинство населения страны не осознает тот глобальный стратегический сценарий, в рамках которого государство участвует в противоборстве геополитических сил на мировой арене для достижения своих национальных интересов. Поэтому у населения не выработано отношение к данному сценарию и практическим шагам государства по его претворению в жизнь. В этом случае действия отдельных лиц государства или групп граждан, выходящие за рамки данного глобального сценария, могут восприниматься в обществе как свободное личное поведение или «самовыражение» в рамках существующей свободы слова, а не как целенаправленные действия, обусловленные уничтожением у них определенной формы сознания и заменой ее другой, искусственно формируемой противником, формой. Однако появление лиц с «замещенным» сознанием в высших органах государственного и военного управления при существующей иерархической централизованной структуре системы управления может привести к катастрофическим последствиям.

Ю.А.ШЕРСТНЕВА

ЭВОЛЮЦИЯ СТРАТЕГИИ, СРЕДСТВ И МЕТОДОВ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Анализ тенденций развития современной стратегии, средств и методов информационного противоборства, направлений деятельности силовых структур ведущих стран мира, в первую очередь США, позволяет говорить о продолжающемся усилении угроз безопасности России, в том числе в информационной сфере.

Россия остается в числе ведущих стран мира, в отношении которой размах действий по подрыву ее безопасности, несмотря на усилия руководства РФ по укреплению экономического и военно-политического статуса, постоянно нарастает.

Нынешняя американская администрация значительно активизировала деятельность на российском пространстве по укреплению возникших здесь структур гражданского общества, которые за последние годы получили статус общегосударственных структур, с которыми

руководство страны ведет активный диалог в отношении направлений развития общества. Ей удалось значительно укрепить позиции в международной информационной сфере, где наблюдается редкое единодушие американских, западных и некоторых российских СМИ в освещении событий на международной арене и внутри России.

Интернет-пространство все чаще становится площадкой, где формируется общественное мнение, что делает его привлекательным объектом информационно-пропагандистской деятельности.

Прошедшие за десятилетие «цветные революции» показывают все возрастающую роль использования информационных технологий в социальных процессах. В связи с этим значительное количество пользователей сети Интернет в РФ создает предпосылки целенаправленного управления ими с помощью социальных сетей, в том числе путем распространения экстремистских материалов и организации массовых выступлений и беспорядков, что подтвердили молодежные волнения в декабре 2010 г. на Манежной площади в Москве и в ряде других городов РФ - Ставрополе, Ростове-на-Дону, Волгограде, Санкт-Петербурге, Самаре, Челябинске.

Созданное при Госдепартаменте США Бюро международных информационных программ постоянно расширяет свое присутствие в вебпространстве и увеличивает количество проектов, используя для «общения с молодежью на интересующие их темы» социальные сети и социальные СМИ.

В результате осмысления агрессии стран Запада против Ливии и освещения событий средствами массовой информации, экспертами был сделан однозначный вывод о целенаправленном использовании СМИ в информационной войне против Ливии. Высказывается мнение, что на Ливии отрабатывается новый сценарий «цветных революций», заключающийся в создании на основе вымышленной информации (не существующие события, фальсифицированные причинно-следственные связи, заранее подготовленные «свидетели», «герои» и «эксперты») сюжетов, формирующих негативный образ государства-жертвы, внедрении их через глобальные СМИ в сознание мирового общественного мнения, принятии на этой основе реальных санкций и осуществления реальных боевых операций, заключающихся как в точечных ударах по ключевым объектам инфраструктуры, так и в полномасштабном вторжении «миротворческих сил».

Необходимо учесть, что за последние десять лет информационное противоборство из теоретических конструкций и отдельных элементов превратилось в реальное оружие, все чаще использующееся в информационном пространстве как средство прямого достижения цели. Кибертеррористические действия и некоторые виды киберпреступлений фактически перешли в разряд военных угроз и приобрели принципиально новое стратегическое значение, сопоставимое по форме и последствиям с применением оружия массового поражения. Эксперты отмечают значительный количественный рост компьютерных преступлений и вирусных атак, масштабность и высокую технологичность их исполнения, высокую потенциальную опасность их последствий, связанных со значительным количеством жертв, снижением уровня обороноспособности и безопасности государства, возможностью разрушения опасных производств и т.д. Этому способствует неразработанность законодательных норм для противодействия кибератакам вследствие их трансграничности, анонимности и латентности.

США приступили к выработке новых подходов к ведению информационного противоборства на основе концепции кибернетической мощи государств (cyberpower) - способности использовать киберпространство в своих интересах для создания в нем преимуществ и возможностей влияния на ситуацию в военно-политической, экономической, информационной и других областях.

В 2011 г. США планируют принять новую доктрину кибербезопасности, построенную на принципах «управления рисками» (баланса потенциальных угроз и затрат по их нейтрализации), в соответствии с главной идеей которой киберпространство считается таким

же потенциальным полем боя, как суша, море и воздух. В октябре 2010 г. начало официальную работу киберкомандование США (US Cyber Command), общая численность которого будет составлять свыше 10 тыс. чел.

Лиссабонский саммит НАТО 2010 г. отметил необходимость разработки стратегии деятельности Альянса в киберпространстве как важного аспекта обеспечения безопасности стран-членов НАТО и партнеров. На состоявшемся 10-11 марта 2011 г. в Брюсселе саммите министры обороны стран НАТО одобрили замысел новой концепции кибероборонь НАТО и обновленную политику киберзащиты, главными задачами которых будут защита политической, экономической и военной инфраструктур стран-членов НАТО от проникновения и разрушения, а также осуществление ответных действий. К декабрю 2012 г. планируется ввод в эксплуатацию центра оперативного реагирования на киберинциденты, под которыми понимаются политически мотивированные атаки кибератывистов и хакеров, кибершпионаж, нанесение ущерба сетям НАТО. Предполагается проведение совместных учений по киберзащите и конференций.

Польша также подтвердила свое намерение занять ведущую роль в запланированной НАТО многонациональной инициативе по кибероборонe, выдвинутой в целях координации усилий и снижения затрат на построение национальных систем обеспечения кибербезопасности.

На прошедшей в феврале 2011 г. мюнхенской конференции по безопасности Великобритания объявила свои планы финансирования национальной программы кибербезопасности в размере 650 млн. ф. ст. и призвала разработать единую стратегию, определяющую векторы международного сотрудничества в построении систем киберзащиты. Также будет создана группа оборонительных кибероперацийи новый центр контроля глобальных операций и безопасности, осуществляющий мониторинг кибератак на военные системы.

Военизированные киберподразделения созданы в США, Великобритании, Франции, Германии, Китае, Индии, Израиле, Австралии, Северной Корее и др.

Повышенную озабоченность вызывают целевые атаки на объекты критической инфраструктуры. Обнаруженный в июне 2010 г. вирус Stuxnet был внедрен в системы сбора данных и оперативного диспетчерского управления стратегическими объектами атомной промышленности Ирана. Эксперты утверждают, что это первый программный продукт, способный физически вывести из строя промышленное оборудование.

Вместе с тем, проведенный в конце 2010 г. корпорацией Symantec опрос 51 российской компании показал, что в России уровень защиты от киберугроз на российских предприятиях стратегических отраслей промышленности значительно ниже, чем в среднем по миру – более половины их них не обеспечивают должных мер информационной безопасности.

РАЗДЕЛ 3
ВОПРОСЫ КРИПТОГРАФИИ

С.В.АГИЕВИЧ

СХЕМА ШНОРРА С УКОРОЧЕННОЙ ЭЦП И ПРЕДВАРИТЕЛЬНЫМ ХЭШИРОВАНИЕМ

Схема

Схемой электронной цифровой подписи (ЭЦП) в современной криптографии принято называть набор из трех алгоритмов: Gen, Sign и Verify.

Алгоритм Gen является вероятностным. Он берет на вход параметр безопасности l и выдает долговременные параметры $params$, личный ключ d и соответствующий ему открытый ключ Q. Параметр l определяет размерности долговременных параметров и ключей. Чем больше l, тем выше уровень стойкости алгоритмов ЭЦП.

Алгоритм Sign также является вероятностным. Алгоритм берет на вход сообщение X, долговременные параметры $params$, личный ключ d и выдает электронную цифровую подпись s.

Алгоритм Verify берет на вход сообщение X, долговременные параметры $params$, открытый ключ Q, подпись s и выдает результат ДА или НЕТ. Ответ ДА означает, что подпись к сообщению X была выработана с использованием личного ключа d и сообщение X не было изменено с момента выработки подписи. Ответ НЕТ означает противное.

Схема ЭЦП является корректной, если равенство

$$\text{Verify}(X, params, Q, \text{Sign}(X, params, d)) = \text{ДА}$$

выполняется для любых допустимых сообщений X и троек $(params, d, Q)$, полученных с помощью алгоритма Gen.

Схема Шнорра [5] является одной из наиболее эффективных и теоретически обоснованных схем ЭЦП. На ее основе построен стандарт Республики Беларусь СТБ 1176.2-99, южнокорейские стандарты KCDSA и EC-KCDSA.

В работе предлагается следующая редакция схемы Шнорра:

1. Алгоритм Gen по заданному уровню стойкости l строит аддитивную группу и находит ее элемент G, который имеет порядок q, $2^{2l-1} < q < 2^{2l}$. Элемент G порождает циклическую группу $\langle G\rangle = \{0, G, 2G, \ldots, (q-1)G\}$.

Алгоритм Gen определяет также функции хэширования $h: \mathsf{X} \to \{0,1,\ldots,2^{2l}-1\}$ и $\varphi: \{0,1,\ldots,2^{2l}-1\} \times \langle G\rangle \to \{2^l, 2^l+1, \ldots, 2^{l+1}-1\}$. Здесь X – множество допустимых сообщений X.

Личный ключ d выбирается наудачу из множества $\{1,2,\ldots,q-1\}$. Открытый ключ определяется как $Q = dG$.

2. Алгоритм Sign состоит из следующих шагов:

a) выбрать наудачу k из множества $\{1,2,\ldots,q-1\}$;

b) $R \leftarrow kG$;

c) $s_0 \leftarrow \varphi(h(X), R)$;

d) $s_1 \leftarrow (k - s_0 d - h(X)) \bmod q$;

e) возвратить (s_0, s_1).

По окончании алгоритма $s_0 Q + (s_1 + h(X))G = (s_0 d + k - s_0 d - h(X) + h(X))G = R$ и, следовательно,

$$\varphi(h(X), s_0 Q + (s_1 + h(X))G) = s_0. \quad (*)$$

3. В алгоритме Verify подпись $s = (s_0, s_1)$ к сообщению X признается действительной, если выполняется равенство (*).

Обсудим особенности предлагаемой схемы.

Длина ЭЦП. Первая часть подписи (s_0) кодируется l-битовым словом, вторая часть (s_1) – $2l$-битовым словом и в целом длина ЭЦП составляет $3l$ битов. Для сравнения, в стандартах СТБ 1176.2-99, ГОСТ Р 34.11-1994, ГОСТ Р 34.10-2001, DSA, ECDSA, KCDSA, EC-KCDSA на паритетных уровнях стойкости вырабатывается $4l$-битовая подпись. Отметим, что самую короткую на сегодняшний день подпись – $2l$ битов – дает схема, предложенная в работе [2]. К сожалению, схема не получила широкого распространения, поскольку при выработке и проверке ЭЦП приходится выполнять трудоемкие вычисления, связанные со спариваниями Вейля на эллиптических кривых.

Уменьшение длины ЭЦП связано с «обрезкой» s_0 с $2l$ до l битов относительно СТБ 1176.2-99, KCDSA и других известных реализаций схемы Шнорра. Фактически «обрезка» была введена в [5], но в дальнейшем по непонятным причинам от нее отказались. Отметим, что в недавней работе [3] «обрезка» была рекомендована как способ повышения эффективности схемы Шнорра при сохранении криптографической стойкости.

«Обрезка» s_0 не только сокращает длину ЭЦП, но и ускоряет вычисление $s_0 Q + (s_1 + h(X))G$ при проверке подписи. Например, при использовании бинарных методов нахождения кратных элементов группы $\langle G \rangle$ проверка ЭЦП будет выполняться примерно на 8% медленнее выработки. Для сравнения, без «обрезки» проверка замедляется на 17%.

При «обрезке» время построения коллизии для φ уменьшается до $O(2^{l/2})$ операций. В связи с этим в выражение для определения s_1 и в проверочное соотношение (1) введены слагаемые $\pm h(X)$. Если бы этих слагаемых не было, то владелец личного ключа смог бы построить одинаковые подписи для двух различных сообщений X и X' за время порядка $2^{l/2}$. Впоследствии владелец мог бы отказаться от факта подписания X', утверждая, что подписывал X. Для проведения атаки владелец выбирает различные X и X' и случайное k до тех пор, пока не будет построена коллизия $\varphi(h(X), kG) = \varphi(h(X'), kG)$. При этом числа $s_0 = \varphi(X, kG)$ и $s_1 = (k - s_0 d) \bmod q$ образуют действительную ЭЦП как для X, так и для X'.

Предварительное хэширование. В алгоритмах Sign и Verify сообщение X предварительно хэшируется с помощью функции h. Предварительное хэширование упрощает встраивание алгоритмов ЭЦП в современные информационные системы. Дело в том, что программные интерфейсы таких систем построены по принципу hash-and-sign. Это значит, что на вход программных функций, реализующих алгоритмы ЭЦП, подаются не сами сообщения X, а их хэш-значения $h(X)$. Например, функция выработки ЭЦП программного интерфейса Microsoft CSP так и называется: CPSignHash («подписать хэш-значение»).

Стойкость

Схема ЭЦП считается криптографически надежной, если для нее вычислительно трудно решить задачу «единичная подделка». Противник, который решает данную задачу, получает в свое распоряжение гипотетическое устройство (назовем его *π-ящиком*), реализующее алгоритмы Gen, Sign, Verify. До передачи π-ящика противнику выполнен

алгоритм Gen и выходные данные алгоритма использованы для инициализации устройства: в защищенной памяти π-ящика сохранен личный ключ d, а в открытой памяти сохранены параметры $params$ и открытый ключ Q. Противник может читать открытую память, т. е. противник знает $params$ и Q.

Алгоритмы Sign, Verify доступны противнику через *оракулов* S и V. В криптографической литературе под оракулом понимается вспомогательный алгоритм, который выполняется за один шаг работы основного алгоритма. Другими словами, при оценке трудоемкости атак противника время работы оракула не учитывается, учитывается только число обращений к нему. Входные данные, которые передаются оракулу, называются вопросом, выходные – ответом.

Оракул S получает вопрос X, читает из памяти $params$ и d и возвращает ответ $\mathrm{Sign}(X, params, d)$. Оракул V получает вопрос (X, s_0, s_1), читает из памяти $params$ и Q и возвращает ответ $\mathrm{Verify}(X, params, Q, (s_0, s_1))$.

Противник может задавать оракулам любые вопросы, получать и анализировать ответы. Задача «единичная подделка» состоит в построении вопроса (X, s_0, s_1) такого, что

1) $V(X, s_0, s_1) = $ ДА;

2) вопрос X до этого не задавался оракулу S.

Будем считать, что противник – это некоторый вероятностный алгоритм A. Работа алгоритма заканчивается формированием искомого вопроса (X, s_0, s_1), обращением к V с этим вопросом и возвратом соответствующего ответа. Пусть $\mathbf{Adv}(A)$ – вероятность того, что будет получен ответ ДА.

При обосновании стойкости требуется показать, что для любого противника A с разумными ограничениями на его ресурсы, вероятность $\mathbf{Adv}(A)$ мала. Для этого доказывают, что алгоритм A, который решает задачу «единичная подделка», может быть преобразован (с незначительными издержками) в алгоритм, который решает другую задачу T. В таких случаях говорят, что задача T редуцируется к задаче «единичная подделка». Редукция означает, что если T – трудная задача, то «единичная подделка» также трудная задача.

В качестве T используем составную задачу $\mathrm{DL}(G) \vee \mathrm{Coll}(h)$ (решить $\mathrm{DL}(G)$ или $\mathrm{Coll}(h)$), в которой

1) $\mathrm{DL}(G)$ – задача дискретного логарифмирования в $\langle G \rangle$: по G и $R \in \langle G \rangle$ определить $k \in \{0,1,\ldots,q-1\}$ такое, что $R = kG$;

2) $\mathrm{Coll}(h)$ – задача построения коллизии для h: найти различные $X, X' \in \mathsf{X}$ такие, что $h(X) = h(X')$.

Если $\langle G \rangle$ и h выбраны как криптографически надежные группа и хэш-функция соответственно, то для решения каждой из задач требуется время порядка 2^l.

Следующая теорема определяет редукцию $\mathrm{DL}(G) \vee \mathrm{Coll}(h)$ к задаче «единичная подделка» в модели ROM (Random Oracle Model). В этой модели π-ящик снабжается еще одним оракулом H, который реализует вычисление значений φ. К оракулу H обращаются оракулы S и V когда им необходимо получить значение φ. Модель ROM идеализирует функцию φ: оракул H выбирает ответ на каждый новый вопрос случайно равновероятно независимо от других ответов.

При доказательстве теоремы использован подход к получению редукционистских выводов, сформированный в [4]. Похожая теорема сформулирована в [3] для классической схемы Шнорра (без предварительного хэширования).

Теорема. Пусть алгоритм A с вероятностью $\mathbf{Adv}(A)$ решает задачу «единичная подделка» в модели ROM, используя β_H обращений к оракулу H и β_S обращений к оракулу S. Пусть $\varepsilon = (\beta_H\beta_S + \beta_S(\beta_S - 1)/2)/q < 1$. Тогда существует алгоритм B, который с вероятностью

$$\mathbf{Adv}(B) \geq \mathbf{Adv}(A)\left(\frac{\mathbf{Adv}(A)}{\beta_H} - \frac{1}{2^l}\right)(1-\varepsilon)^2$$

решает $\mathrm{DL}(G) \vee \mathrm{Coll}(h)$, используя 2 обращения к A и еще $O(\beta_H + \beta_S)$ операций.

Литература

1. Bellare M., Neven G. Multi-signatures in the plain public-key model and a general forking lemma // In: ACM CCS 06, ACM Press, 2006, 390–399.
2. Boneh D., Lynn B., Shacham H. Short Signatures from the Weil Pairings // Advances in Cryptology – ASIACRYPT'01 Proceedings, LNCS 2248, 514-532, 2001.
3. Neven G., Smart N. P., Warinschi B. Hash Function Requirements for Schnorr Signatures // Journal of Mathematical Cryptology, vol. 3, no. 1, 2009, 69–87.
4. Pointcheval D., Stern J. Security arguments for digital signatures and blind signatures // Journal of Cryptology, vol. 13, no. 3, 2000, 361–396.
5. Schnorr C. P. Efficient Signature Generation by Smart Cards // J. Cryptology, vol. 4, no. 3, 1991, 161–174.

А.Н.ГАЙДУК

АНАЛИЗ АЛГОРИТМА A5/1 АЛГЕБРАИЧЕСКИМИ МЕТОДАМИ

Базовый принцип алгебраического криптоанализа восходит к работе Шенона, и состоит в том, что генератор двоичных последовательностей представляется в виде системы алгебраических уравнений относительно секретного параметра. Требование высокой степени входящих в систему уравнений является одним из главных критериев при оценки стойкости генератора к алгебраическим атакам, поскольку сложность решения системы зависит от степени уравнений. Современный подход к построению генераторов двоичных последовательностей основан на использовании линейных регистров сдвига и различных способах повышения нелинейности выходной последовательности генератора. В [1] отмечаются два способа повышения нелинейности выходных последовательностей генераторов основанных на линейных регистрах сдвига. Согласно первому способу, выходная последовательность генерируется как нелинейная функция от состояния линейного регистра сдвига. Другим способом повышения нелинейности выходной последовательности является использование регистров сдвига с неравномерным движением. Управление движением регистров в таких генераторах производится специальным управляющим регистром, либо функцией управления. Техника алгебраических атак различна, для разных видов генераторов (например, фильтрующих генераторов и самосинхронизирующихся генераторов). Алгебраические атаки на фильтрующие генераторы с памятью и без исследовались в работах [2,3,4,5,6]. Алгебраические атаки на генераторы с самоуправлением изучались в работе [7].

Описание алгоритма A5/1

Поточный алгоритм A5 используется в системе GSM для шифрования канала связи между телефоном и базовой станцией. Существует две версии алгоритма A5: более сильная

версия A5/1 и более слабая версия A5/2. Хотя описание алгоритмов не было официально опубликовано консорциумом GSM, в 1994 году Р. Андерсен привел описание алгоритма A5/1, которое было уточнено в работе Брисено [8] в 1999 году.

Криптоалгоритм A5/1 состоит из трех линейных регистров сдвига с обратной связью $LFSR_1, LFSR_2, LFSR_3$ длин $l_1 = 19, l_2 = 22, l_3 = 23$ бит. Обозначим через $g_i(x)$ полином обратной связи для регистра $LFSR_i, i = 1,...,3$. В алгоритме A5/1 полиномы обратной связи имеют следующий вид: $g_1(x) = x^{19} + x^5 + x^2 + x + 1$, $g_2(x) = x^{22} + x + 1$, $g_3(x) = x^{23} + x^{15} + x^2 + x + 1$. Обозначим $S_i(t) = (s_{i,0}(t),...,s_{i,l_i-1}(t)) \in V_{l_i} \setminus O_{l_i}$ – состояние $LFSR_i, i = 1,...,3$, где через V_r обозначено r-мерное пространство на полем $GF(2)$, O_r – нулевой вектор из V_r .

Для управления движением регистров в алгоритме A5/1 используется функция $F(s_{1,8}(t), s_{2,10}(t), s_{3,10}(t)) = s_{1,8}(t)s_{2,10}(t) + s_{1,8}(t)s_{3,10}(t) + s_{2,10}(t)s_{3,10}(t)$, где $s_{1,8}(t), s_{2,10}(t), s_{3,10}(t)$ биты съема регистров $LFSR_1, LFSR_2, LFSR_3$ в текущий момент времени t соответственно. Регистр $LFSR_i, i = 1,...,3$ алгоритма сдвигается в случае, если значение бита съема данного регистра совпадает со значением функции $F(s_{1,8}(t), s_{2,10}(t), s_{3,10}(t))$.Обозначим $c_1(t) = F(s_{1,8}(t), s_{2,10}(t), s_{3,10}(t)) + s_{1,8}(t) + 1, c_2(t) = c_1(t) + s_{1,8}(t) + s_{2,10}(t), c_3(t) = c_1(t) + s_{1,8}(t) + s_{3,10}(t)$, тогда $c(t) = (c_1(t), c_2(t), c_3(t))$ – вектор управления, где $c_i(t)$ управляет движением регистра $LFSR_i, i = 1,...,3$ в момент времени t. Заметим, что $c(t)$ принимает только 4 различных значения. Уравнение для выходного символа в момент времени t имеет вид:

$$z(t) = s_{1,18}(t) + s_{2,21}(t) + s_{3,22}(t). \quad (1)$$

Постановка задачи. Для заданного момента времени t требуется оценить число переменных, количество мономов и степень уравнения для элементов выходных последовательностей $s_{1,18}(t), s_{2,21}(t), s_{3,22}(t)$.

Запишем уравнение для выходных символов каждого из регистров в момент времени t, используя биты съема:

$$s_{1,18}(t) = (s_{1,8}(t-1) + s_{2,10}(t-1))(s_{1,8}(t-1) + s_{3,10}(t-1))(s_{1,18}(t-1) + s_{1,17}(t-1)) + s_{1,17}(t-1), \quad (2)$$

$$s_{2,21}(t) = (s_{1,8}(t-1) + s_{2,10}(t-1))(s_{2,10}(t-1) + s_{3,10}(t-1))(s_{2,21}(t-1) + s_{2,20}(t-1)) + s_{2,20}(t-1), \quad (3)$$

$$s_{3,11}(t) = (s_{2,10}(t-1) + s_{3,10}(t-1))(s_{3,10}(t-1) + s_{1,8}(t-1))(s_{3,21}(t-1) + s_{3,20}(t-1)) + s_{3,20}(t-1). \quad (4)$$

Лемма 1. Для момента времени $t = 1,...,9$ уравнения для элементов выходных последовательностей $s_{1,18}(t), s_{2,21}(t), s_{3,22}(t)$ регистров $LFSR_1, LFSR_2, LFSR_3$ зависят от $4t+1$ переменных, имеют степень меньшую либо равную $4t+1$ и содержат максимум $\sum_{j=1}^{4t+1} C_{4t+1}^{j}$ мономов.

Лемма 2. Для момента времени $t = 10,11$ уравнение для $s_{1,18}(t)$ регистра $LFSR_1$ зависит от $2t+19$ переменных, содержит максимум $\sum_{j=1}^{2t+19} C_{2t+19}^{j}$ мономов и для степени выполнено неравенство $\deg s_{1,18}(t) \le 2t + 19$.

Для момента времени $t = 12,...,21$ уравнение для $s_{1,18}(t)$ регистра $LFSR_1$ будет зависеть от переменных обратной связи второго и третьего регистра, уравнение будет содержать

$2t+22$ переменных, максимум $\sum_{j=1}^{2t+19} C_{2t+22}^{j}$ мономов и для степени будет выполнено неравенство $\deg s_{1,18}(t) \le 2t+19$.

Для момента времени $t=10$ уравнения для элементов выходных последовательностей $s_{2,21}(t), s_{3,22}(t)$ регистров $LFSR_2, LFSR_3$ зависят от $4t+4$ переменных, имеют степень меньшую либо равную $4t+1$ и содержат максимум $\sum_{j=1}^{4t+4} C_{4t+4}^{j}$ мономов.

Для момента времени $t=11$ уравнение для $s_{2,21}(t)$ регистра $LFSR_2$ зависит от $t+37$ переменных, содержит максимум $\sum_{j=1}^{t+37} C_{t+37}^{j}$ мономов и для степени выполнено неравенство $\deg s_{2,21}(t) \le 4t+1$.

Для момента времени $t=12,...,14$ уравнение для $s_{2,21}(t)$ регистра $LFSR_2$ зависит от $2t+29$ переменных, содержит максимум $\sum_{j=1}^{2t+22} C_{2t+29}^{j}$ мономов и для степени выполнено неравенство $\deg s_{2,21}(t) \le 2t+22$.

Для момента времени $t=15,...,21$ уравнение для $s_{2,21}(t)$ регистра $LFSR_2$ зависит от $t+43$ переменных, содержит максимум $\sum_{j=1}^{t+41} C_{t+43}^{j}$ мономов и для степени выполнено неравенство $\deg s_{2,21}(t) \le t+41$.

Для момента времени $t=11$ уравнение для $s_{3,22}(t)$ регистра $LFSR_3$ зависит от $t+38$ переменных, содержит максимум $\sum_{j=1}^{t+38} C_{t+38}^{j}$ мономов и для степени выполнено неравенство $\deg s_{3,22}(t) \le 4t+1$.

Для момента времени $t=12,...,14$ уравнение для $s_{3,22}(t)$ регистра $LFSR_3$ зависит от $2t+29$ переменных, содержит максимум $\sum_{j=1}^{2t+23} C_{2t+29}^{j}$ мономов и для степени выполнено неравенство $\deg s_{3,22}(t) \le 2t+23$.

Для момента времени $t=15,...,21$ уравнение для $s_{3,22}(t)$ регистра $LFSR_3$ зависит от $t+43$ переменных, содержит максимум $\sum_{j=1}^{t+42} C_{t+43}^{j}$ мономов и для степени выполнено неравенство $\deg s_{3,22}(t) \le t+42$.

Теорема 1. Для элементов выходных последовательностей $s_{1,18}(t), s_{2,21}(t), s_{3,22}(t)$ регистров $LFSR_1, LFSR_2, LFSR_3$ в момент времени $t=1,...,21$ справедлива следующая оценка числа переменных, количества мономов и степени уравнения.

Таблица 1. Зависимость числа переменных, числа мономов и степени уравнения от момента времени

Момент времени	$s_{1,18}(t)$			$s_{2,21}(t)$			$s_{3,22}(t)$		
	Число переменных	Число мономов	Степень	Число переменных	Число мономов	Степень	Число переменных	Число мономов	Степень
$t=1,...,9$	$4t+1$	$\sum_{j=1}^{4t+1} C_{4t+1}^{j}$	$4t+1$	$4t+1$	$\sum_{j=1}^{4t+1} C_{4t+1}^{j}$	$4t+1$	$4t+1$	$\sum_{j=1}^{4t+1} C_{4t+1}^{j}$	$4t+1$
$t=10$	39	$\sum_{j=1}^{2t+19} C_{2t+19}^{j}$	$2t+19$	44	$\sum_{j=1}^{4t+4} C_{4t+4}^{j}$	$4t+1$	44	$\sum_{j=1}^{4t+4} C_{4t+4}^{j}$	$4t+1$
$t=11$	41	$\sum_{j=1}^{2t+19} C_{2t+19}^{j}$	$2t+19$	48	$\sum_{j=1}^{t+37} C_{t+37}^{j}$	$2t+2$	49	$\sum_{j=1}^{t+38} C_{t+38}^{j}$	$4t+1$
$t=12$	46	$\sum_{j=1}^{2t+19} C_{2t+22}^{j}$	$2t+19$	53	$\sum_{j=1}^{2t+22} C_{2t+29}^{j}$	$2t+2$	53	$\sum_{j=1}^{2t+23} C_{2t+29}^{j}$	$2t+23$
$t=13$	48	$\sum_{j=1}^{2t+19} C_{2t+22}^{j}$	$2t+19$	55	$\sum_{j=1}^{2t+22} C_{2t+29}^{j}$	$2t+2$	55	$\sum_{j=1}^{2t+23} C_{2t+29}^{j}$	$2t+23$
$t=14$	50	$\sum_{j=1}^{2t+19} C_{2t+22}^{j}$	$2t+19$	57	$\sum_{j=1}^{2t+22} C_{2t+29}^{j}$	$2t+2$	57	$\sum_{j=1}^{2t+23} C_{2t+29}^{j}$	$2t+23$
$t=15,...,20$	$2t+22$	$\sum_{j=1}^{2t+19} C_{2t+22}^{j}$	$2t+19$	$t+43$	$\sum_{j=1}^{t+41} C_{t+43}^{j}$	$t+41$	$t+43$	$\sum_{j=1}^{t+42} C_{t+43}^{j}$	$t+42$
$t=21,...$	64	$\sum_{j=1}^{61} C_{64}^{j}$	61	64	$\sum_{j=1}^{62} C_{64}^{j}$	62	64	$\sum_{j=1}^{63} C_{64}^{j}$	63

Литература

1. Rueppel, R. Analysis and Design of Stream Ciphers//R. Rueppel. – Communications and Control Engineering Series. –Berlin:: Springer-Verlag, 1986.

2. Nicolas, C. Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt// C. Nicolas. – LNCS. 2002. Vol. 2587. P. 182–199.

3. Nicolas, C. Fast algebraic attacks on stream ciphers with linear feedback// C. Nicolas. – LNCS. 2003. Vol. 2729. P. 177-194.

4. Nicolas, C. Algebraic attacks on combiners with memory and several outputs// C. Nicolas. – LNCS. 2004. Vol. 3506. P. 3-20.

5. Frederik, A. Algebraic attacks on combiners with memory. // A. Frederik. – LNCS. 2003. Vol. 2729. P. 162-175.

6. Frederik, A. Improving fast algebraic attacks //A. Frederik, K. Matthias. – LNCS. 2004. Vol. 3017. P. 65-82.

7. Sultan, A.H. Algebraic Attacks on Clock-Controlled Stream Ciphers.// A.H. Sultan, B. Lynm, C. Bernard, W. Kenneth. – LNCS. 2006. Vol. 4058. P. 1-16.

8. Briceno, M. A pedagogical implementation of the GSM A5/1 and A5/2 "voice privacy" encryption algorithms/ M. Briceno, I. Goldberg, D. Wagner. // [Electronic resource]. — Mode of access: http://www.gsm-security.net/papers/a51.shtml. — Date of access: 09.10.2009.

В.Ф.ГОЛИКОВ, Ф.АБДОЛЬВАНД

КОНФИДЕНЦИАЛЬНОЕ ФОРМИРОВАНИЕ ИДЕНТИЧНЫХ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

Во многих задачах защиты информации требуется наличие общего секрета у различных абонентов системы обмена информацией. Таким секретом, например, в задачах аутентификации или шифрования является число (бинарная последовательность). Традиционно задачи доставки этого числа решаются с использованием защищенных от прослушивания каналов или аутентифицированных сеансов связи на базе односторонних функций (алгоритм Диффи-Хеллмана). Вместе с тем представляет интерес поиск других решений, которые в определенных ситуациях могут быть использованы как альтернативные.

В докладе излагается способ формирования идентичных бинарных последовательностей двумя абонентами, имеющими общий незащищенный канал связи посредством аутентифицированных сеансов обмена некоторой информацией. Предлагаемый материал является конкретизацией идеи, изложенной в [1].

Процесс формирования идентичных бинарных последовательностей двумя абонентами, имеющими общий незащищенный канал связи посредством аутентифицированных сеансов обмена некоторой информацией можно разбить на три этапа:

– этап автономного генерирования бинарных последовательностей абонентами системы;

– этап устранения несовпадений в сгенерированных бинарных последовательностях путем обмена информацией об ошибках;

– этап повышения уровня конфиденциальности сформированной общей последовательности до требуемого уровня.

Рассмотрим возможные технологии реализации перечисленных этапов.

Этап автономного генерирования бинарных последовательностей абонентами системы

Известно, что в двух бинарных последовательностях, сформированных независимо друг от друга процент ошибок (несовпадений бит) является случайной величиной с математическим ожиданием, равным 50, и дисперсией, уменьшающейся с увеличением длины последовательности. Возможности по управлению количеством ошибок при этом отсутствуют. В [2] показано, что при такой генерации даже самый наилучший алгоритм исправления ошибок не позволяет их удалить. Таким образом, необходимо так сгенерировать исходные последовательности, чтобы процент ошибок в них был хотя бы в среднем либо меньше 50 процентов, либо больше. Для этого предлагается следующая процедура. Абонент A генерирует бинарную последовательность X^0 длиной n и посылает ее абоненту B. Затем абоненты A и B генерируют независимо друг от друга случайные секретные последовательности чисел соответственно S_A и S_B, при этом $S_A = \{s_1^a, s_2^a, ..., s_{r_a}^a\}$,

$S_B = \{s_1^b, s_2^b, ..., s_{r_b}^b\}$, где $0 \le r_a \le n$, $0 \le r_b \le n$, $s_i^a \in \{1, 2, ..., n\}$, $s_i^b \in \{1, 2, ..., n\}$, причем $s_i^a \ne s_j^a$, $i, j = 1, 2, ..., r_a$ для S_A, $s_i^b \ne s_j^b$, $i, j = 1, 2, ..., r_b$ для S_B. Далее абоненты A и B в соответствии с полученными номерами бит s_i^a и s_i^b инвертируют эти биты в X^0 и получают последовательности X^A и X^B, обладающие следующими свойствами:

– в последовательностях X^A и X^B имеются совпадающие и несовпадающие биты;

– наличие совпадающих бит обусловлено для части бит взаимным инвертированием, для части взаимным не инвертированием;

– наличие несовпадающих бит обусловлено для части бит инвертированием в X^A и не инвертированием X^B и наоборот.

Обозначим число совпадающих взаимно инвертированных бит через $n_{ИС}$, тогда можно показать, что общее число совпадающих бит равно $n_C = n - (r_a + r_b) + 2n_{ИС}$, а число несовпадающих бит равно $n_{НС} = n - (r_a + r_b) - 2n_{ИС}$. Для того, чтобы неопределенность каждой последовательности X^A и X^B была максимальной и равнялась бы неопределенности последовательности, сгенерированной секретным образом, необходимо выполнение следующих условий: $n_{ИС} = n_{НС}$, где $n_{НС}$ - число совпадающих взаимно не инвертированных бит. Очевидно, что $n_C = n_{ИС} + n_{НС}$. В этом случае после удаления ошибок в итоговой последовательности останутся, биты с равной вероятностью принадлежащие исходной последовательности X^0 или ее инвертированному аналогу. С учетом полученных выше соотношений можно записать $n - (r_a + r_b) + 2n_{ИС} = n_{ИС} + n_{НС}$. Откуда $r_a + r_b = n$.

Рассмотрим варианты выбора r_a, r_b. Если выбрать $r_a = r_b = n/2$, то получим: $n_C = 2n_{ИС}$. Так как $n_{ИС}$ случайная величина с математическим ожиданием $\frac{n}{4}$, то и n_C случайная величина с математическим ожиданием $\frac{n}{2}$. Следовательно, при таком выборе значений r_a, r_b устранить в дальнейшем ошибки не возможно.

Если выбрать $r_a = \frac{n}{2} + \alpha$, а $r_b = \frac{n}{2} - \alpha$, то получим: $n_C = 2n_{ИС}$. Так как в данном случае математическое ожидание $n_{ИС}$ меньше чем $\frac{n}{4}$, то математическое ожидание n_C меньше чем $\frac{n}{2}$ (ошибок более 50%). Для этого случая алгоритмы устранения ошибок отсутствуют. Таким образом, варианты выбора r_a, r_b, обеспечивающие максимальную неопределенность итоговой последовательности, отсутствуют.

Рассмотрим компромиссный вариант, при котором удается получить приемлемое (в смысле дальнейшего удаления) число ошибок при некотором снижении неопределенности. Выберем: $r_a = \frac{n}{2} - \alpha$, $r_b = \frac{n}{2} - \alpha$, тогда $r_a + r_b = n - 2\alpha$. Тогда: $n_C = n - (n - 2\alpha) + 2n_{ИС} = 2\alpha + 2n_{ИС}$, $n_{НС} = (n - 2\alpha) - 2n_{ИС} = n - 2\alpha - 2n_{ИС}$. Чтобы выполнялось $n_C \ge n_{НС}$, необходимо обеспечить $\alpha \le \frac{n}{4} - n_{ИС}$. Зная закон распределения $n_{ИС}$ можно задать величину α. Оценим возникающее уменьшение неопределенности итоговой последовательности. Для этого найдем долю $n_{НС}$ и $n_{ИС}$ в итоговой последовательности:

$$\delta_C = \frac{n_{ИС}}{n_C} = \frac{n_{ИС}}{2\alpha + 2n_{ИС}} = 0{,}5\,\frac{n_{ИС}}{\alpha + 2n_{ИС}} \le 0{,}5,\ \delta_{НС} = \frac{n_{НС}}{n_C} = \frac{2\alpha + n_{ИС}}{2\alpha + 2n_{ИС}} = 0{,}5\,\frac{2\alpha + n_{ИС}}{\alpha + n_{ИС}} \ge 0{,}5$$

Следовательно, вероятность попадания в итоговою последовательность инвертированных в исходной последовательности бит оказывается больше, чем не инвертированных. Этот эффект можно значительно снизить на третьем этапе.

Этап устранения несовпадений в сгенерированных бинарных последовательностях путем обмена информацией об ошибках.

Метод устранения несовпадений достаточно подробно описан [3] и его суть заключается в следующем. При большом проценте несовпадающих бит целесообразно каждому абоненту разбить свою последовательность на пары бит случайным, но одинаковым друг с другом образом. Затем абоненты A и B вычисляют четности каждой пары C_i^A, C_i^B, где $i = 1, 2, ..., n/2$, и обмениваются этими числами. Пары, для которых $C_i^A = C_i^B$, остаются в последовательностях, а пары, для которых $C_i^A \neq C_i^B$, удаляются. В парах, оставшихся в последовательностях, удаляется согласовано по одному биту для сохранения неопределенности. Новые последовательности вновь содержат ошибки, т.к. условие $C_i^A = C_i^B$ выполняется как для пар, не имеющих ошибок, так и для пар, содержащих две ошибки. Поэтому процедура повторяется в количестве, обеспечивающем устранение всех ошибок. Моделирование процесса устранения ошибок по данному алгоритму показало, что его эффективность близка к потенциально возможному, обеспечивающему максимальное число совпадающих бит при заданном уровне несовпадающих в исходных последовательностях [4], в соответствии с соотношением

$$n_{ИТ} = n\,(1 - (q \log_2 q + (1-q)\log_2 (1-q))),$$

где $q = d/n$, d – число несовпадающих бит в согласуемых последовательностях.

Этап повышения уровня конфиденциальности сформированной общей последовательности до требуемого уровня.

Необходимость данного этапа обусловлена тем, что в результате прослушивания открытого канала связи, по которому абоненты A и B обмениваются информацией для генерации исходных последовательностей и для устранения имеющихся в них ошибок, криптоаналитику становится известным, например, значения некоторой части бит, вероятности попадания в итоговую последовательность X^{AB} инвертированных или не инвертированных бит из исходной последовательности X^0.

Процедура повышения уровня конфиденциальности позволяет успешно бороться как с первым видом утечки информации, так и со вторым. Ее суть состоит в следующем. Абоненты *A* и *B* согласованно генерируют случайные бинарные последовательности F_i, где $i = 1, 2, ..., n - v$, длиной n. С помощью этих чисел формируются $n - v$ бит итоговой последовательности, каждый из которой есть сумма бит “профильтрованная” с помощью F_i соответствующего участка усиливаемой последовательности, т.е.

$$y_j = \sum_{k=1}^{n} f_k * x_k (\mathrm{mod}\, 2),$$

где $j = 1, 2, ..., n - v$, f_k, x_k – соответствующие биты последовательностей F_i, X^{AB} Можно показать, что для “нейтрализации” известных криптоаналитику бит из X^{AB} достаточно, чтобы каждый бит y_j содержал хотя бы один неизвестный криптоаналитику бит. Так как описываемая процедура сокращает длину итоговой последовательности, то для обеспечения заданных ее размеров необходимо X^{AB} формировать с запасом на величину v. Кроме того, биты y_j в общем случае содержат $n + v$ бит из последовательности X^{AB}, что приводит к компенсации потерь конфиденциальности итоговой последовательности за счет отклонения вероятности попадания в итоговую последовательность инвертированных или не инвертированных бит от значения 0,5.

Литература

1. Голиков В.Ф., Абдольванд Ф. «О распределении ключевой информации в современных информационных системах». XIV международная конференция «Комплексная защита информации». Могилев , 2009.

2. Голиков В.Ф., Абдольванд Ф. «Эффективность устранения ошибок в бинарных последовательностях при разнесенном формировании криптографического ключа». Доклады БГУИР №6 (52), Минск, БГУИР, 2010.

3. Голиков В.Ф., Абдольванд Ф. «Устранение ошибок в бинарных последовательностях при формировании криптографического ключа без использования однонаправленных функции». VI Международная научная конференция «Информационные системы и технологии». 2010 года, Минск.

4. А. Экерт и др. Физика квантовой информации. Постмаркет, М, 2002.

А.Е.ЖУКОВ

ВЫЧИСЛИТЕЛЬНО АСИММЕТРИЧНЫЕ ПРЕОБРАЗОВАНИЯ И СХЕМЫ ИЗ ОБРАТИМЫХ ЭЛЕМЕНТОВ

Для современной криптографии одним из важнейших понятий является понятие однонаправленной функции. Однако, не смотря на многочисленные работы, посвященные этой тематике, строгих доказательств существования или возможности построения таких функций в настоящее время нет. В данной работе будет рассмотрен один подход, позволяющий новым образом взглянуть на явление однонаправленности.

Говоря неформально, однонаправленная функция – это эффективно вычислимая функция, для задачи обращения которой не существует эффективных алгоритмов. В качестве модели обратимого преобразования возьмем подстановку на множестве двоичных наборов; в качестве меры сложности того или иного преобразования – сложность минимальной булевой схемы, реализующей данное преобразование и обозначаемой в дальнейшем через $C(F)$. В качестве модели однонаправленной функции будем рассматривать ***вычислительно-асимметричное преобразование***, т.е. такое обратимое преобразование, сложность которого отличается от сложности обратного преобразования.

Широко известным классом вычислительно асимметричных преобразований являются линейные преобразования, изученные в работах [1], [2]. В работе [2] доказано, что при $n \geq 5$ сложности прямых и обратных преобразований равны соответственно $C(F_n)=n+1$ и $C(F^{-1}{}_n)=[3/2(n-1)]$.

Пытаясь понять природу такого различия, можно задать глупый вопрос: почему схему, реализующую прямое преобразование, нельзя использовать для вычисления обратного преобразования? Ответ очевиден – потому, что логические элементы, отличные от инверсии, необратимы. Однако уже давно известны ***обратимые логические элементы*** [3], примерами которых могут служить такие элементы как NOT, CNOT (Controlled NOT), CCNOT (Controlled Controlled NOT):

Рис. 1. Элемент NOT

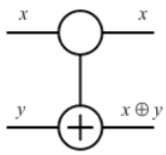


Рис. 2. Элемент CNOT.

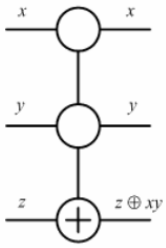


Рис. 3. Элемент CCNOT.

С помощью этих элементов можно построить минимальную схему, реализующую данное преобразование. Для удобства изображения схем и получения обратной схемы будем располагать элементы на параллельных горизонтальных линиях, на которые подаются входные переменные. К схеме возможно добавление дополнительных линий, на которые подается логический 0 и играющая роль «памяти».

Однако, и эта схема не будет обратимой. Дело в том, что в процессе вычисления нашего преобразования на выходе схемы появился не только вектор результатов, но некоторая информация (на выходе дополнительной линии), полученная в процессе вычисления и называемая ***вычислительным мусором*** или просто ***мусором***. Без знания этой информации, а только по выходу вход получить невозможно.

Обратимая схема будет содержать некоторые «лишние» элементы (отмеченные пунктиром), которые не нужны для реализации, например, прямого преобразования, но нужны для реализации обратного преобразования, и наоборот. Рассмотрим, какую роль выполняют эти элементы. Исходная схема необратима, так как для корректного вычисления в обратную сторону нам необходимо подать на дополнительную линию соответствующий «мусор», который в общем случае неизвестен. Для того чтобы схема стала обратимой, надо обнулить «мусор», что достигается введением в схему дополнительных элементов. В обратной же схеме эти элементы будут выполнять необходимые для обратного преобразования функции.

Проанализировав построенную схему из обратимых элементов, можно выдвинуть следующую гипотезу о структуре вычислительно асимметричных преобразований. В ходе работы прямой схемы вычислительно асимметричного преобразования, получается некоторая дополнительная информация («мусор», с криптографической точки зрения играющий роль «лазейки»), которая необходима для получения результата прямого преобразования. При попытке непосредственного обращения по такой схеме, на ее входы необходимо будет подать этот «мусор», который в общем случае неизвестен. Поэтому, чтобы получить обратимую схему, необходимо добавить в нее дополнительные элементы, которые будут удалять «мусор». Возможно, что схемы из обратимых элементов для асимметричных преобразований имеют следующую общую структуру, которая показана на рис. 4. У таких схем есть некоторое «общее тело», а также подсхемы, отвечающие за удаление «мусора» прямого и обратного преобразований. Из-за разницы в сложностях этих подсхем удаления «мусора» и возникает разница в сложности прямого и обратного преобразований.

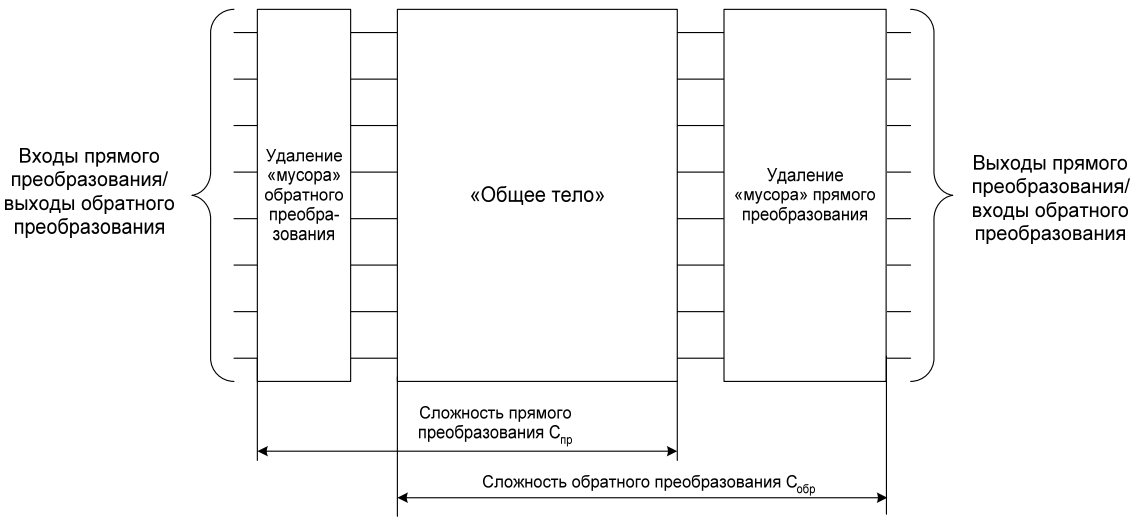


Рис. 4. Возможная структура асимметричных преобразований.

Аргументами в пользу сформулированной выше гипотезы служат обратимые схемы, построенные в [5], [6] для таких известных вычислительно асимметричных преобразований, как нелинейные асимметричные преобразования [2] и двоичный сумматор/вычитатель [4].

Литература

1. Boppana R.B. Lagarias J.C. One-way functions and circuit complexity. Information and Computation, vol. 74 (1987), pp. 226-240.

2. Hiltgen A.P. Cryptographically Relevant Contributions to Combinatorial Complexity Theory. ETH Series in Information Processing, vol. 3 (1993)

3. Toffoli M. Bicontinuous Extensions of Invertible Combinatorial Functions. Math. Syst. Theory, vol. 14 (1981), pp. 13-23

4. Редькин Н.П. О минимальной реализации двоичного сумматора. Проблемы кибернетики, 38 (1981), с. 181-216

5. Чикин А.А. Двоичный обратимый сумматор из обратимых элементов. Курсовая работа. МГТУ им. Н.Э. Баумана, каф. ИУ-8, 2005

6. Засорина Ю.В. Вычислительно асимметричные преобразования и схемы из обратимых элементов. Дипломный проект. МГТУ им. Н.Э. Баумана, каф. ИУ-8, 2007

С.П.КАЛЮТЧИК

ОСОБЕННОСТИ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПРОИЗВОДСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ИНФРАСТРУКТУРАХ

При разработке, создании и реализации мер по обеспечению безопасности информационных систем, управляющих критически важными технологическими процессами, одним из основных аспектов являются особенности структуры задействованных информационно-коммуникационных ресурсов.

Наиболее характерными особенностями с позиции, как непосредственной реализации, так и обеспечения безопасности процессы информатизации обладают в организациях, имеющих территориально распределенную структуру информационно-коммуникационных ресурсов.

Определим структуру территориально распределенной в том случае, когда в организации, имеющей единую организационно-правовую структуру точки реализации финансово-экономических, административно-управленческих, технических или технологических процессов территориально разнесены, полностью, либо частично.

Точки реализации процессов – объекты системы, имеющие характеристики с показателями, критически важными для осуществления процесса полностью, либо частично согласно установленным условиям.

Территориально распределенные структуры могут иметь четкую централизацию по одному или нескольким процессам - финансово-экономическим, организационно-правовым, административно-управленческим, что определяет единство и (или) централизацию применяющихся технологий.

Рассмотрим обеспечение криптографической защиты критически важных производственных процессов, управление которыми строится на основе территориально распределенной информационно-телекоммуникационной инфраструктуры на примере Белорусской железной дороги.

Основной особенностью территориально распределенной информационно-телекоммуникационной инфраструктуры является ее неоднородность с точки зрения качественных характеристик. Практика показывает, что такая неоднородность имеет место как на узлах обработки и хранения данных, так и в отношении каналов передачи данных, причем эти неоднородности зачастую тесно связаны.

Ведомственная информационно-телекоммуникационная система Белорусской железной дороги, повторяя структурную схему основных железнодорожных путей Республики Беларусь является территориально распределенной (рисунок 1).

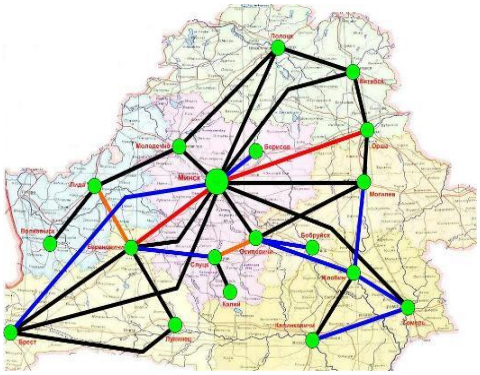


Рисунок 1 – Основные узлы сети передачи данных Белорусской железной дороги

Узлы обработки и хранения информации, обеспеченные наиболее мощными и современными вычислительными средствами компактно сконцентрированы в соответствии с организационно-правовой и административно-управленческой структурой Белорусской железной дороги как государственного объединения (рисунок 2).

Рисунок 2 – Территориальная схема Белорусской железной дороги

Подавляющая часть узлов Белорусской железной дороги использует смешанные каналы передачи данных – оптоволоконные, ADSL (Asymmetric Digital Subscriber Line) и каналы тональной частоты (ТЧ). Наиболее низкими техническими параметрами при передаче информации обладают каналы ТЧ, которые и определяют предельные возможности по условиям передачи трафика.

Так имеющиеся на Белорусской железной дороге каналы ТЧ обладают скоростью передачи 9,6 Кб/сек. В сетях связи ТЧ каналы объединены в группы с суммарной средней скоростью передачи 33,6 Кб/сек.

Вместе с тем значительная часть пользователей услуг производственных информационных систем железнодорожного транспорта равномерно распределена по

территории республики, что не позволяет всем заинтересованным пользоваться возможностями высокоскоростных качественных каналов передачи данных.

Одной из основных задач подсистемы криптографической защиты информации Белорусской железной дороги является задача предоставления услуг электронной цифровой подписи (ЭЦП).

Предоставление услуг ЭЦП обеспечивается с помощью ведомственной инфраструктуры открытых ключей (ИОК). Топология и функционирование ИОК Белорусской железной дороги определяется следующими особенностями, связанными со спецификой производственных процессов железнодорожного транспорта:

– неоднородность качественных характеристик ведомственных каналов передачи данных;

– отнесение значительного числа технологических процессов к критически важным (управление движением поездов, устройствами безопасности движения, электроснабжения и т.п.);

– особенность технологии железнодорожных перевозок, обуславливающая необходимость частого подтверждения валидности сертификата открытого ключа в режиме реального времени при использовании электронных технологических документов;

– наличие интенсивных процедур управления ключами подписи;

– повышенные требования к обеспечению гарантированного непрерывного функционирования основных элементов ИОК.

Задача обеспечения безопасности и гарантированного непрерывного функционирования основных элементов ИОК является приоритетной. Решается путем централизованного размещения удостоверяющего и регистрационного центров в условиях реализации достаточных мер защиты. Однако такой подход вступает в противоречие с задачей проверки валидности сертификата открытого ключа в режиме реального времени в условиях неоднородных качественных характеристик каналов передачи данных.

Общеизвестные технические решения для on-line проверки статуса сертификата, такие как технология OCSP (Online Certificate Status Protocol) также не могут быть применены в полном объеме, поскольку объект, реализующий функцию OCSP при проверке сертификата открытого ключа удаленным пользователем работает как Web-объект, что делает весь механизм полностью зависимым от качественных параметров информационно-телекоммуникационных ресурсов.

При централизованном расположении удостоверяющего центра для проверки статуса сертификата адресатом необходимо осуществление нескольких трансакций. Измерения параметров передачи при одной трансакции показали, что время осуществления необходимого для проверки сертификата информационного обмена для клиентов, подключенных к ТЧ каналам доходит до 42 сек. Указанные сверхдлительные временные интервалы в условиях использования информационных средств обработки перевозочных электронных документов приводят к системным технологическим сбоям, поскольку воспринимаются телекоммуникационным оборудованием в качестве «ошибки связи».

Для решения возникшей проблемы на Белорусской железной дороге разработана и реализована схема, основанная на реплицировании реестров удостоверяющего центра с помощью дополнительных объектов ИОК, размещенных в узлах распределенной информационно-телекоммуникационной сети с однородными качественными характеристиками (рисунок 3). Вышеупомянутые объекты (О) взаимодействуют с удостоверяющим центром посредством специализированного транспортного модуля, обеспечивающего принудительную репликацию базы данных сертификатов открытого ключа при каждом ее изменении.

При подобной схеме построения инфраструктуры открытых ключей время трансъакции при авторизации пользователей и проверке ЭЦП для клиентов узловой сети передачи данных лежит в пределах нескольких миллисекунд.

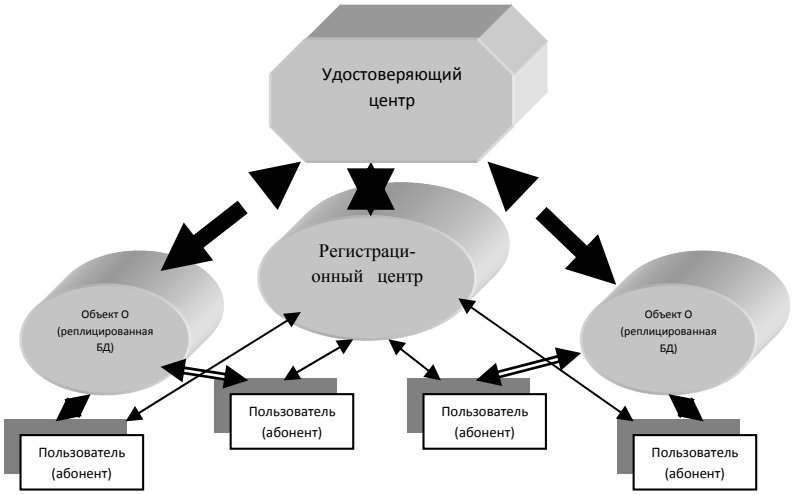


Рисунок 3 - Дополнительный объект инфраструктуры открытых ключей

В.В.КОМИСАРЕНКО

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ТЕХНОЛОГИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

В середине семидесятых прошлого столетия было придумано понятие электронной цифровой подписи (далее - ЭЦП). В девяностых годах ЭЦП стала активно использоваться в информационных технологиях, прежде всего в банковской сфере. Для поддержки практических решений в мире начались процессы стандартизации криптографических алгоритмов. США, Россия, Республика Беларусь и некоторые другие государства вводят в действие государственные стандарты, устанавливающие требования к процедурам выработки и проверки ЭЦП, а также к используемым параметрам. Основные операции в этих стандартах выполняются в конечных числовых полях. В это же время развивается направление, связанное с применением эллиптических кривых в криптографии с открытым ключом.

Начало века связанно с введением ряда стандартов, устанавливающих процедуры ЭЦП с использованием эллиптических кривых. Введены следующие стандарты:

– ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (Россия).

– ДСТУ 4145-2002 «Информационные технологии. Криптографическая защита информации. Цифровая подпись с использованием эллиптических кривых. Формулы выработки и проверки» (Украина).

– ISO/IEC 15946-2:2002 «Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital signatures».

– ANSI X9.62:2005 «Public Key Cryptography for the Financial Services Industry. The Elliptic Curve Digital Signature Algorithm (ECDSA)» (США).

Наиболее проблемной остается область разработки и оценки надежности алгоритмов хэширования, которые используются в процедурах выработки и проверки ЭЦП. Так алгоритмы хэширования, рекомендованные NIST, многократно изменялись в связи с проблемами их надежности. Действующий стандарт прошел следующие модификации: SHA, SHA-1, SHA-2, SHA-224, SHA-256, SHA-384, SHA-512. В настоящее время NIST проводит

конкурс по разработке нового алгоритма SHA-3, который продлится до 2012 года. SHA-3 должен поддерживать размер выходного блока 224, 256, 384 и 512 бит.

В Республике Беларусь на стадии принятия находится проект предварительного стандарта «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи на основе эллиптических кривых». Отличительными особенностями проекта являются:

– оригинальные формулы выработки и проверки подписи (на основе системы Шнора, с использованием модификаций);

– использование трех уровней стойкости 128, 192, 256;

– расширенные требования к параметрам;

– наличие алгоритмов генерации и проверки параметров;

– наличие алгоритма транспорта ключа с возможностью использования параметров алгоритмов выработки и проверки ЭЦП;

– алгоритмам присвоены идентификаторы объектов.

В указанных стандартах использованы различные формулы выработки и проверки подписи. Кроме того, применяемые форматы представления значений ЭЦП на практике тоже различаются. Это приводит к необходимости решения задачи проверки всех видов подписей и разбора их форматов при организации международного взаимодействия. Существует два наиболее распространенных решения. Первое основано на использовании идентификаторов объектов. В соответствующем поле указываются идентификаторы используемых алгоритмов и форматов. Второй способ решения – это использование услуг так называемой «третьей доверенной стороны» (ДТС). ДТС реализует функции проверки наиболее распространенных видов подписей и разбора соответствующих форматов. Между ДТС и абонентами устанавливаются доверенные отношения, основанные на определении ответственности, связанной с проверкой ЭЦП.

В целях решения задач трансграничного взаимодействия в Европейском союзе принят ряд инициатив. Проект PEPPOL (Pan-European Public Procurement Online) направлен на реализацию общих стандартов в рамках осуществления электронных закупок. Предполагается связать национальные системы электронных закупок государств так, чтобы все участники могли пользоваться преимуществами единого европейского рынка. В рамках проекта разрабатываются функциональные спецификации трансграничного использования электронной подписи на электронных торгах.

Решением Еврокомиссии 2011/130/EU от 25 февраля 2011 года установлены форматы ЭЦП, которые должны обрабатываться электронными сервисами. Определены три формата:

1) с использованием спецификаций XML;

2) в соответствии с Cryptographic Message Syntax (CMS);

3) с использованием спецификации PDF.

В целях установления правовых основ применения электронных документов, определения основных требований, предъявляемых к электронным документам, а также правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе, государствами развивается законодательная база. Так в Республике Беларусь вступил в силу Закон «Об электронном документе и электронной цифровой подписи». Это Закон пришел на смену утратившему силу Закону «Об электронном документе», действовавшему с января 2000 года. Особенностью этого Закона является определение Государственной системы управления открытыми ключами, предназначенной для обеспечения возможности получения всеми заинтересованными организациями и физическими лицами информации об открытых ключах и их владельцах в Республике Беларусь и представляющей собой систему взаимосвязанных и аккредитованных в ней поставщиков услуг.

В марте 2011 года в России принят новый Закон «Об электронной подписи», которая определяется как информация в электронно-цифровой форме, использующаяся для идентификации физического или юридического лица. В этом Законе определены три вида электронной подписи: простая, усиленная и квалифицированная электронная подпись. При этом подлинность электронной подписи обеспечивается надежностью средств, при помощи которых осуществляются ее создание и проверка.

Технология ЭЦП продолжает развиваться по всем составляющим ее направлениям и находит все большее применение в современных информационных системах.

П.В.КУЧИНСКИЙ, М.И.НОВИК, Ю.П.ПЕТРУНИН,
П.Ю.ПЕТРУНИН, Н.А.РАЩЕНЯ, А.Л.ТРУХАНОВИЧ

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И КОНТРОЛЯ ДОСТУПА К ПЭВМ

В настоящее время в Республике Беларусь разработаны и эксплуатируются аппаратно-программные устройства криптографической защиты информации, устройства защиты ПЭВМ от несанкционированного доступа (НСД), контроля настроек BIOS и состава устройств ПЭВМ, устройства идентификации и аутентификации операторов. Как правило, каждое из этих устройств выполняет только одну из перечисленных функций. Перечисленные функции можно выполнять стандартными средствами операционных систем (ОС). Однако особенностью использования ОС является то, что полный перечень всех их возможностей полностью не известен пользователю. Поэтому в таких ОС не исключено наличие скрытых возможностей осуществления НСД к информации, обрабатываемой под их управлением. По той же причине программные средства защиты информации, работающие под управлением тех же ОС, представляются также недостаточно надежными. Поэтому системы НСД в настоящее время выполняются на основе аппаратно-программных комплексов, встраиваемых в ПЭВМ.

Использование современной элементной базы позволяет разработать и изготовить аппаратно-программный комплекс, интегрирующий функции аппаратного шифрования информации, идентификации и аутентификации операторов, контроля настроек BIOS и состава устройств ПЭВМ. При этом возможно одновременно обеспечить как защиту ПЭВМ от НСД, так и высокую скорость криптопреобразования, реализацию электронно-цифровой подписи и хэш-функции, открытое распределение ключей. Это, в свою очередь, позволяет уменьшить число аппаратных устройств, встраиваемых в ПЭВМ, и снизить затраты по обеспечению защиты информации, повысить степень доверия и надежность целевых комплексов и средств автоматизации обработки информации по требованиям безопасности.

В разработанном аппаратно-программном комплексе (АПК) «Криптозамок» одновременно реализованы функции контроля доступа к ПЭВМ, включая идентификацию и аутентификацию операторов с использованием аппаратного устройства идентификации, контроль настроек BIOS, состава устройств и вскрытия корпуса ПЭВМ, и функции криптографической защиты информации, обрабатываемой на данной ПЭВМ, включая шифрование, вычисление и проверку электронной цифровой подписи и хэш-функции.

АПК «Криптозамок» состоит из аппаратно-программного устройства «Криптозамок», выполненного в виде платы, помещенной в защитный корпус, устанавливаемой на PCI шину персонального компьютера, аппаратного устройства идентификации, датчиков вскрытия корпуса ПЭВМ и программного обеспечения.

Основными структурными элементами устройства являются: цифровой сигнальный процессор TMS320VC5409, микроконтроллер MSP430F169 (МК), программируемые

логические матрицы (ПЛМИ) интерфейса, серийного номера устройства, ПЗУ памяти программ и данных, энергонезависимое ОЗУ. Процессор обеспечивает выполнение функций устройства «Криптозамок» по криптографической защите информации ПЭВМ. МК отвечает за выполнение функций устройства по контролю доступа к ПЭВМ. Устройство «Криптозамок» обеспечивает два режима работы: основной и дежурный. В основном режиме питание устройства осуществляется от ПЭВМ и в нем включены все элементы. В дежурном режиме в устройстве включенными остается только МК, энергонезависимое ОЗУ. В этом случае питание устройства осуществляется от батареи. При возникновении события НСД в дежурном режиме МК регистрирует это событие во внутренней энергонезависимой Flash-памяти, и по включению ПЭВМ переписывает данные в электронный журнал. При возникновении события НСД в рабочем режиме МК регистрирует это событие и передает сообщение процессору об НСД. Процессор при этом прекращает выполнение текущих операций и уничтожает критическую информацию в своем ОЗУ.

В АПК «Криптозамок» реализована идентификация и аутентификация операторов ПЭВМ с использованием электронного идентификатора и пароля, вводимого с клавиатуры ПЭВМ. При этом используется протокол идентификации и аутентификации на основе криптографического алгоритма ГОСТ 28147-89.

Электронный идентификатор выполнен на миниатюрном микроконтроллере ATtiny2313-20SU. Питание микроконтроллера осуществляется от платы устройства «Криптозамок». Идентификатор имеет уникальный серийный номер, программируемый при производстве. Память микроконтроллера программируется при производстве идентификатора, и после установки бита секретности становится недоступной для обратного считывания из микроконтроллера.

Программное обеспечение АПК «Криптозамок» включает прикладное программное обеспечение и специальное программное обеспечение устройства «Криптозамок».

ППО состоит из: драйвера и библиотеки работы с устройством в ОС Windows и Linux, пользовательского программного обеспечения. Специальное программное обеспечение устройства «Криптозамок» включает программное обеспечение расширения BIOS (ПОBIOS), программное обеспечение процессора устройства (ПОПРР) и программное обеспечение МК устройства (ПОМКР).

ПОBIOS устройства «Криптозамок» во взаимодействии с МК устройства обеспечивает: двухфакторную аутентификацию пользователей по идентификатору и паролю; контроль целостности аппаратных ресурсов ПЭВМ, регистрацию операторов, контроль настроек памяти CMOS ПЭВМ для каждого пользователя (разграничение доступа к аппаратным ресурсам ПЭВМ), синхронизацию часов реального времени ПЭВМ и устройства «Криптозамок», ведение электронного журнала с регистрацией в нем контролируемых событий, управление электронным журналом устройства «Криптозамок» администратором, администрирование пользователей и событий.

ПОПРР и библиотека функций устройства «Криптозамок» обеспечивают: контроль работоспособности процессора, инициализацию устройства, работу с ключами шифрования данных, реализацию криптографических алгоритмов и протоколов. ПОМКР и библиотека функций устройства «Криптозамок» обеспечивают: контроль работоспособности МК, специальный режим работы МК, работу с ключами шифрования.

ПОМКР также обеспечивает выполнение всех функций, связанных с выполнением программы ПОBIOS, регистрацию времени включения устройства «Криптозамок», контроль вскрытия корпуса ПЭВМ, контроль вскрытия корпуса устройства, сброс критической информации в ОЗУН устройства, управление электронным журналом устройства «Криптозамок».

Пользовательское ПО обеспечивает интерфейс оператора для выполнения функций устройства «Криптозамок» под управлением ОС ПЭВМ.

Разработанный аппаратно-программный комплекс обеспечивает функции криптографической защиты информации и контроля доступа к ПЭВМ, включая следующие основные функциональные возможности:

– двухфакторную аутентификацию операторов ПЭВМ до загрузки операционной системы (ОС) с использованием аппаратного идентификатора и пароля, вводимого с клавиатуры ПЭВМ;

– установление подлинности идентификатора оператора с использованием одностороннего протокола строгой аутентификации типа «запрос-ответ» на основе симметричной криптографии (ГОСТ 28147-89);

– разделение полномочий администраторов и пользователей по выбору источника загрузки ОС ПЭВМ, по использованию портов ввода/вывода и сетевых средств ПЭВМ путем установки и контроля конфигурации настроек BIOS ПЭВМ;

– генерацию случайной числовой последовательности с использованием физического источника шума на полупроводниковых диодах;

– тестирование корректности функционирования устройства «Криптозамок», включая самотестирование работоспособности, проверку правильности работы реализованных криптографических функций, контроль качества вырабатываемой случайной числовой последовательности;

– блокирование ПЭВМ при вскрытии корпуса ПЭВМ, предъявлении незарегистрированного в устройстве «Криптозамок» идентификатора оператора или вводе неверного пароля;

– регистрацию вскрытия корпуса устройства «Криптозамок» и ПЭВМ при включенном и выключенном электропитании ПЭВМ;

– регистрацию в защищенном от несанкционированного изменения журнале событий включения, выключения ПЭВМ, результатов идентификации и аутентификации;

– просмотр и очистку записей журнала событий устройства «Криптозамок» только администратором;

– генерацию криптографических ключей идентификаторов операторов с использованием физического источника шума;

– установку, смену и хранение ключей в зашифрованном виде в энергонезависимой памяти устройства «Криптозамок», недоступной программным средствам ПЭВМ;

– уничтожение хранимых в энергонезависимой памяти устройства «Криптозамок» ключей при смене ключей, вскрытии корпуса ПЭВМ и/или устройства «Криптозамок»;

– архивирование и хранение администратором ключевой информации для возможности ее последующего восстановления в случае повреждения ключевой информации в устройстве «Криптозамок»;

– восстановление ключевой информации только администратором;

– реализацию криптографических операций в устройстве «Криптозамок», включая: шифрование по ГОСТ 28147-89 в режимах простой замены, гаммирования и гаммирования с обратной связью; вычисление имитовставки по ГОСТ 28147-89; шифрование по СТБ П 34.101.31-2007 в режимах простой замены, сцепления блоков, гаммирования с обратной связью и счетчика; вычисление имитовставки и функции хэширования по СТБ П 34.101.31-2007;

– возможность авторизованной замены администратором аппаратных и программных средств ПЭВМ.

Таким образом, разработанный и изготовленный аппаратно-программный комплекс позволяет на аппаратном уровне с высокой степенью надежности обеспечить и криптографическую защиту информации, обрабатываемой и хранимой на ПЭВМ, и ее защиту от несанкционированного доступа.

С.В.МАТВЕЕВ, С.Е.КУЗНЕЦОВ

МАТЕМАТИЧЕСКИЕ ПРОБЛЕМЫ «ОБЛАЧНЫХ» ВЫЧИСЛЕНИЙ

В настоящее время становятся популярными так называемые «облачные» вычисления. Одним из основных факторов сдерживающих внедрение «облачных» вычислений являются вопросы обеспечения безопасности и конфиденциальности данных.

С точки зрения безопасности «облачные» среды можно разделить на два вида:

– доверенные,

– недоверенные.

Под доверенным «облаком» будем понимать ресурс с защищенной вычислительной средой (защищенной с точки зрения пользователя). То есть доступ к данным и результатам вычислений имеет только пользователь. Примерами таких «облачных» ресурсов могут служить выделенные ведомственные или корпоративные сети, предоставляющие услуги по хранению и обработки данных.

В недоверенной «облачной» среде доступ к данным и результатам вычислений, возможно, может быть получен третьими лицами. Безопасное (конфиденциальное) хранение данных в такой среде можно обеспечить локальным шифрованием данных с последующей передачей их в ресурсы «облака».

Рассмотрим задачу обеспечения безопасности вычислений в недоверенной «облачной» среде.

Пусть A – некоторое конечное множество, $|A|<\infty$. Обозначим $A^{\infty}=\{(a_1,\ldots,a_n),n=1\ldots\infty,a_i\in A\}$ – множество всех возможных векторов с элементами из множества A, $\Phi=\{\phi: A^{\infty}\rightarrow A^{\infty}\}$- некоторое множество функций (операций) над элементами множества A^{∞}. Задачей обеспечения безопасности «облачного» вычисления, является нахождение некоторого преобразования F, зависящего от ключа k, обладающего свойством $\phi(\bar{a})=F^{-1}(\phi(F(\bar{a}, k)), k)$ для любого элемента $\bar{a} \in A^{\infty}$ и любой операции $\phi\in\Phi$. Криптографические преобразования такого вида называются в литературе гомоморфным шифрованием. Специалистами IBM в 2009 году было найдено решение, которое использует модель под названием «идеальная решетка» и позволяет осуществлять гомоморфное шифрование данных. Однако данное решение является достаточно ресурсоемким и трудно реализуемым на практике (при обеспечении достаточного уровня стойкости преобразования).

Таким образом, актуальным является нахождение гомоморфного преобразования, обеспечивающего для актуального подмножества данных и операций безопасность вычислений.

Отдельной математической проблемой является вопрос проверки правильности результатов вычислений, полученных с помощью «облачных» ресурсов.

Н.А.МОЛДОВЯН, А.А.МОЛДОВЯН

БЕЗОПАСНОСТЬ И ФУНКЦИОНАЛЬНОСТЬ КРИПТОГРАФИЧЕСКИХ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ

Электронная цифровая подпись (ЭЦП) в настоящее время широко применяется в информационных технологиях, используемых в производственной, финансовой и экономической сферах деятельности. При этом потребности практики связаны с использованием протоколов ЭЦП, различных типов. Функциональность и безопасность

криптографических механизмов аутентификации электронной информации имеют существенное значение при принятии решения об их использовании в конкретных информационных технологиях, связанных с циркуляцией юридически значимых сообщений и документов. Часто понятие безопасности криптографических алгоритмов и протоколов сводится к стойкости последних. При этом неявно предполагается, что появление прорывных результатов по разработке алгоритмов решения трудных задач, положенных в основу криптографических механизмов в обозримом будущем имеет достаточно низкую вероятность.

Функциональность механизмов криптографической аутентификации информации можно связать с возможностью придания юридической силы электронным сообщениям при обеспечении некоторых дополнительных свойств, накладываемых особенностями решаемых практических задач. Например, протоколы слепой ЭЦП лежат в основе технологий электронных денег и позволяют построить наиболее эффективные системы тайного электронного голосования. Практический интерес имею также и протоколы групповой ЭЦП как подписи некоторого уполномоченного органа, формируемая штатными сотрудниками последнего. Другим интересным для практики типом криптосхем являются протоколы коллективной ЭЦП, обеспечивающие возможность формирования подписей фиксированного размера, принадлежащие произвольным совокупностям субъектов.

В данном сообщении рассматриваются вопросы интерпретации понятия безопасности криптосхем с учетом вероятности появления прорывных результатов в области решения трудных задач, синтез криптосхем на основе двух независимых трудных задачах, синтез протоколов аутентификации с расширенной функциональностью. Также обсуждается актуальность расширения функциональности официальных стандартов ЭЦП, путем внесения в них дополнительных разделов, специфицирующих использование стандартизованной процедуры проверки подлинности ЭЦП в протоколах коллективной, слепой, групповой и слепой коллективной ЭЦП.

Безопасность криптосхем. Под стойкостью понимается трудоемкость лучшего известного алгоритма взлома криптосхемы. Основной проблемой оценки стойкости криптосхем является то, что трудно доказать, что в ближайшем будущем не будут найдены более эффективные алгоритмы взлома по сравнению с известными в настоящее время. Для криптосистем с открытым ключом, в основу которых ставится некоторая вычислительно трудная задача, следует упомянуть доказуемо стойкие криптосистемы – криптосистемы, для которых можно формально доказать сводимость любого алгоритма взлома к решению базовой трудной задачи. Однако вопрос о том, что в настоящее время известен лучший алгоритм решения базовой трудной задачи, остается открытым, несмотря на то, что, как правило, в качестве базовых трудных задач при построении криптосхем используются давно известные и хорошо изученные задачи. С учетом сделанных замечаний становится понятным, что стойкость отражает одну из двух сторон понятия безопасности криптосхем. Вторым аспектом последнего понятия является вероятность того, что в обозримом будущем не будут получены прорывные результаты по разработке алгоритмов решения используемых трудных задач.

Принятие конкретных оценок стойкости криптосхем связано с ожидание того, что вероятность появления прорывных решений трудных задач, положенных в основу криптосхем является пренебрежимо малой. Количественная оценка порядка этой вероятности является весьма условной и трудно обосновываемой, но она является весьма существенным параметром, который входит составной частью в понятие безопасности. Таким образом, безопасность алгоритмов ЭЦП и других криптосхем связана со следующими двумя моментами: со сложностью лучшего из известных методов решения трудной задачи, положенной в основу алгоритма (текущая стойкость алгоритма) и с вероятностью появления принципиально новых методов и алгоритмов решения базовой вычислительно трудной задачи, имеющих сравнительно низкую трудоемкость (вероятность непредвиденного

взлома). То есть уровень безопасности криптосхем определяется не только сложностью решения базовой трудной задачи, но и тем фактом, что вероятность нахождения прорывных решений базовой трудной задачи в обозримом будущем является достаточно малой. Вероятность появления прорывных решений в течение ближайшего месяца или года можно оценить некоторым малым значением, например 10^{-6} или 10^{-8} (получение каких-то количественных оценок данной вероятности по своей природе относится к экспертным оценкам). Следовательно, для повышения уровня безопасности целесообразно разрабатывать схемы ЭЦП, взлом которых требует одновременного решения двух трудных задач. Существенное уменьшение вероятности взлома за счет появления прорывных решений показывает, что в схемы ЭЦП, основанные на двух трудных задачах, имеют существенно более высокий уровень безопасности. При этом вывод о более высоком уровне безопасности криптосхем, взлом которых требует одновременного решения двух независимых трудных задач определяется тем фактом, что данные вероятности достаточно малы (иначе они не могли бы быть положены в основу используемых в настоящее криптосхем), благодаря чему их перемножение дает существенно более низкие значения.

В то же время имеется вероятность нахождения прорывных подходов, приводящих к одновременному решению обеих используемых трудных задач. Такой случай имеет место в случае появления квантового компьютера при рассмотрении задач факторизации и дискретного логарифмирования. Это показывает, что объективная оценка вероятности появления прорывных атак на криптосистемы, основанные на одной или двух трудных задачах, является достаточно проблематичной. Тем не менее, рассмотрение безопасности криптосхем как векторного параметра, включающего оценку стойкости и вероятности появления прорывных решений является целесообразным и важным. В частности можно рассмотреть вероятности появления прорывных решений задачи факторизации и задачи дискретного логарифмирования в интервале времени от настоящего момента и до момента появления практически действующего квантового компьютера.

Расширение функциональности стандартов ЭЦП. Действующие стандарты ЭЦП относятся только к протоколам индивидуальной ЭЦП. Для того, чтобы способствовать более полному практическому внедрению достижений криптографии в области аутентификации информации представляет интерес вопрос расширения функциональности официальных стандартов ЭЦП при использовании единой процедуры проверки подлинности ЭЦП.

Схемы слепой ЭЦП относятся к криптографическим протоколам, обеспечивающим решение задачи анонимности (неотслеживаемости). Ряд информационных технологий (электронные деньги, тайное электронное голосования) требуют использования таких протоколов. Выполненный анализ возможности реализации протоколов слепой ЭЦП на основе стандартов ЭЦП ряда развитых стран показал, что стандарты России ГОСТ Р 34.10–94 и ГОСТ Р 34.10–2001, Беларуси СТБ 1176.2–99 и Украины ДСТУ 4145–2002 допускают реализацию схем слепой подписи. Другим типом протоколов, имеющих существенную практическую значимость, являются протоколы коллективной подписи, основанные на свертке индивидуальных параметров, генерируемых подписывающими. Установлено, что стандарты DSA, ECDSA и перечисленные ранее могут быть положены в основу протоколов коллективной ЭЦП, сохраняющих специфицированную стандартами процедуру проверки подлинности подписи. Проверочные уравнения стандартов ЭЦП ГОСТ Р 34.10–94, ГОСТ Р 34.10–2001, СТБ 1176.2–99 и ДСТУ 4145–2002 могут быть положены в основу протоколов слепой коллективной ЭЦП, а все упомянутые стандарты – в основу протоколов утверждаемой групповой ЭЦП, разработанных недавно в рамка исследования по расширению функциональности стандартов.

Утверждаемая групповая ЭЦП. В некоторых случаях требуется формирование ЭЦП к электронным документам, издаваемым некоторым коллегиальным органом. Причем должна быть обеспечена реализация следующих свойств протокола ЭЦП: 1) право и возможность подписать документ должен иметь любой представитель некоторой группы

субъектов, возглавляемой лидером; 2) лидер по значению ЭЦП может определить лицо, сформировавшее данную конкретную подпись; 3) ни один из субъектов вне указанной группы не может установить кто конкретно сформировал подпись от имени указанного коллегиального органа. Схемы ЭЦП, удовлетворяющие перечисленным условиям называются протоколами групповой подписи. Протокол утверждаемой групповой ЭЦП обеспечивает реализацию следующих дополнительных свойств: 1) ни один из субъектов внутри указанной группы, кроме лидера, не может установить кто конкретно сформировал данную групповую ЭЦП; 2) личные секретные ключи подписывающих неизвестны вторым лицам, включая лидера; 3) каждый подписанный документ утверждается лидером; 4) произвольные подмножества подписывающих могут подписать электронный документ как единый коллектив, причем состав коллектива подписывающих идентифицируется лидером непосредственно по значению ЭЦП. Были разработаны несколько вариантов утверждаемой групповой подписи, включая протокол, взлом которого требует одновременного решения задачи факторизации и задачи дискретного логарифмирования. Предложены также и варианты протоколов коллективной и слепой ЭЦП, взлом которых требует одновременного решения двух указанных трудных задач.

Разработанные протоколы коллективной, слепой коллективной и утверждаемой групповой подписи используют стандартную инфраструктуру открытых ключей, что упрощает их практическое использование.

Выполненные исследования показали целесообразность расширения функциональности ряда официальных стандартов ЭЦП (ECDSA, ГОСТ Р 34.10–2001, СТБ 1176.2–99 и ДСТУ 4145–2002), что представляется важным для практики информационной безопасности и информационных технологий и минимизирует затраты на разработку стандартов на новые типы протоколов ЭЦП.

И.А.НЕЗДОЙМИНОВ

ПРОВЕРКА КОРРЕКТНОСТИ ВСТРАИВАНИЯ ПРОГРАММНЫХ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

При разработке программного обеспечения средств криптографической защиты информации (далее СКЗИ) очень большое внимание уделяется правильности реализации криптографических алгоритмов. Как правило, программные средства криптографической защиты информации сертифицируются уполномоченными государственными органами. Однако, как показывает практика, большое количество уязвимостей СКЗИ появляется в результате ошибок встраивания отдельных программных модулей в конечный продукт. Данный программный продукт, использующий СКЗИ, подлежит дальнейшей оценке и является объектом оценки (далее ОО). Следствием некорректного встраивания может быть также появление возможности намеренного ослабления защиты путем передачи неверных или заведомо слабых параметров в сертифицированные продукты, неверной настройки критических параметров, сокращения длин паролей и другой ключевой информации, внесения «закладок» в исходный код для раскрытия секретных параметров. Таким образом, при проведении сертификационных испытаний остро стоит проблема проверки корректности встраивания. Эта проблема нуждается в исследовании, формализации требований и введении критериев оценки.

На сегодняшний день, основным подходом при проверке корректности встраивания СКЗИ является проверка исходных кодов экспертом. Экспертный метод определения значений показателей качества программных СКЗИ позволяет получать информацию о

свойствах и характеристиках программных средств на основании мнений группы экспертов-специалистов, компетентных в решении данной задачи на базе их опыта и интуиции.

Для оценки качества выполнения данных требований используются метрики. Использование метрик позволяет вводить критерии для допуска программных продуктов к работе с секретной информацией.

На основании личного опыта при проведении испытаний были сформулированы следующие общие требования:

– требования к криптографическим функциям первого уровня:
  – требования к последовательности вызов;
  – требования к передаче параметров в функции СКЗИ;
  – требования к возвращаемым параметрам и результатам выполнения функции;
– требования к криптографическим функциям второго уровня:
  – требования к последовательности вызовов криптографических функций второго уровня;
  – требования к передаче параметров в криптографические функции первого уровня;
  – требования к возвращаемым параметрам и результатам выполнения функции;
– требования по защищенности активов:
  – требования к конфиденциальности личных активов;
  – требования к целостности личных активов.

Под криптографическими функциями первого уровня (далее КФУ1) будем понимать функции объекта оценки, вызывающие криптографические преобразование средств криптографической защиты информации напрямую (без использования в этих целях вызовов других функций ОО).

Под криптографическими функциями второго уровня (далее КФУ2) будем понимать функции объекта оценки, вызывающие функции средств криптографической защиты информации посредством вызова других функций ОО.

Для оценки требований к криптографическим функциям первого уровня были введены следующие метрики:

D1 – корректность последовательности обращений;

D2 – корректность количества вызовов;

D3 – корректность типов подаваемых данных;

D4 – корректность подаваемых флагов;

D5 – корректность данных, предназначенных для использования в функциях СКЗИ;

D6 – корректность проверки результата выполнения функций СКЗИ;

D7 – корректность возвращаемых параметров при передаче их в вызывающую функцию.

Для оценки требований к криптографическим функциям второго уровня были введены следующие метрики:

D8 – корректность последовательности обращений;

D9 – корректность количества вызовов;

D10 – корректность типов подаваемых данных;

D11 – корректность подаваемых флагов;

D12 – корректность данных, предназначенных для использования в криптографических функциях первого уровня;

D13 – корректность проверки результата выполнения криптографических функций первого уровня;

D14 – корректность возвращаемых параметров при передаче их в вызывающую функцию.

Для оценки требований по защищенности активов были введены следующие метрики:

D15 – корректность считывания, генерации активов;

D16 – корректность передачи активов в процедуры СКЗИ;

D17 – корректность защиты от несанкционированного чтения и записи памяти;

D18 – корректность освобождение и очищение памяти, содержащей актив;

D19 – корректность контроля на предмет несанкционированного чтения и записи памяти, содержащей актив;

D20 – целостность личного ключа;

D21 – целостность открытого ключа;

D22 – целостность криптографических параметров.

Для проверки требований к последовательности вызовов функций СКЗИ криптографическими функциями первого уровня и расчета метрики D1 применяется экспертный и регистрационный метод при определении параметров:

$N1.1$ – количество вызовов функций СКЗИ, выполняемых согласно исходному тексту ОО;

$N1.2$ – количество ошибок в реализации последовательности вызовов функций СКЗИ.

Оцениваемыми показателями при проверке последовательности вызовов функций СКЗИ криптографическими функциями первого уровня являются:

D1 – корректность последовательности обращений.

Значение показателя D1 вычисляется следующим образом:

$$D1 = \begin{cases} 1 - \dfrac{N1.2}{N1.1} & , если\ N1.1 \neq 0 \\ 1 & , если\ N1.1 = 0 \end{cases}$$

где $N1.1$, $N1.2$ – вещественные числа.

Для того чтобы можно было оценить качество встраивания СКЗИ в ОО вводиться понятие комплексного показателя. Под понятием комплексного показателя будем подразумевать показатель качества продукции, характеризующий несколько ее свойств (ГОСТ 15467).

Пусть α_i коэффициент важности показателя D_i. Коэффициенты α_i выбираются фиксированными для каждого типа программного продукта в зависимости от важности показателя D_i. Рекомендуется выбирать коэффициенты $\alpha_i \in [0;1]$.

Комплексный показатель качества оценки требований к криптографическим функциям первого уровня КП1 вычисляется по следующей формуле:

$$КП1 = \sum_{i=1}^{7} \alpha_i D_i$$

Комплексный показатель качества оценки требований к криптографическим функциям второго уровня КП2 вычисляется по следующей формуле:

$$КП2 = \sum_{i=8}^{14} \alpha_i D_i$$

Комплексный показатель качества оценки требований к защищенности активов КП3 вычисляется по следующей формуле:

$$КП3 = \sum_{i=15}^{22} \alpha_i D_i$$

Комплексный показатель КПВ качества корректности встраивания СКЗИ вычисляется по следующей формуле:

$$КПВ = КП1 + КП2 + КП3$$

М.А.ПУДОВКИНА

ОБ АТАКАХ НА СВЯЗАННЫХ КЛЮЧАХ НА АЛГОРИТМЫ БЛОЧНОГО ШИФРОВАНИЯ

Первая в открытой литературе атака на основе метода связанных ключей была применена к алгоритму блочного шифрования LOKI и независимо предложена в работах [1], [2]. Атаки на связанных ключах используют соотношения, возникающие при зашифровании на различных, но связанных некоторым образом ключах.

На первый взгляд атаки на связанных ключах могут показаться не практичными, поскольку атакующий должен контролировать некоторые соотношения между неизвестными ключами. Однако существует ряд примеров, показывающих обратное:

– протокол 2PKDP [3], здесь практически возможны подобные атаки;

– атака на связанных ключах является практической и на протоколы обмена ключом, не гарантирующие целостность ключа. Здесь атакующий может изменять некоторым образом биты ключа без знания самого ключа;

– в протоколах обновления ключа также происходит изменение ключа с использованием известной функции, например, $k, k+1, k+2, \ldots$; например, таким является протокол, используемый во многих банках США при межбанковской коммуникации, в которых после выполнения каждой транзакции ключ увеличивается на единицу;

– атаки на связанных ключах применялись и в дисковых шифрсистемах в случае, когда оператор устанавливал роторы неверно; если оператор затем корректировал положение роторов и заново передавал этот же текст, то противник имел один открытый текст, зашифрованный на двух связанных ключах [4];

– атаки на связанных ключах структурируют множество ключей, что может использоваться для построения других атак.

– блочные шифрсистемы, поддающиеся атаке на связанных ключах, могут иметь проблемы со стойкостью при использовании в других криптосистемах; в частности, они могут оказаться непригодными в функциях хеширования (примером является алгоритм TEA[5], [6]); атака на связанных ключах была применена для вскрытия структуры MicrosoftXbox, которая использует функцию хеширования Davies-Meyer с лежащим в её основе алгоритмом TEA [7];

– иногда стойкость блочной шифрсистемы тесно связана со стойкостью относительно атак на связанным ключом, например, для 3GPP это показано в работе [8].

Также в работе [9] описана атака на связанных ключах на IBM 4758 криптопроцессор, которая может быть реализована на практике. IBM 4758 криптопроцессор используется с ATM машинами (automatic teller machines), в которой хранятся персональные идентификационные номера (пин) и ключи пользователей в защищённом главном компьютере банка. Пины и пользовательские ключи хранятся в IBM 4758 криптопроцессоре в зашифрованном виде. Шифрование происходит алгоритмом 3-DES на 168-битном ключе шифрования. Имеются несколько сценариев работы IBM 4758 криптопроцессора, которые позволяют применить атаки на основе комбинации методов связанных ключей, разностного и методов связанных ключей, сдвигов. Метод связанных ключей применим для режима EDEn, используемого в IBM 4758 криптопроцессоре. Для атаки на основе комбинации методов связанных ключей и разностного для режима EDE3 требует 2 связанных ключа, 4-подобранных открытых текста, $2^{58.5}$ шифрований, а для атаки на IBM 4758 криптопроцессор в режиме EDE5 –2 связанных ключа, 2^{6} подобранных открытых текстов, $2^{58.5}$ шифрований.

В целом, в открытой литературе разработчики криптосистем обычно создают их таким образом, чтобы они могли быть применимы без дальнейшего дополнительного анализа в различных приложениях, протоколах, режимах шифрования и в криптосистемах

хеширования, поскольку пользователи подходят к их применению «творчески». Поэтому разработанная криптосистема должна иметь высокие оценки стойкости при широком выборе сценариев атак.

В настоящее время метод связанных ключей, часто в комбинации с другими методами, применяется для атаки на блочные, поточные шифры и функции хеширования. В последние годы атаки на связанных ключах применяются в комбинации с другими методами. Наиболее часто встречаются следующие атаки:

– атака на основе методов связанных ключей и разностного;
– атака на основе методов связанных ключей и бумеранга;
– атака на основе методов связанных ключей и прямоугольника;
– атака на основе методов связанных ключей и линейного;
– атака на основе методов связанных ключей, разностного и линейного.

Характерной особенностью атак на основе метода связанных ключей на блочные шифрсистемы является использование свойств алгоритма развёртывания ключа. В основном данной атаке подвержены алгоритмы шифрования с простыми алгоритмами развёртывания ключа. В настоящее время атаки на связанных ключах применимы, например, к следующим алгоритмам: LOKI, AES, IDEA, ГОСТ 28147-89, TEA, KASUMI, SHACAL, XTEA, Cobra-H64, Cobra-H128, CIKS-1, SPECTR-H64, Cobra-F64a, Cobra-F64b, Cobra-S128, Square, блочный алгоритм функции хеширования HAS-160 (в режиме шифрования), DES-EXE, DESX+, 3-DES, NewDES-1996, RC2, CAST, G-DES, SAFER, MIBS и др.

В работе [10] считается, что имеется два основных класса атак на связанных ключах. Первый класс состоит из атак, использующие связанные с ключом пары открытых текстов. Этот класс возник ещё в работах [2] и [1]. В этих атаках используются пары ключей, при которых большая часть функций зашифрования похожи. Такие соотношения между парами открытого текста возможны для простых алгоритмов развёртывания ключа. Кроме того, в этом случае раундовая функция не зависит от номера раунда. Второй класс был изначально введён в работах [11], [12]. Состоит из атак, в которых рассматриваются соотношения между связанными ключами, для исследования статистических свойств функции зашифрования. Сюда относится, в частности, в ведение разностей между связанными ключами, которые используются в большой разновидности атак, например, в атаках на основе: методов связанных ключей и разностном, методов связанных ключей и бумеранга, методов связанных ключей и прямоугольника, методов связанных ключей и линейного. В работе [10] объединяются основные идеи из этих двух классов для описания общей атаки на связанных ключах. В работе [13] рассматривается класс итерационных блочных шифров, у которых алгоритм развёртывания ключа задаётся рекуррентой с глубиной зависимости меньше числа раундов, а раундовая функция зависит от ключа, и не зависит от номера раунда. Такой класс алгоритмов развёртывания ключа имеют, например, шифры: 25-раундовый ГОСТ 28147-89, полнораундовые LOKI89, LOKI91, KeeLoq, TREYFER, MMB. Для данного класса блочных шифров предложена атака на основе метода связанных ключей, требующая небольшое число произвольных открытых текстов и с трудоёмкостью практически равной трудоёмкости опробования одного раундового ключа. Получено, что для атаки на такой блочный шифр часто достаточно только двух открытых текстов. Для построения данной атаки использовалась идея из сдвигового метода [14]. Также приведена атака на шифры Фейстеля. Её трудоёмкость почти в корень меньше трудоемкости атаки на итерационный блочный шифр с произвольной раундовой функцией.

Особо отметим атаки на некоторые блочные шифрсистемы. Блочная шифрсистема KASUMI составляет ядро шифрсистем A5/3 и UAE1. Последняя заменяет A5/3 в телефонных сетях третьего поколения. В основе KASUMI лежит блочный алгоритм MISTY. Желая сделать KASUMI более быстродействующим и проще реализуемым аппаратно по сравнению с MISTY, разработчики KASUMI внесли ряд изменений в алгоритм развёртывания ключа KASUMI. Атаки на основе метода связанных ключей описаны в работах [15], [16], [17]. Так в

работе [17] предложена атака на основе связанных ключей и сэндвич-атаки. Сэндвич-атака является обобщением метода бумеранга. Для атаки [17] требуется четыре связанных ключа, 2^{26} – данных (шифртекстов и открытых текстов), 2^{30} байтов памяти и 2^{32} шифрований. При реализации её на одном компьютере (Intel CoreDuo 2, T7200 CPU, 2 GHz, 4 MBL2 Cache, 2 GBRAM, Linux-2.6.27 kernel) 96-битный ключ находится за несколько минут, а весь 128-битный ключ шифрования – менее чем за два часа. Отмечено, что данная атака не может быть применена к MISTY, поскольку использует благоприятную для атаки структуру, которая возникла при изменении алгоритма MISTY. Кроме того, возможно незначительное изменение в структуре алгоритма развёртывания ключа MISTY, которое сделает данную атаку невозможной. Таким образом, модификация алгоритма MISTY привела к более слабому алгоритму KASUMI.

В серии работ [18]–[24] корейских криптографов анализировалось семейство алгоритмов блочного шифрования, основанных на управляемых перестановках, использованных Молдовян Н.А., Молдовян А.А., Гуц Н.Д., Изотов Б.В [25]. К такому классу относятся шифрсистемы CIKS-1, SPECTR, Cobra, Eagle. Эти шифрсистемы имеют простые алгоритмы развёртывания ключа и содержат потенциальные слабости в управляемых перестановках относительно комбинации методов связанных ключей и разностного. Так в работе [22] описаны вероятностные свойства управляемых перестановок раундовых функций Cobra-S128, Cobra-F64a и Cobra-F64b, позволившие найти «хорошую» для криптоанализа разностную характеристику, используемую в атаке на связанных ключах. Работа [23] также посвящена атакам на алгоритмы Cobra-F64a и Cobra-F64b. В ней удаётся найти лучшую разностную характеристику и на основе неё с помощью комбинации методов связанных ключей и прямоугольника атаковать полнораундовые алгоритмы Cobra-F64a и Cobra-F64b. При построении данной разностной характеристики использовалась и простота алгоритмов развёртывания ключа. В работе [23] также отмечается, что при синтезе следует избегать простых алгоритмов развёртывания ключа, чтобы не допустить простые атаки на связанных ключах. В работе [21] атакуются 64-битные алгоритмы CIKS-1, SPECTR-H64 с 256-битным ключом шифрования. Одной из основных слабостей управляемых перестановок, используемых в алгоритмах CIKS-1, SPECTR-H64, является то, что они сохраняют вес Хемминга. Применяя это свойство и простоту АРК, предложены атаки на основе методов связанных ключей и разностного на полнораундовые алгоритмы CIKS-1, SPECTR-H64.

Алгоритм ГОСТ 28147-89, имея простой алгоритм развёртывания ключа, содержит ряд потенциальный слабостей. В частности, это относится к линейности алгоритма развёртывания ключа, использованию блоков ключа в явном виде в раундовых функциях, частичной рекуррентности. В последние годы в открытой литературе появилось немало работ [26]– [30], в которых проводился криптоанализ алгоритма ГОСТ 28147-89 на основе связанных ключей. В работе [28] приведена атака на ГОСТ 28147-89 на основе методов бумеранга и связанных ключей, которая содержит ряд ошибок и реально не работает. Однако основная идея, лежащая в её основе, позволяет подправить предложенную атаку и, внеся дополнительные модификации, получить работающий алгоритм. Это было сделано в работе [29]. В предложенной атаке для нахождения всего ключа шифрования при использовании s-боксов из [30] требуется 18 связанных ключей, а трудоёмкость оценивается в 2^{26} зашифрований. В работе [31] описывается атака на алгоритм ГОСТ 28147-89 на основе четырех и двух связанных ключей. Также в ней получена ещё одна классификация s-боксов, при которых невозможна атака на алгоритм ГОСТ 28147-89 описываемым подходом.

В настоящее время имеется немало атак на связанных ключах на шифрсистему AES, например, [32]–[36]. Так в работе [37] описан ряд атак на основе метода связанных ключей на AES с длиной ключа 256 бит и с 10 раундами. Одна из описанных атак может вскрыть 9-раундовый AES-256 с двумя связанными ключами трудоёмкостью 2^{39} зашифрований, другая вскрывает 10-раундовый AES-256 с четырьмя связанными ключами трудоёмкостью

2^{45} зашифрований. Построение такой атаки на шифр AES-256 возможно из-за «плохих» свойств АРК. Так алгоритм развёртывания ключа: а) перемешивает ключ недостаточно; б) является довольно линейным (в нём недостаточно нелинейных преобразований). Следствием этого является построение разностной характеристики в алгоритме развёртывания ключа, справедливой на большом числе раундов. Сходство между АРК и раундовой функцией позволяет «обнулять» разности между связанными ключами с разностями между промежуточными шифртекстами для большого числа раундов, что приводит к построению локальных коллизий.

Литература

1. *Knudsen L.R.*, Cryptanalysis of LOKI91, AUSCRYPT'92, LNCS, v.718, pp. 196-208, Springer, 1993.

2. *Biham E.*, New Types of Cryptanalytic Attacks Using Related Keys. EUROCRIPT'93, LNCS, v.765, 1994, pp.398-409.

3. *Tsudik G., Van Herreweghen E.*, On simple and secure key distribution. In: Conference on Computer and Communications Security, Proceedings of the 1st ACM conference on Computer and communications security, pp. 49–57. ACM Press, New York, 1993.

4. *Diffie W., Hellman M.E.*, Privacy and Authentication: An Introduction to Cryptography. Proceedings of the IEEE, v.67, N3, March 1979.

5. *Winternitz R.*, Producing One-Way Hash Functions from DES. Advances in Cryptology, Proceedings of Crypto 83, Plenum Press, pp.203-207, 1984.

6. Research and Development in Advanced Communication Technologies in Europe, RIPE Integrity Primitives: Final Report of RACE Integrity Primitives Evaluation (R1040), RACE, Jun 1992.

7. ZDNet, New Xbox security cracked by Linux fans, 2002, http://news.zdnet.co.uk/software/developer/0, 39020387,2123851,00.htm

8. *Iwata T., Kohno T.*, New Security Proofs for the 3GPP Confidentiality and Integrity Algorithms. FSE 2004. LNCS, vol. 3017, pp.427–445. Springer, Heidelberg, 2004.

9. *Phan R. C.-W.*, Handschuh H., On Related-Key and Collision Attacks: The Case for the IBM 4758 Cryptoprocessor.

10. *Biham E., Dunkelman O., Keller N.,* A Unified Approach to Related-Key Attacks, FSE 2008, LNCS, v.5086, pp. 73–96, 2008.

11. *Kelsey J., Schneier B., Wagner D.*, Key-Schedule Cryptanalysis of IDEA, GDES, GOST, SAFER and Triple-DES. Advances in Cryptology, Crypto'96, LNCS, v.1109, pp.237–251, Springer, 1996.

12. *Kelsey J., Schneier B., Wagner D.*, Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, New DES, RC2, TEA. International Conference on Information and Communications Security, ICICS'97, LNCS, v.1334. pp.233–246, Springer, 1997.

13. *Пудовкина М.А.*, О слабом классе алгоритмов развёртывания ключа относительно метода связанных ключей // Прикладная дискретная математика. Приложение. 2010.

14. *Biryukov, A., Wagner, D.*, Slide Attacks. FSE'1999.LNCS, v.1636, pp.245–259.Springer, 1999.

15. *Biham, E., Dunkelman, O., Keller N.A.*, Related-Key Rectangle Attack on the Full KASUMI. ASIACRYPT'2005. LNCS, v.3788, pp.443–461.Springer, 2005.

16. *Kim J., Hong S., Preneel B., Biham E., Dunkelman O., Keller N.*, Related-Key Boomerang and Rectangle Attacks, IACR ePrint report 2010/019

17. *Dunkelman O., Keller N., Shamir A.*, A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony, CRYPTO 2010, LNCS, v.6223, p.393–410, 2010.

18. *Ko Y., Hong D., Hong S., Lee S.*, Lim J, Linear Cryptanalysis on SPECTRH64 with Higher Order Differential Property, MMM-ACNS03, LNCS, v.2776, pp.298-307, Springer, 2003.

19. *Ko Y., Lee C., Hong S., Sung J., Lee S.*, Related-Key Attacks on DDP based Ciphers: CIKS-128 and CIKS-128H. Indocrypt'2004, LNCS, v.3348, pp.191-205, Springer, 2004.

20. *Lee C., Hong D., Lee S., Lee S., Yang H., Lim J.A.*, Chosen Plaintext Linear Attack on Block Cipher CIKS-1.ICICS'2002, LNCS, v.2513, pp.456-468, Springer, 2002.

21. *Ko Y., Lee C., Hong S., Lee S.*, Related Key Differential Cryptanalysis of Full-Round SPECTR-H64 and CIKS-1. ACISP'2004, LNCS, v.3108, pp.137–148, 2004.

22. Lee *C., Kim J., Hong S., Sung J., Lee S.*, Related-Key Differential Attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b. Mycrypt'2005, LNCS, v.3715, pp.244–262, 2005.

23. *Lu J., Lee C., Kim J.*, Related-Key Attacks on the Full-Round Cobra-F64 and Cobra-F64b. SCN'2006. LNCS, v.4116, pp.95–110. Springer, 2006.

24. *Jeong K., Lee C., Sung J., Hong S., Lim J.*, Related-Key Amplified Boomerang Attacks on the Full-Round Eagle-64 and Eagle-128, ACISP 2007, LNCS 4586, p.143–157, 2007.

25. *Молдовян А. А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В.*, Криптография скоростные шифры, Санкт-Петербург, «БХВ-Петербург», 2002.

26. *Seki H., Kaneko T.*, Differential cryptanalysis of reduced rounds of Gost. Selected Areas in Cryptography, v.2012, LNCS, pp.315–323. Springer, 2000.

27. *Ko Y., Hong S., Lee W., Lee S., Kang J.-S.*, Related key differential attacks on 27 rounds of XTEA and full-round GOST. FSE, LNCS, v.3017, pp.299–316, Springer, 2004.

28. *Fleischmann E., Gorski M., Huhne J.-H., Lucks S.*, Key Recovery Attack on full GOST Block Cipher with Zero Time and Memory, WEWoRC, 2009.

29. Rudskoy V., On zero practical significance of "Key recovery attack on full GOST block cipher with zero time and memory", http://eprint.iacr.org/2010/

30. Шнайер Б., Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2002.

31. *Пудовкина М.А., Хоруженко Г.И.*, Атаки на алгоритм блочного шифрования ГОСТ 28147-89 с двумя и четырьмя связанными ключам// Прикладная дискретная математика. Приложение. 2010.

32. *Kim J., Hong S., Preneel B.*, Related-Key Rectangle Attacks on Reduced AES-192 and AES-256, FSE 2007, LNCS 4593, pp. 225–241, 2007.

33. *Biham E., Dunkelman O., Keller N.*, Related-Key Boomerang and Rectangle Attacks. EUROCRYPT 2005. LNCS, vol. 3494, pp. 507–525. Springer, Heidelberg ,2005.

34. *Hong S., Kim J., Lee S., Preneel B.*, Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192. FSE 2005. LNCS, vol. 3557, pp. 368–383. Springer, Heidelberg, 2005.

35. *Zhang W., Zhang L., Wu W., Feng D.*, Related-Key Differential-Linear Attacks on Reduced AES-192, Indocrypt 2007, LNCS 4859, pp. 73–85, 2007.

36. *Biryukov A., Khovratovich D., Nikolic I.*, Distinguisher and Related-Key Attack on the Full AES-256, CRYPTO 2009, LNCS 5677, pp. 231–249, 2009.

37. *Biryukov A., Dunkelman O., Keller N., Khovratovich D.*, Shamir A., Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds// EUROCRYPT 2010, LNCS 6110, pp. 299–319, 2010.

С.Б.САЛОМАТИН, Д.М.БИЛЬДЮК

ДИНАМИЧЕСКОЕ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ В СИСТЕМЕ ГРУППОВОЙ СВЯЗИ

Рассматривается два вида систем. Одна система использует одноключевые алгоритмы шифрования. Вторая система применяет корректирующие коды и однонаправленные хэш-функции.

Система генерации и распределения ключей для одноключевых блочных алгоритмов шифрования

Криптографическая система построена на основе смарт-карт. В качестве криптографических преобразований используются преобразования по ГОСТ 28147 .

Формирование случайных последовательностей в системе осуществляется при помощи генератора случайных чисел реализованного в смарт-картах (на основе тепловых шумов транзисторов).

Любые ключевые данные (К) в системе используются совместно с дата-временной группой (ДВГ – дата и время их формирования) и имитовставкой (И) используемой для контроля целостности ключевых данных.

В общем виде формирование ключевого пространства осуществляется следующим образом:

а) Система генерации и распределения ключевого пространства (СГРКП) формирует Мастер-ключ (МК) и передает его в Диспетчерский Центр (ДЦ) (на смарт-карте).

б) Для каждого Абонентского Устройства (АУ) формируется свой случайный идентификационный номер (ID). Данный ID шифруется на МК по ГОСТ 28147 в режиме простой замены – результат расшифрования принимается в качестве индивидуального ключа (ИК) АУ. ID и ИК передаются на АУ.

Криптографические преобразования информации передаваемой в канале связи происходят на индивидуальных ключах АУ. Для этого каждое АУ перед началом работы регистрирует свой ID в ДЦ. ДЦ, если необходимо, вырабатывает ИК путем расшифрования ID на МК по ГОСТ 28147 в режиме простой замены.

Система генерации и распределения ключей (СГРКП) представляет собой ПЭВМ с соответствующим программным обеспечением (ПО) и базой данных (БД), содержащей иерархию и идентификационные данные абонентских устройств (АУ). ПО реализует интерфейсы по управлению БД и смарт-картами.

Основные криптопротоколы системы:

а) *Регистрация ID.* АУ высылает свой ID и дата-временную группу, соответствующую конкретному МК (т.е. конкретной версии ключевого пространства). Если ДВГ текущего МК и высланного ID совпадает, то регистрация ID считается пройденной успешно (в противном случае может происходить смена ключевого пространства см. ниже).

б) *Взаимная аутентификация АУ и ДЦ.* ДЦ запрашивает в АУ случайное число R1. Далее ДЦ, на основе зарегистрированного ID вычисляет индивидуальный ключ (ИК) АУ ИК = $E_{МК}(ID)$. На основе ИК формируется сессионный ключ (СК) аутентификации: ДЦ формирует случайное число R2, формирует число R=R1|R2, СК=$E_{ИК}(R)$. ДЦ формирует новый случайный ID’ АУ не изменяя при этом его ДВГ (текущий МК не меняется), на основе нового ID’ вычисляется новый ИК’ АУ ИК’ = $E_{МК}(ID’)$. На основе проведенных выше вычислений формируется ответная криптограмма АУ зашифрованная на СК АУ приняв криптограмму отправляет ее в карту АУ. В карте происходит расшифровка и проверка целостности криптограммы на СК.

Процедура аутентификации абонентским устройством диспетчерского центра происходит путем сравнения случайного числа R1, запрошенного ранее диспетчерским центром и хранящегося в памяти карты АУ, и числа R1 переданного в зашифрованном виде в ответной криптограмме. После смены текущего ID и ИК в АУ происходит повторная регистрация нового ID в ДЦ. Процедура аутентификации диспетчерским центром абонентского устройства происходит путем сравнения вновь зарегистрированного ID и ID' отправленного в зашифрованном виде в ответной криптограмме.

Таким образом, каждая регистрация любого АУ в ДЦ приводит к смене ИК в АУ без смены текущего МК.

После успешной регистрации АУ и ДЦ могут вести информационный обмен по защищенному каналу связи на ИК по ГОСТ 28147 в режиме гаммирования с ОС и выработкой имитовставки.

Еще одной дополнительной процедурой работы криптосистемы в основном режиме может быть процедура смены МК или смены ключевого пространства (версии ключевого пространства) системы. Данная процедура сильно напоминает процедуру регистрации АУ, отличие состоит в том, что в результате происходит смена не ID и ИК, а смена только ИК, причем со сменой ДВГ последнего. Со стороны ДЦ сама процедура представляет собой смену одной карты ДЦ на другую. При этом в АУ необходимо сменить текущий ИК (обозначим ИК1), вычисляемый в ДЦ на текущем МК (обозначим МК1), на новый (обозначим ИК2), вычисляемый на новом МК (обозначим МК2).

Метод динамического распределения ключей, использующий разделимый код с максимальным расстоянием (МДР-код)

В качестве МДР- кода используется блочный (n, k)-код, отображающий информационные символы конечного поля GF(q^k) в поле GF(q^n). В процессе кодирование $E(\mathbf{m}) = \mathbf{c}$ сообщение $\mathbf{m} = m_1, m_2,\ldots,m_k$ отображается в кодовое слово $\mathbf{c} = c_1, c_2, \ldots, c_n$. В процессе декодирование происходит восстановление информационного слова $D(c_{i_1}, c_{i_2}, ..., c_{i_k}, i_1, i_2, ..., i_k) = \mathbf{m}$. Минимальное кодовое расстояние МДР-код удовлетворяет равенству $d_{\min} = n - k + 1$. В режиме исправления только стираний достаточно найти решение системы линейных уравнений $\mathbf{y}\mathbf{H}^T = 0$, где $\mathbf{y}$ –декодируемый вектор, $\mathbf{H}$ – проверочная матрица кода. Для (n, k) МДР-кода k символов сообщения $\mathbf{m}$ могут быть восстановлены из любых k символов кодового слова $\mathbf{c}$ [1, 2].

Алгоритм распределения ключа включает три этапа.

1. Центр формирования ключа (ЦФК) группы из p пользователей формирует МДР-код с параметрами (n, k) над полем GF(q), $n > 2k - 1$. ЦФК определяет однонаправленную функцию f(.) над тем же полем.

2. ЦФК объединяет нескольких пользователей в группу авторизованных пользователей. ЦФК от нового пользователя i получает пару (j_i, s_i), где s_i – случайный символ в f(.), j_i – положительное целое, удовлетворяющее следующим требованиям: $k \le j_i \le n$; $j_i \ne j_r$, для всех r пользователей группы. Пара (j_i, s_i) используется как зерно ключа.

3. ЦФК случайным образом выбирает элемент z в заданном поле. Для каждого пользователя формируется элемент $c_{j_i} = \mathrm{f}(s_i \vdots z)$. Используя полученные элементы, вычисляется кодовое слово МДР-кода, размещая на j-й позиции символ c_j и заполняя первые ($k - p$) позиций случайными символами поля. Для МДР-кода кодовое слово $\mathbf{c}$ будет однозначно определяется своими k символами. Далее, используя процедуру кодирования со стираниями, ЦФК вычисляет первые (k – 1) символов $c_1, c_2, ..., c_{k-1}$ кодового слова **c.**

Декодирование **c** позволяет получить сообщение **m** = m_1, m_2,…,m_k и вычислить сессионный ключ K = U(**m**), где U – предопределенная функция, формирующая слово заданного размера.

ЦФК объявляет пользователям группы значение z и $c_1, c_2, ..., c_{k-1}$.

Каждый пользователь группы вычисляет $c_{j_i} = \mathrm{f}(s_i : z)$. Формирует последовательность $c_1, c_2, ..., c_{k-1}, c_{j_i}, k \le j_i \le n$, добавляя в нее вычисленный символ. Применяет к полученной последовательности процедуру декодирования со стираниями МДР-кода и восстанавливает сообщение **m**. После чего вычисляет ключ K = U(**m**).

Свойства МДР-кода гарантируют, что каждый авторизованный пользователь со своим значением c_{j_i} и последовательностью $c_1, c_2, ..., c_{k-1}$ сможет выполнить процедуру декодирования и восстановить сообщение.

Любой неавторизованный пользователь не сможет восстановить сообщение **m** и $c_1, c_2, ..., c_{k-1}$ поскольку не знает требуемого символа c_{j_i}.

Усилия, которые могут быть предприняты для взлома ключа схемы над конечным полем не меньшие, чем усилия атаки грубой силы.

Заметим, что для всех (n, k) МДР-коды над GF(q), $q = 2^m$, q + 1 = 2^m + 1. Сессионный ключ размером l бит, способен поддерживать 2^l пользователей одной группы.

Техническая реализация

Абонентское устройство реализовано на базе микроконтроллера LPC1768 (NXP) с ядром Cortex-M3. ПО для микроконтроллера реализовано на языке C++ с использованием RTOS компании KEIL (RTX). Передача данных осуществляется при помощи GSM-модема Q2686 (Sierra Wireless). ПО модема реализовано на языке C++ с использованием RTOS ADL.

ПО диспетчерского центра и системы генерации ключей является кросплатформенным и реализовано при помощи языка C++ с использованием библиотек QT 4.7 (LGPL).

В качестве устройств криптографического преобразования и защищенного хранения данных использованы смарт-карты с ОС «ОСКАР».

Литература

1. Lihao Xu, Cheng Huang Computation-Efficient Multicast Key Distribution IEEE TRANS. ON PARALLEL AND DISTRIBUTED SYSTEMS,VOL.19, NO.5, MAY 2008.

2. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир. 1986.

С.Б.САЛОМАТИН, А.А.ОХРИМЕНКО

ФОРМИРОВАНИЕ КЛЮЧЕВОГО ПРОСТРАНСТВА НА ОСНОВЕ МОДЕЛИ МНОГОКАНАЛЬНЫХ СЛУЧАЙНЫХ МАРШРУТОВ И ГРАФОВ

Одной из основных задач, возникающей при использовании криптографических методов защиты информации, является формирование ключевого пространства. Методы, использующие однонаправленные функции, не учитывают возможности использования многоканальности сетевых структур.

В настоящей работе рассматривается метод формирования ключевого пространства на основе принципа совершенного шифра и модели многоканальных случайных маршрутов (МСМ).

Модель сети. Сеть моделируется как 2-х мерная квадратная решетка, каждый узел которой связан с четырьмя соседними узлами. Каналы сети отождествляются с ребрами, соединяющие соседние узлы целочисленной решетки на плоскости. Предполагается, что аналитик-оппонент может контролировать любой узел с вероятностью $p_0 \in [0,1]$. Такие узлы определим как незащищенные, в то время как остальные узлы считаются защищенными. Передающая и приемная стороны могут располагаться в любом узле сети [3].

Задача состоит в передачи по сети секретного ключа *K*. Передающая и приемная стороны не знают расположения, но известна вероятность $p_з = 1 - p_0$ существования защищенных узлов. Каждое сообщение, прошедшее через один или несколько незащищенных узлов считается доступным оппоненту.

Алгоритм передачи ключа:

1. Передающая сторона использует процедуру случайного выбора маршрутов, и передают *M* блоков сообщений $m_1, m_2, \ldots, m_M$. Сообщения имеют размер, равный длине ключа *K*.

2. На приемной и передающей стороне вычисляется ключ в результате модулярного сложения сообщений

$$K = \bigoplus_{i=1}^{M} m_i .$$

Для восстановления ключа аналитику требуется перехватить все сообщения $\{m_i\}$. Отсутствие у аналитика хотя бы одной компоненты перехвата, рассматривать *K* как совершенный шифр и определяет уровень защиты ключа.

Для оценки вероятностных характеристик алгоритма используем перколяционную модель [1, 2] графа сети.

Определим регулярный граф $G = < V, E > \in Z^2$, где V – множество вершин, E – множество ребер графа. Вершины графа предполагаются открытыми для наблюдения с вероятностью *p* или закрытыми с вероятностью *(1–p)*. Все ребра графа являются открытыми. Считаем, что путь в графе *G* определяется как последовательность прохождения смежных вершин $\pi = v_1, v_2, \ldots$, где для всех $i \geq 1$, вершины v_i и v_{i+1} – смежные. Путь считается открытым, если все вершины v_i открыты.

Введем обозначение *W(v)* для объединений всех ребер всех проводящих путей, начинающихся в *v*, $v \in Z^2$. Это множество всех точек, которые могут быть достигнуты жидкостью из вершины v. Оно называется связной компонентой или кластером вершины v. Множество *W(v)* пусто тогда и только тогда, когда все четыре ребра, инцидентные вершине v, непроводящие.

Конфигурация занятости есть отображение ω общего множества вершин в множество *{-1, 1}*. Путь в *G* называется занятым путем, если все вершины этого пути являются занятыми. Путь называется свободным путем, если все вершины этого пути свободны.

Перколяционная вероятность $\theta(p)$ определяется как вероятность того, что исходная или любая другая вершина связана с бесконечно открытым кластером $\theta(p) = \mathbf{P}(|C = \infty|) = 1$, где **P** – вероятностная мера

Существует критическое значение (критическая вероятность) $p_c(d)$ для p, такое, что $\theta(p) = 0$ для любого $p < p_c(d)$ и $\theta(p) > 0$ для любого $p > p_c(d)$. Формально критическая вероятность определяется как $p_c = \max\{p : \theta(p) = 0\}$.

Основная задача безопасной сети обеспечить высокий уровень защиты передачи сообщений. В этой связи представляет интерес значения *p*, соответствующие областям $\theta(p) \cong 1$, в которых сеть имеет бесконечно защищенный кластер.

Модель МСМ с фиксированной длиной l пути. Пусть существуют различные пути, которые имеют одинаковую длину *l*. Каждому передаваемому сообщению поставим в соответствие случайно выбранный путь. Вероятность того, что алгоритм успешно выбирает надежный защищенный путь для посылки хотя бы одного сообщения, зависит от вероятности *p* и длины *l*: P (1,*p*,*d*,*l*) = p^l, где *d* – расстояние между взаимодействующими сторонами.

Модель МСМ с требуемой длиной пути k. Алгоритм использует только *k* маршрутов, длины которых кратны *d*. Для каждого сообщения алгоритм выбирает случайное значение *l* из множества чисел, соответствующих кратным длинам и в соответствии с равномерным законом распределением вероятностей. Таким образом, алгоритм с требуемой длиной пути *k* использует алгоритм с фиксированной длиной пути, что гарантирует прохождение сообщением пути длиной *l*.

Основные соотношения стохастического алгоритма.

Вероятность соединения по защищенному пути равна $(\theta(p))^2$. Вероятность того, что алгоритм на основе модели МСМ с требуемой длиной пути k успешно выберет надежный путь для посылки как минимум одного сообщения, равна

$$\beta = [p^d(1 - p^{(k-1)d}] / [(k - 1)d(1 - p)].$$

Динамическая атака. Аналитик-оппонент часто меняет узлы атаки, перебирая множество узлов. Вероятность того, что существует как минимум один надежный путь в *n* маршрутах, оценивается как

$$P(n, p, d, k) = 1 - (1 - \beta)^n.$$

Модель МСМ с использованием LDPC-кода. Ключевая идея состоит в согласовании графа сети с классом графом кода, исправляющего и обнаруживающего ошибки [2]. Модель сети использует дополнительные, избыточные транслирующие узлы и предполагает пространственное кодирование путей сообщений корректирующим LDPC-кодом. Алгоритм кодирования предполагает введение узлов-верификаторов и проверочных узлов, а также организацию пересылки сообщений от каждого из символьных узлов верификаторов к смежным с ним проверочным узлам и обратно. Модель такого типа способна обнаружить не только факт искажения или замены информации, но и факт присутствия криптоаналитика.

Литература

1. G. Grimmett, Percolation, 2nd ed.Springer-Verlag, 1999.

2. P. D. Seymourand, D. J. A.Welsh,“Percolation probabilities on the Square lattice», Ann. Discrete Math.,vol. 3,pp. 227–245, 1978.

3. Q. C. Le, P. Bellot, A. Demaille, «Stochastic Routing in Large Grid Shaped Quantum Networks», in Proc. Of the 5th Int. Conf. on Computer Sciences, Research Innovation and Vision for the Futur, Vietnam, 2007.

4. X. Bao and J.(T). Li «Matching Code-on-Graph with Network-on-Graph: Adaptive Network Coding for Wireless Relay Networks», In Proc. 43rd Allerton Conf. on Communication, Control, and Computing, Sep. 2005.

А.В.СИДОРЕНКО, К.С.МУЛЯРЧИК

ЦИФРОВЫЕ ОТОБРАЖЕНИЯ ДЛЯ СИСТЕМ ШИФРОВАНИЯ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА

Эффективное применение информационных технологий в различных сферах деятельности человека является стратегическим фактором роста обмена информацией, проведения переговоров, обеспечения управления производством и бизнесом.

Для обеспечения защиты информационных ресурсов, включая конфиденциальность, целостность и доступность информации, выделяются технологии криптографической защиты данных.

Развитие теории динамического хаоса в последние годы способствовало разработке на ее основе новых методов защиты информации. Хаос и криптография имеют ряд общих фундаментальных свойств, среди которых чувствительность к начальным условиям и апериодичность траекторий в фазовом пространстве хаотических динамических систем, обеспечивают такие свойства криптографических систем как запутывание и рассеяние [1, 2].

Система криптографической защиты информации состоит из определенного числа блоков. Как правило, структурная схема криптографической защиты информации включает: источник информации, блок шифрования, канал передачи данных, блок расшифрования, приемник информации. В нашей работе [3] рассматривается модификация метода шифрования данных, основанного на использовании tent-отображения в схеме с нелинейным подмешиванием информационного сигнала к хаотическому. При анализе системы отмечается важность выбора хаотического отображения.

В цифровой криптографической системе на основе динамического хаоса выбор хаотического отображения приобретает принципиальное значение, что обусловлено необходимостью целочисленного представления информации.

Целью работы является определение условий использования хаотических отображений при построении алгоритмов шифрования данных на основе цифровых хаотических систем.

Для цифровых хаотических систем одними из основных показателей хаотического поведения являются дискретный показатель Ляпунова и энтропия. Известно, что устойчивость по Ляпунову характеризует устойчивость конкретного режима функционирования динамической системы. Показатель Ляпунова определяет устойчивость фазовой траектории динамической системы. Установлено, что при отрицательных значениях показателя Ляпунова фазовая траектория системы является устойчивой, при положительных – неустойчивой. В свою очередь, энтропия соответствует мере неопределенности появления очередного значения последовательности. Известно, что чем выше энтропия, тем меньше вероятность появления определенного значения последовательности. Нулевая энтропия определяет полностью стационарный (детерминированный) процесс.

Таким образом, цифровая система является хаотической, если ее дискретный показатель Ляпунова положителен при стремлении размерности фазового пространства системы M к бесконечности [1].

В работе [4] сообщается, что дискретный показатель Ляпунова характеризует свойство запутывания криптографических систем. Поэтому использование указанного показателя позволяет оценить пригодность того или иного цифрового хаотического отображения для применений в алгоритмах шифрования.

Дискретный показатель Ляпунова λ_{F_m} для цифрового отображения $F:\{0,1,...,M-1\}\to\{0,1,...,M-1\}$ определяется выражением

$$\lambda_{F_M}=\frac{1}{M}\left[\sum_{i=0}^{M-2}\ln\left|F_M(i+1)-F_M(i)\right|\right]+\frac{1}{M}\ln\left|F_M(M-2)-F_M(M-1)\right|$$

Для периодической орбиты $\alpha = \{a_0, a_1 = F(a_0), ..., a_{T-1} = F(a_{T-2})\}$ с периодом T отображения F при условиях, что $a_0 \neq a_1 \neq ... \neq a_{T-1}$ и $F(a_{T-1}) = a_0$ (что аналогично $F^T(a_0) = a_0$) дискретный показатель Ляпунова записывается в виде

$$\lambda_{(F,\alpha)} = \frac{1}{T}\sum_{k=0}^{T-1} \ln\left|F_M(a_k + 1) - F(a_k)\right|$$

С другой стороны, дискретный показатель Ляпунова отображения F может быть определен как взвешенная сумма дискретных показателей Ляпунова всех периодических орбит отображения F

$$\lambda_F = \sum_j \frac{T_j}{M}\lambda_{(F,\alpha_j)}.$$

Очевидно, что дискретный показатель Ляпунова отображения F изменяется в пределах $0 \le \lambda_F \le \ln(M-1)$. Отображение с нулевым дискретным показателем Ляпунова будет иметь вид $F(x) = x$ для каждого $x \in \{0,1,..., M-1\}$.

Среди свойств показателя Ляпунова отмечается, что для любого отображения F на множестве $\{0,1,..., M-1\}$ дискретный показатель Ляпунова $\lambda_F \le \lambda_{F_{\max}}$, где $\lambda_{F_{\max}}$ - максимальный дискретный показатель Ляпунова среди всех отображений на дискретном фазовом пространстве размерностью M.

Вторым важным показателем хаотического поведения цифровых отображений является дискретная энтропия, определенная в [5] следующим образом:

$$\overline{H}_\delta^{(n)}(F) = -\frac{1}{n-1}\sum_{\pi\in\sigma_n} q_\pi \log q_\pi ,$$

где $\overline{H}_\delta^{(n)}(F)$ – дискретная энтропия порядка n цифрового отображения F, q_π – вероятность применения перестановки π к последовательности длиной n, которая, в свою очередь определяется следующим выражением:

$$q_\pi(n) = \frac{|Q_\pi(n)|}{\sum_{\pi\in\sigma_n}|Q_\pi(n)|},$$

где

$$Q_\pi(n) = \left\{s \in S : F^{\pi(0)}(s) < ... < F^{\pi(n-1)}(s)\right\}$$

s – количество точек фазового пространства $S = \{0,1,..., M-1\}$, каждая из которых, посредством следующей за ней последовательности длины n, формирует перестановку π. Усредненная дискретная энтропия для отображения определяется как

$$h_\delta(F) = \frac{1}{n_{\max} - 1}\sum_{n=2}^{n_{\max}} \overline{H}_\delta^{(n)}(F).$$

Для анализа были выбраны шесть типов цифровых хаотических отображений:

№ 1 - тент-отображение

$$F(X) = \begin{cases} \left\lceil \frac{M}{A} X \right\rceil, 0 \le X \le A, \\ \left\lfloor \frac{M}{M-A}(M-X) \right\rfloor + 1, A < X \le M-1 \end{cases}$$

№ 2 - логистическое

$$F(X) = 4X(M - X) \bmod M$$

№ 3 - пилообразное

$$F(X) = (AX) \bmod (M - 1) + 1$$

№ 4 - сдвиговое

$$F(X) = (AX) \bmod M$$

№ 5 - Чебышева 2го порядка

$$F(X) = (2X^2 - 1) \bmod M$$

№ 6 - Чебышева 3го порядка

$$F(X) = (4X^3 - 3X) \bmod M$$

Результаты расчета дискретных показателей Ляпунова и энтропии для выбранных отображений при разных значениях размерности дискретного фазового пространства M приведены в таблице 1.

Таблица 1. Значения дискретного показателя Ляпунова λ_F и $\lambda_{F\max}$ для исследуемых отображений при различной размерности M

M , бит	$\lambda_{F\max}$	λ_F № 1	λ_F № 2	λ_F № 3	λ_F № 4	λ_F № 5	λ_F № 6
16	10.397	0.693	9.592	6.531	6.530	9.591	9.589
20	13.170	0.693	12.363	9.304	9.304	12.363	12.363
24	15.942	0.693	15.136	12.076	12.076	12.136	15.135
28	18.715	0.693	17.908	14.849	14.849	17.908	17.908
32	21.488	0.693	20.681	17.152	17.152	20.681	20.681

Проведенный анализ результатов рассчитанных показателей Ляпунова $\lambda_{F\max}$ и λ_F показывает, что для всех исследованных отображений дискретный показатель Ляпунова λ_F является положительным, что свидетельствует о хаотическом поведении систем. Однако, отображения на основе полиномов, включая логистическое и отображения Чебышева, имеют показатель Ляпунова, наиболее близкий к максимальному значению $\lambda_{F\max}$. Следовательно, данные отображения являются более предпочтительными для применения в системах шифрования на основе динамического хаоса.

Таблица 2. Значения усредненной дискретной энтропии $h_\delta(F)$ для исследуемых отображений

M , бит	$h_\delta(F)$ № 1	$h_\delta(F)$ № 2	$h_\delta(F)$ № 3	$h_\delta(F)$ № 4	$h_\delta(F)$ № 5	$h_\delta(F)$ № 6
8	1.204	1.360	1.619	1.605	1.330	1.513

Анализ полученных результатов показывает, что все представленные отображения обладают свойством перемешивания, наличием «кажущегося случайным» поведения, что подтверждается отличными от нуля значениями энтропии.

Таким образом, результаты проведенной работы показывают, что при выборе хаотических отображений для цифровых систем шифрования на основе динамического хаоса необходимо руководствоваться критериями близости значений дискретных показателей Ляпунова к максимальному значению, а также отличным от нуля значением дискретной энтропии. Данные критерии позволяют не только исследовать хаотическое поведение цифровых отображений, но и выбрать наиболее подходящие из них для применения в алгоритмах шифрования данных на основе динамического хаоса.

Список литературы

1. Kocarev, L. Discrete Chaos—I: Theory / L. Kocarev, J. Szczepanski, J.M. Amigó, I. Tomovski // IEEE Transactions on Circuits and Systems Part I: Fundamental Theory and Applications. – 2006. – №53 – С. 1300-1309.

2. Kocarev, L. Chaos-based cryptography: a brief overview / L. Kocarev // IEEE Circuits and Systems Magazine. – 2001. – №1. – С. 6-21.

3. Сидоренко А.В. Модификация метода шифрования данных на основе динамического хаоса / А.В. Сидоренко, К.С. Мулярчик // Информатика. – 2011. – № 1. – С. 95-106.

4. Kocarev, L. Finite-Space Lyapunov Exponents and Pseudochaos / L. Kocarev, J. Szczepanski // Physical Review Letters. – 2004. – №93. – С. 234101.

5. Amigo, J.M. Discrete entropy / J.M. Amigo, L. Kocarev, I. Tomovski // Physica D: Nonlinear Phenomena. – 2007. – №228. – P. 77-85.

Ю.С.ХАРИН, Е.В.ВЕЧЕРКО, М.В.МАЛЬЦЕВ

МАТЕМАТИЧЕСКИЕ МОДЕЛИ НАБЛЮДЕНИЙ В СТЕГАНОГРАФИИ

Введение. Стеганография скрывает сам факт передачи информации. В настоящее время эта область стремительно развивается [1-4]. В литературе вероятностно-статистические вопросы стеганографии малоизученны. В случае, когда математическая модель наблюдений неизвестна, используются “слепые” методы стеганализа [4]. В качестве математических моделей данных в стеганографии могут выступать векторные двоичные случайные последовательности, которые исследуются в данной работе, и дискретные случайные поля. Проблема построения и исследования математических моделей наблюдений актуальна, так как это направление недостаточно проработано в стеганографии. Такое исследование позволяет определить условия надежного встраивания информации.

Марковская векторная двоичная последовательность. В качестве математической модели контейнеров и стегоконтейнеров иногда используется последовательность независимых одинаково распределенных случайных векторов [1]. Однако в этом случае модель не учитывает зависимости между случайными векторами, которая существует в реальных данных. Поэтому будем полагать, что контейнер $x=(x_1',...,x_n')'\in V^{Nn}$, $V=\{0,1\}$, есть векторная стационарная цепь Маркова 1-ого порядка с пространством состояний V^N, стационарным распределением вероятностей $\pi=(\pi_0,...,\pi_{2^N-1})'$ и матрицей вероятностей одношаговых переходов P:

$$\pi_i=P\{< x_t >= i\},\ P=(p_{ij}),\ p_{ij}=P\{< x_t >= j \mid < x_{t-1} >= i\},\ i,j\in A, \tag{1}$$

где $A=\{0,1,...,2^N-1\}$, $< x_t >=\sum_{j=1}^{N}2^{j-1}x_{tj}\in A$ – число, с которым отождествляется двоичный вектор $x_t\in V^N$. Введем обозначения:

$$x_t=(x_{t1},...,x_{tN})'=(x_t^{(1)},x_t^{(2)'})'\in V^N,\ x_t^{(1)}=x_{t1}\in V, x_t^{(2)}=(x_{t2},...,x_{tN})'\in V^{N-1}. \tag{2}$$

С учетом введенных обозначений (2) справедливо тождество: $2<x_t^{(2)}>=<x_t>-x_t^{(1)}$.

Обычно до встраивания сообщение подвергается криптографическому преобразованию, поэтому считаем, что сообщение $m_t\in V$ является последовательностью независимых случайных величин Бернулли:

$$L\{m_t\}=Bi(1,\theta),\ P\{m_t=1\}=1-P\{m_t=0\}=\theta\in(0,1), \tag{3}$$

где $L\{\}$ – закон распределения вероятностей.

Ключевой информацией является начальное значение, используемое для инициализации генератора псевдослучайных чисел, который порождает последовательность, называемую стегоключом. Эта последовательность определяет моменты времени, в которые часть сообщения встраивается в контейнер. Поэтому считаем, что стегоключом ξ_t, $t = 1,...,n,$ является последовательность независимых в совокупности случайных величин, имеющих бернуллиевский закон распределения вероятностей:

$$L\{\xi_t\} = Bi(1,\beta),\ P\{\xi_t = 1\} = 1 - P\{\xi_t = 0\} = \beta. \tag{4}$$

Рассмотрим распространенный метод вкрапления сообщения, в котором изменяются наименее значимые биты (LSB) контейнера x [2,3]:

$$\widetilde{x}_t^{(1)} = \xi_t m_{\tau(t)} + (1-\xi_t)x_t^{(1)} = \begin{cases} m_{\tau(t)}, \xi_t = 1, \\ x_t^{(1)}, \xi_t = 0 \end{cases},\ \widetilde{x}_t^{(2)} = x_t^{(2)}, \tag{5}$$

$$\tau(t) = \tau(t, \xi_{1,},..., \xi_t) = \sum_{j=1}^{t} \xi_j,\ t = 1,..., n. \tag{6}$$

где $\widetilde{x} = (\widetilde{x}_1,...,\widetilde{x}_n)' \in V^{Nn}$ – контейнер, содержащий сообщение m_t, называемый стегоконтейнером. В этом случае стеганографический объем равен $\lfloor \beta n \rfloor$.

Основная цель стеганографии - скрыть факт наличия или передачи информации. Согласно определению К. Кашена [4] стеганографическая схема является ε-надежной, если относительная энтропия, известная как расстояние Кульбака-Лейблера, между распределением вероятностей контейнера и распределением вероятностей стегоконтейнера не превосходит ε.

Случайные последовательности $x, \{\xi_t\}, \{m_t\}$ предполагаются взаимно независимыми, так как контейнер, сообщение и стегоключ порождаются независимыми механизмами.

Описанная модель также может применяться в случае, когда увеличена эффективность встраивания с использованием методов теории кодирования (“matrix embedding” [4]). Эффективность встраивания – это число бит сообщения, встраиваемого при изменении не более одного бита контейнера.

Теорема 1 устанавливает s-мерное ($s \geq 2$) распределение вероятностей стегоконтейнера $\widetilde{x}$ для произвольного значения параметра $\beta \in [0,1]$.

Теорема 1. Пусть x – векторная стационарная цепь Маркова (1), стегоконтейнер $\widetilde{x}$ строится согласно (5), тогда для s-мерного ($s \geq 2$) распределения вероятностей $\widetilde{\pi}_{<J_0>,...,<J_{s-1}>} = P\{\widetilde{x}_t =< J_0 >,..., \widetilde{x}_{t+s-1} =< J_{s-1} >\}$, $J_0,...,J_{s-1} \in V^N$, стегоконтейнера справедливо выражение:

$$\begin{aligned}
\widetilde{\pi}_{<J_0>,...,<J_{s-1}>} &= (1-\beta)^s \pi_{<J_0>} \prod_{i=0}^{s-2} p_{<J_i>,<J_{i+1}>} + \sum_{K \in V^s, 0<w(K)<s} \beta^{w(K)} (1-\beta)^{s-w(K)} \times \\
&\times \theta^{w(K'J^{(1)})} (1-\theta)^{w(K)-w(K'J^{(1)})} \sum_{U=(u_j)' \in V^{w(K)}} \pi_{2<J_0^{(2)}>+(1-k_0)J_0^{(1)}+k_0 u_{k_0-1}} \times \\
&\times \prod_{i=0}^{s-2} p_{2<J_i^{(2)}>+(1-k_i)J_i^{(1)}+k_i u_{\varphi(i,K)}, 2<J_{i+1}^{(2)}>+(1-k_{i+1})J_{i+1}^{(1)}+k_{i+1}u_{\varphi(i+1,K)}} + \\
&+ \beta^s \theta^{w(J^{(1)})} (1-\theta)^{s-w(J^{(1)})} \sum_{U=(u_j)' \in V^s} \pi_{2<J_0^{(2)}>+u_0} \prod_{i=0}^{s-2} p_{2<J_i^{(2)}>+u_i, 2<J_{i+1}^{(2)}>+u_{i+1}},
\end{aligned} \tag{7}$$

где $w(J)$ – вес Хемминга двоичного вектора J, $J^{(1)} = (J_0^{(1)},..., J_{s-1}^{(1)})' \in V^s$, $\varphi(i,K) = \sum_{j=0}^{i} k_j - 1$.

Следствие 1. Если $\beta = 1$, то $\forall \theta \in (0,1)$, $\forall J_0,...,J_{s-1} \in V^{N-1}$ и любых $U, H \in V^s$, таких что $w(U) = w(H)$, справедливо следующее свойство s-мерного распределения вероятностей:

$$\widetilde{\pi}_{2<J_1>+u_0,2<J_2>+u_1,...,2<J_{s-1}>+u_{s-1}} = \widetilde{\pi}_{2<J_1>+h_0,2<J_2>+h_1,...,2<J_{s-1}>+h_{s-1}}. \quad (8)$$

Следствие 2. Если $\beta = 1$ и $\theta = 1/2$, то для s-мерного распределения вероятностей стегоконтейнера справедливо соотношение:

$$\widetilde{\pi}_{<J_0>,...,<J_{s-1}>} = 2^{-s} \sum_{U=(u_j)' \in V^s} \pi_{2<J_0^{(2)}>+u_0} \prod_{i=0}^{s-2} p_{2<J_i^{(2)}>+u_i,2<J_{i+1}^{(2)}>+u_{i+1}}. \quad (9)$$

Теорема 1 позволяет ввести функционалы, характеризующие наличие или отсутствие скрытой информации.

Цепь Маркова условного порядка. Также имеется возможность использовать цепь Маркова условного порядка [5] как математическую модель данных в стеганографии. Для описания модели примем следующие обозначения: $\mathbf{N}$ – множество натуральных чисел; $J_n^m = (j_n, j_{n+1}, \dots, j_{m-1}, j_m) \in A^{m-n+1}$, $m \geq n$, – мультииндекс; $< x_t > \in A$, $t \in \mathbf{N}$, – однородная цепь Маркова s-го порядка $(2 \leq s < +\infty)$, заданная на вероятностном пространстве (Ω, F, P), с $(s+1)$-мерной матрицей вероятностей одношаговых переходов $P = (p_{J_1^{s+1}})$, $p_{J_1^{s+1}} = \mathrm{P}\{< x_{t+s} >= j_{s+1} | < x_{t+s-1} >= j_s, \dots, < x_t >= j_1\}$, $\forall t \in \mathbf{N}$; $B_* \in \{1,2,\dots,s-1\}$, $K = 2^{NB_*} - 1$ – целые числа; $Q^{(1)},\dots,Q^{(M)}$ – семейство M $(1 \leq M \leq K+1)$ различных квадратных стохастических матриц порядка 2^N: $Q^{(m)} = (q_{i,j}^{(m)})$, $i, j \in A$, $1 \leq m \leq M$.

Цепь Маркова s-го порядка $< x_t > \in A$ назовем цепью Маркова с условной глубиной памяти [5], если вероятности одношаговых переходов имеют следующее малопараметрическое представление:

$$p_{J_1^{s+1}} = \sum_{k=0}^{K} [\sum_{l=s-B_*+1}^{s} 2^{N(l-s+B_*-1)} j_l = k] q_{j_{b_k}, j_{s+1}}^{(m_k)}, \quad (10)$$

где $1 \leq m_k \leq M$, $1 \leq b_k \leq s - B_*$, $0 \leq k \leq K$, $\min\limits_{0 \leq k \leq K} b_k = 1$, [ ] – скобка Айверсона. Последовательность элементов $J_{s-B_*+1}^s$, определяющую условие в формуле (10), назовем базовым фрагментом памяти (БФП) случайной последовательности; B_* – длина БФП. Из (10) видно, что для данной модели состояние x_t процесса в момент времени t зависит не от всех s предыдущих состояний, а от $B_* + 1$ состояний $(j_{b_k}, J_{s-B_*+1}^s)$, причем БФП определяет не только состояние j_{b_k}, но и условный порядок цепи Маркова $s_k = s - b_k + 1 \in \{B_* + 1, B_* + 2, \dots, s\}$, а также матрицу переходов $Q^{(m_k)}$.

Заметим, что при $B_* = s - 1$, $b_0 = \dots = b_K = 1$, получаем полносвязную цепь Маркова порядка s; отметим также, что при $b_0 = \dots = b_K = s - B_*$, получаем полносвязную цепь Маркова порядка $B_* + 1$.

В докладе приводятся численные результаты, иллюстрирующие применения указанных моделей в стеганографии.

Литература

1. Харин, Ю.С. Стеганографические методы защиты информации: обзор / Ю.С. Харин, М.С. Абрамович // Управление защитой информации. Т. 13. 2009. С.58-66.

2. Харин, Ю.С. О некоторых задачах статистической проверки гипотез в стеганографии / Ю.С. Харин, Е.В. Вечерко // Весці НАН Беларусі. Серыя фіз.-мат. навук. Вып. 4. 2010. С.5–12.

3. Kharin, Yu.S. On statistical hypotheses testing of embedding / Yu.S. Kharin, E.V. Vecherko // Proc. of the 9-th international conference Computer Data Analysis and Modeling. Vol. 2. Minsk, 2010. P.26–29.

4. Fridrich, J. Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities / J. Fridrich, T. Pevny, J. Kodovsky // Proc. 9th ACM Multimedia & Security Workshop. Dallas, 2007. P.3–14.

5. Харин, Ю. С. Алгоритмы статистического анализа цепей Маркова с условной глубиной памяти / Ю. С. Харин, М. В. Мальцев // Информатика. – 2011. – №1. – С.34–43.

РАЗДЕЛ 4
СОЗДАНИЕ ЗАЩИЩЕННЫХ ОБЪЕКТОВ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ. ЗАЩИТА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

В.В.АНИЩЕНКО, Д.А.ВЯТЧЕНИН, А.М.КРИШТОФИК

ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ НА ОСНОВЕ ПРИМЕНЕНИЯ СИСТЕМ НЕЧЕТКОГО ВЫВОДА

На современном этапе развития средств вооружения и военной техники резко возрастает роль автоматизированных систем управления войсками и оружием, систем поддержки принятия решений, а также систем автоматизированной обработки информации, позволяющих адекватно оценивать складывающуюся оперативную обстановку, прогнозировать дальнейшее развитие ситуации и оперативно принимать соответствующие складывающейся обстановке решения. В частности, в работе [1] подчеркивается, что в будущем «в содержании военных действий неизмеримо возрастет значение фактора времени. Быстродействие и дальность применяемого оружия приведут к необходимости повышения оперативности действий и стратегической мобильности войск во всех формах и способах военных действий вооруженных сил в войне». Совершенно естественно, что возникает проблема оценки защищенности систем вышеуказанного типа, являющаяся, как отмечается в работе [2], «одним из ключевых вопросов на всех этапах их жизненного цикла при различном объеме априорных знаний», причем особенно актуальным оказывается быстродействие средств защиты информационных систем военного назначения.

В силу того, что поступающая из различных источников информация зачастую носит неполный, неточный и противоречивый характер, то при проектировании как собственно информационных систем военного назначения, так и систем, позволяющих производить оценку их защищенности, особое внимание должно уделяться разработке соответствующего математического и программного обеспечения. Одним из наиболее перспективных подходов к решению указанной проблемы, сочетающих в себе, с одной стороны, высокую точность, а с другой – релевантность полученного результата, является аппарат нечеткой математики, в частности, методов нечеткой классификации [3].

В базовой модели объекта информатизации, предложенной в [2], рассматривается взаимодействие трех множеств: множества активов, то есть информации или ресурсов, которые должны быть защищены, множества угроз активам, исходящих из окружающей среды объекта и создающих опасность для его функционирования, а также множества уязвимостей объекта защиты, то есть состояний или свойств объекта, способствующих осуществлению угрозы. Каждый элемент любого из этих множеств может описываться вектором признаков, принимающих значение в некоторой количественной шкале, что позволяет производить их классификацию, для чего представляется целесообразным использование систем нечеткого вывода [4].

Главным элементом систем нечеткого вывода, или, сокращенно, FIS – по аббревиатуре используемого в англоязычной литературе термина fuzzy inference system – является база нечетких продукционных правил, в наиболее общем случае имеющих вид

l: ЕСЛИ $\hat{x}^1$ есть B_l^1 И … И $\hat{x}^m$ есть B_l^m ТО y_1 есть C_1^l И … И y_c есть C_c^l, (1)

где $l \in \{1,\ldots,c\}$ – номер правила, $\hat{x}^t \in \hat{X}^t$, $t \in \{1,\ldots,m\}$ – входные переменные, и $\hat{X}^t$ – область определения соответствующей переменной, $y_l \in Y_l$, $l \in \{1,\ldots,c\}$ – нечеткие выходные переменные, причем Y_l – область определения соответствующего заключения, а B_l^t, C_l^l – нечеткие множества с функциями принадлежности $\gamma_{B_l^t}(\hat{x}^t)$ и $\gamma_{C_l^l}(y_l)$, определенные на соответствующих универсумах. Следует отметить, что в правиле вида (1) m посылкам соответствует c заключений, так что структура правил вида (1) в специальной литературе именуется MIMO-структурой – от англоязычного термина Multi Inputs – Multi Outputs [4], и является наиболее общей. База нечетких правил может формироваться на основе обработки данных об элементах обучающей выборки, для чего чаще всего используются оптимизационные методы нечеткой или возможностной кластеризации [5] – при этом исследуемая совокупность $X = \{x_1,\ldots,x_n\}$ объектов обучающей выборки обрабатывается каким-либо алгоритмом кластеризации с последующим проецированием значений принадлежности, или значений типичности того или иного нечеткого кластера A^l, $l = 1,\ldots,c$ на координатные оси признакового пространства $I^m(X)$. Данный подход обладает довольно существенным недостатком – в силу того, что в оптимизационных методах нечеткой и возможностной кластеризации первоначальное разбиение формируется, как правило, случайным образом, то зачастую для получения приемлемого результата классификации в виде нечеткого c-разбиения или возможностного разбиения, необходимым является проведение серии вычислительных экспериментов. Указанного недостатка лишен предложенный в [6] метод прототипирования систем нечеткого вывода, основанный на обработке данных об объектах обучающей выборки эвристическим D-AFC(c)-алгоритмом возможностной кластеризации [7].

Сущность предлагаемого подхода к решению задачи оценки защищенности объекта информатизации заключается в следующем: для каждого из k множеств, отношения между элементами которых описывают объект информатизации при воздействии угроз безопасности на активы, в соответствии с предложенным в [6] методом строится система нечеткого вывода, позволяющая классифицировать каждый вновь поступающий на распознавание элемент, а результирующие значения нечетких выходных переменных правил вида (1) являются, в свою очередь, значениями входных переменных системы нечеткого вывода следующего уровня, как это схематично изображено на рис. 1.

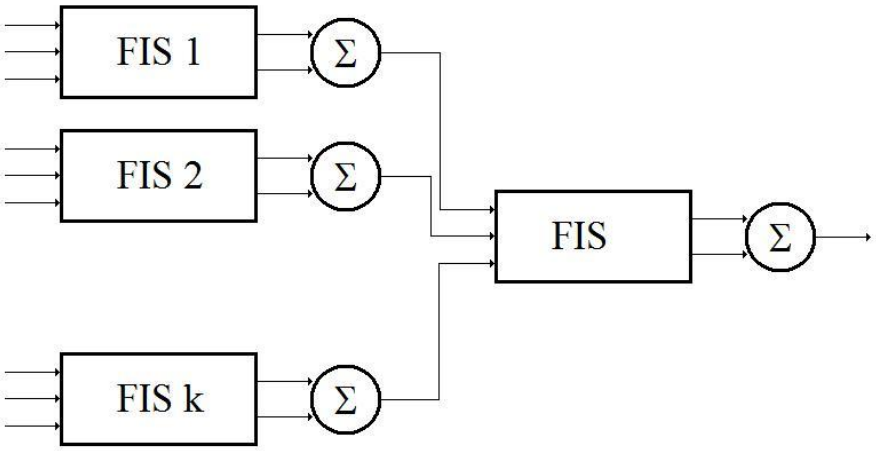


Рис. 1. Общая схема ансамбля нечетких классификаторов для оценки защищенности объекта информатизации

Необходимо указать, что в изображенном на рис.1 двухуровневом ансамбле нечетких классификаторов символом $\sum$ обозначены модули, реализующие алгоритм активации

значений одной или нескольких выходных переменных из множества $y_l \in Y_l$, $l \in \{1,\ldots,c\}$, зависящий, в свою очередь, от разновидности используемого системой алгоритма нечеткого вывода [4]. Результатом работы ансамбля классификаторов будет общая оценка защищенности объекта информатизации в зависимости от значений, характеризующих соответствующие входные элементы, такие, к примеру, как угроза и уязвимость.

Следует также отметить, что архитектура ансамбля нечетких классификаторов, в общем, зависит от способа реализации угроз через уязвимости – к примеру, в [8] рассматриваются такие разновидности, как реализация нескольких различных угроз через некоторую одну определенную уязвимость, реализация одной угрозы через несколько определенных уязвимостей, реализация нескольких различных угроз через несколько определенных уязвимостей и реализация одной угрозы через одну определенную уязвимость.

Метод прототипирования систем нечеткого вывода, предложенный в [6], позволяет генерировать базу правил вида (1) в режиме времени, близком к реальному, что является весьма существенным фактором при проектировании информационных систем военного назначения и систем оценки их защищенности; кроме того, указанный метод позволяет извлекать нечеткие правила из интервально-значных данных [9], что, в общем, позволяет решать также сформулированную в [10] задачу определения критически важных информационных объектов.

Литература

1. Мальцев Л.С. Вооруженные Силы Республики Беларусь: История и современность. – Мн.: Асобны Дах, 2003 – 245 с.
2. Анищенко В.В., Криштофик А.М. Актуальные вопросы оценки защищенности информационных систем военного назначения // Наука и военная безопасность. – 2005. – № 1. – С. 30-34.
3. Вятченин Д.А., Вятченин В.А. Перспективы применения методов нечеткой кластеризации в военных целях // Военная мысль. – 2011. – № 1. – С. 46-55.
4. Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. – М.: Горячая линия – Телеком, 2007. – 284 с.
5. Fuzzy Cluster Analysis: Methods for Classification, Data Analysis and Image Recognition / Hoeppner F., Klawonn F., Kruse R., Runkler T. – Chichester: Wiley Intersciences, 1999. – 289 p.
6. Viattchenin D.A. Automatic generation of fuzzy inference systems using heuristic possibilistic clustering // Journal of Automation, Mobile Robotics and Intelligent Systems. – 2010. – Vol. 4, No. 3. – P. 36-44.
7. Viattchenin D.A. A new heuristic algorithm of fuzzy clustering // Control & Cybernetics. – 2004. – Vol. 33, No. 2. – P. 323-340.
8. Криштофик А.М. Модель системы защиты информации от несанкционированного доступа с учетом рисков остаточных уязвимостей // Информатика. – 2008. – № 1. – С. 58-68.
9. Viattchenin D.A. Derivation of fuzzy rules from interval-valued data // International Journal of Computer Applications. – 2010. – Vol. 7, No. 3. – P. 13-20.
10. Бобовик А.П. Определение критически важных информационных объектов на основе экспертных оценок // Наука и военная безопасность. – 2005. – № 1. – С. 3-6.

В.В.АНИЩЕНКО, Ю.В.ЗЕМЦОВ, А.М.КРИШТОФИК, В.И.СТЕЦЮРЕНКО

ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ НАЦИОНАЛЬНОЙ ГРИД-СЕТИ

При создании национальной грид-сети Республики Беларусь использовались следующие технологии защиты:

– инфраструктура открытых ключей для создания удостоверяющего центра;

– криптографическая защита телекоммуникаций специализированной грид-сети при обмене информацией ограниченного распространения (для служебного пользования).

– управление доступом к вычислительным ресурсам и ресурсам хранения данных опытного участка грид-сети.

1. Создание удостоверяющего центра

На основе надежной и широко используемой технологии инфраструктур открытых ключей разработан, создан и введен в эксплуатацию удостоверяющий центр национальной грид-сети. Удостоверяющий центр должен гарантировать безопасную работу в незащищенных сетях общего доступа, обеспечивая функционирование таких сервисов, как аутентификация, конфиденциальность, контроль целостности и доказательное подтверждение авторства при передаче информации, а также единый вход в грид-сеть.

При этом получены следующие основные результаты:

– разработана концепция создания и обеспечения информационной безопасности сертификационного центра корпоративной грид-системы;

– разработана политика применения сертификатов и регламент удостоверяющего центра национальной грид-сети;

– разработан программный комплекс удостоверяющего центра национальной грид-сети с набором программной, технической и нормативной документации;

– обеспечено функционирование удостоверяющего центра национальной грид-сети в соответствии с международными стандартами, что являлось необходимым условием для создания безопасной и совместимой с международной грид-инфраструктуры электронной науки;

– организована и проведена аккредитация удостоверяющего центра национальной грид-сети в международной организации EUgridPMA, разрабатывающей и обеспечивающей соблюдение правил функционирования международных грид-инфраструктур;

– удостоверяющий центр национальной грид-сети введен в качестве полноправного члена в состав международной организации EUgridPMA;

– разработан ряд справочных документов и руководств для абонентов удостоверяющего центра.

Наиболее трудоемкой и значимой в рамках данного задания была задача, связанная с проектированием и программной реализацией программного комплекса удостоверяющего центра национальной грид-сети. Созданный программный комплекс представляет собой надежный, высокопроизводительный, платформонезависимый, гибкий и модульный центр сертификации инфраструктуры открытых ключей. Программный комплекс разработан на основе Java-технологий и может работать под управлением различных операционных систем, например, таких как GNU/Linux, Windows, Solaris, FreeBSD, MacOS. Основное функциональное назначение программного комплекса удостоверяющего центра – выпускать сертификаты для абонентов, серверов и служб национальной грид-сети. Созданный программный комплекс функционирует в строгом соответствии с основным нормативно-техническим документом удостоверяющего центра – Политикой применения сертификатов и регламентом, который также разработан в рамках задания. Программный комплекс поддерживает решение следующих важных задач, без которых невозможна эффективная работа инфраструктуры открытых ключей.

– обработка запросов на выдачу сертификатов, утвержденных регистрационным центром;

– издание, распространение и хранение сертификатов открытых ключей и списков отозванных сертификатов открытых ключей;

– изготовление и обеспечение жизненного цикла (хранение, приостановление действия, возобновление, отзыв) самоподписанного (корневого) сертификата открытого ключа;

– обработка запросов на отзыв сертификатов открытых ключей;

– отзыв сертификатов открытых ключей;

– обеспечение доступности списка отозванных сертификатов открытых ключей;

– ведение реестров действующих и отозванных сертификатов открытых ключей;

– ведение архивов сертификатов открытых ключей и списков отозванных сертификатов открытых ключей;

– регистрация владельцев личных ключей;

– регистрация запросов на выдачу и отзыв сертификатов открытых ключей.

Программный комплекс удостоверяющего центра имеет модульную структуру и состоит из:

– подсистемы хранения данных;

– модуля регистрационного центра;

– модуля сертификационного центра;

– модуля аудита действий администратора;

– модуля онлайн-репозитория.

2. Система защиты телекоммуникаций специализированной грид-сети

Специализированная грид-сеть в контексте исследований рассматривалась как сегмент национальной грид-сети со специализированной политикой безопасности, базируемой на криптографической защите служебной информации ограниченного распространения, на основе национального криптоалгоритма СТБ П 34.101.31-2007.

Основные задачи:

– обеспечение конфиденциальности и целостности информации ограниченного распространения (Для служебного пользования – ДСП) в процессе ее передачи по системе телекоммуникаций за счет использования программных и программно-аппаратных средств криптографической защиты информации;

– реализация комплексного использования криптографического алгоритма блочного шифрования СТБ П 34.101.31-2007 как для защиты данных на жестких дисках компьютеров и внешних носителях, так и для передачи данных в зашифрованном виде по сети телекоммуникаций;

– разработка организационно-распорядительных документов по обеспечению безопасного функционирования специализированной Грид-сети.

Методология исследований основывалась на анализе состава структуры и текстов программ зарубежных криптографических алгоритмов и протоколов с целью разработки возможных вариантов встраивания программ, реализующих национальный криптоалгоритм СТБ П 34.101.31-2007, в стандартные криптоалгоритмы стека TCP/IP.

Результаты работы:

– русифицированные алгоритмы безопасного протокола транспортного уровня на основе национального криптоалгоритма СТБ П 34.101.31-2007;

– профиль защиты системы защиты телекоммуникаций специализированной Грид-сети;

– «Библиотека базовых криптографических функций СТБ П 34.101.31-2007» БГЛИ. 50663-01- ЛУ в составе «Спецификации», «Описание программы», «Руководства оператора», «Руководства программиста». «Тексты программ», «Удостоверяющего листа»;

– программный комплекс криптографической защиты информации сетевого уровня (шифр ПККЗИ-IPSec), в котором за счет модернизации и расширения функциональности Crypto API ядра 2.6.30 операционной системы Feodora 11 и модернизации пакета StrongSwan обеспечивается поддержка криптографического протокола IPSec со встроенной программой «Библиотека базовых криптографических функций СТБ П 34.101.31-2007»;

– опытный образец системы защиты телекоммуникаций специализированной Грид-сети с системным и прикладным программным обеспечением ПККЗИ-IPSec.

3. Управление доступом к вычислительным ресурсам и ресурсам хранения данных опытного участка грид-сети

Работы по управлению доступом к вычислительным ресурсам и ресурсам хранения данных опытного участка грид-сети выполнялись по следующим направлениям:

– управление доступом на уровне программного обеспечения промежуточного уровня Unicore;

– управление доступом на уровне ресурсов.

В рамках первого направления разработано на базе программного обеспечения промежуточного уровня Unicore программное обеспечение «Брокер грид-серды». Предоставляет функционалы по управлению ресурсами, планированию заданий, позволяет пользователю запускать задания на ресурсах, наиболее подходящих заданию, как в ручном, так и в автоматизированном режиме. Выполняет функции: регистрация на известных сервисах UNICORE Regestry, отправление информации о себе во все сервисы UNICORE Regestry; получение запросов от пользовательского интерфейса на поиск целевой системы; обработка пользовательских запросов (планирование). Выполняет: подбор для задания пользователя конкретной целевой системы грид-среды UNICORE; запрос сервиса UNICORE Regestry на получение информации обо всех зарегистрированных информационных сервисах грид-среды; опрос всех известных информационных сервисов IAS грид-среды. Обеспечивает контроль и управление доступом стандартными средствами UNICORE, ведение журнала событий. Доступ к службе Broker происходит с использованием сертификатов стандарта X509. При планировании Broker использует сервис IAS для получения информации от статических и динамических параметрах целевых систем. Сервис Broker реализуется как веб-служба и для обмена данными по сети использует протокол SOAP);

Для подключения сетевых файловых хранилищ выполнены работы по расширению функциональности компонента TSI национальной грид-сети, что позволило создать технологию подключения территориально распределённых файловых хранилищ к сайтам национальной грид-сети. С использованием разработанной технологии для набора узлов можно применять любые конфигурации сетевых файловых хранилищ, что является принципиальным отличием от существующей схемы, где файловое хранилище для TSI, СПО и всех узлов должно быть общим и единственным.

Для управления доступом на уровне ресурсов проведена доработка и осуществлен перенос программного обеспечения СПО Torque на платформу операционных сред семейства Windows, что позволяет прозрачно подключать ресурсы под управлением указанных операционных сред и весьма актуально для настольных компьютеров и некоторых специализированных рабочих станций. Система пакетной обработки прошла тестирование и апробацию в Республике Беларусь и Соединенных штатах и в настоящее время включена в официальную версию PBS Torque 2.5, которая находится в депозитарии фирмы Cluster Resources - держателя open-source дистрибутива Torque. Она обеспечивает управление ресурсами на уровне ОС, пользователями и безопасностью.

В.В.АНИЩЕНКО, А.М.КРИШТОФИК

СОЗДАНИЕ ОПЫТНОГО УЧАСТКА ГРИД-СЕТИ СОЮЗНОГО ГОСУДАРСТВА В РАМКАХ ПРОГРАММЫ «СКИФ-ГРИД»

Одним из важных аспектов сотрудничества *Республики Беларусь и Российской Федерации,* декларированных Договором о создании Союзного государства от 8 декабря 1999 года, является формирование и эффективное функционирование единого научно-технологического пространств в интересах ускоренного использования достижений науки и технологий в инновационной деятельности и последовательного роста на этой основе конкурентоспособности экономики Беларуси и России.

Создание опытного участка грид-сети Союзного государства осуществлялось в рамках выполнения программы «Разработка и использование программно-аппаратных средств Грид-технологий и перспективных высокопроизводительных (суперкомпьютерных) вычислительных систем семейства «СКИФ» (шифр «СКИФ-ГРИД») (далее – Программа).

При освоении грид-технологий выполнены работы по разработке технологий объединения ресурсов путем создания компьютерной инфраструктуры нового типа, обеспечивающей глобальную интеграцию информационных и вычислительных ресурсов на основе сетевых технологий и специального программного обеспечения промежуточного уровня, а также набора стандартизованных служб для обеспечения надежного совместного доступа к географически распределенным информационным и вычислительным ресурсам: отдельным компьютерам, кластерам, хранилищам информации и сетям.

На основе проведенных исследований выбрана платформа UNICORE в качестве базовой для построения опытного участка грид-сети Союзного государства. Учеными и специалистами в части грид-технологий для программного обеспечения промежуточного уровня UNICORE разработаны комплекты программного обеспечения и программной документации мониторинга и тестирования сайтов; системы анализа, статистики и учета ресурсов; брокера ресурсов; системы пакетной обработки для платформы ОС Windows; сервисов и средств файлового обмена, собственного дистрибутива UNICORE, включающего дополнительно все разработанные сервисы.

В результате выполнения мероприятий Программы создан опытный участок грид-сети Союзного государства, который объединил суперкомпьютерные ресурсы, сервера и рабочие станции, который является базисом для построения интегрированного научно-образовательного пространства и основой для освоения и разработки новых технологий, повышения конкурентоспособности стран-участниц. Разработаны и созданы практически действующие участки грид-сетей на уровне корпоративных и локальных информационных вычислительных систем (ИВС), а также для решения конкретных прикладных задач.

В рамках выполнения суперкомпьютерного направления получены конструкторско-технологические решения и результаты, соответствующие лучшим мировым аналогам. Повышена производительность существующих суперкомпьютерных конфигураций семейства «СКИФ». Созданы суперкомпьютерные кластерные системы «СКИФ-МГУ», «СКИФ-Аврора» ЮУрГУ, «СКИФ-ОИПИ», «СКИФ-GPU», «СКИФ-ГРИД», «ПСК-СКИФ». Аппаратная платформа «СКИФ» ряда 4 обладает рядом преимуществ по сравнению с существующими мировыми разработками: высокой энергоэффективностью, масштабируемостью, плотностью упаковки вычислительной мощности. На основе платформы «СКИФ» ряда 4 открывается возможность по развертыванию вычислительных систем вплоть до петафлопсного уровня производительности с использованием оригинальных отечественных разработок.

Использование опытного участка грид-сети Союзного государства и созданных суперкомпьютерных установок позволили в рамках выполнения мероприятий программы разработать ряд методик виртуального проектирования изделий машиностроительного

профиля, смоделировать отдельные процессы, происходящие на атомных электростанциях, практически реализовать ряд проектов для решения задач с применением грид- и суперкомпьютерных технологий в различных областях науки и техники, таких как инженерное моделирование в грид-среде, решение задач аэро-гидродинамики и молекулярной биологии, проведение расчетов в области физики ионосферы, моделирование систем передачи цифровой информации, моделирование устойчивого развития регионов, и т.д.

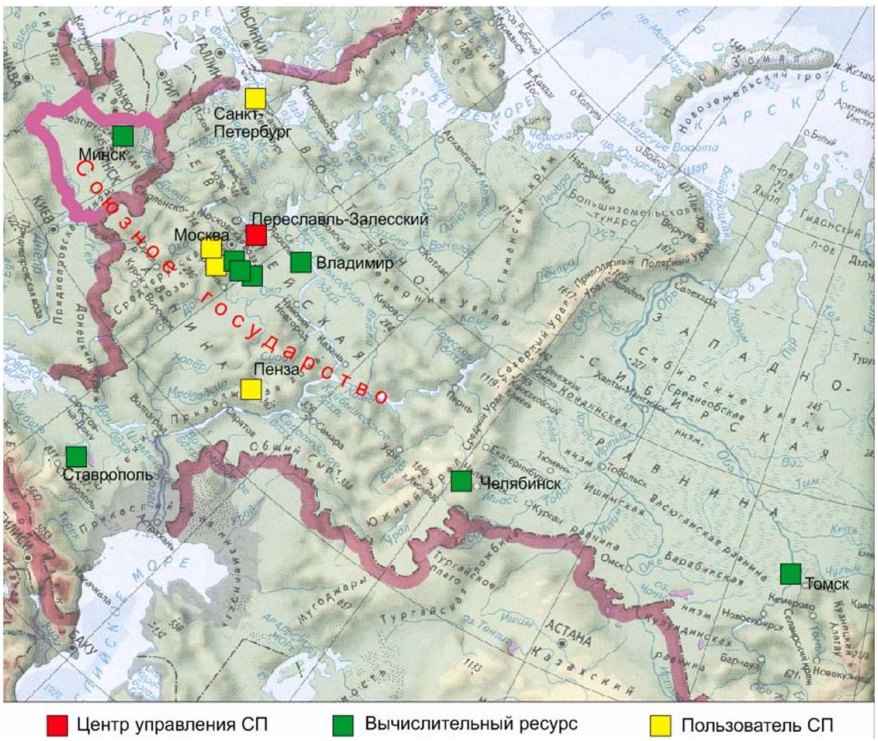


Рисунок. Распределенная вычислительная система СКИФ-Полигон

В медицинской сфере получены результаты, соответствующие лучшим мировым научным аналогам, позволяющие начать разработки диагностических препаратов к хантавирусам, существенно повысить точность и качество диагностирования онкобольных, ускорить разработку и оценку эффективности новых лекарственных средств.

Обеспечена информационная безопасность при решении прикладных задач с использованием грид-технологий и высокопроизводительных вычислений на опытном участке грид-сети Союзного государства.

В ходе выполнения Программы проведены две международные конференции «Суперкомпьютерные системы и их применение», в работе которых приняло участие около 260 представителей Беларуси, России, Армении, Молдовы, Казахстана, Латвии, Литвы, Эстонии, Польши, Швеции, Германии. На пленарных и секционных заседаниях, стендовой сессии было заслушано и обсуждено более 140 докладов ученых, специалистов и практических работников в области грид и суперкомпьютерных технологий и их практического использования. Прошли обучение 36 молодых специалистов организаций и ВУЗов по курсу начальной подготовки пользователей в грид-среде gLite на ресурсах Познаньского суперкомпьютерного центра, выданы сертификаты.

По тематике выполняемых работ подготовлено и сделано более 100 научных докладов на международных конференциях, проводимых в России, Странах Балтии, Швеции, Европы, Америки.

Работы, предусмотренные программой, выполнены в полном объеме в соответствии с техническими заданиями и календарными планами.

Финансирование Программы осуществлялось своевременно и в полном объеме.

Белорусскими исполнителями по Программе за 2007-2010 гг. израсходовано 233 181,2 тыс. российских рублей, что составляет 99,4% от плана финансирования по Программе белорусской стороны в российских рублях за счет средств бюджета Союзного государства. Привлечено внебюджетных средств на сумму 126 735,7 тыс. российских рублей, что составляет 108 % от плана.

Российскими исполнителями по Программе за четыре года (2007–2010 гг.) израсходовано 446,5 млн. российских рублей, что составляет 100 % от плана финансирования по Программе за счет средств бюджета Союзного государства. Привлечено из внебюджетных источников (средства предприятий-исполнителей Программы) – 223,3 млн. российских рублей, что составляет 100 % от плана.

По результатам проверок Постоянного Комитета Союзного государства, Комитета государственного контроля Республики Беларусь, Счётной палаты Российской Федерации, Комиссии Федеральной службы по интеллектуальной собственности, патентам и товарным знакам (Роспатент) выявленные ими недостатки устранены. Государственные заказчики извещены об их устранении.

Реализация Программы дала ощутимый эффект в экономической, научно-образовательной и социальной сферах:

повышен статус стран-участниц Союзного государства на международной арене как государств с высоким потенциалом науки и возможного надежного партнера для проведения совместных научных исследований;

прямые зарубежные инвестиции составили 29 816 150 российских рублей; прямые инвестиции в инфраструктуру –3 830 000 рос. рублей;

экономия бюджетных средств за счет выполнения отечественными специалистами работ по программе в области высокопроизводительных вычислений и грид-технологий – **64 000 000 (долл.) рос. рублей;**

стоимость созданной интеллектуальной собственности – 18 млн. рос. рублей;

снижение затрат на создание высокопроизводительных вычислительных систем по отношению к закупке у зарубежных производителей – не менее 10%;

получено от зарубежных партнёров интеллектуальной собственности на сумму в 440.66 млн. рос. рублей;

созданы рабочие места для высококвалифицированных специалистов на промышленных предприятиях;

подготовлены специалисты промышленных предприятий для решения практических задач;

разработаны новые технологии эффективного решения прикладных задач для промышленности и др.

В целом в Беларуси и России создана определенная база для развития инфраструктуры по освоению новых технологий в различных отраслях национальных экономик. Складывается позитивное отношение руководства промышленных предприятий к вопросам внедрения методов виртуального проектирования промышленных изделий в целях разработки наукоемкой конкурентоспособной продукции.

В оборонной сфере созданы условия для использования инфраструктуры и технологий для решения задач обороноспособности и безопасности.

В научно-образовательной – для развития науки и образования с использованием разработанных технологий, получения эффекта практически во всех отраслях экономики.

В социальной сфере создана базовая инфраструктура и условия для использования новых информационных технологий для диагностики заболеваний и созданию новых лекарственных форм.

В.В.АНИЩЕНКО, Е.П.МАКСИМОВИЧ, В.К.ФИСЕНКО

АТТЕСТАЦИЯ. ОБСЛЕДОВАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕАЛЬНЫХ УСЛОВИЯХ ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ/ИНФОРМАЦИОННЫХ СИСТЕМ

Организационная защита информации - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или существенно затрудняющая нарушение информационной безопасности. Данный тип защиты включает организацию режима охраны, организацию работы с сотрудниками, организацию работы с документами, организацию использования технических средств, работу по анализу угроз информационной безопасности, планирование восстановительных работ и др.

Организационно-технические требования разрабатываются на этапе проектирования объекта/системы и представляются в Задании по безопасности аттестуемого объекта информатизации/информационной системы (ОИ/ИС). Данные требования направлены на обеспечение конфиденциальности, целостности, доступности информации и подлинности электронных документов. Выполнение организационно-технических требований обеспечивается посредством соответствующих организационно-технических мероприятий, реализуемых в реальной среде эксплуатации аттестуемого ОИ/ИС.

Для обследования порядка выполнения организационно-технических требований информационной безопасности Заявитель (Владелец) ОИ/ИС представляет пакет организационно-распорядительных документов, включающий:

– Устав организации;

– Концепцию или политику информационной безопасности организации;

– Перечень информационных ресурсов, подлежащих защите, не только по уровню конфиденциальности, но и по уровню ценности информации (определяемой величиной возможных прямых или косвенных экономических потерь в случае нарушения целостности или несвоевременности представления информации);

– инструкции, связанные с обеспечением безопасной работы в ИС (Инструкции по внесению изменений в списки пользователей ИС и наделению их полномочиями доступа к ресурсам ИС; Инструкции по установке, модификации и техническому обслуживанию программного обеспечения, программно-аппаратных и аппаратных средств; Инструкцию по организации антивирусной защиты; Инструкцию по организации парольной защиты; Инструкцию по использованию Интернет; Инструкцию по работе с электронной почтой; Инструкцию о порядке работы с носителями ключевой информации; должностные инструкции разных категорий сотрудников (пользователей, технического персонала, разработчиков и др.); Инструкции системного администратора, администратора безопасности);

– документы о порядке разработки, проведения испытаний и передаче в эксплуатацию создаваемой и принимаемой к эксплуатации программно-технической продукции;

– планы обучения, повышения квалификации и периодической аттестации сотрудников в части их компетенции в вопросах информационной безопасности;

– организационно-распорядительные документы по обеспечению регламентированного доступа пользователей к защищаемым информационным ресурсам в связи с кадровыми перемещениями, акты и предписания по результатам выполнения требований данных документов.

При обследовании порядка выполнения организационно-технических требований целесообразно проверить реализацию следующих мероприятий: обеспечение классификации информации в соответствии с ее важностью; обеспечение прав доступа к активам ИС для

разных категорий сотрудников; распределение ответственности за организацию и обеспечение защиты информации; обеспечение периодического системного контроля за качеством защиты информации посредством проведения соответствующих регламентных работ; организация физической защиты средств компьютерной техники, поддержка процедур безопасного обращения с защищаемой информацией, порядок реагирования на инциденты безопасности, поддержка работоспособности ОИ/ИС, поддержка эффективной эксплуатации системы защиты информации, обеспечение необходимого уровня подготовки кадров и т.д.

В процессе обследования необходимо учесть возможное наличие разных типов организационно-технических мероприятий:

– разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия, например, мероприятия по созданию нормативно-методологической базы, мероприятия по проектированию, строительству и оборудованию компонентов ОИ/ИС, по проектированию, разработке и вводу в эксплуатацию технических средств и программного обеспечения;

– мероприятия, проводимые при возникновении определенных изменений в ОИ/ИС, например, мероприятия, осуществляемые при кадровых изменениях в составе персонала ОИ/ИС, при ремонте и модификациях оборудования и программного обеспечения (санкционирование, рассмотрение и утверждение изменений, проверка их на удовлетворение требованиям информационной безопасности, документальное отражение изменений и т.п.), мероприятия по проверке поступающего оборудования на наличие специально внедренных закладных устройств, по инструментальному контролю технических средств на наличие побочных электромагнитные излучения и наводок, по совершенствованию оборудования ОИ/ИС устройствами защиты от сбоев электропитания и помех в линиях связи, оформление юридических документов по вопросам регламентации отношений с пользователями и третьей стороной, связанным с информационным обменом;

– периодически проводимые мероприятия, например, распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.), периодический анализ системных журналов (журналов регистрации), принятие мер по обнаруженным нарушениям правил политики безопасности, пересмотр правил разграничения доступа пользователей к ресурсам ИС, плановый полномасштабный анализ состояния и эффективности применяемых средств и мер защиты, анализ мер по необходимому совершенствованию системы защиты;

– постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия, например, мероприятия по обеспечению достаточного уровня физической защиты (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности технических средств, носителей информации и т.п.), мероприятия по непрерывной поддержке функционирования и администрированию используемых средств защиты, организация текущего контроля за работой пользователей и персонала, контроль за реализацией выбранных мер защиты в процессе функционирования, обслуживания и ремонта ИС, текущий анализ состояния и эффективности применяемых мер и средств защиты.

При оценке организационно-технических требований следует учесть наличие в организации различных категорий сотрудников способных повлиять на информационную безопасность ОИ/ИС. В качестве таких категорий сотрудников могут выступать: сотрудники структурных подразделений (конечные пользователи ИС); разработчики прикладного программного обеспечения; сотрудники подразделения внедрения и сопровождения программного обеспечения, поддерживающие нормальное функционирование и установленный порядок инсталляции и модификации прикладных программ; сотрудники подразделения эксплуатации технических средств; системные администраторы; администраторы безопасности, сотрудники подразделения защиты информации; руководители организации.

Для оценки качества выполнения организационно-технических требований в докладе предлагается следующая методика. В качестве **показателя** оценки реализации требований принимается **степень выполнения требований** организационно-технического уровня. А в качестве **критерия принятия решений –** следующее правило**:** если при проверке на реальном ОИ/ИС конкретное организационно-техническое требование соответствует требованиям инструкций, нормативным и организационно-распорядительным документам, то оно считается выполненным. Степень соответствия определяет эксперт.

Для определения степени выполнения организационно-технического требования используется лингвистическая и количественная шкалы оценок (таблица 1).

Таблица 1 – Соответствие между лингвистической и интервальной шкалами оценок степени выполнения требований организационно-технического уровня

Лингвистическая оценка степени соответствия	Интервал количественных оценок
Высокая степень выполнения	0,75 – 1,0
Допустимая степень выполнения	0,5 – 0,74
Средняя степень выполнения	0,25 – 0,49
Низкая степень выполнения	0,01 – 0,24

Совокупность оценок качества выполнения организационно-технических требований определяется качеством реализации соответствующих организационно-технических мероприятий в реальных условиях эксплуатации ОИ/ИС.

Общая количественная оценка E^{org} качества выполнения организационно-технических требований вычисляется по формуле:

$$E^{org} = \frac{\sum_{k=1}^{t} E^{orgk}}{t},$$

где E^{orgk} – количественная оценка экспертом степени успешности реализации требования k, t – количество организационно-технических требований, представленных в Задании по безопасности для аттестуемого ОИ/ИС.

Лингвистическая оценка качества выполнения организационно-технических требований определяется на основании количественной оценки E^{org} в соответствии с таблицей 1.

Экспертное заключение о качестве выполнения организационно-технических требований формируется на основе следующих правил:

– совокупность организационно-технических требований, общая количественная оценка E^{org} которых находится в пределах 1,0-0,5, удовлетворяет требованиям качества;

– если количественная оценка E^{org} находится в пределах 0,49 – 0,01, то созывается согласительное совещание с Заявителем, на котором принимается одно из следующих решений:

1) осуществить доработку реализованных организационно-технических мероприятий в течение периода аттестации и провести повторную их оценку в части проверки устранения выявленных недостатков;

2) в случае отказа Заявителя от доработки принимается решение в отказе выдачи аттестата соответствия.

О.К.БАРАНОВСКИЙ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В УСЛОВИЯХ ПРИМЕНЕНИЯ ИМПОРТНЫХ ПРОДУКТОВ И СИСТЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Стремление государства и общества к повышению степени информатизации процессов во всех сферах деятельности ставит их безопасность в зависимость от защищенности используемых информационных технологий. Компьютерные системы (КС) и телекоммуникации являются одним из факторов, определяющих надежность систем безопасности страны, обеспечивая хранение важной информации, ее обработку, передачу и представление целевым пользователям. Повсеместное применение КС, позволившее решить задачу автоматизации процессов обработки непрерывно возрастающей по объему и скорости поступления информации, сделало эти процессы чрезвычайно уязвимыми по отношению к агрессивным информационным воздействиям, непреднамеренным внутренним сбоям и отказам, внешним явлениям техногенного и природного характера.

Защита КС и телекоммуникаций, обеспечивающих функционирование объектов критически важной инфраструктуры государства, должна осуществляться в комплексе с построением систем жизнеобеспечения этих объектов.

Состав единой автоматизированной системы безопасности и жизнеобеспечения зависит от назначения и значимости определенного объекта, конкретных условий реализации функций ее назначения и может включать следующие подсистемы [1]:

– дежурно-диспетчерскую;
– производственно-технологического контроля;
– охранной и тревожной сигнализации;
– пожарной сигнализации;
– контроля и управления доступом;
– видеонаблюдения;
– досмотра и поиска;
– пожарной автоматики (пожаротушения, противодымной защиты, оповещения, эвакуации);
– связи с объектом;
– защиты информации;
– инженерно-технических средств физической защиты;
– инженерного обеспечения объекта;
– электроосвещения и электропитания;
– газоснабжения, водоснабжения, канализации;
– поддержания микроклимата (теплоснабжение, вентиляция, кондиционирование).

В современной среде функционирования эффективность единой автоматизированной системы безопасности и жизнеобеспечения критически важных объектов (КВО) все в большей мере определяется технической защитой информации, так как преобладающая доля ее подсистем является КС.

Актуальные угрозы информации на КВО можно разделить на три типа:

– угрозы несанкционированного доступа к информации и воздействия на нее;
– угрозы непреднамеренных воздействий на информацию;
– угрозы утечки информации по техническим каналам.

Под несанкционированным доступом к информации и воздействием на нее понимают действия, направленные на получение доступа к защищаемой информации с нарушением установленных прав и (или) правил разграничения доступа, приводящие к разрушению, уничтожению, искажению, подделке, незаконному перехвату и копированию, распространению, блокированию доступа к информации, а также утрате, уничтожению или сбою функционирования носителя информации.

Под непреднамеренным воздействием на информацию понимают ошибки пользователя, сбои технических и программных средств, природные явления или иные нецеленаправленные на изменение информации события, приводящие к разрушению, уничтожению, искажению, копированию, распространению, блокированию доступа к информации, а также утрате, уничтожению или сбою функционирования носителя информации.

Под утечкой информации по техническим каналам понимают неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до заинтересованного субъекта, не имеющего прав доступа к ней и имеющего возможность ее перехвата.

Сегодня специфика проблемы технической защиты КС состоит в том, что повсеместно используемые популярные импортные продукты и системы не рассчитаны или не прошли процедуру подтверждения соответствия для применения в тех ситуациях, когда безопасность имеет существенное значение. Зачастую встраивание дополнительных средств защиты в эти продукты и системы в силу особенностей их архитектуры не может обеспечить требуемый уровень безопасности информации.

С учетом практикуемых методов перекрытия технических каналов утечки и подходов к обеспечению надежности КС, актуальной задачей остается защита информации от несанкционированного доступа и воздействия на нее.

Защита КС КВО от несанкционированного доступа включает, помимо применения технических средств защиты, поиск недекларированных функций и закладных устройств (аппаратных закладок), перекрытие скрытых каналов (СК) передачи данных.

Взаимодействие функциональных элементов КС между собой и с другими КС происходит с использованием каналов управления и передачи данных. В связи с этим необходимо обеспечить невозможность передачи информации (снижения до приемлемого уровня пропускной способности) наружу и внутрь систем в нарушение политики безопасности.

Использование межсетевых экранов, детекторов вторжений, средств антивирусной защиты и криптографии не обеспечивает гарантированной защиты от утечки информации и передачи команд деструктивного воздействия на КС КВО в условиях применения продуктов информационных технологий и средств защиты информации импортного производства. Программные и аппаратно-программные агенты, внедренные в ключевые элементы КС, могут устанавливать каналы связи с внешними субъектами, находящимися за пределами контролируемого периметра, по так называемым скрытым каналам.

В связи с этим должны предприниматься меры по выявлению недекларированных функций в программном обеспечении и закладных устройств в технических средствах КС.

Однако, известные методы поиска недокументированных возможностей являются весьма трудоемкими и не позволяют обеспечить высокое доверие к функционированию КС, содержащей продукты импортного производства.

Угрозами безопасности КС являются [2]:

– внедрение вредоносных программ и данных;

– подача злоумышленником команд внедренному агенту;

– утечка криптографических ключей или паролей;

– утечка отдельных информационных объектов.

По механизму передачи данных СК можно разделить на две группы [3]:

– стеганографические (технически скрытые в сообщении-«контейнере»);

– сублимографические (организационно нарушающие действующую политику безопасности).

Каналы первой группы используют для скрытой передачи данных стеганографические схемы, которые призваны скрыть сам факт передачи информации на

фоне передачи данных, не вызывающих подозрений, – «контейнера» (например, скрытие в видео и музыке, пакетах стандартных протоколов сетей передачи данных).

Сублимографические СК представляют собой информационные потоки, неразрешенные реализованной политикой безопасности. Для СК данного типа характерно использование для передачи нелегальной информации некоторого разделяемого информационно-вычислительного ресурса. В зависимости от способа использования разделяемого ресурса среди упомянутых СК можно выделить каналы по времени, каналы по памяти, каналы в базах данных и знаний.

В зависимости от используемого при передаче информации механизма кодирования, СК можно классифицировать как детерминированные и стохастические. Стохастический СК использует для передачи информации изменение параметров любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями.

СК могут быть сформированы на различных уровнях функционирования системы:

– на аппаратном уровне;

– на уровне микрокодов и драйверов устройств;

– на уровне операционной системы;

– на уровне прикладного программного обеспечения;

– на уровне функционирования каналов передачи данных и линий связи.

СК по пропускной способности подразделяют на:

– каналы с низкой пропускной способностью;

– каналы с высокой пропускной способностью.

При организации взаимодействия КС с внешними КС в создаваемых системах защиты информации особенно важно предусматривать применение средств обнаружения и перекрытия (снижения до приемлемого уровня пропускной способности) СК.

Стоит отметить, что информационно-техническое воздействие на КС может осуществляться по беспроводным недокументированным интерфейсам с малой пропускной способностью и сигналами на уровне фоновых шумов. При учете такой угрозы перекрытие СК осуществляется экранированием КВО в рамках мероприятий по защите информации от утечки по техническим каналам, а также с применением систем мониторинга параметров физической среды.

Для снижения рисков нарушения функционирования КС от деструктивных воздействий закладных устройств, запрограммированных на срабатывание по прошествии заданного промежутка времени или выполнения заданного количества операций, применяют резервирование элементов КС.

Обеспечение заданного уровня доверия к используемым на КВО продуктам и системам информационных технологий импортного производства, на которые конструкторская и программная документация не предоставлены, а доступ к контролю технологических процессов производства не разрешен, должно выполняться в рамках процедур подтверждения соответствия в устанавливаемых с учетом степени критичности объектов объемах и соотношениях работ по поиску недокументированных возможностей и перекрытию СК как внутри КС, так и за их пределы.

Литература

1. ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования.

2. ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения

3. Ловцов Д.А. Информационная безопасность эргасистем: нетрадиционные угрозы, методы, модели // Info Security.– № 4, 2009.

А.Е.БЛИНЦОВ, Е.В.МОЖЕНКОВА, А.Н.СОЛОВЬЯНЧИК,
Г.В.СЕЧКО, А.С.ТУРОК, Д.В.ШЕРЕМЕТ

ИСПОЛЬЗОВАНИЕ ПОКАЗАТЕЛЯ ПОТЕРЬ ИНФОРМАЦИИ ЗА СЧЁТ ОТКАЗОВ ДЛЯ ОЦЕНКИ СТЕПЕНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В работе [1] для оценки степени информационной безопасности информационного объекта (ИО) по причине его ненадёжности предложено использовать показатель потерь информации (ПИ) относительно отказов и сбоев. При этом под ИО понимается среда, в которой информация создается, передается, обрабатывается или хранится [2]. В [1] показано, что ПИ информационного объекта относительно отказов и сбоев в процентах может быть оценен как разность ста процентов и умноженного на 100 % коэффициента готовности ИО. Математически ПИ – это умноженное на 100 % частное от деления среднего времени восстановления работоспособного состояния ИО к сумме этого же времени и наработки ИО на отказ [3]. Пример [1]: коэффициент готовности компьютера равен 0,996. Тогда уровень ПИ равен (1-0,996)*100%= 0,4 %. Рассмотрим, как практически можно найти исходные данные для расчёта показателя ПИ для различных видов ИО. Проще всего этот показатель оценивать для вычислительных устройств. С помощью проведения наблюдений за устройством в период эксплуатации обслуживающим персоналом ИО фиксируются данные об отказах и наработках объекта, затем рассчитывается коэффициент готовности и определяется ПИ. Примеры таких наблюдений и обработки их результатов для компьютеров описаны в [4], для сложнейших вычислительных устройств – современных кассовых аппаратов – в [5]. Регистрацию данных об отказах в [4, 5] предложено вести с помощью специально-разработанных для Microsoft Excel форм (аппаратного журнала из пяти различных листов), которые для дальнейшей обработки загружаются в специальную базу данных [6], способную автоматически рассчитать коэффициент готовности.

Для более сложных ИО, таких, как особо ответственные серверы, а также телефонные станции как средства телекоммуникаций, за работой ИО, кроме персонала и чаще всего в автоматическом режиме, следят специальные программные и технические устройства. Например, при работе автоматической телефонной станции АТСЭ-ФМ параллельно со станцией работает автоматизированное рабочее место (АРМ) оператора централизованного технического обслуживания (ЦТЭ) производства ОАО "Связьинвест" (Минск). АРМ оператора станции инициирует передачу всех аварийных сообщений с АТСЭ-ФМ на АРМ оператора ЦТЭ. Сообщения выдаются в формате «блокнот» или «txt». В этих условиях выдаваемые с АРМ оператора ЦТЭ аварийные сообщения, которые влияют на коэффициент готовности АТСЭ-ФМ, должны быть включены в компьютерную базу данных по результатам наблюдений за работой АТСЭ-ФМ. Самый простой способ решения этой задачи – это ручной ввод данных в базу с бумажной распечатки аварийных сообщений. Однако не стоит забывать и о компьютерной трансформации аварийных сообщений из формата «блокнот» или «txt» в формат, требуемый для базы.

Некоторые вычислительные устройства работают очень короткий срок по причине своего морального старения и постоянного обновления. В течение этого срока устройства работают практически безотказно, т.е. с коэффициентом готовности, равным 1. Однако из-за того, что некоторые производители компьютерных комплектующих (например, компания GIGABYTE Technology CO., LTD (Тайвань, город Тайбэй [7]) не применяют в техпроцессе их изготовления операции приработки (электротермотренировку, термовыдержку, термоциклирование, вибротряску), их изделия становятся более дешёвыми, т.е. более привлекательными по цене для малоимущих покупателей. В результате на начальном этапе

эксплуатации возникают ранние отказы, но отказавшие изделия продавцы в период гарантии меняют на годные. Для расчёта ПИ в этом случае наработку на отказ можно принять равной сроку безотказной эксплуатации устройства (сроку морального старения), а время восстановления работоспособного состояния – времени от момента проявления раннего отказа устройства до момента начала эксплуатации годного изделия или изделия с годным комплектующим. При этом в состав времени восстановления работоспособного состояния должно входить время на обращение к продавцу и получение годного изделия взамен отказавшего.

И наиболее сложным, на наш взгляд, является задача получения исходных данных для оценки ПИ в особо популярных и общедоступных интернет-сайтах, также представляющих собой сложнейшие программные информационные системы. Угроза безопасности информации в таких сайтах может возникать не только в результате преднамеренных атак на информационную систему или неправильных действий пользователя, но также и из-за потерь информации по причине перегрузки сайта в критических режимах, то есть из-за превышения критической нагрузки на систему. Примером перегрузки информационной системы в критических режимах является практический отказ сайта Microsoft Web news 11 сентября 2001 года, когда новости об атаках на Всемирный торговый центр и здания Пентагона вызвали существенные изменения в трафике сайта – сайт работал очень медленно, а иногда и вовсе был недоступен, что означало для пользователей практическую потерю информации. Другим, причём недавним примером перегрузки сайта, является недоступность 8 и 9 марта 2011 года сайта Нацбанка Беларуси, куда постоянно обращалось множество пользователей за информацией о несостоявшейся девальвации белорусского рубля. И в том, и в другом примере причиной перегрузки сайтов являлось недостаточное нагрузочное тестирование перед эксплуатацией их программных обеспечений. Чтобы собрать исходные данные для оценки ПИ для таких сайтов визуального наблюдения недостаточно. Необходим специальный программно-технический комплекс типа АРМ оператора ЦТЭ для АТСЭ-ФМ.

Литература

1. Гайдук В.Ю., Сахнович К.Е., Сечко Г.В., Федюкович А.М. Уровень защиты информации в компьютерах относительно одной из угроз техногенного характера // Материалы 14-й межд. НТК «Комплексная защита информации», 19-22 мая 2009 года, Могилёв / Российско-белорусский журнал «Управление защитой информации». – Мн.: НИИТЗИ, 2009. – С. 75.

2. Голиков В.Ф., Лыньков Л.М., Прудник А.М., Борботько Т.В. Правовые и организационно-технические методы защиты информации. – Мн.: БГУИР, 2004. – 81 с.

3. ГОСТ. 27.002-89. Надёжность в технике. Термины и определения. – М.: Изд-во стандартов, 1989. – 37 с.

4. Бахтизин В.В., Леванцевич В.И., Лукашик О. ,Сечко Г.В. Организация наблюдений за работой оборудования компьютерного класса / Современная радиоэлектроника: научные исследования и подготовка кадров: сб. материалов (по итогам работы МНПК, Минск, 10-11 апреля 2007 г.): в 4 ч. – Мн.: МГВРК, 2007. – Ч. 2 (196 с.). – С. 19-21.

5. Сечко Г.В., Таболич Т.Г., Федюкович А.М., Худик П.И. Наблюдения за работой кассовых суммирующих аппаратов как один из способов борьбы с угрозами информационной безопасности // Тез. докл. межд. НПК «Современная радиоэлектроника. Научные исследования и подготовка кадров» Минск, 23-24 апреля 2008 года. – Мн.: МГВРК, 2008. – Ч. 1. – С. 127.

6. Калачёв И.А., Пачинин В.И., Сечко Г.В., Таболич Т.Г. База данных по результатам наблюдений за работой вычислительной техники // Материалы 16-й межд. НТК «Информационные системы и технологии ИСТ-2010», 23 апреля 2010 года, Нижний Новгород. – Нижний Новгород: НГТУ, 2010. – С. 204

7. Моженкова Е.В., Николаенко В.Л., Сечко Г.В., Таболич Т.Г. Влияние ранних отказов аппаратной части компьютера на надёжность его программного обеспечения // Информационные системы и технологии (IST”2010): Материалы VI Междунар. конф. (Минск, 24-25 ноября 2010 г.). – Мн.: А.Н.Вараксин, 2010. – 694 с. – С. 352-356.

М.Н.БОБОВ

ОЦЕНКА ПРОПУСКНОЙ СПОСОБНОСТИ МЕЖСЕТЕВЫХ ЭКРАНОВ

Межсетевые экраны обеспечивают барьер между сетями и предотвращают или блокируют нежелательный или несанкционированный трафик. Единственного определения для межсетевого экрана не существует. В данной работе будем использовать следующее определение межсетевого экрана: межсетевой экран - система или группа систем, используемая для управления доступом между доверенными и не доверенными сетями на основе предварительно сконфигурированных правил.

Межсетевой экран (МСЭ) включает в себя набор интерфейсов, между которыми он изолирует движение трафиков. Самая простая конфигурация МСЭ имеет один внешний и один внутренний интерфейс, как показано на рис. 1.

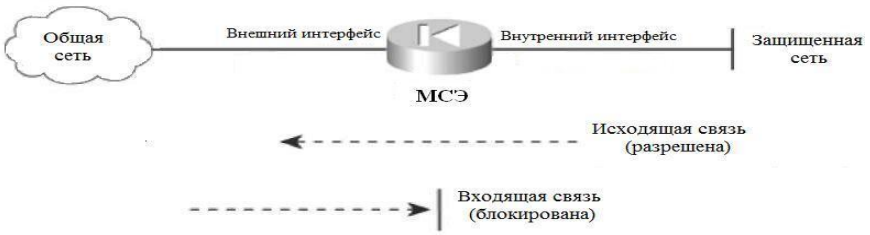


Рис. 1. Простой МСЭ с двумя интерфейсами

Межсетевой экран обеспечивает защиту информационно-телекоммуникационных сетей (ИТС) посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) ИТС на основе заданных правил. Каждое правило запрещает или разрешает передачу информации определенного вида между внешними и внутренними интерфейсами МСЭ. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

В ИТС МСЭ является транспортно узким местом. В большинстве конфигураций, где МСЭ являются единственной связью между сетями, при перегрузках сети он может стать единственной точкой отказа обслуживания и заблокировать трафик. С другой стороны, так как весь межсетевой трафик проходит через МСЭ существует большая вероятность перегрузки сети в результате атаки. Поэтому для ИТС, подключённой к Интернет высокоскоростными каналами, при организации её защиты посредством МСЭ одним из основных параметров является его пропускная способность. Оценка пропускной способности имеет комплексный характер и зависит от набора выполняемых МСЭ функций. Разработчиками МСЭ в качестве эксплуатационной характеристики указывается его производительность в Мбит/с при максимальном количестве одновременных соединений и задействованных функций проверки трафика.

Таким образом, можно сказать, что МСЭ представляет собой одноканальную систему передачи информации без буфера входящих сообщений. Если на такую систему занятую проверкой очередного пакета поступит следующее сообщение, то оно будет отброшено, а система будет считаться заблокированной. Эта модель полностью соответствует модели

одноканальной системы массового обслуживания (СМО) с отказами, используемой в задачах теории массового обслуживания.

Данная система массового обслуживания состоит только из одного канала (n = 1) и на нее поступает пуассоновский поток заявок с интенсивностью λ, зависящей, в общем случае, от времени:

$$\lambda = \lambda(t)$$

Заявка, заставшая канал занятым, получает отказ и покидает систему. Обслуживание заявки продолжается в течение случайного времени $T_{об}$, распределенного по показательному закону с параметром μ:

$$f(t) = \mu e^{-\mu t} \quad (t > 0)$$

Из этого следует, что «поток обслуживания» — простейший, с интенсивностью μ.

Рассмотрим единственный канал обслуживания как физическую систему S, которая может находиться в одном из двух состояний: S_0 — свободен, S_1 — занят. Из состояния S_0 в S_1 систему, очевидно, переводит поток заявок с интенсивностью λ, а из S_1 в S_0 — «поток обслуживания» с интенсивностью μ. Вероятности состояний S_0, S_1 обозначим соответственно $p_0(t)$ и $p_1(t)$. Очевидно, для любого момента t:

$$p_0(t) + p_1(t) = 1.$$

Для одноканальной СМО с отказами вероятность p_0 есть не что иное, как относительная пропускная способность q. Действительно, p_0 есть вероятность того, что в момент t канал свободен, или вероятность того, что заявка, пришедшая в момент t, будет обслужена. Следовательно, для данного момента времени t среднее отношение числа обслуженных заявок к числу поступивших также равно p_0 $(q = p_0)$

Решение дифференциальных уравнений Колмогорова для вероятностей состояний данной СМО в пределе, при $t \to \infty$, когда процесс обслуживания уже установится, даёт предельное значение относительной пропускной способности в виде:

$$q = \frac{\mu}{\lambda + \mu}$$

Задав относительную пропускную способность системы q (вероятность того, что пришедшая в момент t заявка будет обслужена), легко найти допустимую нагрузку на МСЭ и оценить предельно допустимый поток пакетов, который может обслужиться практически без потерь.

$$\lambda = \frac{1 - q}{q}\,\mu$$

Параметр **μ** зависит от производительности МСЭ по проверке трафика и для различных моделей составляет от 400 до 800 мегабит в секунду. Если принять q = 0,9, то для МСЭ с производительностью μ = 600 Мбит/с допустимый поток пакетов должен иметь скорость не выше λ = 400 Мбит/с.

В настоящее время наиболее эффективным методом защиты от сетевых атак является создание в составе ИТС с помощью МСЭ особой демилитаризованной зоны. Структура такого защищённого типового элемента ИТС, может быть представлена в следующем виде (Рис.2).

Защищённая ЛВС содержит три зоны безопасности:

– зону подключения к глобальной сети – демилитаризованную зону;

– зону управления безопасностью и ресурсами сети;

– зону защищаемых данных, обрабатываемых в ЛВС.

Зона подключения к глобальной сети включает в себя пограничный маршрутизатор, внешний МСЭ, почтовый сервер и сервер WEB. Пограничный маршрутизатор представляет собой первую линию защиты и обеспечивает защиту внешнего МСЭ от трафика,

направленного на IP-адреса МСЭ. Внешний МСЭ обеспечивает защиту ЛВС от атак извне и разрешает ограниченный набор трафика в соответствии с принятой политикой безопасности.

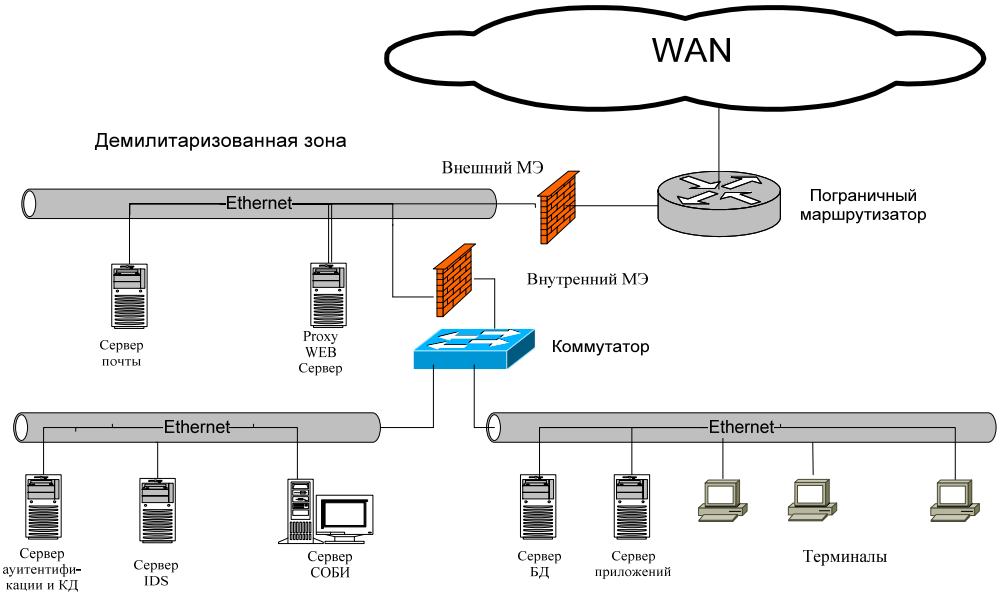


Рис. 2. Архитектура защищенной сети

Для разделения зоны подключения к глобальной сети и зоны внутренних сетей используются внутренний МСЭ и коммутатор. Внутренний МСЭ служит для контроля информационных потоков между внутренними сетями и обеспечивает:

– изоляцию зоны управления от остальной сети;

– защиту внутренней сети путем запрета трафика из менее защищенной зоны внешних подключений.

Зона управления безопасностью и ресурсами сети включает в себя сервер аутентификации и контроля доступа, сервер IDS, сервер СОБИ.

Зона защищаемых данных включает в себя сервер БД, сервер приложений и терминалы.

Относительная пропускная способность МСЭ при организации демилитаризованной зоны в пределе, при $t \to \infty$, когда процесс обслуживания уже установился, может быть определена по формуле

$$Q = \frac{\frac{\mu_1}{\lambda + \mu_1} \cdot \mu_2}{\lambda + \mu_2} = \frac{\mu_1 \mu_2}{(\lambda + \mu_1)(\lambda + \mu_2)}$$

где: μ_1 - интенсивность обслуживания внешнего МСЭ;

μ_2 - интенсивность обслуживания внутреннего МСЭ.

Преобразование выражения для Q дает квадратное уравнение относительно переменной λ:

$$Q\lambda^2 + Q\lambda(\mu_1 + \mu_2) + Q\mu_1^2\mu_2^2 - \mu_1 \mu_2 = 0.$$

Решение данного уравнения имеет один положительный корень

$$\lambda = \frac{-Q(\mu_1 + \mu_2) + \sqrt{Q^2(\mu_1 - \mu_2)^2 + 4Q\mu_1\mu_2}}{2Q}.$$

Используя вышеприведенные исходные данные и полагая μ_2 = 400 Мбит/с получим, что допустимый поток пакетов для данной структуры должен иметь скорость не выше λ = 13,9 Мбит/с.

П.Л.БОРОВИК

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ ВИДЕОКОНФЕРЕНЦСВЯЗИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Термин «видеоконференцсвязь» (ВКС) можно интерпретировать как интерактивное общение между людьми с помощью электронных средств. Опыт использования данной технологии в системе правоохранительных органов показал, что системы передачи видеоданных могут эффективно использоваться при проведении следующих мероприятий:

проведение допросов защищаемых лиц при нахождении последних вне зала судебного заседания (в соответствии со ст. 68 ч. 3 Уголовно-процессуального кодекса Республики Беларусь от 16.07.1999 N 295-З (с изменениями и дополнениями по состоянию на 10 июля 2009 года);

проведение опросов свидетелей с искажением голоса и скрытия глаз по уголовному или иному судебному делопроизводству в соответствии с законодательными правовыми актами по защите свидетелей;

проведение дистанционных консультаций, оперативных совещаний, семинаров по обмену опытом, интерактивное дистанционное обучение сотрудников правоохранительных органов;

проведение кассационных и надзорных судебных процессов с использованием ВКС для взаимодействия судей, прокуроров и адвокатов, находящихся в зале судебного процесса суда общей юрисдикции с одним или несколькими осужденными в одном или нескольких исправительных учреждениях в реальном масштабе времени.

При этом современные средства ВКС предоставляют широкие возможности для совместной работы с данными и различными приложениями, вплоть до подписания документов электронной цифровой подписью, а существующие средства криптозащиты позволяют сохранить конфиденциальность содержания сеансов видеосвязи.

Таким образом, использование ВКС в практической деятельности органов внутренних дел Республики Беларусь позволяет значительно снизить транспортные и иные затраты, связанные с командировками сотрудников, осуществить более эффективный сбор и оперативную обработку информации в режиме удаленного доступа, наладить новый уровень коммуникации.

Вместе с тем, необходимость использования технологии видеоконференцсвязи для повышения эффективности практической деятельности сотрудников органов внутренних дел требует разработки и реализации средств защиты информации, циркулируемой по каналам связи.

Основная проблема, на наш взгляд, заключается в протоколе IP, при разработке которого, как известно, не учитывались вопросы безопасности. Передача голосового трафика по IP является приложением, причем таким приложением, которое может охватывать значительную часть инфраструктуры органов внутренних дел. Эта инфраструктура уязвима

для сетевых атак. И если при создании системы ВКС заранее не предусмотреть вопросы информационной безопасности, то в результате может быть нарушена сетевая защита всей информационно-коммуникационной среды.

В настоящее время на рынке средств информационной безопасности в основном представлены средства по защите систем ВКС зарубежного производства. Данное обстоятельство в значительной степени делает уязвимой инфраструктуру правоохранительных органов и актуализирует вопросы построения систем защиты ВКС в нашей стране. В настоящем докладе представлены некоторые технические аспекты построения отдельных элементов системы защиты ВКС в органах внутренних дел.

По мнению специалистов, средства защиты ВКС должны обеспечивать как противодействие внешнему нарушителю, воздействующему на сеть передачи данных, так и внутреннему, в качестве которого выступает оборудование видеоконференцсвязи [1, с. 112].

Для реализации защиты систем ВКС предлагается использовать технологии на основе программно-аппаратных маршрутизаторов. В данном случае система защиты состоит из следующих элементов:

программного маршрутизатора контроля доступа, обеспечивающего защиту аппаратных средств ВКС, реализующего функции идентификации и аутентификации пользователей, а также обеспечение защиты от недокументированных возможностей и программных закладок;

терминалов (рабочих станций) безопасного управления, реализующих доверенный способ ввода информации в систему защиты, и предназначенных для санкционирования сеансов связи пользователями;

сервера управления доступом, обеспечивающего централизованное управление всей системой, и используемого как автоматизированное рабочее место администратора системы ВКС.

Предложенный подход позволяет строить системы защищенной видеоконференцсвязи, реализующие до трех различных моделей разграничения доступа.

Следует констатировать, что надежная идентификация и аутентификация затруднена по ряду принципиальных причин. Во-первых, любая компьютерная система основывается на информации в том виде, в каком она была получена; строго говоря, источник информации остается неизвестным. Например, злоумышленник мог воспроизвести ранее перехваченные данные. Следовательно, необходимо принять меры для безопасного ввода и передачи идентификационной и аутентификационной информации. Во-вторых, почти все аутентификационные данные можно узнать, похитить или подделать. В-третьих, существует противоречие между надежностью аутентификации с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности следует с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это повышает вероятность подглядывания за вводом. В-четвертых, чем надежнее средство защиты, тем оно дороже.

В последнее время набирает популярность аутентификация путем выяснения координат пользователя. Идея состоит в том, чтобы пользователь посылал координаты спутников системы GPS (Global Positioning System), находящихся в зоне прямой видимости. Сервер аутентификации знает орбиты всех спутников, поэтому может с точностью до метра определить положение пользователя.

Поскольку орбиты спутников подвержены колебаниям, предсказать которые крайне сложно, подделка координат оказывается практически невозможной. Ничего не даст и перехват координат - они постоянно меняются. Непрерывная передача координат не требует от пользователя каких-либо дополнительных усилий, поэтому он может без труда многократно подтверждать свою подлинность. В настоящее время аппаратура GPS сравнительно недорога и апробирована, поэтому в тех случаях, когда легальный

пользователь должен находиться в определенном месте, данный метод проверки подлинности представляется весьма привлекательным с точки зрения надежности и экономической целесообразности.

Угрозу безопасности, связанную с несанкционированным подключением к терминалам ВКС можно снизить путем отключения неиспользуемых портов коммутаторов, а также фильтрацией по MAC-адресам и IP-адресам, повышением степени идентификации и аутентификации пользователей. Кроме того, в целях обеспечения информационной безопасности беспроводных каналов связи ВКС необходимо разработать отдельный нормативный документ, регламентирующий политику безопасности системы.

Важным представляется вопрос обеспечения высокой надежности передачи видеоданных по каналам связи.

Существующие системы видеоконференцсвязи в основном используют кодеки сжатия видеоинформации на базе стандартов семейства MPEG (H.264/AVC, MPEG-2 и т.д.) и MJPEG, MJPEG2000. Данные кодеки, обеспечивая высокую эффективность сжатия видеоданных, не обладают высокой надежностью и устойчивостью при передаче по каналам связи.

По мнению некоторых специалистов, альтернативой перечисленным выше решениям могут стать методы сжатия видеоданных на основе трехмерного дискретного косинусного преобразования (ДКП), которые обеспечивают более устойчивую передачу видеоданных по каналам связи [2, с. 33].

Видеоданные, сжатые на основе ДКП, более устойчивы к потерям пакетов в каналах связи. Надежная передача видеоданных обеспечивается за счет использования неравномерного помехоустойчивого кодирования. Адаптация битовой скорости видеоданных к быстроменяющейся пропускной способности канала связи осуществляется путем последовательной передачи сначала базового уровня иерархии, а затем уточняющих уровней за фиксированное время, по истечении которого неотправленные уровни иерархии удаляются из буфера передатчика [2, с. 33].

Заключительным этапом при вводе в эксплуатацию системы ВКС являются мероприятия по оценке защищенности инфраструктуры ВКС.

Мероприятия по оценке защищенности включают в себя три этапа: подготовительный этап, этап оценки уязвимости сети и заключительный этап.

На первом этапе, с помощью аппаратно-программных средств (например, AirMagnet Enterprise) осуществляется оценка уязвимости сети. Для целей уточнения зоны обслуживания сети можно использовать программу Netstumbler. Программа проста в использовании и достаточно информативна.

Второе, что необходимо сделать при оценке уязвимости сети - произвести поиск несанкционированно включенных в общую сеть беспроводных маршрутизаторов или точек доступа, а также клиентских устройств, находящихся в общей сети с включенными беспроводными адаптерами.

Для обнаружения всех точек доступа, в том числе и скрытых можно использовать беспроводной сниффер (например, Kismet). Данный программный продукт идентифицирует сети, пассивно собирая пакеты и анализирует их, и поэтому способен обнаружить скрытые беспроводные устройства и сети.

Третий этап анализа защищенности - обследование имеющихся отклонений в реализации политики безопасности принятой в организации. Для реализации данного этапа можно использовать программу Kismet или набор программ Aircrack-ng, предназначенных для обнаружения беспроводных сетей, перехвата передаваемого через беспроводные сети трафика, взлома WEP и WPA/WPA2-PSK ключей шифрования, а также анализа беспроводных сетей [3, с. 91].

Вышеуказанные подходы позволят обеспечить требуемый уровень информационной безопасности при использовании технологии ВКС в органах внутренних дел.

Литература

1. ООО «НеоБИТ» Подход к построению системы защищенной видеоконференцсвязи с многоуровневым контролем доступа // Региональная информатика (РИ-2010): труды конференции / СПОИСУ. – СПб, 2010. – 394 с.

2. Беляев, Е.А. Сжатие видеоинформации при помощи трехмерного дискретного псевдокосинусного преобразования / Е.А. Беляев // Региональная информатика (РИ-2010): труды конференции / СПОИСУ. – СПб, 2010. – 394 с.

3. Башмаков, А.В Программно-аппаратные средства защищенности беспроводных сетей передачи данных / А.В. Башмаков, А.П. Нырков // Региональная информатика (РИ-2010): труды конференции / СПОИСУ. – СПб, 2010. – 394 с.

К.А.БОЧКОВ, П.М.БУЙ, В.И.КУШНЕРОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АППАРАТНО-ПРОГРАММНЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

В настоящее время для всех аппаратно-программных систем железнодорожной автоматики и телемеханики (АПС ЖАТ) критичных к безопасности движения поездов, согласно законодательства Республики Беларусь [1], неизбежным становится вопрос аттестации на защищенную информационную систему. В целом, это касается не только систем автоматики и телемеханики, но и любых других систем железнодорожного транспорта, оперирующих в процессе своей работы информацией, распространение которой ограничено (служебной информацией ограниченного распространения).

На пути к аттестации АПС ЖАТ необходимо разработать задание по безопасности, провести его оценку и, подготовив соответствующую документацию [1, приложение 2] подать заявку на аттестацию. Для выполнения этих этапов необходимо привлекать посторонних исполнителей, имеющих соответствующие лицензии, которые, к сожалению, не всегда бывают знакомы с особенностями функционирования IT систем железнодорожного транспорта и компетентны в системах ЖАТ. Поэтому выполнение работ по разработке задания по безопасности, проведения его оценки и аттестации АПС ЖАТ на защищенную информационную систему может вызвать существенные затруднения у исполнителя и заказчика.

Тем не менее, при всем многообразии АПС ЖАТ, их функционирование и способы организации, в силу специфики железнодорожного транспорта и высоких требований к обеспечению безопасности движения поездов, можно назвать типовыми и классифицировать по ряду ключевых признаков.

В основу классификации АПС ЖАТ следует положить принципы классификации, указанные в стандарте [2]. Однако к системам АПС ЖАТ применимы только классы А2, Б2 и В2.

Подкласс 2 характеризует совокупность объектов информатизации, на которых обрабатывается информация, содержащая сведения, отнесенные в установленном порядке к служебной информации ограниченного распространения, а также иная информация, охраняемая в соответствии с законодательством Республики Беларусь, за исключением сведений, отнесенных в установленном порядке к государственным секретам.

Подклассы А, Б и В характеризуют размещение технических средств совокупности объектов информатизации и покрытие их комплексом средств безопасности объекта (КСБО).

Отнесение АПС ЖАТ к тому или иному классу объектов информатизации влияет на содержание задания по безопасности и, следовательно, на ее оценку и процесс аттестации на защищенную информационную систему.

Для упрощения процессов разработки задания по безопасности, ее оценки и аттестации на защищенную информационную систему предлагается сформировать перечень требований по обеспечению информационной и функциональной безопасности АПС ЖАТ и, при использовании более подробной их классификации, выделить для каждого класса те требования, удовлетворение которых необходимо для построения защищенной информационной системы.

В качестве основных признаков для классификации АПС ЖАТ могут быть выбраны следующие:

– количество уровней конфиденциальности информации, обрабатываемой в системе;

– количество субъектов (пользователей) одновременно работающих с системой;

– количество уровней полномочий доступа субъектов к информации и т. п.

Так микропроцессорная централизация (МПЦ) (класс А2, согласно [2]) может быть отнесена к классу АПС ЖАТ, в которой используется информация нескольких уровней конфиденциальности, одновременно может работать только один субъект и используется несколько уровней полномочий доступа субъектов к информации (управление объектами станции, получение диагностической информации о системе).

В качестве групп требований по обеспечению информационной и функциональной безопасности АПС ЖАТ можно выделить следующие: аутентификации, управления доступом, мониторинга и учета, криптографической защиты, обеспечения целостности, обеспечения надежности и т. п.

Все представленные выше группы должны состоять из конкретных четко сформулированных требований, выполнение которых, по мнению специалистов разрабатывающих задание по безопасности, проводящих его оценку и аттестацию системы, необходимо для права носить статус защищенной информационной системы.

Разработка строгой классификации АПС ЖАТ и формулирование требований для построения защищенной информационной системы в совокупности позволит унифицировать и типизировать процессы разработки задания по безопасности АПС ЖАТ, проведения его оценки и аттестации на защищенную информационную систему.

Литература

1. Постановление Совета министров Республики Беларусь № 625 «О некоторых вопросах защиты информации» от 26 мая 2009 года.

2. СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация».

А.В.ГЛЕВИЧ, Ю.В.ЗЕМЦОВ

ВНУТРЕННИЙ АУДИТ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА НАЦИОНАЛЬНОЙ ГРИД-СЕТИ

В интересах ускоренного использования достижений международной науки и технологий в инновационной деятельности и последовательного роста на этой основе конкурентоспособности экономики Республики Беларусь в 2008-2010 годах была создана совместимая с общеевропейской национальная грид-сеть. Национальная грид-сеть обеспечивает научным организациям возможность получать доступ к консолидированным высокопроизводительным компьютерным ресурсам в Беларуси и Европе в целом, а также создает условия для эффективного ведения совместной научно-исследовательской деятельности на международном уровне.

Для того чтобы оценить значимость достигнутого результата, поясним, что представляет собой грид-сеть. Грид-сеть – это распределенная программно-аппаратная компьютерная среда, с принципиально новой организацией вычислений и управления потоками заданий и данных. Такая компьютерная инфраструктура предназначена для объединения вычислительных мощностей различных организаций. Более того, на основе грид-технологий происходит формирование региональных, национальных и даже международных вычислительных компьютерных инфраструктур для создания объединенных глобальных интернациональных ресурсов, предназначенных для решения крупных научно-технических задач. Название «грид» объясняется некоторой аналогией с электрическими сетями (от англ. powergrid – энергосеть), предоставляющими всеобщий доступ к электрической мощности. Как и в случае электрических сетей, в грид-инфрастуктуре интегрируется большой объем географически удаленных компьютерных ресурсов, причем пользователю такой инфраструктуры не важно, где находятся используемые им ресурсы.

Среди основных возможных направлений использования национальной грид-сети можно выделить:

– организацию эффективного использования ресурсов для небольших задач, с утилизацией временно простаивающих компьютерных ресурсов;

– распределенные супервычисления, решение очень крупных задач, требующих огромных процессорных ресурсов, памяти и т.д., например, в инженерных науках и биоинформатике;

– вычисления с привлечением больших объемов географически распределенных данных, например, в медицине, метеорологии и геофизике;

– коллективные вычисления, в которых одновременно принимают участие пользователи из различных организаций, например, проекты Европейской организации по ядерным исследованиям.

Важнейшим компонентом национальной грид-сети является удостоверяющий центр. Удостоверяющий центр национальной грид-сети (УЦ) призван гарантировать безопасную работу в незащищенных сетях общего доступа, обеспечивая функционирование таких сервисов, как аутентификация, конфиденциальность, контроль целостности и доказательное подтверждение авторства при передаче информации, а также единый вход в грид-сеть.

На настоящий момент в рамках работ по созданию удостоверяющего центра получены следующие основные результаты:

– разработан основополагающий документ УЦ «Политика применения сертификатов и регламент удостоверяющего центра национальной грид-сети»;

– разработан программный комплекс удостоверяющего центра национальной грид-сети с набором программной, технической и нормативной документации;

– обеспечено функционирование удостоверяющего центра национальной грид-сети в соответствии с международными стандартами, что являлось необходимым условием для создания безопасной и совместимой с международной грид-инфраструктуры электронной науки;

– организована и проведена аккредитация удостоверяющего центра национальной грид-сети в международной организации EUgridPMA, разрабатывающей и обеспечивающей соблюдение правил функционирования международных грид-инфраструктур;

– удостоверяющий центр национальной грид-сети введен в качестве полноправного члена в состав международной организации EUgridPMA;

– разработан ряд справочных документов и руководств для абонентов удостоверяющего центра.

С момента аккредитации в международной организации EUgridPMA удостоверяющий центр национальной грид-сети принимает активное участие в деятельности данной организации, сотрудники центра посещают регулярно проводимые семинары и конференции EUgridPMA, участвуют в совместной работе над техническими и нормативными

документами, касающимися правил функционирования международных грид-инфраструктур и национальных грид-сетей.

В соответствии с требованиями EUGridPMA удостоверяющий центр национальной грид-сети должен разработать методику внутреннего аудита и регулярно отчитываться по результатам проверки, проводимой в соответствии с данной методикой.

Разработанная сотрудниками УЦ методика внутреннего аудита основана на проверке соответствия функционирования УЦ требованиям нормативно-технической документации EUGridPMA и требованиям, предъявленным в документе "Политика применения сертификатов и регламент УЦ". Методика внутреннего аудита включает проверку документации, действий, которые УЦ выполняет при осуществлении своих функций, опрос персонала, ответственного за управление и функционирование УЦ, проверку квалификации персонала, а также проверку оборудования, которое содержится в структуре УЦ.

Процедура аудита выполняется в три этапа: предварительный, основной и заключительный. На предварительном этапе рецензируется документация, на основном – проверяется выполнение требований к функционированию УЦ, а на заключительном этапе составляется отчет о результатах аудита. Аудиторы должны иметь соответствующую квалификацию по проведению проверок удостоверяющих центров, обладать опытом работы с инфраструктурой открытых ключей, криптографическими технологиями, программным обеспечением УЦ.

При предварительной проверке аудиторам должны быть предоставлены все документы УЦ: Политика применения сертификатов и регламент УЦ, руководства абонента, руководства оператора и администратора УЦ, списки отозванных сертификатов, сертификаты (физических лиц, серверов и служб, а также корневой сертификат УЦ). Указанные материалы должны быть доступны в репозитории УЦ, однако аудиторы могут запросить, чтобы УЦ предоставил другие документы, имеющие отношение к функционированию УЦ. Таким образом, на данном этапе аудиторы оценивают выполнение предъявляемых к УЦ требований, используя, главным образом, публично доступную информацию.

Основная проверка осуществляется при личной явке аудиторов в УЦ. Аудиторы проводят собеседования с персоналом, ответственным за управление и функционирование УЦ, инспектируют документы (например, архив журналов регистраций), проверяют оборудование. Аудиторы должны оценить выполнение требований, которые не могли быть оценены при предварительной проверке. На данном этапе проверяются следующие объекты: помещение УЦ; оборудование УЦ (сервер репозитория, подписывающая ЭВМ, рабочие места операторов УЦ); защищенное место хранения (сейф) и наличие в нем резервной копии личного ключа УЦ, запечатанного конверта, содержащего пароль к личному ключу УЦ, архива журналов проверок; сертификаты (если не были доступны при предварительной проверке); записи регистраций действий СЦ/РЦ; записи регистраций обращений к репозиторию УЦ; записи регистраций использования личного ключа УЦ; журнал регистраций доступа в помещение УЦ; другие документы (например, отчеты операторов УЦ).

На заключительном этапе аудиторы составляют отчет согласно результатам предварительной и основной проверок. Заключение аудитора должно включать: дату проведения аудита, ФИО аудиторов, ФИО участников, оценки соответствия требованиям аудита и комментарии к ним.

Если в результате аудиторской проверки выявлено несоответствие действий УЦ требованиям нормативно-технической документации EUGridPMA или требованиям, предъявленным в документе "Политика применения сертификатов и регламент УЦ", выполняются следующие действия:

1) несоответствие фиксируется в отчете о результатах аудиторской проверки;

2) аудитор сообщает УЦ о выявленном несоответствии;

3) персонал, ответственный за управление и функционирование УЦ, принимает решение о том, какие действия следует предпринять для устранения выявленного несоответствия, после чего без промедления указанное несоответствие устраняется.

В зависимости от значимости и природы выявленного несоответствия и количества времени, требуемого для его устранения, деятельность УЦ может быть приостановлена, корневой сертификат УЦ отозван, или произведены другие необходимые действия. Решение о применении конкретного действия должно базироваться на степени тяжести несоответствия и степени возникающих рисков.

Окончательный отчет об изменениях в функционировании УЦ (о выявленном несоответствии и мерах, принятых для его устранения) предоставляется аудиторам и EUGridPMA.

С.А.ГОЛОВИН

РАЗРАБОТКА ИНФОРМАЦИОННЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ОБЩИХ ИНФОРМАЦИОННЫХ РЕСУРСОВ БЕЛАРУСИ И РОССИИ

Одной из важных задач по совершенствованию информационного обеспечения деятельности органов и специалистов Союзного государства в области защиты информации в рамках выполнения программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006 – 2010 годы» была определена задача создания автоматизированного фонда документов в области технической защиты информации и обеспечения безопасности информации в критически важных системах информационной инфраструктуры Союзного государства.

В интересах решения указанной задачи были проведены работы по созданию электронной базы данных с документами Союзного государства в указанной области.

Электронная база данных реализована с использованием средства разработки приложений Borland Delphi, функционирует на платформе Microsoft Windows и использует в качестве хранилища электронных версий документов (текстов документов) систему управления базами данных Microsoft Access.

По уровню реализованных в данной электронной базе данных алгоритмических и программных решений она соответствует лучшим образцам программной продукции в области объектно-ориентированных локальных баз данных.

Проведены работы по заполнению базы данных электронными документами по технической защите информации и обеспечению безопасности информации в критически важных системах информационной инфраструктуры Союзного государства.

В электронную базу данных включены 72 документа и проектов документов, разработанных в ходе выполнения программ Союзного государства в области защиты общих информационных ресурсов Беларуси и России в период с 2000 по 2010 годы, а также дополнительно 126 документов Российской Федерации в области технической защиты информации, обеспечения безопасности информации в ключевых системах информационной инфраструктуры и в смежных областях.

Электронная база данных с документами Союзного государства в области технической защиты информации и обеспечения безопасности информации в критически важных системах информационной инфраструктуры Союзного государства в настоящее время находится в опытной эксплуатации в ГНИИИ ПТЗИ ФСТЭК России.

Д.В.ГРУШИН, С.М.ШПАК

ПОСТРОЕНИЕ ВЕДОМСТВЕННЫХ РЕЖИМНЫХ СЕТЕЙ СВЯЗИ НА БАЗЕ ЗАЩИЩЕННОЙ АТСЭ ФМС ОАО “СВЯЗЬИНВЕСТ” С РЕАЛИЗАЦИЕЙ РПУ И БСВ

При построении ведомственных сетей для режимных предприятий и ведомств в Республике Беларусь остро встают вопросы по выбору оборудования, в условиях жесткого бюджетирования, учитывающего как существующий парк спец. аппаратуры, так и возможности дальнейшей модернизации такой сети с учетом перспективы миграции на новые протоколы каналообразования, одновременно соответствуя жестким требованиям по защищенности информации от несанкционированного доступа и утечек по каналам побочного электромагнитного излучения и наводок. Зачастую приходится сталкиваться с задачей построения защищенной сети связи, эксплуатирующей параллельно как откровенно старые образцы оборудования, так новые.

В отдельных случаях необходимо было единовременно заменить устаревшие коммутаторы П-209И и режимные АТС старого парка без установки стороннего дополнительного оборудования, таких как вокодеры и устройства взаимодействия (АРПУ и БСВ), при этом в целом повысить отказоустойчивость системы, снизить энергопотребление, одновременно предоставляя гораздо больший уровень сервисных услуг и качества речи, чем ранее.

Широкое применение интерфейса Ethernet и задача по вставке и выделению из цифрового потока Е-1 каналов ТЧ для внешних потребителей (аппаратуры ЗАС, тонального телеграфирования, прямой связи, оповещения и др.), и необходимость подключения уже засекреченных каналов n*64кбит\с с интерфейсом Ethernet 10BaseT для сетей передачи данных подтолкнула к реализации функций первичного мультиплексора на базе защищенной АТС.

Учитывая область применения подобных АТС: узлы связи пунктов управления силовых ведомств, других органов государственного управления, которые должны быть как стационарными, так и мобильными – возникла необходимость в компактном мобильном исполнении, предназначенном для установки на автомобильных шасси.

В итоге возникли требования к специальной защищенной АТС, соответствующей требованиям группы 1.7 ГОСТ В 20.39.304-76 для техники, работающей на ходу, климатического исполнения УХЛ и осуществляющей:

– организацию внутренней, исходящей, входящей и транзитной спец. связи в автоматическом или полуавтоматическом (через оператора –телефониста, выполненного на базе ПЭВМ), как с абонентами своего пункта управления, так и прочими абонентами ведомственных засекреченных сетей связи;

– выделение из засекреченных цифровых потоков аналоговых и цифровых каналов связи для категорированных сетей передачи данных или других пользователей;

– поддержку всех доступных на сегодняшний день стыков и протоколов таких как: аналоговые 2-х проводные и 4-х проводные линии; цифровые потоки Е-1; каналы связи по стыку С1-ФЛ-БИ с использованием аппаратуры ЗАС.

Очевидным путем решения поставленных задач для построения защищенных сетей связи явилась разработка специальной защищенной АТС белорусского производства, позволившей добиться

– полной совместимости с аппаратурой засекречивания старого парка;

– уже интегрированные в АТС речепреобразующие устройства БСВ и РПУ;

– возможности одновременного функционирования засекреченных сетей связи с использованием аппаратуры старого и нового (засекречивания цифровых каналов связи) парков;

– постепенной миграции с существующих сетей спец. связи на более высокий технический уровень без существенных затрат;

– единовременной замены коммутатора П-209И и режимных АТС старого парка, обеспечивая гораздо больший уровень сервисных услуг и качества речи, чем ранее; при этом вокодеры и устройства взаимодействия (АРПУ и БСВ) физически реализованы непосредственно в АТС и не требуются при работе с засекречивающей аппаратурой комплекса Т-230-03;

– реализации функции первичного мультиплексора;

– стационарного и мобильного (для размещения на автомобильном шасси в полевых аппаратных связи) исполнения;

– гибкости построения сетей и направлений прямой связи специального назначения;

– возможности модернизации аппаратных засекреченной связи старого парка путем простой замены оборудования;

– высокой надежность;

– повышенной гарантии до 5 лет.

В качестве примера построения подобных защищенных конвергентных сетей в Республике Беларусь можно привести автоматические телефонные станции АТСЭ ФМС – защищенные АТС, стационарного и мобильного исполнения, предназначенные для организации обмена телефонной информацией в сетях спец. связи. АТСЭ ФМС соответствует техническим требованиям по защите и безопасности информации Оперативно-аналитического центра при Президенте Республики Беларусь (сертификат соответствия № BY/112 03.1.3.ИВ0049).

Д.В.ГРУШИН, С.М.ШПАК

ПЕРСПЕКТИВНЫЕ СРЕДСТВА ЗАЩИТЫ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ, ДОСТУПНЫЕ НА ТЕРРИТОРИИ РЕСПУБЛИКИ БЕЛАРУСЬ

Переход в сети Интернет на предоставление услуг по технологии WEB2.0 и соответственно динамически меняющегося контента и геометрический рост трафика данных, подтолкнуло индустрию защиты IT-инфраструктуры предприятий на поиск новых решений по защите критичной информации на уровне шлюза (прокси-устройств).

Одним из способов повышения производительности подобных систем является тенденция увеличения аппаратных средств, по сравнению с программными, другой - тенденция миграции части функций в облачную среду, а так же выделение отдельных функций в отдельные физические устройства.

Новые требования времени – быстрее и оперативнее доставлять приложения к сотрудникам, где бы они не находились, одновременно обеспечивая защиту данных и приемлемую производительность. Ответом на данную IT-задачу явилось создание специальных сетей между специализированными прокси-устройствами. Как пример, можно привести Сеть Доставки Приложений (Application Delivery Network, ADN) - инфраструктуры, обеспечивающей 100% идентификацию приложений, их ускорение и безопасность. Устройства ProxySG поддерживает сеть ADN, являясь интегрированной ее частью.

Задача защиты и одновременного ускорение критичных для бизнеса приложений и контента, включая Web, SSL, мультимедиа и электронную почту подтолкнула к разработке новой линейки прокси-серверов. Таким образом, появились устройства с обратным прокси в DMZ, изолируя веб-сервера от прямого контакта с интернет, одновременно ускоряя веб-приложения. Дополнительной задачей в условиях роста плотности трафика явилась

необходимость поддержки существенного снижения требований к пропускной способности каналов, что изящно решается при помощи введения кэширования. Благодаря технологии MACH5, с помощью устройств ProxySG, можно значительно улучшить связь между удаленными офисами за счет кэширования повторяющегося трафика, управления пропускной способностью, оптимизации протоколов, кэширования объектов и сжатия.

Как дополнительным уровнем защиты, так и необходимостью повышения производительности было вызвано появление на данной платформе прокси-устройств собственной ОС. Семейство ProxySG основано на SGOS - защищенной специализированной объектно-ориентированной операционной системе, предоставляющей гибкое управление внутренними правилами и политиками организации для контента, групп пользователей, приложений и протоколов. Blue Coat ProxySG позволяет анализировать и контролировать действия пользователей в Интернет, определять, к каким категориям сайтов и какому содержимому они получат доступ.

Передача некритичных функций, таких как, веб-фильтрация Облаку, позволила блокировать фишинговые и пиринговые атаки, а так же производить постоянное обновление базы данных на предмет последних версий вредоносных и шпионских программ на основе Динамической Рейтинговой Системы Реального Времени (DRTR), являющейся на сегодняшний день уникальной инновационной технологией, оценивающей боле 30 миллиардов запросов к веб-страницам в день.

Выделение функционала по антивирусной защите в отдельное решение – ProxyAV, предоставляющего выбор из множества антивирусов, обеспечивается как разгрузка вычислительной мощности прокси-устройств, так и способность блокировать неизвестные программные коды, атакующих через HTTP, FTP и HTTPS протоколам.

В настоящее время в Республике Беларусь доступны решения по безопасности IT-инфраструктуры предприятий от таких производителей, как Blue Coat Systems Inc., соответствующие техническим требованиям по защите и безопасности информации

Линейка прокси-серверов соответствует требованиям инсталляций любых размеров – от малых офисов из десяти сотрудников до головных офисов и датацентров.

Оперативно-аналитического центра при Президенте Республики Беларусь (Экспертное заключение ОАЦ РБ № 173 от 14.01.2010).

Blue Coat Systems Inc., основанная в 1996 г. в Саннивейл, Калифорния, США (Sunnyvale, California), специализируется на решениях, разработанных непосредственно для обеспечения безопасности Web-коммуникаций и многократного ускорения работы бизнес-приложений по всей распределённой структуре предприятий. Blue Coat обеспечивает создание интеллектуальных точек контроля, управляемых централизованно на основе политик. В свою очередь, настраиваемые политики имеют многоуровневую структуру, поддерживают изменяемые списки, категории, формируют действия на события, что позволяет ИТ организациям оптимизировать безопасность и производительность для различных групп пользователей и приложений.

Решения Blue Coat инсталлированы в транснациональных компаниях и у сервис-провайдеров по всёму миру. В их числе NASDAQ, JP Morgan, Boeing, Wal-Mart, Sony, General Electric, Volkswagen, United States Air Force, HSBC, и многих других. Благодаря глобальной системе поддержки и ‘on-line’ обслуживания, Заказчики могут обеспечивать бесперебойный контроль политик, защиту и производительность работы свох ИТ-структур.

По оценке IDC компания Blue Coat в настоящее время занимает первое место в мире на рынке систем защиты контента и доставки приложений.

А.А.ГРУШО, Е.Е.ТИМОНИНА

ЯЗЫК ЗАПРЕТОВ ДЛЯ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

1. Введение

Предположим, что корреспондент A передает информацию для корреспондента B. Передача представляет собой логически связанную последовательность выражений в языке общения A и B. Предположим, что скрытый агент на стороне A хочет передать сообщение скрытому агенту на стороне B в рамках общения A и B без нарушения логической связанности информации, передаваемой от A к B. Существуют известные способы реализации такой передачи, некоторые из которых имеют вполне легальный характер. Например, передаваемая от A к B информация делится на куски, формируются пакеты, в которые вставляется служебная информация, содержащая информацию, предаваемую от скрытого агента в A к скрытому агенту в B.

Предположим, что существует контролер, анализирующий передаваемую информацию с целью выявления скрытого общения агентов в A и в B. Контролер представляет собой программно-аппаратное решение, в которое заложена интеллектуальная функция выявления признаков скрытой передачи. Существует два пути противодействия контролеру.

Первый путь состоит в исключении признаков, по которым контролер выявляет скрытую передачу.

Второй путь основан на том, что ни один контролер, основанный на искусственном интеллекте, не в состоянии анализировать контекст общения A и B. Последний вариант является принципиальной слабостью всех систем защиты, контролирующих взаимодействие реальных информационных систем.

При построении безопасных интерфейсов между взаимодействующими информационными системами (межсетевые экраны, системы обнаружения вторжений и т.д.) невозможно учесть богатство языка, требуемого для взаимодействия сложных систем. Поэтому безопасные интерфейсы нельзя назвать высокоинтеллектуальными системами. Отсюда следует неустранимая уязвимость такого взаимодействия, основанная на том, что безопасный интерфейс не в состоянии распознать скрытые сообщения, выраженные на языке взаимодействия сложных информационных систем.

Вместе с тем возникает вопрос о способах и методах встраивания скрываемых сообщений в логически связанные информационные потоки на языке общения систем A и B.

Конечные вероятностные пространства часто используются как модели data mining, компьютерного моделирования, компьютерной безопасности, криптографии и т.д. Мы рассматриваем последовательность конечных вероятностных пространств, перенумерованных натуральными числами.

2. Математическая модель

Пусть X_i, i=1,.2,…, – последовательность конечных множеств, $\prod_{i=1}^{n} X_i$ – декартово произведение множеств X_i, i=1,.2,…, X^{∞} – множество всех последовательностей, в которых i-й элемент принадлежит их X_i. Определим минимальную σ-алгебру $\mathcal{A}$, порожденную цилиндрическими множествами. $\mathcal{A}$ также является борелевской σ-алгеброй в Тихоновском произведении X^{∞}, где X_i, i=1,.2,…, имеют дискретную топологию.

На (X^{∞} , $\mathcal{A}$) определена вероятностная мера P_0. Пусть $P_{0,n}$ проекция P_0 на первые n координат последовательностей из X^{∞}. Ясно, что для любого $B_n \subseteq \prod_{i=1}^{n} X_i$

$$P_{0,n}(B_n) = P_0(B_n \times X_n^{\infty}),$$

где $X_n^{\infty} = \prod_{i=n+1}^{\infty} X_i$. Пусть $D_{0,n}$ носитель меры $P_{0,n}$:

$$D_{0,n} = \{\vec{x}_n \in \prod_{i=1}^{n} X_i \ , \ P_{0,n}(\vec{x}_n) > 0\}.$$

Обозначим $\Delta_{0,n} = D_{0,n} \times X_n^{\infty}$. Последовательность $\Delta_{0,n}$, n=1,2,..., является невозрастающей и

$$\Delta_0 = \lim_{n\to\infty} \Delta_{0,n} = \bigcap_{n=1}^{\infty} \Delta_{0,n} .$$

Множество Δ_0 замкнуто и является носителем меры P_0.

Если $\overline{\omega}^{(k)} \in \prod_{i=1}^{k} X_i$, то $\widetilde{\omega}^{(k-1)}$ получается из $\overline{\omega}^{(k)}$ отбрасыванием последней координаты.

Определение 1. Запретом в мере $P_{0,n}$ называется вектор $\overline{\omega}^{(k)} \in \prod_{i=1}^{k} X_i$, $k \le n$, такой, что $P_{0,n}(\overline{\omega}^{(k)} \times \prod_{i=k+1}^{n} X_i) = 0$. $\overline{\omega}^{(k)}$ - наименьший запрет, если $P_{0,k-1}(\widetilde{\omega}^{(k-1)}) > 0$.

Если $\overline{\omega}^{(k)}$ запрет в $P_{0,n}$, тогда для любого $k \le s \le n$ и для любой последовательности $\overline{\omega}^{(s)}$, начинающийся с $\overline{\omega}^{(k)}$, мы имеем

$$P_{0,s}(\overline{\omega}^{(s)}) = 0. \qquad (1)$$

Действительно, если $P_{0,k}(\overline{\omega}^{(k)}) = 0$, тогда $P_0(\overline{\omega}^{(k)} \times X_k^{\infty})$ и $P_0(\overline{\omega}^{(k)} \times \prod_{i=k+1}^{s} X_i \times X_s^{\infty}) = 0$. Следовательно,

$$P_{0,s}(\overline{\omega}^{(s)}) = P_0(\overline{\omega}^{(s)} \times X_s^{\infty}) \le P_0(\overline{\omega}^{(k)} \times \prod_{i=k+1}^{s} X_i \times X_s^{\infty}) = 0.$$

Если существует $\overline{\omega}^{(n)} \in \prod_{i=1}^{n} X_i$ такой, что $P_{0,n}(\overline{\omega}^{(n)}) = 0$, тогда существует наименьший запрет. Если $P_{0,n-1}(\widetilde{\omega}^{(n-1)}) > 0$, тогда утверждение доказано. Обратно, если $P_{0,n-1}(\widetilde{\omega}^{(n-1)}) = 0$, то мы можем повторить предыдущие рассуждения. Отсюда следует, что $\overline{D}_{0,n} \neq \varnothing$ однозначно определяется наименьшими запретами в том смысле, что все элементы $\overline{D}_{0,n}$ получаются всеми возможными расширениями наименьших запретов до длины n.

3. Использование запретов для скрытой передачи

Легко видеть, что наименьшие запреты в $\prod_{i=1}^{n} X_i$ образуют префиксный код. Действительно, любой наименьший запрет не может быть частью другого наименьшего запрета в силу (1). Это означает, что если $|X_i| = m_i$, то последовательность наименьших запретов должна удовлетворять аналогу неравенства Крафта.

Теорема. Пусть ν_h, $h = \overline{1,n}$, число наименьших запретов длины h в мере $P_{0,n}$. Тогда для всех h, $h = \overline{1,n}$, $|X_i| = m_i$, $i = \overline{1,n}$, имеем

$$\nu_1 \prod_{i=2}^{h} m_i + \nu_2 \prod_{i=3}^{h} m_i + \cdots + \nu_{h-1}\, m_h + \nu_h + |D_{0,h}| = \prod_{i=1}^{h} m_i . \qquad (2)$$

В частном случае, когда $m_i = m$ для всех i мы имеем

$$\nu_1\, m^{n-1} + \cdots + \nu_{n-1} m + \nu_n + |D_{0,n}| = m^n$$

для всех n=1,2,....

Вернемся к рассмотрению скрытой передачи в рамках легального общения А и В. Естественно, что легальная передача от А к В представляет собой последовательность, каждый начальный кусок которой лежит в носителе меры $P_{0,n}$. Фиксируем последнюю букву в переданном легально векторе длины n. Рассмотрим n_1 и множество минимальных запретов, начинающихся в выделенной фиксированной точке, длины которых не превосходят n_1. Эти минимальные запреты определены однозначно.

Как было показано раньше, множество этих минимальных запретов образует префиксный код, на котором мы можем записать любое сообщение конечной длины. Данное сообщение может быть вставлено в текст после выделенной точки в конце вектора длины n. И после его передачи мы можем вернуться к выделенной точке и продолжить передавать исходное сообщение от А к В.

Естественно, мы требуем, чтобы агент на приемном конце В обладал достаточным знанием запретов в данной точке, чтобы выделить и прочитать передаваемое ему префиксным кодом сообщение. Убрав это сообщение, агент в В передает легальное сообщение собственно информационной системе В.

«Невидимость» скрываемого переданного сообщения для контролера определяется тем, что он не может идентифицировать содержание сообщения от А к В и, тем самым, не может определить как используемый префиксный код, так и выражение, записанное с помощью этого кода.

Литература

1. Бурбаки Н. Общая топология. Основные структуры. М.: Наука, 1968.

2. Грушо А.А., Тимонина Е.Е. Некоторые связи между дискретными статистическими задачами и свойствами вероятностных мер на топологических пространствах. Дискретная математика, 2006. – т. 18. – № 4. –128-135.

3. Грушо А.А., Тимонина Е.Е. Запреты в дискретных вероятностно-статистических задачах. Дискретная математика. – М.: Наука, 2011 (в печ.)

4. Фано Р. Передача информации. Статистическая теория связи. М.: Мир, 1965.

5. A. Grusho, N. Grusho, E. Timonina. Problems of Modeling in the Analysis of Covert Channels // Proceedings of 5th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2010, St. Petersburg, Russia, September 2010. – Springer, 2010. – p. 118-124.

6. Simmons G.J. The prisoner`s problem and the subliminal channel // Proc. Workshop on Communications Security (Crypto`83). – 1984. – p. 51-67.

Е.А.ДОЦЕНКО, И.А.КАРТУН

ПРОБЛЕМЫ АТТЕСТАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

Создание системы защиты информации информационной системы – это всего лишь первый шаг к обеспечению должного уровня информационной безопасности.

Для гарантии того, что система защиты выполняет все предписанные ей функции и установленные требования, нужно провести ее проверку, то есть пройти процедуру аттестации.

В Республике Беларусь мероприятия по аттестации систем защиты информации регулируются постановлением Совета Министров Республики Беларусь от 26 мая 2009 года №675 (далее Постановление) и являются обязательными. К этому постановлению прилагаются три Положения, одно из которых называется «Положение о порядке аттестации систем защиты информации». Оно определяет аттестацию, как комплекс организационно-технических мероприятий, в результате которых подтверждается соответствие системы защиты информации требованиям нормативных правовых актов в области защиты информации, в том числе технических нормативных правовых актов, и оформляется аттестатом соответствия.

Для проведения аттестации необходимо выполнить ряд действий, осуществление которых без дополнительных пояснений и разъяснений может вызвать трудности.

Согласно Закону Республики Беларусь от 10 ноября 2008 г. N 455-З «Об информации, информатизации и защите информации» (далее Закон) информационная система – это совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

Согласно СТБ 34.101.30-2007 под объектом информатизации понимаются средства электронной вычислительной техники (автоматизированные системы различного уровня и назначения, вычислительные сети и центры, автономные стационарные и персональные электронные вычислительные машины, а также копировально-множительные средства, в которых для обработки информации применяются цифровые методы) вместе с программным обеспечением, которые используются для обработки информации.

Возникает первый вопрос: информационная система и объект информатизации – это одно и то же? Видимо да, если в Постановлении сказано о необходимости отнесения информационной системы к классу типовых объектов информатизации согласно СТБ 34.101.30-2007. Тогда возникает второй вопрос: к какому типу объекта информатизации отнести информационную систему?

Разберем определение информационной системы дальше… *Банк данных* – организационно-техническая система, включающая одну или несколько баз данных и систему управления ими. *Комплекс программно-технических средств* – совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий. *Информационная технология* – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и **защиты информации**. То есть неотъемлемой составляющей информационных систем является обеспечение защиты информации.

Обратимся снова к Постановлению. Там сказано, что для защиты информации в информационных системах создается система защиты информации. Получается – система защиты информации – часть информационной системы. Постановление определяет систему защиты информации как совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, функционирующих по правилам, установленным соответствующими нормативными правовыми актами в области защиты информации, в том числе техническими нормативными правовыми актами. Таким образом, система защиты включает в себя персонал. Дополнительно доказательством этому является проведение при аттестации проверки уровня подготовки кадров и распределения ответственности персонала за организацию и обеспечение выполнения требований по защите информации. Следовательно, информационная система не может существовать без персонала.

Вернемся к вопросу об определении типа объекта информатизации применительно к информационной системе. Копировально-множительным средством, вычислительной сетью, центром, автономной стационарной или персональной электронной вычислительной машиной она быть не может хотя бы потому, что персонал не является их неотъемлемой частью. Остаются автоматизированные системы различного уровня и назначения.

ГОСТ 34.003-90 говорит о том, что автоматизированная система – это система, состоящая из **персонала** и **комплекса средств автоматизации (**все компоненты автоматизированной системы за исключением людей) его деятельности, реализующая **информационную технологию** выполнения установленных функций. Банки данных относятся к комплексу средств автоматизации.

Таким образом, получается, что информационная система есть не что иное, как автоматизированная система, что не согласуется с определением Закона.

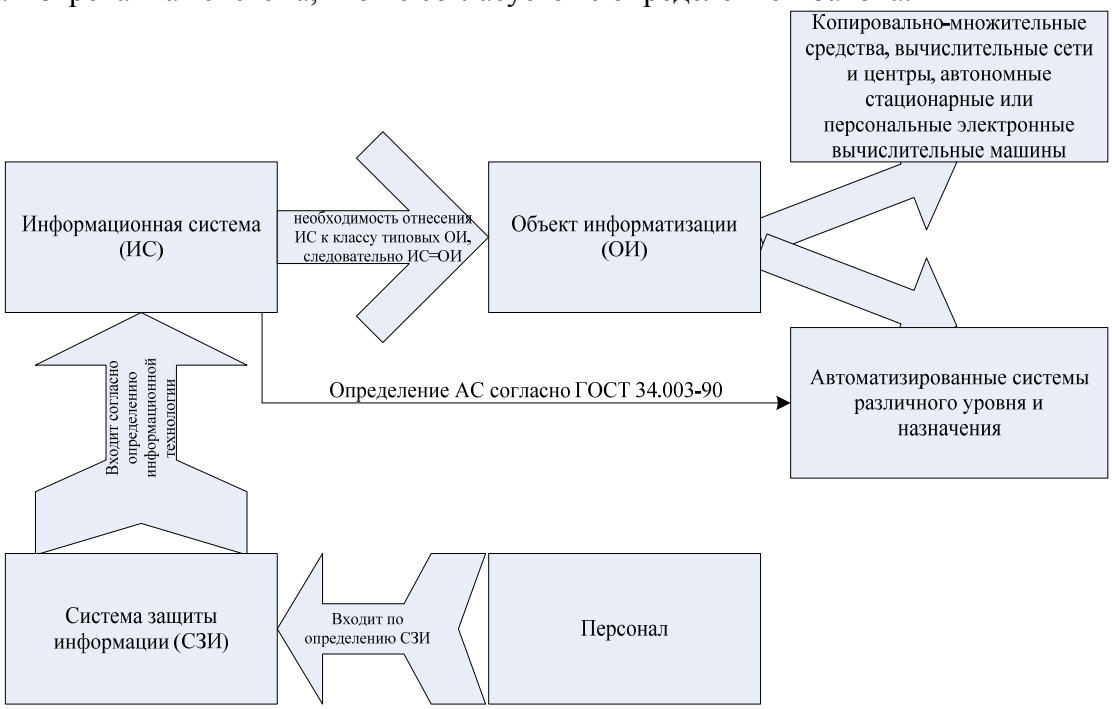


Рисунок – Логическая цепочка

Помимо всего вышеизложенного, процедура аттестации включает анализ наличия и основных характеристик средств физической защиты информационной системы (помещений, где обрабатывается защищаемая информация и хранятся информационные носители). Да, такой анализ нужен для проведения комплексной оценки информационной безопасности. Исключить этот пункт нельзя. Но как-то не вписывается это в описанную

логическую цепочку. Единственным решением может стать корректировка термина того, что мы все-таки аттестуем.

Возможно, стоит аттестовать не систему защиты информации по требованиям защиты информации, а то, частью чего она является. Т.е. аттестовать автоматизированную систему вместе с помещениями. Скорее всего, стоит данные слагаемые назвать единым целым, например «объектом информатизации», с последующим пересмотром СТБ 34.101.30-2007 и, соответственно Постановления.

Вопросы эти важны, требуют большого внимания, т.к. актуальность аттестации возрастает с каждым днем.

В заключение хотелось бы сказать, что проблема терминологии очень остра. До выхода Постановления на государственном уровне был внедрен ряд **прикладного программного обеспечения** (именно прикладного программного обеспечения), для облегчения взаимодействия между государственными органами. Примеры: Автоматизированная информационная система «Резерв», Автоматизированная информационная система «Кадастры» и т.д. Появляются проблемы аттестации систем защиты информации данных «информационных систем»:

1. Проблема финансирования. «Резерв» распределен по всей стране во многих ведомствах. Определить источник финансирования проведения аттестации не представляется возможным.
2. Проблема многократной аттестации для одной организации. Если система локальная, но организация пользуется кроме нее еще и другими «информационными системами», установленными в рамках одной и той же локальной вычислительной сети, то возникает закономерный вопрос об аттестации систем защиты информации каждой из них на одном и том же комплексе программно-технических средств. Т.е. система защиты будет одна и та же.

Объяснить и решить эти проблемы можно просто – данные системы не являются информационными системами (или тем более автоматизированными системами), чьи системы защиты информации нужно аттестовывать.

Необходима корректировка законодательства в области защиты информации, где аттестации будут подвергаться не системы защиты информации, а автоматизированные системы вместе с помещениями, в которых они располагаются, которые принадлежат одной организации и объединены общими функциональных задачами автоматизации.

Н.С.ЗАХАРЕВИЧ, Е.В.ШАКУН

АТТЕСТАЦИЯ. ОБСЛЕДОВАНИЕ РЕАЛИЗАЦИИ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ В РЕАЛЬНЫХ УСЛОВИЯХ ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ /ИНФОРМАЦИОННЫХ СИСТЕМ

В качестве исходной информации для обследования реализации функциональных требований используются следующие данные, приведенные в Задании по безопасности:

– перечень функциональных требований, а также их наименование и формулировка;

– перечень средств безопасности, а также их наименование и функции;

– таблица установления однозначного соответствия между функциональными требованиями безопасности и их реализующими средствами безопасности.

Кроме того, при обследовании используются подготовленные разработчиком следующие документы:

– методика тестирования объекта информатизации/ информационной системы;

– технический отчет о результатах тестирования объекта информатизации/ информационной системы.

На основе приведенных исходных данных составляется таблица обследования, описывающая процедуру обследования. Пример такой процедуры представлен в таблице 1. Перечень тестов, действия по тестированию и ожидаемые результаты тестирования определены в методике тестирования. Если для какого-то функционального требования методика не содержит нужного теста, то эксперт – специалист по тестированию определяет вид такого теста, формулирует действия по операции тестирования и прогнозирует ожидаемые результаты тестирования.

Таблица 1 – Пример процедуры обследования реализации функциональных требований

Функциональное требование безопасности (идентификатор, наименование, формулировка)	**Средство безопасности, реализующее обследуемое функциональное требование (идентификатор, наименование, функции)**	**Формулировка проверки**	**Наименование теста, реализующего данный вид проверки**	**Действия по операции тестирования**	**Ожидаемые результаты тестирования**	**Фактические результаты тестирования**
FAU_SAR.1 Просмотр данных аудита. Состав: FAU_SAR.1.1 КСБО должен обеспечить [назначение: авторизованным пользователям] возможность читать [назначение: список данных аудита] из записей данных аудита. FAU_SAR.1.2 КСБО должен представлять записи аудита в таком виде, чтобы пользователю было удобно интерпретировать информацию.	СБ «Аудит». Обеспечивает: – просмотр журнала регистрации событий.	Тестирование возможности просмотра данных аудита.	Test_FAU_SAR.1	Войти в систему в качестве главного администратора и попытаться просмотреть журнал аудита.	КСБО предоставляет возможность чтения журнала аудита в удобном виде.	

Примечание: В качестве главного администратора может выступать авторизованный пользователь, наделенный соответствующими правами.

Оценка результатов тестирования проводится с использованием показателя: **степень реализации требования безопасности**. Для данного показателя устанавливается лингвистическая и количественная шкалы оценок (таблица 2).

Экспертное заключение по степени реализации конкретного требования безопасности формулируется с использованием следующего правила принятия решений:

– если количественное значение степени реализации функционального требования лежит в интервале 1,0 – 0,5, что соответствует лингвистическим оценкам «Высокая степень реализации» и «Удовлетворительная степень реализации», то принимается решение: функциональное требование (наименование требования) реализовано средством безопасности (наименование средства безопасности);

– если количественное значение степени реализации функционального требования лежит в интервале 0,49 – 0,01, что соответствует лингвистическим оценкам «Степень реализации неполная» и «Требование не реализовано», то принимается одно из двух решений:

1) Заявитель в течение договорного срока аттестации устраняет выявленные недостатки, и Исполнитель проводит повторную аттестацию;

2) Заявитель не может обеспечить устранение выявленных недостатков в установленное время, то принимается решение о продолжении процедуры тестирования.

Таблица 2 – Соответствие между лингвистической и количественной шкалами оценок

Лингвистическая оценка степени реализации требований	Интервал количественной оценки
Высокая степень реализации	1,0-0,75
Удовлетворительная степень реализации	0,74-0,5
Степень реализации неполная	0,49-0,25
Требование не реализовано	0,24-0,01

После обследования реализации всего согласованного между Заявителем и Исполнителем перечня функциональных требований безопасности определяется обобщенная оценка степени реализации (таблица 3).

Таблица 3 – Обобщенная оценка степени реализации

Лингвистическая оценка степени реализации всего перечня требований	Интервал количественной оценки
Весь перечень требований реализован	1.0-0,75
Допущены незначительные отклонения в реализации отдельных незначительных по значимости требований	0,74-0,5
Допущены отклонения в реализации отдельных требований	0,49-0,25
Требования в полном объеме не реализованы	0,24-0,01

Экспертное заключение по степени реализации всего перечня требований безопасности формулируется с использованием следующего правила принятия решений:

– если количественное значение обобщенной количественной оценки лежит в интервале 1,0 – 0,5, что соответствует лингвистическим оценкам «Весь перечень требований реализован» и «Допущены незначительные отклонения в реализации отдельных незначительных по значимости требований», то принимается решение: функциональные требования реализованы;

– если количественное значение обобщенной количественной оценки лежит в интервале 0,49 – 0,01, что соответствует лингвистическим оценкам «Допущены отклонения в реализации отдельных требований» и «Требования в полном объеме не реализованы», то принимается одно из двух решений:

1) Заявитель в течение договорного срока аттестации устраняет выявленные недостатки, и Исполнитель проводит повторную аттестацию;

2) Заявитель не может обеспечить устранение выявленных недостатков в установленное время, то принимается решение об отказе в выдаче аттестата соответствия.

А.М.КАДАН

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ СИСТЕМ БИЗНЕС ИНТЕЛЛЕКТА

Масштабы внедрения компьютерных технологий в работу организаций, объемы накопленных данных, современные экономические условия породили рост потребности в получении качественной и достоверной аналитической информации, необходимой для принятия управленческих решений. Для многих компаний внедрения аналитических систем, известных как системы Бизнес Интеллекта (Business Intelligence, БИ), стали приоритетными и определяющими проектами, реализующими потребность в создании более совершенных систем управления и контроля, позволяющих не использовать локальные решения и обеспечивающих высокую эффективность бизнес-процессов.

К классу БИ относят системы, основанные на использовании технологий хранилищ данных, технологий многомерного представления данных и OLAP-технологий. Основная гипотеза их разработки и использования предполагает, что интеграция разнородных данных и новые формы их организации и представления позволят менеджерам и аналитикам не только получить новые знания о предметной области, не только предоставят возможность самостоятельно производить поиск и анализ информации, но и обеспечат выявление неочевидных закономерностей и фактов, которые не обнаруживаются стандартными методами классической статистики, искусственного интеллекта и машинного обучения.

Кроме того, использование таких систем способствует значительной экономии материальных, временных и трудовых ресурсов. Востребованность систем БИ подтверждается в последние годы стабильным ростом числа масштабных проектов. По данным DSS Consulting количество внедрений систем класса БИ в 2010 году в России выросло по сравнению с 2009 годом на 48%, что доказывает устойчивый рост потребности в бизнес-аналитике. Рынок белорусских систем БИ пока не имеет такой динамики роста.

При использовании систем БИ защита данных критически важна, так как практически вся информация, касающаяся работы предприятия находится в базах системы БИ, являясь критически важной для самого предприятии, его персонала и партнеров. Также очень важно обеспечить безопасность самой системы, защитив ее от вторжений и саботажа.

Авторы имеют почти десятилетний опыт разработки систем БИ и их компонентов. В рамках Региональной научно-технической программы Гродненской области была разработана автоматизированная система информационного обеспечения для сбора, хранения, защиты и анализа статистической информации для поддержки принятия решений органов местного управления (АСИО «Статистика») для которой задачи обеспечения безопасности выдвигались как первоочередные [1], начаты работы по созданию системы БИ университета [2]. Реализация всех указанных систем велась с использованием ОС Windows 2003, сервера баз данных MS SQL Server, служб MS Analysis Services, IIS различных версий.

Решения БИ опираются на четырехслойную архитектуру [2], которая включает:

1. слой источников операционных данных (транзакционные системы);
2. слой извлечения, преобразования и загрузки первичных баз данных;
3. слой хранилищ и витрин данных (data warehouse, data smart);
4. слой OLAP-инструментов и пользовательского интерфейса.

Технологии безопасности, лежащие в основе защиты системы, данных и организации защищенного обмена конфиденциальной информацией в системах БИ, можно традиционно разделить на шесть основных технологических групп и дать им краткую характеристику с учетом используемых программных средств:

идентификация и аутентификация – на основе имени и пароля с использованием: при соединении по TCP/IP технологий аутентификации Negotiate, Kerberos, NTLM, Anonimous User; при соединении по HTTP - методов аутентификации IIS (Internet Information

Services) – встроенная аутентификация Windows (Integrated Windows Autentification), Basic-аутентификация, анонимный доступ.

авторизация - процесс установления прав объекта (пользователь, группа пользователей, сервер, клиент) по отношению к ресурсам (системе в целом, файлам, принтерам, таблицам базы данных, кубам и витринам данных, элементам многомерной модели данных и т.п.). Основные механизмы авторизации: *Списки контроля доступа*, описывающие возможности манипулирования ресурсом; *Привилегии*, описывающие возможности пользователей отношении различных операций, например, запуск сервисов, удаленная регистрация в системе; *Разрешения* на создание, чтение, модификацию и удаление различных объектов Microsoft SQL Server;.

аудит – проводится с целью сбора информации о попытках доступа к объектам, применении привилегий и прочих, важных с точки зрения безопасности действиях и протоколирование этих событий для дальнейшего анализа. Поддерживаются следующие журналы аудита: журнал безопасности операционной системы, журнал Internet-сервера, журнал сервера баз данных, журнал OLAP-сервера.

конфиденциальность и целостность – являются взаимосвязанными группами. Обеспечение конфиденциальности данных помогает предотвратить их раскрытие и незаконную модификацию/удаление. Нарушение целостности может привести к принятию решений на основе недостоверной информации Обеспечение их реализуется использованием: протокола безопасных соединений (SSL); протокола защиты транспортного уровня (TLS); защищенного IP-протокола (IPS).

доступность - реализуется с помощью программных и аппаратных средств обеспечения отказоустойчивости (Failover hardware and software), встроенных в используемые в системе средства.

невозможность отрицания факта транзакции - обеспечивается средствами аутентификации, авторизации, аудита и целостности данных. Кроме того, доверитель извещается о том, что за действие, которое он собирается предпринять, он несет ответственность (юридическую).

При рассмотрении проблем безопасности системы БИ должны учитываться все перечисленные факторы и контекст, в котором будет применяться решение.

Из четырех указанных выше слоев архитектуры рассмотрим два последних, как непосредственно отражающие особенности систем БИ.

Обеспечение безопасности слоя хранилищ и витрин данных

Используемые в системах БИ стратегии безопасности данных базируются на стратегиях безопасности, реализованных в рамках Microsoft SQL Server, который выполняет роль защищенной платформы баз данных, обеспечивает безопасное хранение и обмен конфиденциальными данными. Предполагается работа SQL Server в интегрированном режиме, с использованием средств аутентификации ОС, реализованных через интерфейс SSPI на основе учетных записей диспетчера защиты Windows (Security Account Manager) или учетных данных Active Directory.

Помимо объектных (разрешения для объектов) и командных (разрешения для операторов) прав доступа, предполагается комбинирование различных компонентов SQL Server, чтобы упростить администрирование и улучшить систему безопасности:

– управление системой безопасности с помощью ролей. Члены одной группы получают одинаковые права доступа к объектам на основе ролей;

– использование представлений для обеспечения безопасности данных. Позволяет ограничить объем данных, доступ к отдельным строкам и столбцам таблиц, которые пользователь может просматривать и модифицировать;

– использование хранимых процедур для обеспечения безопасности данных. Позволяет сократить процесс выдачи прав доступа ко всем таблицам и представлениям, на которые есть ссылки в хранимой процедуре;

– использование триггеров для проверки данных. Применяется тип триггера, который следит за тем, кто выполнил последнее изменение в таблице и когда оно произошло.

Так как по умолчанию практически все данные, кроме идентификатора пользователя и пароля, передаются по сети в открытом виде, то сетевой трафик между клиентским компьютером и сервером должен шифроваться средствами протокола IPS. Шифрование трафика самого SQL Server'а осуществляется его встроенными механизмами. Шифрование входящего и исходящего трафика SQL Server обеспечивается средствами специализированных многопротокольных сетевых библиотек.

Обеспечение безопасности слоя OLAP-инструментов

Модель безопасности OLAP-сервера включает пять подсистем безопасности, взаимодействие которых обеспечивает безопасность всей системы: доступа к серверу (отвечает за аутентификацию и авторизацию, необходимые для определения набора прав пользователя); управления многомерной моделью (обеспечивает администрирование многомерной модели данных на уровне прав пользователя); доступа к данным многомерной модели (управление доступом на различных уровнях детализации); доступа к источникам данных (права доступа к внешним источникам данных (реляционным базам, файловой системе); выполнения кода пользователя.

Ограничение доступа к OLAP-серверу и конкретным базам данных и кубам этих баз основано на использовании ролевого механизма. Пользователи, выполняющие одинаковые функции, объединяются в роль. На уровне базы данных OLAP-сервера определяются роли администратора системы, администратора базы данных, пользователя.

Однако уровень безопасности куба совершенно недостаточен для практических целей баз данных OLAP, поэтому реализованы более детализированные уровни безопасности - на уровне измерений (с ограничением многомерного пространства) и на уровне ячейки куба (не ограничивая многомерное пространство). Возможен – неограниченный, полностью ограниченный и настраиваемый доступ к измерениям куба. Возможна настройка маршрута доступа к сечениям. Существует возможность предоставить доступ для чтения определенных уровней измерений. Например, можно установить параметры безопасности для роли руководителей подразделений, позволяющие просматривать данные персонала организации на их уровне и ниже.

Возможность ограничения прав доступа к индивидуальным элементам (ячейкам) куба очень важна для приложения OLAP. Концепция безопасности на уровне ячеек позволяет создавать кубы, содержащие все необходимые данные, а затем ограничивать доступ к ним на основе различных критериев. Параметры безопасности на уровне ячейки устанавливаются для роли на уровне куба, а не для роли на уровне базы данных.

Особого внимания требует работа с моделями интеллектуального анализа данных (ИАД). Чтобы аналитик мог использовать ИАД, он должен иметь административные разрешения на базу данных, в которой хранятся эти модели, а это позволяет изменять объекты, не связанные с ИАД. Одно из решений - создание отдельной базы данных, специально для работы с моделями ИАД или создание отдельных баз данных для каждого аналитика. Хотя для создания моделей ИАД обычно требуется максимальный уровень разрешений, доступом для осуществления других операций, таких как просмотр или выполнение запросов, можно управлять с помощью средств безопасности на основе ролей.

Кроме того, модели ИАД часто ссылаются на источники данных, содержащих конфиденциальные сведения, поэтому необходимы меры для скрытия таких сведений.

Литература

1. Кадан, А.М. Технологии Microsoft SQL Server решении задач хранения и анализа статистической информации региона / А.М. Кадан. - Информационные системы и технологии (IST-2006): Материалы III Междунар. конф. (Минск, 1-3 ноября 2006 г.): В 2 ч. Ч.1. – Мн.: БГУ, 2006. – С.81-85

2. Кадан, А.М. Информационно-технологические решения на основе Бизнес Интеллекта в сфере управления университетом / А.М. Кадан, Е.Н. Ливак. - Вестник ГрГУ, Серия 2, Математика. Физика. Информатика, вычислительная техника и управление. Биология.– Гродно: ГрГУ, 2010. - №2(96). – С. 123-131.

В.В.КИСЕЛЁВ, Л.В.ГОРОДЕЦКАЯ, Ю.И.КАРНИЦКИЙ

ЗАЩИТА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ИНФРАСТРУКТУР С ВНЕДРЕНИЕМ МУЛЬТИМОДАЛЬНЫХ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ ИДЕНТИФИКАЦИИ

1. Введение

Цель любой системы контроля доступа заключается в предоставлении лицам, имеющим соответствующие полномочия, возможность доступа в разрешенные для данных лиц зоны. Любая система контроля доступа основана на идентификации или аутентификации абонентов этой системы. Наиболее эффективно применение характерных свойств и признаков определенной личности, которые можно использовать для ее идентификации, путем применения биометрических систем.

Достоинства применения бесконтактных мультимодальных биометрических систем поиска

Большинство биометрических систем безопасности, применяемых в настоящее время, основаны только на одной уникальной поведенческой или физической характеристике человека, другими словами, для таких систем характерна унимодальность.

Основной целью применения биометрических технологий является создание механизма однозначной идентификации, использование только одной уникальной характеристики человека не позволяет с достаточной точностью осуществлять идентификацию личности.

В связи с этим становится очевидна необходимость комбинирования метода голосовой идентификации, как признака, характеризующегося дистанционным захватом биометрического материала, с подобными же технологиями. Поскольку другим бесконтактным методом биометрической идентификации является фотографическое изображение лица человека, он может быть выбран в качестве второго элемента бимодальной биометрической системы.

В связи с вышесказанным следует отметить следующие достоинства бесконтактных мультимодальных биометрических систем:

– Как в случае записи голоса, так и получения фотографии нет необходимости в физическом контакте с человеком;

– В результате комбинирования двух биометрических методов имеется большее количество идентификаторов, а значит система высокой достоверности;

– Низкие затраты при сборе голосового и графического материала, развертывании и эксплуатации системы;

– Обе биометрические технологии идеально приспособлены для работы на больших базах данных.

Выбирая в качестве идентификационных биометрических признаков записи голоса и фотографии лица человека в совокупности, удаётся получить очень высокие показатели точности, при этом сохраняя низкую стоимость получения образцов, объединённую с высочайшей скоростью поиска даже в базах данных национального масштаба.

Достоинства систем голосовой биометрии

Среди ключевых достоинств систем голосовой биометрии можно выделить следующие:

– Наличие огромного количества речевого материала в каналах связи.

– Бесконтактная и скрытая природа получения образцов речи.

– Низкая стоимость оборудования для сбора образцов.

– Высокая скорость поиска по архиву образцов речи.

– Возможность оперативного поиска в канале связи в реальном времени.

– Наличие богатого экспертного опыта и специализированных средств криминалистического исследования фонограмм речи.

2. Технология голосового биометрического поиска и идентификации

Процедура поиска интересующего диктора (идентификации) заключается в автоматическом попарном сравнении «голосовых моделей», в которых закодированы индивидуальные биометрические характеристики голоса и речи дикторов. По результатам сравнения выводится ранжированный список фонограмм, содержащих с указанной вероятностью речь интересующих дикторов.

Поиск осуществляется посредством трех биометрических методов идентификации по голосу с принятием обобщенного решения.

2.1. Порядок работы алгоритмов автоматической голосовой биометрии

2.1.1. Оценка качества речевого материала и автоматическая сегментация

На этапе ввода фонограммы в систему производится сегментация – процесс предварительной автоматической обработки звуковых файлов с целью отсечения непригодных неречевых фрагментов звукового сигнала.

2.1.2. Автоматическое разделение дикторов в фонограмме

Система автоматически обрабатывает двухканальные фонограммы, в которых один диктор записан в левом, а другой в правом канале, предоставляет возможность проведения разделения диалога на сегменты речи, принадлежащие разным дикторам посредством обработки их в звуковом редакторе, ориентированном на быструю и удобную сегментацию фонограмм речи.

2.1.3. Автоматическое выделение биометрических признаков голоса и речи

На основе автоматического исследования речи и голоса диктора выделяются биометрические признаки из речевого сигнала, и строится «Голосовая Модель» для каждой фонограммы каждого диктора с указанием внутридикторской и междикторской вариативности. Голосовые модели хранятся в базе данных (или временной папке) в соответствующем методу формате.

2.1.4. Поиск и идентификация

Для идентификации образца речи система автоматически попарно сравнивает «Голосовые Модели» посредством использования трех независимых биометрических методов (спектрально-формантный, основного тона, использование смесей гауссовых распределений). Сравнение «Голосовых Моделей» осуществляется для каждого из трех методов, затем на основе такого сравнения система принимает общее решение, вычисляя

единую метрику принятия решения. Суть его сводится к методу взвешенного голосования, где сходство двух фонограмм определяется по сложной композитной формуле.

По результатам сравнения выводится ранжированный список фонограмм, содержащих, с указанной степенью сходства, речь интересующих дикторов.

Кроме ранжирования результатов по убыванию, система также характеризует каждый найденный результат одним из четырёх цветовых маркеров. Такая классификация позволяет быстро отбирать результаты с необходимой вероятностью пропуска цели и ложной тревоги

2.1.5. Формирование отчета

Система предоставляет возможность формирования отчетов, различных по содержанию: от наиболее полного отчета со всеми статистическими данными по каждому методу до самого краткого отчета по первому диктору в списке похожих с пометкой «совпал», «похож» и «не похож».

Система предоставляет возможность визуализации результатов с помощью графиков двух типов (графики FR-FA и DET-график FR-FA), построенных по каждому биометрическому методу.

2.2. Параметры точности

Точность любой биометрической системы характеризуется вероятностями ложного принятия (ложной тревоги) и ложного отклонения (пропуска цели). Эти параметры всегда связаны, и соотношение их значений характеризует точность работы биометрического алгоритма.

FR – вероятность ложного отклонения

FA – вероятность ложного принятия

Порог принятия решения о сходстве или различии биометрических признаков в двух образцах устанавливается различным в зависимости от поставленной задачи.

Для установления личности методом биометрического поиска (идентификации) алгоритмы настраиваются на фиксированные значения FA и FR. Настройка на фиксированное значение FA обозначает ограничение размера списка подозреваемых до заданного количества процентов от всего списка принятых в рассмотрение образцов. Достигнутое при этом значение FA характеризует качество работы системы — чем оно меньше, тем меньше шансов пропустить цель, проанализировав полученный список. Ниже приведён пример типовой настройки фильтров принятия решений для задачи биометрического поиска по образцу речи:

1) Жёсткий фильтр - FA = 0,5%, FR = 2,51%

2) Средний фильтр - FA = 1%, FR = 2%

3) Мягкий фильтр - FA = 2,97%, FR = 1%

Для проверки, или верификации личности порог принятия решения настраивается таким образом, чтобы обеспечивать равные ошибки пропуска цели **FR** и ложного срабатывания **FA**. Данная величина ошибки называется **Equal Error Rate (EER)** – величина равновероятной ошибки.

2.3. Параметры быстродействия

Время поиска по «горячему списку» из 20000 образцов при 105 одновременных запросах	Не более 10 минут
Время поиска по базе из 600000 образцов при 16 одновременных запросах	Не более 45 минут
Количество сравнений за 10 минут, показанное на испытаниях	Более 3 млн.
Скорость добавления образцов речи в систему в пакетном режиме	До 15000 в час
Количество образцов голоса, проходящих полный цикл рабочего процесса в автоматическом режиме в сутки	Более 20000

При необходимости обработки потока входящих фонограмм, например, с систем перехвата, система может комплектоваться модулями, выполняющими запись речевого потока и голосовой поиск в реальном масштабе времени. Такое решение позволяет осуществлять идентификацию говорящего ещё до окончания звонка. Такая система может масштабироваться модулями по 60 каналов записи, что позволяет строить решения, контролирующие до нескольких тысяч телефонных линий.

2.4. Требования к фонограммам

– Формат звукового файла: ИКМ 16 бит RIFF WAV (и a-law для некоторых модулей системы);

– Минимальная необходимая для обеспечения заявленной надежности продолжительность речевого сигнала: 16 секунд;

– Система воспринимает на вход сигналы от 3 секунд длительности, но с пометкой о необходимости обратить внимание на результат, как не надежный;

– Частотный диапазон: 330-3400 Гц и лучше;

– Отношение сигнал/шум в частотном диапазоне 330-3400 Гц: не менее 10 дБ;

– Неравномерность АЧХ в частотном диапазоне 330-3400 Гц: не более 20 дБ.

3. Системы бимодальной бесконтактной биометрии

Линейка готовых продуктов, представлена следующими системами:

1) Система ***STC Grid ID-*** бесконтактная бимодальная биометрическая система, голосовая идентификация с идентификацией личности по фотографическому изображению лица.

2) Система ***VoiceGrid RT-*** аппаратно-программный комплекс, мониторинг и запись каналов связи в реальном времени, определение фонограмм, содержащих речь интересующих дикторов.

3) Система ***VoiceNet ID-*** автоматизированная система фоноучета и голосового поиска, предназначена для создания, ведения и автоматизации местных, региональных и национальных фоноучетов; оперативного установления личности подозреваемых и лиц, причастных к совершению правонарушений; криминалистического исследования фонограмм речи для последующего представления результатов в судебные органы.

Заключение

Среди ключевых достоинств систем голосовой биометрии можно выделить следующие. Наличие огромного количества речевого материала в каналах связи, возможность оперативного поиска в канале связи в реальном времени: подозреваемый может быть опознан ещё до окончания разговора, кроме того, его местоположение может быть эффективно локализовано в пространстве при помощи географической привязки канала связи.

Литература

1. М.Шредер «Computer Speech: Recognition, Compression, Synthesis» (Берлин, 1999 г.).

2. Г.Зубов, М.Хитров «Состояние и перспективы голосовой биометрии» (по итогам участия ЦРТ в Voice Biometrics Conference 2007.

3. Е.Маковский «Обман» биометрических систем доступа, использующих дактилоскопическую идентификацию личности., 2010.

4. Dan Miller «Voice Biometrics in Multifactor Authentication», 2011.

5. Dan Miller «Voice Biometrics Update 2011: Attacking Adjacent Markets».

6. Pierre Berlemont «La biométrie vocale fait parler d'elle» CNRS 2007.

Д.А.КОМЛИКОВ

ОПРЕДЕЛЕНИЕ КРИТЕРИЕВ ОТНЕСЕНИЯ ОБЪЕКТОВ К КРИТИЧЕСКИ ВАЖНЫМ С ИСПОЛЬЗОВАНИЕМ РОБАСТНОГО АЛГОРИТМА ОБРАБОТКИ ОЦЕНОК

Ограниченные ресурсы, которые государство может направить на защиту информации, требуют новых организационных решений и подходов в области информационной безопасности. Таким образом, приоритетной является задача выделения из всей совокупности объектов тех, которые по тем или иным условиям требуют специального, отличного от других подхода. Такие объекты будем считать критически важными объектами (КВО).

Характеризуя особенности обеспечения информационной безопасности (далее – ИБ) на КВО, необходимо учитывать следующие обстоятельства:

– основные принципы обеспечения ИБ КВО информационно-телекоммуникационной инфраструктуры (ИТИ) аналогичны принципам, применяемым для обычных объектов;

– государственный контроль за мерами обеспечения ИБ таких объектов должен осуществляться на всех уровнях управления.

При обеспечении безопасности ИТИ основное внимание следует уделить бесперебойному и устойчивому функционированию КВО с обеспечением доступности услуг и информации уполномоченным пользователям, а также целостности системы и информации, и при необходимости – конфиденциальности информации. Ресурсы и информация КВО могут защищаться в рамках правовых мероприятий, например, отнесение информации к государственным секретам, или организационно-технических мероприятий, обеспечивающих безопасность информации, циркулирующей в КВО. Вариантами организацион0-технических мероприятий, обеспечивающих безопасность информации, циркулирующей в КВО, могут рассматриваться режимы обеспечения: доступности и целостности информации; конфиденциальности и доступности информации; конфиденциальности и целостности информации; конфиденциальности, целостности и доступности информации.

Одним из подходов в отнесении объектов к критически важным, является метод учета остаточных рисков, использующий статистические оценки рисков на объекте [1]. Для этих оценок одним из важнейших параметров является их устойчивость, робастность.

Робастность в статистике предоставляет подходы, направленные на снижение влияния выбросов и других отклонений в исследуемой величине в отличие от моделей, используемых в классических методах статистики. На практике наличие в выборках даже небольшого числа резко выделяющихся наблюдений способно фатально повлиять на результат статистического исследования (примером может служить метод наименьших квадратов или метод максимального правдоподобия), и характеристики, получаемые в результате таких статистических исследований - не будут отражать фактическое отклонение исследуемой величины при проведении исследования. Для того чтобы избежать подобного, необходимо сформировать оптимальную модель, в которой необходимо максимально учесть влияние «плохих» наблюдений, либо вовсе исключить их.

Таким образом, очевидно, что, используя вышеописанные методы, можно повысить робастность оценок отнесения объектов к числу КВО, что существенно может уменьшить применение избыточного количества технических средств и объёма капитальных вложений при создании КВО.

Литература

1. Макаров О.С., Орлов А.В., Тепляков А.А. Формирование требований к нормативному регулированию параметров критически важных объектов. Управление защитой информации. Мн.: 2009.

2. Хампель Ф., Рончетти Э., Рауссеу П., Штаэль В. Робастность в статистике. Подход на основе функций влияния. = Robust statistics: the approach based on influence functions. — М.: Мир, 1989.

3. Хьюбер П. Робастность в статистике. — М.: Мир, 1984.

4. Кендалл М., Стьюарт А. Статистические выводы и связи. — М.: Наука, 1973.

В.Ю.ЛИПЕНЬ, Д.В.ЛИПЕНЬ, С.А.ШАВРОВ

ПРОЕКТ ВЕБ-СЕРВИСА «СОЗДАНИЕ И СЕТЕВАЯ ВЕРИФИКАЦИЯ БУМАЖНЫХ И ЭЛЕКТРОННЫХ ВЕРСИЙ ДОКУМЕНТОВ»

Базой для предлагаемого проекта, имеющего целью внедрение нового вида государственных информационных услуг с использованием ресурса Общереспубликанской автоматизированной информационной системы (ОАИС), являются результаты разработок ИТ-специалистов ОИПИ НАН Беларуси [1-4] и НИРУП «ИППС» в области сбора и обработки персональных данных и защиты документов. Внедрение подобного Веб-сервиса могло бы послужить целям реализации основных положений Национальной программы ускоренного развития услуг в сфере информационных технологий на период 2011-2015 годы. В первую очередь речь идет о пунктах программы, устанавливающих требования по опережающему развитию в Беларуси собственной информационной индустрии, обеспечивающей производство оригинальных технологий, ресурсов и услуг, в результате внедрения которых в республике должны быть достигнуты соответствующие современным требованиям качественные и количественные показатели использования ИКТ.

Назначение Веб-сервиса «Создание и сетевая верификация бумажных и электронных версий документов» заключается в предоставлении принципиально нового вида государственных информационных услуг, основанных на использовании оригинальных компьютерных технологий создания, доверенного хранения и удаленной сетевой верификации электронных и бумажных версий документов на протяжении их жизненного цикла. Потенциальными потребителями подобных услуг являются органы государственного управления и контроля, юридические и физические лица. Внедрение технологии Контроль обращения документов (КОД) призвано обеспечить улучшение качества документооборота и снижение потерь от экономических преступлений, включая и коррупционные. Подобные преступления в ряде случаев совершаются с использованием фальсифицированных (незаконно эмитированных) бумажных документов и паспортов (этикеток) товаров, являющихся, как правило, контрафактной или распространяемой без уплаты акцизных сборов продукцией. Недавний пример таких преступлений приведен в [5], где сообщается о раскрытии группы злоумышленников, изготавливавших на Борисовском предприятии Гознака неучтенные партии бланков строгой отчетности и товарных накладных.

Общим недостатком традиционных методов контроля бумажных документов является то, что установление подлинности предъявленного документа осуществляется человеком-контролером преимущественно путем анализа реквизитов документа, визуального контроля защитных элементов бланка (спецполиграфия, юниграммы, муаровые знаки и др.), а также оттисков печатей и мануальных подписей. При этом возможно проявление «человеческого фактора» – невнимательность, ошибки, недостаточная квалификация контролера или отсутствие в месте предъявления документа специальных приборов технической экспертизы,

сознательное игнорирование контролером подделок вследствие подкупа или шантажа со стороны предъявителя документа. Как правило, защищается бланк документа, а не его содержание (контент).

Новизна подхода авторов проекта к организации контроля обращения документов заключается в том, что достоверность предъявляемой к проверке бумажной версии документа, может быть установлена с использованием сетевого компьютера в любое время и в любом месте. При этом предполагается, что испытуемая бумажная версия документа была создана с использованием технологии КОД, о чем свидетельствуют специальная подпись и идентификационный маркер системы КОД, например, в виде специального штрихового кода (ШК). Предусматривается автономная и удаленная сетевая верификация криптографического идентификатора (КИ) документа, для чего осуществляется считывание ШК или клавиатурный ввод цифрового значения КИ. Для сетевой верификации КИ его цифровой эквивалент необходимо отправить на адрес Веб-сервиса. Достоверность предъявленного бумажного документа в полной мере может быть установлена путем сравнения его содержания с электронным оригиналом документа, который был принят средствами Веб-сервиса на доверенное хранение. В случае подтверждении проверяющим необходимого для этого уровня полномочий, ему может быть предоставлен сетевой доступ к электронной версии (оригиналу) документа. Комплекты цифровых идентификаторов, используемых для верификации бумажных и электронных версий документов в системе КОД, генерируются специальной криптографической программой по оригинальному алгоритму, который характеризуется высокими показателями защищенности [6,7].

Организациями, которые могли бы выдавать и принимать юридически значимые документы, созданные с использованием технологии КОД, могут быть исполкомы всех уровней, органы МВД и ЗАГС, суды и прокуратура, кадастровая и налоговая служба, санитарная и пожарная инспекция, таможенные органы, Госстандарт, Торгово-промышленная палата, Мингорисполком, нотариальные службы, предприятия оптовой и розничной торговли и др. Документами, которые в соответствии с технологией КОД на протяжение жизненного цикла существуют в виде маркированной бумажной копии и сохраняемого в репозитории электронного оригинала, могут являться служебные удостоверения, ID-карты граждан (включая несовершеннолетних), дипломы, документы ЗАГС, лицензии, сертификаты, технические паспорта, документы о владении собственностью, больничные листы, специальные разрешения, заключения экспертов, товарные накладные, этикетки и упаковки товаров, акцизные марки и др.

Для того, чтобы воспользоваться услугами Веб-сервиса, не требуется установка на компьютере потребителя дополнительного ПО. Специальные услуги по обеспечению компьютерного контент-анализа сохраняемых в репозитории электронных версий могут предоставляться службам государственного контроля, финансовых расследований и правоохранительным органам для целей контроля движения документов, встречных проверок субъектов коммерческой деятельности, предотвращения и раскрытия экономических и коррупционных преступлений. Функции системы подобны функциям эксплуатируемой в Беларуси системы финансового мониторинга, оперирующей с электронными банковскими переводами.

Внедряемые в ряде ведомств системы электронного документооборота (ЭДО) оперируют, как правило, со специальными электронными формами, которые удобны для компьютерной обработки, но могут существенно отличаться от документов традиционного вида, с которыми привык работать человек. Для получения заверенного с помощью электронной цифровой подписи (ЭЦП) электронного оригинала или создания внешней формы представления оригинала в виде заверенной бумажной копии необходимо, чтобы потребитель услуг (физическое или юридическое лицо) являлся субъектом системы ЭДО. Подобные заверенные копии субъекты ЭДО вынуждены изготавливать при взаимодействии с иными организациями, в которых не обрабатываются электронные документы. В отличие

от существующих ведомственных систем ЭДО, предлагаемый Веб-портал является легкодоступным ресурсом для всех сетевых абонентов, число которых с учетом бурного роста продаж мобильных смартфонов с беспроводным доступом к Интернет уже приближается в Беларуси к 4 млн.

Веб-сервис и сертифицированная система КОД могут выступить в качестве «третьей доверенной стороны» или «электронного нотариата» по отношению к территориально удаленным субъектам хозяйствования, оформляющим двусторонние договорные отношения. При этом договорные документы могут быть согласованы представителями организаций-контрагентов по сети без их личной встречи. Сохранение целостности электронного оригинала документа может быть обеспечено посредством его заверения с помощью ЭЦП контрагентов и/или администратора системы КОД. Перспективным для подобных транзакций является использование криптографических технологий «secret sharing». При этом возможно изготовление маркированных бумажных версий договора, заверяемых традиционным способом. В этом случае сертифицированный Веб-сервис будет гарантировать идентичность текстов заверенного электронного оригинала, принятого на доверенное хранение, и переданных в адреса контрагентов заданий на печать бумажных версий договора.

Ряд производителей высококачественной лицензируемой продукции, несущих значительные убытки от конкуренции на рынке с более дешевыми контрафактными товарами, могут воспользоваться услугой Веб-сервиса, заключающейся в формировании средствами системы КОД больших серий уникальных криптоидентификаторов для маркировки товаросопроводительных документов, справок об уплате акцизов, этикеток, первичных и вторичных упаковок товаров. Корректность и отсутствие тиражирования данных КИ может устанавливаться как автономно в месте контроля товара, так и в сети посредством отправки при каждой проверке значений считанных штрих-кода (RFID-меток) или клавиатурного ввода и отправки последовательности цифр уникального КИ на общедоступный адрес Веб-сервиса. Ответ формируется автоматически и возвращается абоненту мгновенно. Особенно полезен подобный способ быстрой сетевой верификации практически из любой точки торгового пространства для проверки достоверности сведений сертификатов о производителе и характеристиках дорогих или опасных лекарств, сложной техники и деталей (например, самолетов и автомобилей), дорогостоящих украшений, парфюмерии и алкоголя.

Аналогичным образом может подтверждаться факт уплаты государству акцизных сборов за подакцизную продукцию. Практикуемое в Беларуси подтверждение уплаты акцизов посредством наклеивания на каждый пакет или бутылку минеральной воды акцизных марок (юниграмм), суммарное количество которых исчисляется, вероятно, миллиардами, является примером разбазаривания народнохозяйственных ресурсов и невнимания к этой сфере отечественных ИТ-специалистов. Следует отметить, что достоверность наклеиваемых марок практически никто не проверяет, а партии товаров из соседних стран поставляются с уже наклеенными марками. Крайне неудачное внедрение в России гигантской системы ЕГАИС для компьютерного контроля производства и обращения алкогольной продукции с использованием ЭЦП, фиксируемых на этикетках в виде двумерных кодов, также не может служить для отечественных ИТ-специалистов примером для подражания. Более подробно эти проблемы освещены в публикации в газете «Республика» [8].

Разработка и экспериментальная апробация макета системы КОД, которая предлагается в качестве прототипа, осуществлялась в ОИПИ НАН Беларуси в 2005-2010 гг. в ходе выполнения НИОКР по заданию Инфотех-04. Положительная оценка результатов работ подтверждается протоколом межведомственной комиссии, содержащим рекомендацию к внедрению технологии КОД в виде одного из Веб-сервисов ОАИС. В настоящее время разработка продолжается в рамках ГПНИ «Информатика и космос». Макет Веб-портала,

который может послужить в качестве прототипа при реализации системы КОД в среде ОАИС, доступен по адресу [9]. Докладчиком демонстрируются страницы действующего Веб-портала и документы различных типов, созданные с использованием технологии КОД.

Литература

1. Липень В.Ю. Экспериментальная система «Контроль обращения документов / В.Ю.Липень [Д.В.Липень, Л.Н.Ловчева, Е.Н.Сбитнева, В.Ф.Тарасевич] // Развитие информатизации и государственной системы научно-технической информации: материалы VIII Междунар. конф. РИНТИ-2009 Беларусь, Минск, 16 ноября 2009 г. – Минск, 2009. – С. 81-85.
2. Абламейко, С.В. Защита электронных и бумажных документов в системах предоставления государственных информационных услуг / С.В. Абламейко, В.Ю. Липень // Управление информационными ресурсами: материалы V Междунар. науч.-практ. конф., Минск, 17 мая 2007 г. – Минск, 2007. – С. 267-280.
3. Липень В.Ю. Об использовании технологии «Штрих-код» для создания и верификации документов / В.Ю. Липень [и др.] // Комплексная защита информации: материалы XI Междунар. науч.-практ. конф., Новополоцк, Беларусь, 20-23 марта 2007 г. – Минск: Амалфея, 2007. – С. 153-156.
4. Липень, В.Ю. Криптографические процедуры создания и верификации идентификаторов документов и товаров / В.Ю. Липень // Технические средства защиты информации: материалы VI Бел.-росс. науч.-техн. конф., Минск, 21-22 мая 2008 г. / БГУИР. – Минск, 2008. – С. 20-21.
5. http://news.tut.by/148065.html
6. Берник, В.И. Метод создания и верификации криптографических идентификаторов и программный комплекс для его реализации / В.И. Берник, Н.И. Калоша, В.Ю. Липень // Комплексная защита информации: материалы 14-й Междунар. науч.-практ. конф., Могилев, 19-22 мая 2009 г. – Могилев, 2009. – С. 36-37.
7. Метод формирования и верификации уникальных криптографических идентификаторов / В.И.Берник [Н.И.Калоша, В.Ю.Липень, Д.В.Липень] // Технические средства защиты информации: материалы VII-ой Белорусско-рос. науч.-техн. конф., Минск, 23-24 июня 2009 г. / БГУИР – Минск, 2009. – С. 1.
8. http://www.respublika.info/4935/science/article37061/
9. http://e-vote.basnet.by/infotech

Д.А.КОСТЮК, С.С.ДЕРЕЧЕННИК

ПОСТРОЕНИЕ ПРОЗРАЧНЫХ ВИРТУАЛИЗОВАННЫХ ОКРУЖЕНИЙ ДЛЯ ИЗОЛЯЦИИ УЯЗВИМЫХ ПРОГРАММНЫХ СИСТЕМ

По статистике средний компьютер большую часть времени использует не более 5-7% своей вычислительной мощности. Современные системы виртуализации лишь незначительно увеличивают этот показатель, но взамен пользователь получает ощутимо более гибкую и удобную в управлении среду. Гостевая операционная система (ОС), запускаемая в виртуализованном окружении, абстрагирована от разнообразия компьютерных комплектующих и необходимых драйверов, менее подвержена внешним угрозам безопасности. Для нее становится доступным мгновенное восстановление от сбоев и нарушения работоспособности ПО благодаря механизму снимков (snapshots) виртуальной машины (ВМ), что позволяет не только возвращать систему к сохраненному состоянию, но и легко тиражировать готовое к использованию виртуализованное окружение [1, 2].

Понятие виртуализации рабочих станций (desktop virtualization) в настоящий момент используется в двух вариациях. В более распространенном случае ВМ с гостевой ОС запускается на сервере локальной сети, а рабочая станция играет роль удаленного терминала. Для используемых при таком подходе т.н. тонких клиентов характерны редуцированные аппаратные ресурсы и низкое энергопотребление. Во втором случае хост-система с ВМ и гостевой ОС устанавливается непосредственно на рабочую станцию, и пользователь имеет выбор, работать ли с хост-системой, или с гостевой.

Прозрачная виртуализация, в нашем понимании, предполагает только опосредованное взаимодействие пользователя с ВМ, скрывая разницу между запуском ОС на хост-системе и в гостевом окружении. Такое прозрачное взаимодействие характерно для виртуализации рабочих станций, построенной в рамках первого подхода. Однако на практике нередки ситуации, когда использование централизованного терминального сервера и тонких клиентов оказывается нецелесообразным [1]. Более характерна совместная работа в локальной сети стандартных офисных компьютеров. Хотя приемлемые готовые решения, предоставляющие для такой системы прозрачную виртуализацию, отсутствуют, она может быть сравнительно легко организована с применением ряда программных пакетов с открытым исходным кодом.

Рассмотренная задача решалась нами на примере виртуализации учебного класса университета для помещения ОС от Microsoft, программирование для которых входит в учебные программы ряда профильных специальностей, в изолированные окружения, с переносом функций аутентификации пользователей на более защищенную хост-систему. Изоляция гостевой ОС от внешней сетевой активности и делегирование задач аутентификации хост-системе позволяет решить следующие проблемы:

– упростить (либо вообще исключить необходимость) восстановления системы после некорректных действий пользователей либо активности вредоносного ПО;

– избавить рабочие станции от необходимости в антивирусном мониторе, требующем регулярных обновлений и периодически ощутимо снижающем производительность системы;

– затруднить ряд несанкционированных активностей, в первую очередь связанных с сетевым взаимодействием между рабочими станциями.

Персональные компьютеры типичного для вузов учебного класса подвергаются постоянной смене пользователей, эксплуатируются совместно с широким спектром прикладного программного обеспечения, часто страдают от неквалифицированных действий пользователей и их безответственного отношения к возможности распространения вредоносного программного кода. Таким образом, учебный класс оказывается подходящим полигоном для тестирования технологий защиты и автоматического восстановления программного обеспечения в среде со сложной и динамичной картой распределения неблагоприятных факторов [3].

Особенности типичного офисного оборудования (в первую очередь отсутствие аппаратной поддержки виртуализации в дешевых процессорах) оставляет систему виртуализации Oracle VirtualBox в качестве единственного решения приемлемой производительности, не требующего оплаты лицензий и обладающего открытым исходным кодом (нами использована полностью открытая версия системы без проприетарных модулей расширения SUN/Oracle). По аналогичной причине в качестве хост-системы выбрана ОС GNU/Linux. Если возможность бесплатного использования выбранного ПО актуальна для вузов, то доступ к исходным кодам с возможностью их аудита может оказаться важным фактором для потребителя, нуждающегося в изоляции уязвимых систем средствами заведомо безопасного (свободного от оставленных производителем брешей в защите) программного решения.

Изначально проект VirtualBox не предусматривает многопользовательской работы с отдельной ВМ. Однако перенос ее конфигурации из домашнего каталога пользователя в общедоступную область и помещение ссылки на него в шаблон домашних каталогов

обеспечивает раздельный доступ к ВМ нескольких пользователей, обладающих соответствующими правами доступа. При необходимости ограничить доступ к администрированию ВМ для запуска гостевой ОС может применяться упрощенный полноэкранный интерфейс, а доступ к основному интерфейсу ограничивается на уровне прав пользователей.

Сеть гостевой системы VirtualBox, по умолчанию, настроена в режиме трансляции адресов, и ВМ не имеет реального сетевого адреса. Результатом является недоступность гостевой ОС извне при сохранении комфортного доступа из нее к сетевым сервисам – в точности так же, как это происходит с рабочими станциями локальной сети, имеющими только локальные сетевые адреса и соединяющимися с внешней сетью proxy-сервером. Данный режим является предпочтительным, т.к. ограничивает нежелательные сетевые взаимодействия для вирусов и возможного шпионского ПО. Однако если сетевое взаимодействие необходимо (например, в учебных целях), режим может быть изменен с выделением ВМ внешних сетевых адресов – ценой незначительного роста вычислительной нагрузки и снижения защищенности гостевой ОС [1].

Для упрощения администрирования компьютерного парка и с учетом отсутствия закрепления рабочей станции за конкретным пользователем в учебном классе, в сети организован сервер аутентификации, хранящий дерево учетных записей пользователей и предоставляющий к нему доступ средствами OpenLDAP. Хост-системы рабочих станций, работающие под управлением дистрибутива GNU/Linux, получают доступ к учетным записям и персональным файлам пользователя на файл-серверах сети с помощью стандартных модулей системы аутентификации Linux. При этом рабочие станции различаются только IP-адресом, выделяемым им сервером с привязкой к MAC-адресам сетевых адаптеров, и имеют идентичный дисковый образ, не требующий модификации, что выгодно отличается от невиртуализованного решения с ОС от Microsoft, работающей под управлением контроллера домена [3]. Каталоги файл-сервера однотипно монтируются в файловую систему рабочей станции как при входе пользователя в гостевое окружение, так и при входе в графическую оболочку на хост-системе. В качестве последней используется окружение рабочего стола GNOME, поэтому входом пользователя управляет менеджер сеансов GDM. Для обеспечения прозрачности доступа к виртуализованному окружению, запуск нужной ВМ включен в список доступных графических оболочек на хост-системе и выбирается пользователем при вводе логина и пароля в менеджере сеансов GDM. Так как современные версии GDM сохраняют информацию о предпочитаемом менеджере сеанса для каждого пользователя, выбор гостевой ОС в списке производится только при первом входе или при необходимости изменить предпочтения.

Доступ гостевой ОС к автоматически монтируемым ресурсам файл-сервера осуществляется через механизм разделяемых папок (shared folders) VirtualBox, позволяющий получить доступ из гостевой системы к заданному каталогу хост-системы.

Таким образом, гостевая система работает в однопользовательском режиме, автоматически монтируя при запуске каталоги хост-системы, уже отображающие необходимые для конкретного пользователя сетевые ресурсы. Монтируемые каталоги хост-системы сами являются подмонтированными файловыми системами, поэтому их подключение в качестве «сетевых» ресурсов гостевой ОС возможно только при уже запущенной ВМ. В качестве менеджера сеанса запускается несложный скрипт, в свою очередь запускающий ВМ (в полноэкранном режиме), подключающий необходимые точки монтирования и ожидающий завершения ее работы.

Дисковый образ гостевой ОС при завершении сеанса работы автоматически откатывается к исходному состоянию (фиксация дискового образа выполняется функцией «immutable disk image» VirtualBox). Гостевое окружение благодаря этому становится «неповреждаемым», что позволяет безопасно работать в нем с правами администратора.

При необходимости автоматизировать передачу USB-накопителей в гостевое окружение, проброс может автоматически выполняться VirtualBox, для чего необходимо создание соответствующего фильтра устройств в настройках. Фильтрация USB-устройств позволяет в ряде случаев обеспечить дополнительную безопасность гостевой системы: например, может быть разрешен только проброс аппаратных ключей защиты, с игнорированием накопителей и других устройств, подсоединяемых к USB-разъемам.

Таким образом, процесс подготовки рабочей станций состоит из ряда этапов, требующих ознакомления с технической документацией, редактирования конфигурационных файлов и создания несложных скриптов. Дополнительно предполагается наличие как минимум одного сервера аутентификации, а также файл-сервера с личными каталогами пользователей и, вероятно, интегрированным антивирусом ClamAV. Однако результатом является универсальный, тиражируемый без дополнительных настроек дисковый образ, рассчитанный на запуск как минимум двух ОС и изолирующий более уязвимую (менее надежную) из двух систем. Получаемое гостевое окружение не требует от пользователя непосредственного взаимодействия с дополнительным системным ПО, и при этом приобретает достоинства, нехарактерные для ОС семейства Windows. В первую очередь, это полная устойчивость к выполнению вредоносных воздействий при сохранении полного доступа пользователей к функциям администрирования. Кроме того, в гостевом окружении ОС Windows получает, по сравнению с установкой непосредственно на хост-систему, повышенные производительность и скорость реакции. Последнее обеспечивается как эффективностью файлового кэширования GNU/Linux, так и косвенными факторами: отсутствием влияния антивирусного монитора и постоянным сохранением высокой скорости реакции, характерной для только что установленных версий Windows.

Литература

1. Д. Костюк, А. Приступчик. Особенности прозрачной виртуализации небезопасных и уязвимых систем для упрощенного администрирования учебных классов // Свободное программное обеспечение в высшей школе: тезисы докладов 6-й конференции (Переславль-Залесский, 29–30 января 2011 г.). – М.: Институт логики, 2011. – С. 66– 68.

2. П.С. Пойта, В.И. Драган, А.П. Дунец, Д.А. Костюк, В.И. Хведчук, С.С. Дереченник. Подход к модернизации гетерогенной сетевой инфраструктуры на примере информационно-вычислительной сети университета // Вестник БрГТУ. – 2010. – №5: Физика, математика, информатика. – С. 75–78.

3. Д.А. Костюк, Р.В. Сченснович. Использование в образовательном процессе вычислительных сетей на базе Windows Server 2008 // Информационные технологии в образовании: материалы Международной научно-практической конференции (Минск, 21–22 мая 2009). – Мн.: БНТУ, 2009. – С. 109–113.

А.М. КРИШТОФИК, В.В. АНИЩЕНКО

СОЗДАНИЕ И ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОГО ВЫСОКОПРОИЗВОДИТЕЛЬНОГО ПРОСТРАНСТВА (КИБЕРИНФРАСТРУКТУРЫ) СОЮЗНОГО ГОСУДАРСТВА

Необходимым условием функционирования экономики современного развитого государства, избравшего путь построения экономики, основанной на знаниях, является национальная информационная вычислительная инфраструктура (часто используют термин «киберинфраструктура»), которая базируется на наборе технологий, в котором господствующие позиции занимают высокопроизводительные вычислительные средства

(суперкомпьютеры) и телекоммуникационные технологии, а также программные средства эффективного использования киберинфраструктуры. Эти технологии являются критическими и системообразующими, имеют стратегический и фундаментальный характер. Киберинфраструктура, или электронная инфраструктура науки (рис. 1.) используется научным мировым сообществом как технологическая платформа для развития различных отраслей науки и создания технологических основ для разработки наукоемких технологий с последующим их внедрением в различные отрасли экономики. Киберинфраструктура является инновационной электронной инфраструктурой для конкурентоспособного развития экономики страны.

Возможность создания и использования киберинфраструктуры во всем мире относится к факторам стратегического потенциала оборонного, научно-технического и экономического значения, ибо прогресс любой развитой страны в современном мире невозможен без компьютеризации во всех сферах деятельности. При этом все более проявляется связь между достижениями страны в области создания и овладения передовыми компьютерными технологиями и ее потенциальными возможностями решать ключевые проблемы научно-технического прогресса. Особенно это проявляется в отношении решения научных фундаментальных и прикладных проблем.

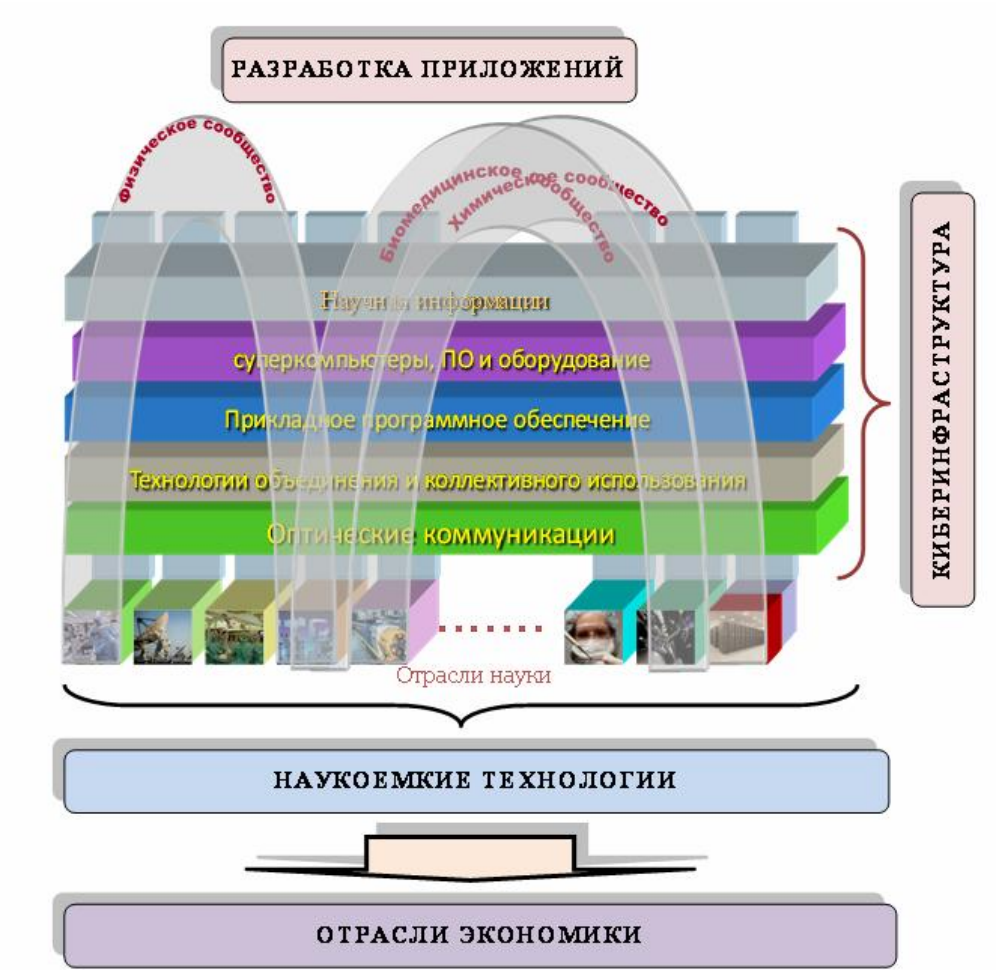


Рис. 1. Содержание киберинфраструктуры и результаты ее использования

Администрации США при президентах Буше и Обаме неоднократно обозначали развитие суперкомпьютеров национальным приоритетом на самом высшем уровне:

– в 2004 году был принять специальный план по дополнительному ускорению развития высокопроизводительных вычислений;

– в 2006 году суперкомпьютеры, наряду с нанотехнологиями и альтернативными источниками энергии были указаны в качестве приоритета в обращении Дж. Буша к конгрессу США;

– создание компьютера производительностью в 1 экзафлоп (1 000 000 000 000 000 000 операций в секунду) объявлено одним из «великих вызовов 21 века» в «Стратегии американских инноваций» экономического совета при президенте США;

– развитие технологий суперЭВМ также объявлено приоритетом в области информационно-телекоммуникационных технологий в том же документе.

Европейский Союз (ЕС) также проводит целенаправленную политику по развитию суперкомпьютерного направления:

– в 2008 году сформирована инициатива PRACE, направленная на создание сети суперкомпьютеров петафлопного уровня производительности в странах ЕС;

– в рамках 6 и 7 рамочных программ финансируется проект распределенной европейской инфраструктуры для суперкомпьютерных приложений – «Distributed European Infrastructure for Supercomputing Applications (DEISA)».

В результате реализации политики, обозначенной на самом высшем уровне, развитие высокопроизводительных систем в США и Объединенной Европе происходит форсированными темпами.

Происходит экспоненциальный рост возможностей вычислительной техники. За 15 лет производительность суперкомпьютерных установок увеличилась в 11 тыс. раз, а суммарная производительность – в 22 тыс.).

Помимо экспоненциального роста производительности, прогресс микроэлектроники приводит к постоянному росту объема данных, получаемых либо за счет более совершенных научных приборов, средств наблюдения, средств коммуникации и более детализированных математических моделей. Вследствие высоких достижений в вычислении, хранении данных, и коммуникаций, информационные технологии на пороге достижения уровня Peta (10^{15}) - объемов памяти, скорости связи и быстродействия вычислений (уже достигнуто). Несколько лабораторий Министерства энергетики США (DOE) создали системы хранения, рассчитанные на петабайты, и существуют некоторые научные базы данных, которые превысили размер в один петабайт.

Закон Мура предсказывает удваивание плотности элементов на кристалле каждые 18 месяцев. Эндрю Одлизко и Керри Коффман доказали, что это не так. Они продемонстрировали, что удваивание происходит каждые 12 месяцев. Закон Джилдера предсказывает, что полная емкость оптических транспортных систем удваивается каждые шесть месяцев, что предъявляет повышенные требования к системам хранения и каналам передачи данных.

Так, например, современные научные приборы такие как Большой Адронный Коллайдер, Австралийский Радиотелескоп или Гавайский панорамный телескоп создают объемы данных от 1 петабайта (10^{15} байт) в год.

Большие объемы данных генерируются в науках о жизни – секвенирование геномов отдельных организмов в настоящее время не представляет существенных трудностей, и соответствующие базы данных испытывают экспоненциальный рост. Например, приборы Тихоокеанской Северо-западной национальной лаборатории США могут генерировать до 480 гигабайт данных в день.

Большие объемы данных (до сотен петабайт), как ожидается, будут накапливаться и анализироваться в центрах дистанционного зондирования Земли. На рисунке 2 приведен ожидаемый рост объемов хранения данных в центре спутниковых данных по окружающей среде национальной службы мониторинга океана и атмосферы США (NESDIS NOAA) - лишь один из примеров.

Все большим объемом данных оперируют при создании прогнозов погоды и в исследованиях климата. Например, Немецкая национальная метеорологическая служба генерирует более 2,5 петабайт данных каждый год.

Данные «транспетабайтного» объема накапливаются и в коммерческом секторе, например, в системах обработки транзакций больших компаний. Анализ таких данных может дать конкурентное преимущество за счет более эффективной организации бизнес-процессов.

Ответом на рост объемов данных является с одной стороны - наращивание мощностей хранения, создание специализированных решений для хранения больших объемов информации, а с другой – неуклонное расширение пропускной способности каналов связи, использование более совершенных технологий объединения отдельных хранилищ данных и мощных суперЭВМ в единую киберинфраструктуру (проекты Open Science Grid, TeraGrid, National Lambda Rail и другие).

Важно отметить, что в ряде случаев желаемый результат без масштабных вычислений не достижим в принципе (например: перспективные наноматериалы, микроэлектроника, новейшие лекарства, расшифровка генома и т. п.) Будущие технологии и открытия напрямую зависят от используемых вычислительных ресурсов. Так, заместитель министра энергетики США Рэймонд Орбах отметил, что суперкомпьютер *"позволит ученым моделировать физические процессы, об изучении которых прежде не было и речи"*, а также назвал *"развитие суперкомпьютерной техники, наряду с проведением экспериментов и разработкой теорий, одним из ключевых факторов для научных открытий"*.

Информационно- вычислительное высокопроизводительное пространство (киберинфраструктура) Союзного государства – это совокупность суперкомпьютерных центров, систем хранения данных, систем связи и технологий, обеспечивающих предоставление ресурсов пользователям и приложениям и их эффективное использование, реализующих функции глобальных вычислений; Сервисные технологии для глобальных вычислений являются логическим продолжением и развитием грид-технологий.

Создание базовой киберинфраструктуры Союзного государства обеспечит:

– ускоренное развитие средств математического моделирования в прикладных и фундаментальных научных исследованиях, достижение мирового уровня исследований и разработок;

– широкое развитие наукоемких технологий во всех сферах экономики;

– уменьшение потребления электроэнергии и, как следствие, уменьшение затрат на содержание вычислительных ресурсов;

– снижение стоимости эксплуатации;

– увеличение эффективного использования ресурсов за счет уменьшения времени их простоя;

– увеличение эффективного использования ресурсов за счет снижения порога доступности и упрощения технологий доступа;

– увеличение эффективного использования дорогого программного обеспечения;

– снижение совокупной стоимости владения.

Таким образом**,** киберинфраструктура, является ключевым элементом в обеспечении технологической безопасности стран участниц Союзного государства, способствует решению приоритетных задач модернизации экономики в части развития наукоемких, конкурентоспособных технологий.

Э.П.КРЮКОВА

СОВРЕМЕННЫЕ ПОДХОДЫ К КЛАССИФИКАЦИИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ПО УРОВНЮ БЕЗОПАСНОСТИ

Объекты информатизации (ОИ) представляют собой автоматизированные системы, устройства, компоненты различной степени сложности и назначения, реализованные на основе электронно-вычислительной техники и информационных технологий, обеспечивающие важнейшие функции управления основными процессами объектов инфраструктур. В современных условиях информационного противоборства критически важные ОИ (КВОИ), являющиеся основой управления объектами инфраструктур, жизненно важных для жизнедеятельности государства, общества, граждан, являются наиболее вероятными целями атак различного рода.

Причины этих атак исходят из стратегической и оперативной важности КВОИ. Помимо угроз, следующих из планируемых действий, небрежность персонала, ошибки аппаратных средств, программного обеспечения и форс-мажор также угрожают их безопасности. Обеспечение безопасности КВОИ требует организации их защиты, адекватной их важности для функционирования объекта инфраструктуры.

Можно выделить два основных вида компьютерных систем, которые могут рассматриваться как КВОИ: информационные системы и управляющие системы.

Критически важные информационные системы обеспечивают сбор, обработку и предоставление информации в удобном для человека виде. Основная роль принадлежит человеку, а компьютер играет вспомогательную роль, выдавая ему необходимую информацию.

Критически важные управляющие системы обеспечивают наряду со сбором информации ее обработку по специальным алгоритмам и выдачу команд непосредственно исполнителям или исполнительным механизмам. Управляющие системы работают обычно в реальном масштабе времени, т.е. в темпе технологических или производственных операций. Важнейшая роль принадлежит машине, а человек контролирует и решает наиболее сложные вопросы, которые по тем или иным причинам не могут решить вычислительные средства системы.

Существующая система категорирования информационных систем по важности относится к категорированию систем организационного типа, используемых или эксплуатируемых органами государственной власти, организациями, работающими по контракту с государственными органами, или им подчиненными [1]. Информационная безопасность (ИБ) рассматривается через обеспечение задач безопасности – конфиденциальности, целостности, доступности.

Категория важности информации связывается и с информацией пользователя, и с системной и может быть применима к информации в электронной и в неэлектронной форме. Установление соответствующей категории безопасности для каждого вида информации по существу требует определения потенциального влияния невыполнения каждой задачи безопасности, связанной с использованием информации конкретного вида, на организацию или отдельных лиц:

низкая (Low) – требования по обеспечению всех задач безопасности низкие;

умеренная (Moderate) – требования по обеспечению хотя бы одной задачи безопасности оцениваются как умеренные и ни одна задача безопасности не превышает уровень «умеренная»;

высокая (High) – требования по обеспечению хотя бы одной задачи безопасности оцениваются как высокие.

Ущерб при нарушении этих задач ИБ оценивается степенью нарушения деятельности организации, экономическими потерями, стоимостью потерянных активов или прибыли,

ущербом здоровью людей, репутации владельца организации и др. Конкретное содержание показателей ущерба для отнесения ОИ к критически важным может устанавливаться актами информационного законодательства или владельцами информации или системы.

Широкое применение компьютерной техники в автоматизации процессов управлении важными производственными процессами, необходимость оценки их безопасности требует более четкого подхода к классификации ОИ, учитывающего особенности их функционирования в реальных условиях эксплуатации.

Она требует сочетания детерминированного и вероятностного подходов к оценке важности функциональности ОИ для выполнения основных процессов, которая применяется ко всем системам, устройствам, компонентам, автоматизирующим функции объекта инфраструктуры на основе электронной вычислительной техники [2], [3].

Детерминированный подход требует подробного анализа функций объекта управления, осуществляемых ОИ (включая операции персонала, средств технического обслуживания, оборудования и др.), оценки их влияния на миссию объекта инфраструктуры и возможные последствия отказа ОИ.

Вероятностный подход требует оценки риска, т.е. анализа уязвимости ресурсов КВОИ, выделения актуальных угроз уязвимым ресурсам, определения вероятности отказов функций, реализуемых этими ресурсами, анализа надежности функционирования КВОИ с учетом качества его разработки, изготовления и контроля до поставки (при контроле, сборе, испытаниях) и оценки надежности в эксплуатации [4].

Конкретное содержание показателей ущерба для отнесения ОИ к критически важным может устанавливаться актами законодательства или владельцами объектов инфраструктуры. При оценке тяжести последствий отказов должны приниматься во внимание частичные отказы, влияние отказов КВОИ на другие системы и другие аспекты.

Риск нарушения безопасности оценивается произведением вероятности отказа системы на размер средневзвешенного ущерба объекту инфраструктуры по причине этого отказа. Классификация КВОИ по безопасности с применением описанных выше подходов осуществляется по схеме:

а) исходя из важности основных процессов и/или функций объекта инфраструктуры, определяется категория важности ОИ, который реализует функции или управление ими: высокая, средняя, низкая;

б) исходя из оценки последствий отказа, снижения качества выполнения функций или разрушения ОИ, определяются последствия отказа ОИ (тяжесть ущерба для объекта инфраструктуры): высокая, средняя, низкая;

в) с учетом тяжести ущерба и вероятности отказа ОИ определяется риск невыполнения важных функций и процессов объекта инфраструктуры;

г) исходя из категории важности ОИ и уровня риска, осуществляется отнесение ОИ к соответствующему классу безопасности в соответствии с таблицей 1.

Таблица 1– Классификация КВОИ по уровню безопасности

Вероятность отказа	**Ущерб**		
	высокий	**умеренный**	**низкий**
	Класс безопасности (уровень риска)*		
высокая	**G** максимальный	**H** высокий	**M** средний
средняя	**H** высокий	**M** средний	**L** низкий
низкая	**M** средний	**L** низкий	**базовый уровень**

Требования класса G соответствуют максимальным требованиям безопасности, класса L – самому низкому уровню ИБ. Исходным для назначения требований ИБ является базовый состав требований, который обязателен для КВОИ всех классов (базовый уровень). Каждому классу КВОИ соответствуют специальные требования, дополняющие требования базового уровня.

Для назначения требований КВОИ в зависимости от уровня безопасности используются основные характеристики КВОИ различных уровней безопасности [5] и основные требования безопасности [3].

Базовый уровень. Требования базового уровня безопасности устанавливаются для КВОИ, которые характеризуются незначительным уровнем риска. Требования безопасности для них не являются жесткими: отказ в доступе может составлять несколько десятков часов в год, степень конфиденциальности сведений не высока. Примерами таких систем являются практически все системы, где не требуется высокая оперативность выполнения функций.

Правила обеспечения режима ИБ в подобных случаях обычно обеспечивается совокупностью проверенных практикой правил обеспечения ИБ на всех этапах жизненного цикла КВОИ (концепция базового уровня). Эти правила должны носить комплексный характер, то- есть охватывать административный, процедурный, программно - технический уровни.

Для обеспечения **базового уровня** ИБ КВОИ должны выполняться следующие требования:

для каждого уровня устанавливаются политика безопасности и правила эксплуатации;

процедуры управления ИБ должны быть разработаны для всех пользователей и изучены всеми пользователями;

пользователи должны получать доступ только к тем функциям компьютерной системы, которые им необходимы в соответствии с полномочиями;

должен быть обеспечен соответствующий контроль доступа и установление подлинности пользователей;

персонал, которому разрешается доступ к компьютерной системе, должен иметь соответствующую квалификацию и опыт работы;

должна поддерживаться система или процедура мониторинга злоумышленной деятельности;

где возможно, должны применяться средства обнаружения и обработка вредоносного программного обеспечения (ПО);

должно проводиться управление обновлениями ПО (периодичность и выбор заплат зависят от рассматриваемых систем и зоны);

где возможно, необходимо существенно усилить системы информационно-телекоммуникационных технологий;

должны быть обеспечены регистрация и мониторинг действий на компьютерной системе;

сменные носители информации должны контролироваться в соответствии с процедурами управления безопасностью;

должны быть обеспечены строгая регистрация и мониторинг средств безопасности (например, межсетевых экранов, систем обнаружения вторжения, систем защиты информации, серверов VPN и т.д.);

по возможности, использовать сервера систем обнаружения вторжения на основе хостов и межсетевых экранов;

должны быть в наличии соответствующие процедуры обеспечения непрерывности процессов, включая процедуры резервирования и/или восстановления;

физическая защита должна обеспечиваться в соответствии с особенностями применяемой компьютерной системы, маршрутизаторов, кабелей, терминалов и др.;

при проектировании компьютерной системы должна рассматриваться необходимость физической защиты и применяться принцип глубоко эшелонированной обороны («defence-in-depth»).

Класс L (низкий уровень ИБ). Основные характеристики:

обеспечение конфиденциальности информации не требуется;

ошибки могут быть допущены, если они не срывают выполнение задач;

не допустим долговременный отказ в доступе к системе, однако допустимы умеренные периоды простоя (надежность $0,75>P\geq 0, 50$).

Обобщенный критерий: нарушение безопасности КВОИ вызывает незначительный ущерб объекту инфраструктуры, но существенно ухудшает качество информационного обслуживания или условия жизнедеятельности субъектов.

Для обеспечения ИБ КВОИ класса L дополнительно к требованиям базового уровня должны выполняться следующие основные требования:

разрешение на модификацию системы дается только квалифицированным пользователям, имеющим соответствующие полномочия;

доступ пользователей к сети Интернет должен осуществляться с использованием обычных мер защиты, соответствующих действующим отраслевым стандартам;

межсетевые экраны должны базироваться на новейших технологиях и строго поддерживаться в работоспособном состоянии;

должны использоваться и строго поддерживаться в работоспособном состоянии системы обнаружения вторжения в сеть и системы защиты информации;

обнаружение и обработка вредоносного ПО должна базироваться на новейшей технологии и/или сигнатурах;

заплаты для приложений и операционных систем должны применяться регулярно и своевременно;

удаленный внешний доступ должен разрешаться только авторизованным пользователям с использованием технологий строгой аутентификации, при условии, что удаленный компьютер и пользователь полностью соблюдают разработанную политику безопасности и следующие из нее технические требования (применение современной антивирусной защиты, защиты от вредоносных программ, версий заплат, принципов персонального межсетевого экрана и др.);

должно периодически проводиться тестирование на проникновение в компьютерные системы и сети.

Класс M (средний уровень ИБ**)**. Основные характеристики:

гарантируется защита важной информации, предназначенной для использования только внутри учреждения;

допустимы незначительные ошибки;

ошибки, которые существенно нарушают выполнение задач, должны быть обнаружены и устранены;

время простоя не должно превышать заданные пределы (надежность $0,80>P\geq 0,75$).

Обобщенный критерий: при нарушении безопасности КВОИ имеет место срыв функционирования объекта инфраструктуры.

Для обеспечения ИБ КВОИ класса M дополнительно к требованиям базового уровня должны выполняться следующие основные требования:

между соседними зонами безопасности должны применяться хорошо поддерживаемые и настроенные межсетевые экраны, защищающие от вхождения команд от систем более низкого класса;

подключения (из зон систем класса L и базового) к сетям передачи данных класса M разрешаются, но они должны быть защищены современными техническими средствами, гарантирующими высокую целостность данных;

поток данных разрешается только между системами внутри зоны и к системам классов L и базового;

все интерфейсы и подключения к компьютерам должны строго контролироваться во избежание несанкционированного вмешательства;

удаленный доступ для обслуживания разрешается в зависимости от обстоятельств и при условии, что он жестко контролируется;

должны использоваться технологии сильной аутентификации аналогичные технологиям класса L;

удаленная система и пользователь должны соблюдать определенную политику безопасности (в соответствии с контрактом) и вытекающие из нее технические требования (например, применение современной антивирусной защиты, защиты от вредоносных программ, версий заплат, правил персонального межсетевого экрана и др.);

функции системы, доступные пользователям, должны контролироваться с учетом иерархии полномочий посредством паролей или более сильных механизмов логического контроля доступа. Любое отступление от этого принципа должно быть тщательно исследовано, а защита обеспечена другими средствами (например, ограничением физического доступа);

со всей должной осторожностью должны периодически проводиться испытания на проникновение, касающиеся проверки доступности и целостности тестируемых систем (некоторые системы могут не тестироваться, если они высоко критичны).

Класс H (высокий уровень ИБ). Основные характеристики:

защита критичной информации должна соответствовать требованиям законодательства и быть повышенной в важных областях;

обрабатываемая информация должна быть точной, любые ошибки должны быть обнаружены и исправлены;

на процессы, действующие в пределах жесткой временной шкалы, приходятся основные области деятельности;

широкомасштабные задачи объекта инфраструктуры выполняются только с применением ИТ;

разрешаются только короткие периоды простоя (надежность $0{,}93 > P \geq 0{,}87$).

Обобщенный критерий: при нарушении безопасности АС объект инфраструктуры не может выполнять необходимый объем функций для поддержки основных процессов. Результат – значительное нарушение функций собственно объекта и третьих сторон.

Для обеспечения ИБ КВОИ класса H дополнительно к требованиям базового уровня должны выполняться следующие основные требования:

разрешается односторонний поток данных, направленный от систем класса H только наружу, к системам классов M, L и базового. Другими словами, никакой поток данных не разрешается для входа в зоны систем класса H из систем более низких классов;

никакие управляющие команды не принимаются из зон систем более низкого класса (в частности, никакие соединения не должны идти из этих зон). В обратном направлении могут быть приняты только внутренние подтверждающие сообщения или сообщения о контролируемом сигнале (свободный односторонний принцип связи);

удаленный доступ на обслуживание системы может быть разрешен в зависимости от обстоятельств и на определенный промежуток рабочего времени, при этом он должен быть защищен шифрованием и строгой аутентификацией;

на удаленной системе должно применяться шифрование и строгая аутентификация пользователя;

удаленная система и пользователь должны соблюдать определенную политику безопасности и вытекающие из нее технические требования (например, применение современной антивирусной защиты, защиты от вредоносных программ, версий заплат, правил персонального межсетевого экрана и др.);

количественный состав персонала, которому предоставляется доступ к КВОИ, должен быть минимальным;

должны быть реализованы высокий уровень контроля физического и логического доступа к системе и высокий уровень аутентификации и идентификации пользователей;

должны быть приняты все обоснованные меры для гарантии целостности и доступности системы;

испытания на проникновение могут привести к нестабильности работы устройств или процессов и поэтому должны выполняться только с использованием испытательных стендов или в ходе заводских приемочных испытаний.

Класс G (максимальный уровень ИБ). Основные характеристики:

защита критичной информации в важных областях деятельности должна быть гарантированной и соответствовать строгим требованиям секретности;

информация должна быть максимально точной;

основные задачи учреждения не могут выполняться без использования ОИ;

малое время реакции для принятия важных решений требует постоянного наличия актуальной (обновляемой) информации;

время простоя не допускается (надежность $P \geq 0{,}95$).

Обобщенный критерий: нарушение безопасности КВОИ ведет к прекращению функционирования объекта инфраструктуры или имеет серьезные последствия для значительной части общества или сферы деятельности учреждения.

Для обеспечения ИБ КВОИ класса G дополнительно к требованиям базового уровня должны выполняться следующие требования:

ни данным, ни информации какого-либо вида (подтверждение, сигнализация и т.д.) не разрешается входить в зону систем этого класса. Возможна передача, направленная только строго наружу;

для гарантии надежности системы (доступности и целостности ее ресурсов) следует рассмотреть возможность резервирования;

должны быть реализован «жесткий» принцип односторонней связи (исключены TCP-IP и другие протоколы, подтверждающие установление связи даже при контролируемых направлениях соединений);

должны быть предусмотрены избыточность или теневое оперативное запоминающее устройство, соответствующее критерию единичного отказа, что означает, что компьютеры имеют полностью горячий резервный узел, способный восстанавливать исходное состояние системы в любое время;

удаленный доступ на обслуживание запрещается;

количество персонала, имеющего доступ к системам, должен быть сокращен до абсолютного минимума;

должен осуществляться строгий контроль доступа к компьютерным системам и строгая авторизация пользователей;

должен применяться принцип «два человека/4 глаза», что означает, что должны быть всегда два человека, дающие совместное разрешение на любые разрешенные модификации, выполняемые в компьютерных системах;

должны обеспечиваться все меры для гарантии целостности и доступности компьютерной системы;

организационные и административные процедуры по применению автономной связи, передачи данных, внешних носителей данных, обслуживанию ПО и аппаратных средств

ЭВМ, обновлению, разгрузке и модификации ПО должны соответствовать установленным уровням важности систем защиты и безопасности.

По исполнению КВОИ могут варьироваться от абсолютно специализированных ИТ систем (например, классы G,H) до, по большей части, серийных (типовых) компьютерных архитектур (классы M,L, базовый). Для всех классов КВОИ важно обеспечить адекватный уровень безопасности по всем задачам одновременно.

Поэтому классификация ОИ только по требования защиты информации от несанкционированного доступа [6],[7] при отсутствии явных ограничений на другие задачи (целостность, доступность, готовность, надежность) является неоправданно широкой для назначения требований безопасности КВОИ и требует конкретизации этих задач в соответствии с приведенной классификацией. Итоговый уровень безопасности, расходы, меры, действия и процедуры должны быть соответствующими и пропорциональными объему и степени зависимости объекта инфраструктуры от КВОИ и тяжести, вероятности и размеру ущерба от нарушения его функционирования.

Для типовых ОИ стандарт «Общие критерии», имеющий библиотечную структуру, обеспечивает подход к созданию защищенных ИТ систем «снизу вверх» – от отдельных требований безопасности к общей функциональности. Для КВОИ предпочтительным является подход «сверху вниз» – от требуемой функциональности и установления категории важности функций к механизмам обеспечения безопасности и реализующим эти механизмы системам и средствам [8], [9].

Защита КВОИ от полного спектра угроз требует использования методов многоуровневой, с перекрытием защиты, ориентированной на человеческий, технический и эксплуатационный аспекты. Это необходимо из-за высоко интерактивного характера различных систем и сетей инфраструктур и того факта, что любой отдельный КВОИ не может быть адекватно защищен и функционировать с высокой надежностью, если остальные взаимодействующие с ним ОИ не защищены так же.

Таким образом, для обеспечения безопасности КВОИ, наряду с основными задачами, относящимися к применению технических средств, обеспечивающих защиту его функций, должны учитываться и нетехнические аспекты, такие как политика безопасности, эксплуатационные процедуры, уровень подготовки пользователя и др.

Литература

1. NIST Special Publication 800-53 «Information Security. Recommended Security Controls for Federal Information Systems», 2009

2. IEC/TR 61838 Nuclear power plants. Instrumentation and control for systems plants important to safety. Use of probabilistic safety assessment for the classification of function.

3. CEI/IEC 61513-2001. Nuclear power plants – Instrumentation and control for systems plants important to safety – General requirements for systems

4. ГОСТ 27.310 – 95 Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения.

5. An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12 «IT Baseline Protection Manual», 1995

6. СТБ П 34.101.38–2009. Информационные технологии и безопасность. Классификация объектов информационных технологий по требованиям информационной безопасности.

7. СТБ 34.101.30–2007. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация.

8. ГОСТ Р ИСО/МЭК 19791 – 2008: Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

9. Профили защиты на основе «Общих критериев». Аналитический обзор. Бетелин В.Б., Галатенко В.А., Кобзарь М.Т., Сидак А.А., Трифаленков И.А.—JET INFO, 2003 год.

В.В.МАЛИКОВ

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

В настоящее время обеспечение информационной и инженерно-технической защиты ***критически важных объектов*** является одной из приоритетных задач современного общества. Данная проблема приобретает сегодня особую значимость и для Республики Беларусь в связи с научным и технологическим развитием в промышленности, проектированием и строительством собственной атомной станции, а также иных объектов государственной важности с режимом ограниченного доступа.

Критически важные объекты (КВО) - объекты, нарушение (или прекращение) функционирования которых приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению (или разрушению) или существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени.

Публикуемые в открытых источниках информации материалы по методикам создания и функционирования КВО имеют общий характер, а почти все статистические данные по безопасности данных объектов являются закрытыми. Однако, учитывая то, что функционирование КВО осуществляется в рамках единого административно-территориального и экономического пространства государства, то можно предположить для указанных объектов в той или иной мере будут применимы общие подходы по выделению данных, связанных с нарушением их информационной и инженерно-технической защиты.

В Республике Беларусь отмечаются следующие тенденции роста угроз, связанных с использованием компьютерной техники, программных средств и сети интернет:

– 2008 г. выявлено 1622 преступления, за 2009 г. - 2160 (в 2003 г. - 119);

– рост киберпреступности в 2008 г. составил 62 %, в 2009 г. - 33,8 %.

В целом, анализируя статистические данные по нарушению инженерно-технической защиты объектов различных категорий, следует выделить следующие тенденции:

– незначительное снижение (до 5 - 8 %) общего числа попыток несанкционированного доступа к объектам различных категорий;

– значительное увеличение попыток (более 100 %) проникновений на объекты, которые можно отнести к КВО.

Для анализа реализации угроз в области информационной и инженерно-технической защиты объектов от несанкционированного доступа в Республике Беларусь и выявления потребности в совершенствовании нормативно-правовой базы в области защиты объектов от преступных посягательств проведено статистическое исследование в форме анкетирования руководителей служб безопасности организаций и банков, руководителей фирм-разработчиков систем безопасности, слушателей курсов повышения квалификации.

По результатам проведенного исследования можно сделать основной вывод: вопросы реализации угроз в области информационной и инженерно-технической защиты объектов от несанкционированного доступа в Беларуси носят ярко-выраженный характер, т.е. являются важными для всех категорий респондентов.

Для рассмотрения возможностей существующих технических решений, применяемых для обеспечения безопасности КВО, был проведен сравнительный анализ ИС ТСО, СПИ, которые получили наибольшее распространение на территории стран СНГ и являются лучшими по своей функциональности.

По результатам проведенного исследования можно сделать основные выводы:

1. Эксплуатируемые в рамках СПИ средства и системы охраны обеспечивают отражение только части программно-технических и физических угроз КВО и, в целом, не всегда отвечает современным требованиям к комплексным системам защиты объектов.

2. При использовании технологий передачи данных в системах защиты необходимо учитывать как категорию защищаемого объекта, так и пропускную способность каналов связи, параметры их надежности и помехоустойчивости.

Для построения эффективной системы комплексной безопасности КВО необходимо проведение анализа и оценки рисков, которые заключаются в определении характеристик объекта, информационной системы и их ресурсов. На основе анализа существующих методов оценки эффективности систем защиты КВО показано, что существующие подходы не позволяют проводить полный анализ и динамическую коррекцию результатов оценки.

Для реализации комплексного подхода в области безопасности КВО, решения проблем согласованного взаимодействия заинтересованных структур, централизации управления при обеспечении защиты КВО, а также достижения требуемого уровня защиты при проектировании систем информационной и инженерно-технической защиты КВО необходима разработка концептуальных основ проектирования таких систем.

По результатам проведенного статистического исследования и анализа нормативно-правового обеспечения в области безопасности объектов, в качестве системообразующего документа в области информационной и инженерно-технической безопасности КВО предложен проект «Концепции обеспечения безопасности критически важных объектов в Республике Беларусь», позволяющий сформировать концептуальные требования к проектированию систем информационной и инженерно-технической защиты КВО.

В целях снижения общих затрат на проектирование, мониторинг, техническое обслуживание средств и систем защиты для крупных организаций, ведомств Республики Беларусь, а также обеспечения должного реагирования на сигналы «тревога», рекомендуется построение системы информационной и инженерно-технической защиты КВО на базе эксплуатируемой системы АСОС «Алеся» Департамента охраны МВД Республики Беларусь.

Предлагается следующее построение территориальной структуры распределенной комплексной системы мониторинга и управления: главный (республиканский) центр, областные центры, районные центры мониторинга и управления.

В настоящее время для построения систем безопасности КВО уже разработаны и широко используются различные аппаратно-программные и инженерно-технические средства и системы защиты объектов. Однако их применение проводится с учетом имеющегося подхода в раздельном обеспечении информационной и инженерно-технической защиты КВО, заключающемся в использовании нескольких независимых систем безопасности. Применение указанного подхода при построении систем защиты не учитывает взаимные достоинства и недостатки типовых средств и систем безопасности, что в целом ослабляет эффективность использования таких систем.

Использование разработанных методических основы выбора и применения типовых аппаратно-программных и инженерно-технических средств и систем защиты КВО позволяет систематизировать подход к проектированию комплексных систем защиты КВО. На основе результатов исследования показано, что эффективность проектирования комплексных систем защиты, в том числе за счет использования разработанных методических основ, позволяет получить значительный экономический эффект за счет снижения на 20 % от времени необходимого для существующего типового проектирования систем защиты.

Для осуществления оперативного мониторинга состояния охраны объекта и обеспечения управления системой защиты КВО, а также реагирования на угрозы безопасности предложена методика построения комплексной (11 видов систем охраны и жизнеобеспечения) системы информационной и инженерно-технической защиты КВО, основанная на оперативном аудите угроз для объекта, позволяющая обеспечить их

локализацию и предотвратить развитие вторжения на территорию объекта при введении объединенной (до 4-х служб) оперативно-дежурной службы, охватывающей не менее 90 % территории Республики, а также существенно снизить уязвимость КВО и его информационной системы.

Предлагаемая структура распределенной системы информационной и инженерно-технической защиты КВО состоит из трех уровней: объектового, каналов сопряжения и телекоммуникации, обеспечения и управления безопасностью.

Для эффективного управления распределенной системой информационной и инженерно-технической защиты КВО введены 5 специализированных служебных сигналов: $СИС_{1,2,3}$, $СИС_{СПИ}$, РИПС.

Существующая сегодня классификация КВО:

– по критериям информационной безопасности не может быть распространена на КВО в виду использования ограниченного числа параметров, использующихся при классификации, и она применима лишь для средств и систем, обрабатывающих государственные секреты;

– по критериям инженерно-технической безопасности также не может быть распространена на КВО в виду использования ограниченного числа параметров и их показателей, использующихся при классификации и учитывающих, как правило, только величину ущерба, выраженную в стоимостном (денежном) выражении.

Для осуществления классификации КВО по комплексным показателям информационной и инженерно-технической защиты с учетом особенностей доступа, введены следующие показатели: организационная структура управления объектом, функционально-экономическая организация процесса деятельности объекта, риск нанесения ущерба.

С учетом изложенного выше предлагается введение классификации объектов с группировкой их по категориям (критерий близости - уровень доступа): упрощенный доступ, ограниченный доступ, важный доступ, доступ с расширенной защитой, доступ с максимальной защитой. При этом к КВО предлагается относить три последние группы объектов.

Для обеспечения своевременного выявления открытых / скрытых уязвимостей в системе безопасности КВО, необходимо разработать соответствующие подходы, связанные с эффективным реагированием на угрозы безопасности КВО, а также разработать и/или внедрить механизмы реагирования на появление новых прогнозируемых угроз системе безопасности КВО.

При рассмотрении угроз информационной и инженерно-технической безопасности КВО необходимо выполнять их анализ с учетом жизненного цикла системы защиты и предъявляемых к ней требований, что в совокупности гарантирует защиту КВО от НСД.

На основании проведенного исследования предложен подход и проведена классификация угроз (8 видов, 17 подвидов) для системы информационной и инженерно-технической защиты КВО, основанный на учете этапов их жизненного цикла, который позволяет усовершенствовать процесс проектирования и обеспечить гарантированную защиту КВО.

Для оценки состояния системы безопасности КВО, устанавливающей уровень ее соответствия определенным показателям и критериям, необходимо проведение оценки эффективности информационной и инженерно-технической защиты КВО. Существующие в настоящее время методы оценки эффективности систем защиты КВО, а также программные комплексы, разработанные на их основе, имеют недостатки и уязвимости, а также значительную (во многих случаях избыточную) стоимость и низкую функциональность.

Разработанный методический подход по оценке эффективности систем защиты КВО позволяет проводить анализ и динамическую коррекцию результатов оценки с учетом:

– появления новых, ранее не классифицированных видов угроз, а также изменения приоритетов оценки, углубления и детализации ранее классифицированных угроз;

– появления новых средств и систем безопасности в области информационной и инженерно-технической защиты КВО, а также изменения приоритетов в оценке действующих систем защиты на основе анализа их эффективности.

О.В.МЕЛЕХ, В.К.ФИСЕНКО

АТТЕСТАЦИЯ. ОБСЛЕДОВАНИЕ РЕАЛИЗУЕМОСТИ ТРЕБОВАНИЙ ФИЗИЧЕСКОЙ ЗАЩИТЫ В РЕАЛЬНЫХ УСЛОВИЯХ ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ /ИНФОРМАЦИОННЫХ СИСТЕМ

Требования к физической защите объектов информатизации/информационных систем (ОИ/ИС) должны быть определены и согласованы до разработки информационных систем. Средства физической защиты оказываются значительно более дешевыми и эффективными, если они решают одновременно задачи защиты как самого ОИ/ИС, так и защиты организации, где они используются.

Все требования к физической защите определяются на стадии разработки задания на проектирование системы физической защиты объекта. Требования к физической защите и средства безопасности должны отражать ценность информационных ресурсов для организации, а также возможные последствия от нарушения режима безопасности или отсутствия средств физической защиты для производственных процессов.

Обследование реализуемости требований к физической защите следует проводить на стадии анализа требований к каждому проекту разработки систем.

Основу обследования реализуемости требований к физической защите составляют:

– рассмотрение необходимости обеспечения конфиденциальности, целостности и доступности информационных ресурсов;

– определение возможностей использования различных средств контроля для предотвращения и выявления случаев нарушения физической защиты объектов информатизации/информационных систем, а также восстановления работоспособности систем после их выхода из строя и инцидентов в системе безопасности.

В частности, при проведении такого обследования следует рассмотреть необходимость:

– *Требования размещения ОИ/ИС* (требования к выбору площадки, требования к организации транспортной сети, требования к размещению ОИ/ИС в зданиях и помещениях организации, требования к организации въездов на территорию размещения ОИ/ИС, требования по оборудованию периметров охраняемых зон, требования к размещению КПП (для персонала, транспорта) на периметрах защищенных зон ОИ/ИС, требования к коммуникациям, пересекающим периметр защищаемых зон, требования к пропускной способности КПП, количества проходов и проездов (для персонала, транспорта), требования к количеству и местам дислокации постов охраны, требования к размещению караульного помещения и его вместимости, к размещению авто- и бронетехники, требование к размещению бюро пропусков, требования к размещению помещений для личного состава службы безопасности, требования к размещению центральных и локальных пультов управления).

– *Требования к архитектурно-строительным и конструктивным решениям зданий и помещений, в которых размещается ОИ/ИС* (общие требования к архитектурно-строительным и конструктивным решениям; требования к зданиям (сооружениям), имеющим категорированные помещения; требования к центральному и локальным пунктам управления; требования к КПП (для персонала, транспорта); требования к зданию караульного помещения; требования к проходам; требования к помещениям для личного

состава службы безопасности; требования к защитно-оборонительным сооружениям для часовых; требования к стенам зданий и сооружений, образующих периметр; требования по защите коммуникаций, пересекающих периметр защищенных зон).

– *Требования к структурным компонентам и элементам инженерно-технических средств физической защиты* (состав и задачи комплекса инженерно-технических средств физической защиты; состав и задачи инженерных средств физической защиты; состав и задачи комплекса технических средств физической защиты).

– *Требования к структурным компонентам (функциональным системам) комплекса технических средств физической защиты* (требования к системам охранной сигнализации; требования к тревожно-вызывной сигнализации; требования к системе контроля и управления доступом; требования к системе оптико-электронного наблюдения и оценки ситуации; требования к системе оперативной связи и оповещения; требования к системе обнаружения проноса (провоза) взрывчатых веществ, предметов из металла; требования к системам электропитания и освещения; требования к размещению и техническому оснащению рабочих мест операторов центрального и локальным пунктам управления; требования к техническому оснащению рабочих мест аналитической работы; требования к техническому оснащению рабочих мест для проведения регламентных работ и технического обслуживания; требования к техническому оснащению мест обучения и переподготовки персонала).

– *Требования к охраняемым зонам* (требования к оснащению защищаемых зон; требования к оснащению важных зон; требования к оснащению особо важных зон; требования к оснащению зон ограниченного доступа).

– *Требования к выбору и размещению технических средств физической защиты* (общие требования к выбору и размещению технических средств физической защиты; требования к оборудованию КПП; требования по оборудованию категорированных помещений; требования по оборудованию помещений центрального и локального пунктов управления; требования по защите выходов инженерных коммуникаций зданий (сооружений); требования по защите крыш, окон, дверей и других конструктивных элементов зданий (сооружений); требования к оборудованию караульного помещения).

Средства физической защиты, обеспечивающие физическую защиту аттестуемого ОИ/ИС, могут быть скомпрометированы, если обслуживающий их персонал и пользователи не будут их знать. Поэтому необходимо явно определить эти средства в соответствующей документации.

В качестве исходной информации для обследования реализации требований к физической защите используются следующие данные, приведенные в Задании на проектирование системы физической защиты:

– перечень требований к физической защите ОИ/ИС, а также их наименование и формулировка;

– перечень средств безопасности, а также их наименование и функции;

– таблица установления однозначного соответствия между требованиями к физической защите и их реализующими средствами безопасности.

Кроме того, при обследовании используются подготовленные разработчиком следующие документы:

– Методика проведения проверок физической защиты ОИ/ИС;

– Отчет о результатах проведения проверок реализации требований к физической защите ОИ/ИС.

На основе приведенных исходных данных составляется таблица обследования, описывающая процедуру обследования и содержащая перечень проверок, действия по проверке и ожидаемые результаты проверки, определенные в методике проведения проверок физической защиты ОИ/ИС. Если для какого-то функционального требования методика не содержит нужной проверки, то эксперт- специалист по физической защите ОИ/ИС

определяет вид проверки, формулирует действия по проведению этой проверки и прогнозирует ожидаемые результаты.

Оценка результатов проведения проверок физической защиты ОИ/ИС проводится с использованием показателя: **степень реализации требования физической защиты**. Для данного показателя устанавливается лингвистическая и количественная шкалы оценок (таблица 1).

Таблица 1 – Соответствие между лингвистической и количественной шкалами оценок

Лингвистическая оценка степени реализации требований	Интервал количественной оценки
Высокая степень реализации	1.0-0,75
Удовлетворительная степень реализации	0,74-0,5
Степень реализации неполная	0,49-0,25
Требование не реализовано	0,24-0,01

Экспертное заключение по степени реализации конкретного требования к физической защите ОИ/ИС формулируется с использованием следующего правила принятия решений:

– если количественное значение степени реализации требования лежит в интервале 1,0-0,5, что соответствует лингвистическим оценкам «Высокая степень реализации» и «Удовлетворительная степень реализации», то принимается решение: требование к физической защите (наименование требования) реализовано средством безопасности (наименование средства безопасности);

– если количественное значение степени реализации требования к физической защите лежит в интервале 0,49-0,01, что соответствует лингвистическим оценкам «Степень реализации неполная» и «Требование не реализовано», то принимается одного из двух решений:

1) Заявитель в течение договорного срока аттестации устраняет выявленные недостатки и Исполнитель проводит повторную аттестацию;

2) Заявитель не может обеспечить устранение выявленных недостатков в установленное время, то принимается решение о продолжении процедуры проведения проверок физической защиты ОИ/ИС.

После обследования реализации всего согласованного между Заявителем и Исполнителем перечня требований к физической защите ОИ/ИС определяется обобщенная оценка степени реализации (таблица 2).

Таблица 2 – Обобщенная оценка степени реализации требований к физической защите ОИ/ИС

Лингвистическая оценка степени реализации всего перечня требований	Интервал количественной оценки
Весь перечень требований реализован	1.0-0,75
Допущены незначительные отклонения в реализации отдельных незначительных по значимости требований	0,74-0,5
Допущены отклонения в реализации отдельных требований	0,49-0,25
Требования в полном объеме не реализованы	0,24-0,01

Экспертное заключение по степени реализации всего перечня требований к физической защите ОИ АЭС формулируется с использованием следующего правила принятия решений:

– если количественное значение обобщенной количественной оценки лежит в интервале 1,0-0,5, что соответствует лингвистическим оценкам «Весь перечень требований

реализован» и «Допущены незначительные отклонения в реализации отдельных незначительных по значимости требований», то принимается решение: требования к физической защите ОИ/ИС реализованы;

– если количественное значение обобщенной количественной оценки лежит в интервале 0,49 – 0,01, что соответствует лингвистическим оценкам «Допущены отклонения в реализации отдельных требований» и «Требования в полном объеме не реализованы», то принимается одного из двух решений:

1) Заявитель в течение договорного срока аттестации устраняет выявленные недостатки и Исполнитель проводит повторную аттестацию;

2) Заявитель не может обеспечить устранение выявленных недостатков в установленное время, то принимается решение об отказе в выдаче аттестата соответствия.

Д.Н.НИКИПЕЛОВ

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК СРЕДСТВО КОНТРОЛЯ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ СРЕДЫ

В современном информационном мире все большую актуальность приобретают вопросы противодействия вторжения в замкнутую информационную среду. Перспективным и актуальным в данной области является способ принятия превентивных мер по противодействию внешним вторжениям. Для выбора эффективного механизма противодействия и анализа защищенности информационной среды рекомендуется проводить аудит информационной безопасности.

Аудит информационной безопасности – это системный процесс получения объективных оценок текущего состояния информационной безопасности организации (предприятия) в соответствии с определенными критериями информационной безопасности, который включает комплексное обследование различных сред функционирования ИС, проведения тестирования на уязвимости ИС, анализ и оценку защищенности ИС, формирование отчёта и разработку соответствующих рекомендаций.

Основной целью аудита информационной безопасности ИС является оценка текущего состояния информационной безопасности учреждения или предприятия, а также подготовка исходных данных для формирования требований к комплексной системе защиты информации (КСЗИ) ИС.

Существуют два способа проведения аудита информационной безопасности ИС:

– классический аудит;

– эвристический аудит (тесты на уязвимости).

Классический аудит является формализованной процедурой и включает в себя:

– Проверка наличия документации на ИС и ее предварительный анализ.

– Проверка наличия распорядительных документов на ИС и их предварительный анализ.

– Сбор сведений об общей структурной схеме ИС, ее компонентах – *состав оборудования, технических и программных средств, их связи, особенности конфигурации, архитектуры и топологии, программные и программно-аппаратные средства защиты информации, взаимное размещение средств*.

– Сбор сведений информации о видах каналов связи, их характеристики.

– Сбор сведений об особенностях взаимодействия отдельных компонентов ИС.

– Сбор сведений о технологии обработки информации в ИС.

– Сбор сведений об информационных потоках ИС.

– Сбор сведений о предъявляемых в организации требований к защите информации в ИС.

– Сбор сведений о режиме доступа к информационным ресурсам ИС.

– Сбор сведений об информационных носителях и правилах работы с ними.

– Проверка наличия документации на компоненты физической среды ИС и ее предварительный анализ.

– Сбор сведений о территориальном размещении компонентов ИС.

– Сбор сведений о наличии охраняемой территории и пропускного режима на объекте.

– Сбор сведений о наличии на объекте или объектах категорированных помещений.

– Сбор сведений о наличии на объекте или объектах охранной, пожарной сигнализации, систем видеонаблюдения и контроля доступа.

– Сбор сведений о режиме доступа к компонентам физической среды ИС.

– Сбор сведений о наличии в помещениях, где функционирует ИС, элементов коммуникаций, систем жизнеобеспечения и связи, имеющих выход за пределы контролируемой территории.

– Сбор сведений о наличии системы заземления оборудования ИС и ее технических характеристик.

– Сбор сведений об условиях хранения магнитных, оптико-магнитных, бумажных и других носителей информации.

– Анализ полученной информации.

Недостатком классического аудита ИБ является невозможность выявления сложных уязвимостей информационной системы в виду отсутствия эвристических алгоритмов в механизме аудита.

Эвристический аудит (тесты на уязвимости) – современный метод превентивного выявления существующих и потенциальных уязвимостей. Является не формализованной процедурой и представляет из себя имитацию аудитором действий потенциального злоумышленника. Может проводиться по различным сценариям, с применением или без применения технических и программных средств. При проведении подобного аудита, аудитор получает полную свободу действий в рамках полномочий потенциального нарушителя (внешнего или внутреннего). Аудит считается завершенным тогда, когда аудитор исчерпал свои навыки в попытках проникновения, либо когда попытка проникновения в информационную систему завершилась успехом. После устранения уязвимости проводится повторное тестирование.

Недостатком данного метода является необходимость привлечения аудитора весьма высокой квалификации, а также невозможность отражения полной картины состояния вопросов ИБ в организации.

Для проведения качественного анализа состояния защищенности информационной среды необходимо использовать комплексный подход, включающий в себя применение обоих способов аудита информационной безопасности.

Наиболее интересным с практической стороны является одновременное проведение мероприятий классического аудита с позиции контроля за работой системы информационной безопасности предприятия при проведении тестов на проникновение. При этом практически проверяется грамотность и слаженность персонала, исправность резервных копий СУБД, возможности резервного оборудования и т.д. Аудитор, имитирующий действия злоумышленника создает нештатную ситуацию, а аудитор, находящийся на объекте, контролирует действия персонала и работу оборудования в реальном масштабе времени. При этом необходимо исключить возникновение реальной нештатной ситуации. Сложность данного подхода заключается в том, что при проведении подобных мероприятий требуется весьма высокая подготовка аудиторов и слаженность в их действиях.

После проведения подобных тестов проводится разбор ситуаций, и принимаются решения по улучшению действующей системы информационной безопасности.

Э.Г.НОВОСЕЛЕЦКАЯ, Е.П.МАКСИМОВИЧ, В.К.ФИСЕНКО

АТТЕСТАЦИЯ. ПОКАЗАТЕЛИ И КРИТЕРИИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ОЦЕНКЕ ИСХОДНЫХ ДАННЫХ И ДОКУМЕНТОВ ПО АТТЕСТУЕМЫМ ОБЪЕКТАМ ИНФОРМАТИЗАЦИИ/ИНФОРМАЦИОННЫМ СИСТЕМАМ

Исходные данные по аттестуемому объекту информатизации/информационной системе (ОИ/ИС) представляются Заявителем в соответствии с перечнем, установленным Постановлением №675. Специализированная организация, уполномоченная на проведение аттестации, должна произвести их оценку, предварительно разработав для этого соответствующую рабочую методику оценки. Однако нормативная база по разработке подобных методик в настоящее время отсутствует, вследствие чего каждая организация должна решать эту проблему самостоятельно. В докладе предлагается типовая методика оценки, которая может быть использована при разработке рабочих методик оценки исходных данных и документов для конкретных ОИ/ИС. Данная методика включает: методику оценки исходных данных и документов по показателям полноты и качества и методику оценки соответствия исходных данных и документов требованиям нормативных правовых актов в области защиты информации.

Методика оценки по показателям полноты и качества

Полнота представленных исходных данных и документов определяется с помощью следующего критерия принятия решений: Представленные Заявителем (Владельцем) ОИ/ИС исходные данные и документы обладают свойством полноты в том случае, если они по составу и назначению полностью соответствуют требованиям Постановления № 675.

Полнота определяется лингвистической и интервальной количественной оценками (таблица 1).

Таблица 1 – Соответствие между лингвистической и интервальной шкалами оценок по показателю полноты исходных данных и документов

Лингвистическая оценка полноты совокупности исходных данных и документов	Интервал количественных оценок
Комплект исходных данных и документов по составу и назначению соответствует требованиям Постановления № 675	0,75 – 1,0
В комплекте исходных данных и документов допущены незначительные отклонения от требований Постановления № 675	0,5 – 0,74
По некоторым (не менее двух) исходным данным и документам допущены значительные отклонения от требований Постановления № 675	0,25 – 0,49
Комплект исходных данных и документов по составу и назначению не соответствует требованиям Постановления № 675	0,01 – 0,24

С учетом того, что отдельные элементы исходных данных и документы различаются по степени своей важности с точки зрения обеспечения информационной безопасности, они ранжируются по значимости. **Значимость** элементов исходных данных и документов определяется лингвистической и интервальной количественной оценками (таблица 2).

Качество всей совокупности исходных данных и документов определяется совокупностью оценок качества отдельных элементов исходных данных и документов.

Качество отдельного элемента исходных данных или документа характеризуется следующими показателями: **адекватность отображения и достаточность уровня детализации.**

Таблица 2 – Соответствие между лингвистической и интервальной шкалами оценок значимости исходных данных или документов

Лингвистическая оценка значимости элемента исходных данных или документа	Интервал количественных оценок
Весьма значимый	0,75 – 1,0
Значимый	0,5 – 0,74
Средней значимости	0,25 – 0,49
Наименее значимый	0,01 – 0,24

Для показателя **адекватность отображения** применяется следующий критерий принятия решений: *представленный Заявителем (Владельцем) ОИ/ИС элемент исходных данных или документ, содержащий данные в виде конкретных характеристик аттестуемого ОИ/ИС, в полной мере соответствует характеристикам реального ОИ/ИС.*

Адекватность отображения отдельных элементов исходных данных или документов определяется лингвистической и интервальной количественной оценками (таблица 3).

Таблица 3 – Соответствие между лингвистической и интервальной шкалами оценок по показателю адекватности отображения

Лингвистическая оценка адекватности отображения	Интервал количественных оценок
Строгое соответствие	0,75 – 1,0
Высокая степень соответствия	0,5 – 0,74
Средняя степень соответствия	0,25 – 0,49
Несоответствие	0,01 – 0,24

Для показателя достаточность уровня детализации применяется следующий критерий принятия решений: уровень детализации информации, представленной в элементе исходных данных или документе, является достаточным в том случае, если:

– представленная информация содержит минимальный, но достаточный набор показателей для принятия экспертом правильного решения относительно качества, целевого назначения и реализуемости представленных положений;

– представленная информация определяет все основные концептуальные положения, на базе которых сформулированы основные функциональные положения;

– представленная информация содержит обоснование принятых основных положений или ссылку на ранее реализованное положение, программу или устройство;

– представленная информация не является избыточной, что может привести к ошибкам в принятии решений.

Достаточность уровня детализации отдельных элементов исходных данных или документов определяется лингвистической и интервальной количественной оценками (таблица 4).

Основные этапы оценки исходных данных и документов по показателю качества состоят в следующем.

1. Эксперт ранжирует исходные данные и документы по значимости, устанавливая их лингвистические и количественные оценки (в соответствии с таблицей 2).

2. Эксперт определяет совокупности оценок по показателям адекватности отображения и достаточности уровня детализации для представленных видов исходных данных и документов, устанавливая для каждого из них лингвистическую и количественную оценки (в соответствии с таблицей 3). Если документ включает несколько подразделов, то

его количественные оценки определяются на основе вычисления аддитивных сверток соответствующих количественных оценок подразделов с последующим определением лингвистических оценок в соответствии с таблицами 3-4.

Таблица 4 – Соответствие между лингвистической и интервальной шкалами оценок по показателю достаточности уровня детализации

Лингвистическая оценка достаточности уровня детализации	Интервал количественных оценок
Положительная оценка по всем составляющим показателя	0,75 – 1,0
Допущены незначительные отклонения по некоторым составляющим показателя	0,5 – 0,74
Допущены отклонения хотя бы по одной составляющей показателя	0,25 – 0,49
Допущены значительные отклонения по нескольким составляющим показателя	0,01 – 0,24

3. Эксперт вычисляет интегральную количественную оценку качества каждого вида исходных данных и документа как среднее арифметическое оценок по показателям адекватности отображения и достаточности уровня детализации и устанавливает соответствующую лингвистическую оценку в соответствии с таблицами 3-4.

4. Эксперт вычисляет интегральную количественную оценку всего комплекса представленных исходных данных и документов на основе вычисления взвешенной аддитивной свертки их отдельных количественных оценок.

5. Эксперт формирует заключение по результатам оценки исходных данных и документов на основе следующих правил:

– комплект исходных данных и документов, для которого обе интегральные количественные оценки по показателям полноты и качества находятся в пределах 1,0-0,5, удовлетворяет требованиям по критериям полноты и качества;

– если хотя бы для одного из показателей полноты или качества интегральная количественная оценка находится в пределах 0,49 – 0,01, то созывается согласительное совещание с Заявителем, на котором принимается одно из следующих решений;

1) осуществить доработку документов в течение периода аттестации и провести повторную оценку исходных данных и документов, потребовавших доработки;

2) в случае отказа Заявителя от доработки принимается решение в отказе выдачи аттестата соответствия.

Методика оценки соответствия требованиям нормативных правовых актов в области защиты информации

Оценка соответствия исходных данных и документов требованиям нормативных правовых актов в области защиты информации производится по следующим показателям: соответствие требованиям нормативных правовых актов, подтверждение соответствия, схема (порядок) подтверждения.

Под **оценкой соответствия документа** понимается деятельность эксперта по определению соответствия назначения и структуры разработанного документа требованиям нормативных правовых и технических нормативных правовых актов в области информационной безопасности, определенных в Национальной системе подтверждения соответствия в области технического нормирования и стандартизации. Под **подтверждением соответствия** понимается вид оценки соответствия, результатом осуществления которой является документальное удостоверение соответствия объекта оценки требованиям нормативных правовых и технических нормативных правовых актов в области технического нормирования и стандартизации. Под **схемой (порядком) подтверждения** соответствия понимается установленная последовательность действий, результаты которых

рассматриваются в качестве доказательства соответствия разработанных документов требованиям нормативных правовых и технических нормативных правовых актов.

Методика формирования оценки и экспертного заключения аналогична методике оценки исходных данных и документов по показателям полноты и качества.

Д.В. ПЕРЕВАЛОВ

ОТНЕСЕНИЕ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ К КРИТИЧЕСКИ ВАЖНЫМ ОБЪЕКТАМ: ПРОЦЕДУРНЫЙ ПОДХОД

В настоящее время всё большую актуальность приобретает проблема защиты критически важных объектов (далее – КВО), функционирующих в различных системах (в том числе и в информационно-телекоммуникационной инфраструктуре (далее – ИТИ)) от различного вида угроз. В Республике Беларусь также уделяется значительное внимание этой проблеме. В частности, в Концепции национальной безопасности Республики Беларусь, утв. Указом Президента Республики Беларусь от 09.11.2010 № 575, отмечается, что информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями (п.5). Кроме того, в Концепции национальной безопасности Республики Беларусь в качестве основных направлений нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности предусмотрено обеспечение материально-технической основы безопасности функционирования КВО, а также разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность (абз.5 п.51, абз.2 п.54).

При разработке данной проблематики одним из приоритетных направлений исследования является создание методик для отнесения соответствующих объектов к категории критически важных.

При определении объектов в качестве критически важных, обоснованным представляется подход, предложенный в Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов, утв. распоряжением Правительства Российской Федерации от 27.08.2005 № 1314-р, и в Основах государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов, утв. письмом Президента Российской Федерации от 28.09.2006 № ПР-1649. В соответствии с п.5 указанной концепции и п.2 указанного письма к КВО относятся объекты, нарушение (или прекращение) функционирования которых приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, её необратимому негативному изменению (или разрушению) или существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени. Аналогичного подхода придерживаются и исследователи сферы обеспечения безопасности КВО.

В настоящее время для отнесения объектов к категории критически важных используется в основном методический подход, в основе которого лежит такой критерий как важность объекта. Формирование такого показателя осуществляется в рамках таких групп как: субъекты природных монополий, которые ведут деятельность на общегосударственном

рынке товара; предприятия, оборонно-промышленного комплекса, составляющие научно-технический потенциал страны; предприятия, на которых работают более 10 тыс. человек и т.д. При этом для оценки важности объектов в масштабе указанных групп разрабатывается специальная система рамочных критериев, которые характеризующихся такими показателями как: значимость объекта для экономики страны; нанесение ущерба престижу государства, возможные угрозы населению и территориям.

Однако в данном случае не решается вопрос о том, каким образом тот или иной объект становится КВО. В связи с этим кроме методического подхода представляется необходимым использовать процедурный подход, который устанавливает соответствующие процедуры по отнесению объекта к КВО в той или иной системе.

Использование процедурного подхода позволяет решать следующие задачи:

– учесть особенности функционирования объекта в зависимости от его характеристик при его переводе в категорию КВО;

– дифференцировать ресурсы на перевод объекта в категорию КВО;

– осуществить нормативное закрепление порядка и процедур включения объекта в систему КВО.

Процедурный подход на современном этапе исследования проблемы целесообразно рассматривать как научно обоснованный и предусмотренный действующим законодательством последовательный и взаимосвязанный процесс отнесения объекта к категории КВО.

Процедурный подход имеет чётко выраженный процессуальный характер, а его содержание будут составлять следующие стадии:

1) принятие решения о создании системы КВО;

2) определение общих и частных критериев отнесения объектов к КВО;

3) определение соответствия объекта критериям КВО;

4) принятие решения о включении объекта в систему КВО (об отказе во включении);

5) принятие решения о включении объекта в Реестр КВО;

6) получение сертификата КВО.

Данный подход в полном объёме может быть применён для отнесения объектов информатизации к критически важным объектам информатизации (далее – КВОИ). В целом изложенный процедурный подход реализован в проекте Положения об отнесении объектов информатизации к критически важным, организации функционирования и обеспечения безопасности критически важных объектов информатизации, которое предполагается утвердить Указом Президента Республики Беларусь.

При этом под объектом информатизации следует понимать автоматизированные системы различного уровня и назначения, вычислительные сети и центры, автономные стационарные и персональные электронные вычислительные машины, используемые для обработки информации. А под КВОИ – объект информатизации, нарушение (прекращение) функционирования которого может привести к чрезвычайной ситуации техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны, либо для жизнедеятельности населения, проживающего на соответствующей территории, на длительный период времени

Одной из наиболее важных стадий является определение критериев отнесения объекта информатизации к КВОИ. Основным общим критерием отнесения объекта информатизации к КВОИ является уровень возможных последствий нарушений его функционирования. К таким последствиям следует относить:

1) нарушение штатного режима функционирования объекта информатизации, обеспечивающего функционирование экологически опасных и (или) социально значимых производств, и (или) технологических процессов, которое приведёт к чрезвычайной ситуации техногенного характера;

2) нарушение функционирования объекта информатизации, осуществляющего функции информационной системы, которое приведёт к значительным негативным для государства последствиям;

3) нарушение режима предоставления объектом информатизации значительного объема информационных услуг, которое приведёт к прекращению предоставления таких услуг.

Объект информатизации следует считать КВОИ, если в результате нарушения его функционирования промышленному, транспортному предприятию, предприятию связи или иной организации, в составе которой он функционирует, может быть причинён соответствующий вред, который вызвал бы указанные выше последствия. Исходя из положений ст.460 Уголовно-процессуального кодекса Республики Беларусь и п.8 Постановления Пленума Верховного Суда Республики Беларусь от 28.09.2000 № 7 «О практике применения судами законодательства, регулирующего компенсацию морального вреда» к такому вреду следует относить:

– имущественный вред, который охватывает уничтожение средств электронной вычислительной техники, программного обеспечения, информационных систем и (или) иных компонентов КВОИ либо такое их повреждение, когда они не могут быть использованы для поддержания функционирования объекта информатизации;

– физический вред, который выражается в причинении смерти или телесных повреждений работникам, использующим КВОИ, в результате которых они не смогут выполнять необходимые действия по обеспечению деятельности объекта или обслуживанию его средств электронной вычислительной техники, программного обеспечения, информационных систем и (или) иных компонентов;

– неимущественный вред, то есть:

а) вред деловой репутации объекта – формирование негативного общественного мнения о профессиональных достоинствах и недостатках КВОИ, снижающего эффективность его функционирования;

б) моральный вред – причинение физических (физическая боль, функциональное расстройство организма, изменения в эмоционально-волевой сфере, иные отклонения от обычного состояния здоровья) или нравственных (ощущение страха, стыда, унижения, иные неблагоприятные психологические переживания) страданий работникам, использующим КВО, в результате чего они не смогут выполнять необходимые действия по обеспечению деятельности объекта или обслуживанию его средств электронной вычислительной техники, программного обеспечения, информационных систем и (или) иных компонентов.

К частным критериям отнесения объектов информатизации к КВО необходимо относить конкретные количественные показатели последствий, являющихся компонентами основного общего критерия. В данном случае как раз должен применяться методический подход. При этом важность объекта определяется применительно к конкретной сфере, в которой функционирует объект информатизации.

Конкретные количественные показатели последствий нарушения функционирования КВО необходимо определять экспериментальным путём посредством применения комплекса различных мероприятий: экспертного опроса специалистов в той или иной сфере; предварительной оценке возможного ущерба, который может быть причинён в результате нарушения функционировании КВОИ и т.п.

П.С.ПОЙТА, В.И.ДРАГАН, Б.Н.СКЛИПУС,
Д.А.КОСТЮК, А.П.ДУНЕЦ, С.С.ДЕРЕЧЕННИК

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА В РАМКАХ ЛОКАЛЬНОЙ СЕТИ УНИВЕРСИТЕТА

Одной из проблем, сопутствующих развитию современного учебного заведения, как и любой иной крупной организации, является обеспечение внутреннего информационного пространства, объединяющего вычислительные ресурсы подразделений. Технические и организационные решения, обеспечивающие функционирование локальной вычислительной сети (ЛВС), должны, помимо функций хранения и передачи информации, выполнять защиту данных и программного обеспечения компьютерного парка от различных внешних и внутренних угроз. Грамотная организация сети и выбор технологий, используемых на серверах и рабочих станциях, позволяют упростить процедуры обслуживания ЛВС и восстановления после сбоев, исключить воздействие ряда вредоносных факторов, значительно увеличить обнаруживаемость вандальных воздействий, ускорить устранение их последствий.

Нами рассмотрен подход к защитным мерам, принимаемым при организации крупной ЛВС, на примере информационно-вычислительной сети Брестского государственного технического университета (БрГТУ).

Сервисы (службы), предоставляемые пользователям в рамках ЛВС БрГТУ и в той или иной степени универсальные для высших учебных заведений, можно разделить на следующие категории [1]:

– аутентификация пользователей для работы в сети;

– хранение файлов на сетевых дисках;

– веб-хостинг (сайт университета) и электронная почта;

– предоставление доступа в Интернет с дополнительной аутентификацией и хранением статистики сетевой активности.

Можно выделить три основные роли пользователей локальной сети: студенты, преподаватели и административно-управленческий персонал.

Защита информации в рамках обеспечения учебного процесса в целом и предоставления пользователям перечисленных сервисов в частности, в свою очередь, подразделяется на следующие категории:

– физическая защита аппаратных средств;

– защита от вредоносной активности со стороны пользователей;

– защита от внешних угроз;

– защищенность резервного копирования системных и прикладных данных.

Физическая защита аппаратных средств осуществляется использованием отдельных помещений с ограниченным доступом для размещения коммутационных узлов локальной сети и серверов, что гарантирует как сохранность дорогостоящего оборудования, так и свободную работу администраторов по его настройке и профилактике. Опорная сеть (совокупность линий связи между зданиями университетского комплекса) обеспечивает однотипный доступ пользователей к необходимым информационным ресурсам, что особенно важно для университетов с их обширным компьютерным парком, размещенным в нескольких корпусах различной степени территориальной рассредоточенности. В БрГТУ для соединения зданий между собой в большинстве случаев используются оптические кабели, что обеспечивает необходимую помехозащищенность и надежность одновременного подключения большого числа компьютеров; при этом критичный участок между основными корпусами имеет резервную линию оптической связи. Однако в ситуации, когда оправдана экономия средств, используются недорогие линии связи и соответствующее оборудование:

так, расположенный в отдельном корпусе небольшой физический сегмент ЛВС из 16 точек подключен с помощью телефонной линии и модемов VDSL.

Имеющаяся в настоящее время схема маршрутизации сети БрГТУ сформирована в ходе постепенного наращивания сложности ЛВС после ее первоначального развертывания и с учетом опыта эксплуатации. В составе ЛВС выделено несколько подсетей:

– основная ЛВС университета;
– ЛВС бухгалтерии;
– защищенный сегмент, в котором находятся ректорат и приемная комиссия;
– отдельная подсеть для студенческих компьютеров в общежитиях;
– Интернет-сегмент университета;
– отдельные подсети кафедр компьютерного профиля.

Приведенное разделение выполнено с учетом требований по защищенности и необходимости оптимизации потоков передаваемых данных. В частности, наличие подсетей последнего типа позволяет кафедрам, обладающим сотрудниками надлежащей квалификации, выполнять администрирование собственного сегмента и тестировать новые подходы к организации вычислительного процесса без влияния на остальные сегменты сети [2, 3].

Защита от вредоносной активности со стороны пользователей выполняется как заданием прав доступа, ограничивающих их активность в пределах конкретных наборов действий и сегментов сети, так и разграничением сегментов сети межсетевыми экранами, блокирующими межсегментные коммуникации по любым сетевым портам кроме строго необходимых для авторизации пользователей и доступа к файл-серверу с методическими материалами и программным обеспечением. Авторизация пользователей выполняется сервером Novell, предоставляющим LDAP-базу пользовательских учетных записей. Доступ к большинству прикладных программ на рабочих станциях осуществляется через сетевую систему Novell ZENworks, благодаря чему исключена необходимость установки множества различных прикладных пакетов на рабочие станции и достигнута унификация дисковых образов последних.

В качестве недостатка применяемых мер защиты можно отметить непродолжительную пиковую загрузку сети при запуске прикладных программных пакетов, а также использование на рабочих станциях антивирусного пакета AVP 6-й корпоративной версии, оказывающей заметный негативный эффект на производительность рабочей станции. Для усиления защиты на рабочих станциях учебных классов отключены сменные флеш-накопители, из конфигураций рабочих станций исключены DVD-приводы, а содержимое активных разделов жесткого диска возвращается к исходному состоянию при каждой перезагрузке с помощью специально модифицированной версии операционной системы.

В подсетях кафедр компьютерного профиля перечисленные ограничения рабочих станций сняты – взамен дополнительных мер контроля сетевого трафика на шлюзах, соединяющих их с основной ЛВС. Снятие указанных выше локальных ограничений вызвано, в первую очередь, требованиями учебного процесса, т. к. в рамках ряда дисциплин, изучаемых специалистами компьютерного профиля, требуется предоставить студентам более полный доступ к аппаратной подсистеме рабочих станций и сетевых коммуникаций [2, 4]. Кроме того, в рамках подсети кафедры электронных вычислительных машин и систем действует специализированная лаборатория для изучения аппаратно-программных систем защиты информации. Лаборатория оснащена комплектом средств «Аккорд NT/2000», «Аккорд – РАУ» и «Шипка–1.6», предоставленных университету в 2009 году ОКБ «САПР» и Всероссийским НИИ проблем вычислительной техники и информатизации в рамках Соглашения о научно-техническом сотрудничестве. Практикумы, выполняемые студентами в данной лаборатории, также являются причиной модификаций политики администрирования рабочих станций кафедры.

На серверах ЛВС, предоставляющих услуги электронной почты и веб-доступа внутренним пользователям и пользователям из сети Интернет, применяются дополнительные меры защиты от вандальных воздействий. Внешняя защита обеспечивается настройками межсетевых экранов и мониторингом вирусной активности, а для доступа локальных пользователей сети к внешним ресурсам используется наложенная частная сеть (VPN).

Сеть VPN функционирует поверх существующей инфраструктуры ЛВС университета, обеспечивая доступ к сети Интернет для сотрудников и студентов университета с учетом требований защищенности передаваемой информации и вопросов безопасности пользования соответствующими услугами. Учитывая обширность компьютерного парка, для разделения нагрузки в рамках ЛВС для различных сегментов сети применено четыре сервера VPN-доступа. Данные сервера работают под управлением Debian Linux, а защищенную авторизацию пользователей для доступа к Интернет централизованно выполняет пакет FreeRADIUS, установленный на одном из серверов. Журналирование сетевой активности выполняется с использованием мощной СУБД и соответствующего сервера с большим дисковым массивом, что позволяет в случае возникновения чрезвычайной ситуации выяснить время недопустимых сетевых действий, локализовать использованный для их осуществления компьютер и пользователя, учетная запись которого была при этом задействована. Для минимизации вероятности работы пользователей под чужими учетными записями на сервере введены: запрет на одновременный вход на нескольких компьютерах и обязательное требование периодической смены пароля.

Частью системы обеспечения бесперебойной работы ЛВС является проведение регулярного резервного копирования системных и прикладных данных. В рамках ЛВС наблюдается большое разнообразие типов оборудования, программного обеспечения (в т.ч. серверных операционных систем), данных различных типов, что порождает большой перечень требуемых процедур резервного копирования и их разнородность. Информация на серверах сети преимущественно хранится в RAID-массивах; кроме того, в рамках ЛВС выделены два сервера под управлением Windows 2003, выполняющие автоматизированную архивацию данных. Резервное копирование в ЛВС университета осуществляется для многих сервисов корректно и в достаточном объеме; однако вместо использования стандартных средств резервирования на ряде серверов в настоящий момент применяются ручные процедуры либо автоматизация посредством нестандартизированных программных средств собственной разработки.

Приведенный комплекс мер и программно-аппаратных решений позволяет обеспечить достаточный уровень безопасности и устойчивости к возможной случайной или умышленной вредоносной активности, несмотря на территориальную распределенность, исторически сложившуюся многокомпонентную гетерогенную архитектуру информационно-вычислительной сети и значительное расхождение в требованиях и подходах к эксплуатации компьютерного парка среди подразделений университета.

Литература

1. П.С. Пойта, В.И. Драган, А.П. Дунец, Д.А. Костюк, В.И. Хведчук, С.С. Дереченник. Подход к модернизации гетерогенной сетевой инфраструктуры на примере информационно-вычислительной сети университета // Вестник БрГТУ. – 2010. – №5: Физика, математика, информатика. – С. 75–78.

2. Б.Н. Склипус, С.С. Дереченник, А.А. Склипус. Универсальный реконфигурируемый микропроцессорный стенд для лабораторных занятий / Проблемы проектирования и производства РЭС: сб. материалов V международной НТК (Новополоцк, Май 29–30, 2008). – Т. III, Информатика. – Р. 233–237.

3. Д.А. Костюк, Р.В. Сченснович. Использование в образовательном процессе вычислительных сетей на базе Windows Server 2008 // Информационные технологии в

образовании: материалы Международной научно-практической конференции, 21–22 мая 2009. / БНТУ. – Минск, 2009. – С. 109–113.

4. Д.А. Костюк. Изучение низкоуровневого программирования и вычислительной архитектуры на базе платформы GNU/Linux // Свободное программное обеспечение в высшей школе: тезисы докладов 5-й конференции (Переславль-Залесский, 30–31 января 2010 г.). - М.: Институт логики, 2010. – С. 32–35.

А.В.ПУГАЧ

ИСПОЛЬЗОВАНИЕ ПРОФИЛЕЙ ЗАЩИТЫ ПРИ ПРОЕКТИРОВАНИИ СИСТЕМ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Информация, содержащаяся в продуктах или системах информационных технологий (далее – ИТ), является важнейшим ресурсом, позволяющим организациям успешно выполнять их функции. В системах ИТ может находиться также информация, отнесенная к государственным секретам или информация, критичная к сохранению своих свойств. Продукты или системы ИТ такого рода должны выполнять свои функции при соответствующих гарантиях защиты информации от несанкционированного доступа, изменения или потери.

Значительным шагом вперед в решении проблем безопасности продуктов и систем ИТ (к которым относятся автоматизированные системы (далее - АС), в том числе и специального назначения) явилось введение в действие стандартов [1]–[3], которые определяют структуру и содержание двух документов – профиль защиты (далее – ПЗ) и задание по безопасности (далее – ЗБ) и содержат библиотеку требований, которые выбираются и включаются в ПЗ и ЗБ. С одной стороны, ПЗ может рассматриваться как детальное определение требований безопасности и гарантий, которые пользователи хотят видеть в продукте или системе ИТ. ПЗ – независимая от реализации структура для определения и обоснования требований безопасности, представляющая собой набор задач безопасности, функциональных и гарантийных требований. ПЗ разрабатывается для новых продуктов и систем. С другой, ЗБ может рассматриваться как описание в терминах требований безопасности того, что предлагает разработчик.

Главная задача ПЗ и ЗБ – создание основы для взаимодействия между потребителями (заказчиками), производителями и экспертами по сертификации продуктов и систем ИТ по требованиям безопасности. Каждая из этих сторон имеет свои интересы и взгляды на проблемы информационной безопасности.

Потребители заинтересованы, во-первых, в методике, позволяющей обоснованно выбрать продукты, отвечающие их потребностям, для чего им необходима шкала оценки безопасности ИТ, во-вторых, нуждаются в инструменте, с помощью которого они могли бы формулировать свои требования производителям. При этом потребителям важны характеристики и свойства конечного продукта. С этой точки зрения шкала оценки безопасности выглядит следующим образом:

Уровень 1. Система для обработки общедоступной информации, критичной к сохранению, например, свойств целостности и доступности информации.

Уровень 2. Система для обработки информации ограниченного распространения, например, с грифом не выше «для служебного пользования», и т. д.

Производители, в свою очередь, нуждаются в инструментах для сравнения возможностей своих продуктов, в применении процедуры сертификации для объективной оценки их свойств, а также в стандартизации набора требований безопасности. С точки зрения производителя, требования безопасности должны быть максимально конкретными и

регламентировать необходимость применения тех или иных средств, механизмов, алгоритмов и т. д.

Эксперты по безопасности и специалисты по сертификации нуждаются в инструменте, позволяющем оценить уровень безопасности, обеспечиваемый продуктами ИТ. С одной стороны они, как и производители, заинтересованы в четких и простых критериях оценки безопасности продукта ИТ. С другой стороны, они должны дать обоснованный ответ пользователям – удовлетворяет продукт их нуждам или нет. Именно эксперты принимают на себя ответственность за безопасность продукта, получившего оценку уровня безопасности и прошедшего сертификацию.

Таким образом, примирение этих точек зрения и создание эффективного механизма взаимодействия всех сторон – сложная задача. Причем, если не принять во внимание потребность хотя бы одной из сторон, то это не позволит решить общую задачу – создать систему обработки информации, соответствующую требованиям безопасности ИТ.

Государственным учреждением «Научно-исследовательский институт Вооруженных Сил Республики Беларусь» был разработан ПЗ систем ИТ, относящихся к классу Б1 в соответствии с классификацией, приведенной в [4]. ПЗ может быть использован для формирования требований безопасности АС органов государственного управления, обрабатывающих информацию, отнесенную к категории государственных секретов.

Выводы:

1. Наличие каталога ПЗ продуктов и систем ИТ в значительной степени упрощает взаимодействие заказчиков и производителей, а также процедуру сертификации продукта или системы ИТ по требованиям безопасности.

2. Наличие ПЗ и разработанного на его основе ЗБ позволяет уже на этапе формирования требований к АС иметь определенные гарантии того, что реализация АС будет соответствовать требованиям безопасности ИТ.

Литература

1. СТБ 34.101.1-2004. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

2. СТБ 34.101.2-2004. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

3. СТБ 34.101.3-2004. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности.

4. СТБ 34.101.30-2004. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация.

Н.В.РУЧАНОВА

СРЕДСТВА ОЦЕНКИ РИСКОВ КАК ВАЖНЕЙШИЙ ЭЛЕМЕНТ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

В настоящее время организация режима информационной безопасности (далее – ИБ) становится критически важным стратегическим фактором существования и развития любой организации, вне зависимости от формы собственности. В Республике Беларусь создана и развивается национальная нормативно-правовая база в области защиты информации, регламентирующая порядок создания и эксплуатации информационных систем. Вместе с тем многие организации сегодня осознают важность дополнительных инициатив, направленных

на обеспечение устойчивости и стабильности функционирования корпоративных информационных систем для поддержания непрерывности бизнеса в целом, таких как:

– анализ информационных рисков компании и управления ими;

– оценка непрерывности бизнеса организации;

– оценка экономической эффективности корпоративных систем защиты информации;

– оценка совокупной стоимости владения (TCO) системы защиты информации;

– оценка возврата инвестиций (ROI) компании в информационную безопасность;

– планирование и управления бюджетом на информационную безопасность.

Основной из перечисленных задач является *анализ и управление информационными рисками.* Подобная оценка особенно важна в тех случаях, когда к информационной системе организации предъявляются повышенные требования в области информационной безопасности. Квалифицированно выполненный анализ информационных рисков позволяет:

– провести сравнительную оценку по критерию «эффективность-стоимость» различных вариантов защиты информации;

– выбрать адекватные контрмеры для защиты информации;

– оценить уровень остаточных информационных рисков компании.

Можно выделить два подхода обоснования стоимости создания (развития) системы защиты информации в организации. *Первый подход* заключается в получения метрики и меры безопасности, проведении оценки стоимости защищаемой информации, определении вероятностей потенциальных угроз и уязвимостей, а также потенциального ущерба. *Второй подход* заключается в поиске инварианта стоимости системы защиты информации с учетом вероятностей наступления событий, повлекших за собой ущерб (по аналогии со стоимостью страхования автомобиля в размере 5% от его рыночной стоимости). Так по сложившейся практике эксперты в области защиты информации оценивают стоимость системы ИБ примерно в 10-20% от стоимости информационной системы организации - в зависимости от уровня конфиденциальности информации.

В общепринятой международной практике (bestpractice) обеспечения режима информационной безопасности под информационной безопасностью (ИБ) понимается защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, приводящих к нанесению ущерба владельцам и пользователям информации, а также поддерживающей инфраструктуре в целом. Вне зависимости от размеров организации и специфики ее информационной системы работы по обеспечению режима ИБ обычно состоят из этапов, приведенных на рис. 1.

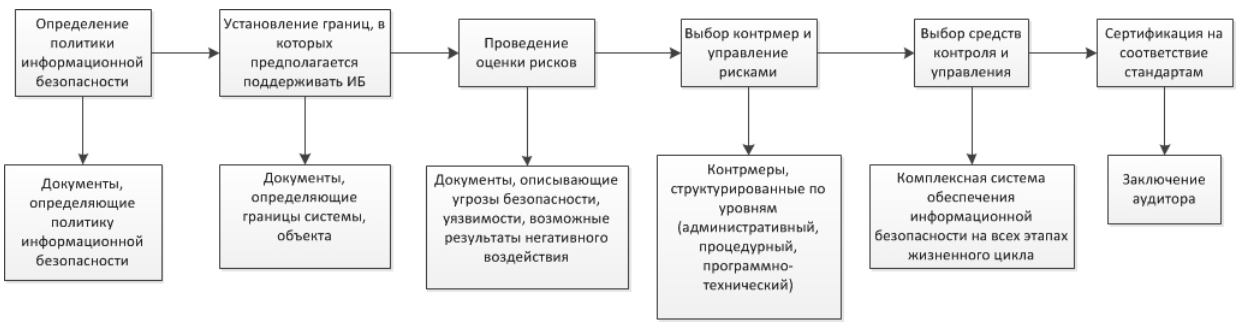


Рисунок 1. Этапы создания системы защиты информации

Выбор подхода к оценке рисков зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер по защите информации. В случаях, когда нарушения режима ИБ ведут к тяжелым последствиям и базового уровня требований к режиму ИБ недостаточно, предъявляются дополнительно

повышенные требования. Для формулирования дополнительных повышенных требований необходимо:

– определить ценность ресурсов;

– к стандартному набору (вирусы, сбои оборудования, несанкционированный доступ и т.д.) добавить список угроз, актуальных для исследуемой информационной системы;

– рассчитать вероятности угроз;

– выявить уязвимости ресурсов;

– оценить потенциальный ущерб от воздействий злоумышленников.

На этапе управления рисками разрабатывается стратегия управления рисками (уменьшение риска, уклонение от риска; изменение характера риска; принятие риска).

На следующем этапе выбирается комплекс контрмер для защиты информации, структурированных по нормативно-правовому, организационно-управленческому, технологическому и аппаратно-программному уровням обеспечения информационной безопасности. В дальнейшем предлагаемый комплекс контрмер реализуется в соответствии с принятой стратегией управления информационными рисками.

В целях автоматизации работы специалистов в области защиты информации рекомендуется использовать инструментальные средства анализа рисков, осуществляющих оценку или переоценку информационных рисков предприятия.

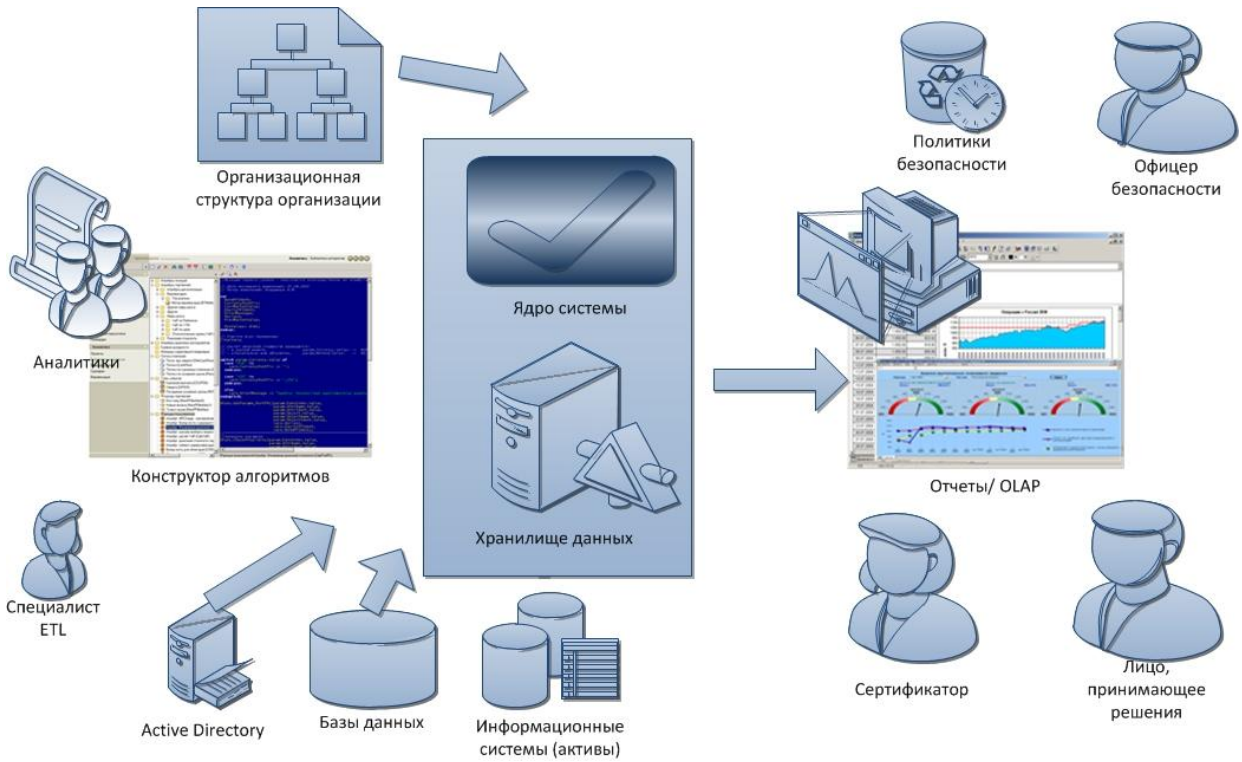


Рисунок 2. Возможная архитектура системы управления рисками информационной безопасности

Компания «ПРОГНОЗ» имеет богатый и успешный опыт по разработке и внедрению хранилищ данных. Для этого специалистами компании применяются как классические, так и уникальные решения по проектированию и созданию хранилищ данных. Разработанные компанией «ПРОГНОЗ» хранилища данных используются как единый информационный ресурс для решения следующих задач:

– консолидация данных и подготовка отчетности;

– мониторинг ключевых показателей;

– моделирование и многовариантное прогнозирование;

– комплексный анализ состояния;

– оценка эффективности принимаемых управленческих решений;

– и других.

Кроме того, инструментальные средства анализа рисков АК «Прогноз», основанные на современных базах данных и знаний в области защиты информации, дают возможность построить:

– структурные и объектно-ориентированные модели современных корпоративных информационных систем;

– модели угроз и модели рисков, связанных с отдельными составляющими элементами корпоративной информационной системы, и, таким образом, выявлять те сегменты и объекты информационных систем, риск нарушения безопасности которых является критическим, то есть неприемлемым;

– различные модели защиты информационных систем, а также сравнивать между собой по критерию «эффективность-стоимость» варианты мер по защите (контрмер) и также вести контроль выполнения требований к организации режима информационной безопасности на предприятии.

Решения, построенные на базе АК «Прогноз», полностью поддерживают как процессную модель, так и PDCAмодель, что согласуется с лучшими практиками и рекомендациями группы стандартов ISO/IEC 27001:2005(E). Сочетание данного подхода с информационными системами, построенными с учетом требований по информационной безопасности Республики Беларусь, группы стандартов СТБ 34.101.1-3 позволяют создать взаимоувязанный и согласованный комплекс организационных мер и технических средств автоматизированной информационной системы и среды эксплуатации для любой организации.

А.М.САПРЫКИН

ПРАКТИКА ПРИМЕНЕНИЯ И ПЛАНЫ РАЗВИТИЯ BEL VPN ПРОДУКТОВ

В связи со вступлением в силу и развитием национального законодательства по защите информации на рынке возникла потребность в средствах криптографической защиты информации сетевого уровня (VPN). Если ниша персональных и встроенных в программные приложения СКЗИ на основе национальных стандартов развивалась в республике уже продолжительное время и представлена развернутым перечнем средств шифрования, то VPN-решения предлагают пока лишь две компании. В их числе – Bel VPN продукты компании «С-Терра Бел».

Bel VPN – это линия VPN продуктов, предназначенных для построения сертифицированных в соответствии с требованиями белорусского законодательства защищенных сетей на основе некриптографического инструментария разработки от российской компании «С-Терра СиЭсПи».

Продукты Bel VPN предназначены, прежде всего, для использования в составе решений мирового лидера сетевой индустрии Cisco Systems, но могут применяться и в сетях любых других производителей.

Хронология создания Bel VPN продуктов

В июле 2008 года компания «С-Терра Бел» получила лицензию Оперативно-аналитического центра при Президенте Республики Беларусь на осуществление деятельности по технической защите информации, в том числе криптографическими методами, включая применение ЭЦП.

В 2008-2009 гг. совместно с ЗАО «Авест» ведется разработка Bel VPN продуктов на основе нейтрального (некриптографического) инструментария, полученного от «С-Терра СиЭсПи». В частности, разрабатывается (и сертифицируется) средство ЭЦП и шифрования «AvCrypt ver.5.0» (под ОС Linux, Solaris и Windows), которое затем встраивается в программное обеспечение Bel VPN. Наряду с пятью белорусскими криптостандартами в Bel VPN продуктах реализован ряд международных технических стандартов RFC, которые делают их технологичными и универсальными в применении.

В сентябре 2009 года продукты компании – «Шлюз безопасности Bel VPN Gate 3.0» и «Клиент безопасности Bel VPN Client 3.0» проходят государственную экспертизу в Оперативно-аналитическом центре при Президенте Республики Беларусь.

Описание Bel VPN продуктов

Шлюз безопасности Bel VPN Gate – масштабируемый набор шлюзов безопасности для защиты трафика (данных) в процессе межсетевого взаимодействия. Поставляется заказчику партнерами компании – системными интеграторами в виде аппаратно-программных комплексов на базе серверов Hewlett-Packard, Sun Microsystems, Tonk под управлением Unix-систем: Linux, Solaris. Имеются следующие версии поставки шлюзов безопасности:

– Bel VPN Gate 3000 – шлюз безопасности для защиты сетей средних офисов (до 250 компьютеров) с количеством туннелей шифрования до 1 000:
  – Bel VPN Gate 3000 Low End – производительность не менее 200 Мб/с;
  – Bel VPN Gate 3000 Standard – производительность не менее 300 Мб/с;
  – Bel VPN Gate 3000 High Perfomance – производительность не менее 400 Мб/с.
– Bel VPN Gate 7000 – шлюз безопасности для защиты сетей крупных офисов (свыше 250 компьютеров) с неограниченным количеством туннелей шифрования:
  – Bel VPN Gate 7000 Standard – производительность не менее 500 Мб/с;
  – Bel VPN Gate 7000 High Perfomance – производительность до 2 Gb/c.

Модуль NME-APPRE. Шлюз безопасности Bel VPN Gate 3.0 устанавливается на сетевом модуле общего назначения – NME-APPRE-302-K9 и используется в составе маршрутизаторов серии Cisco 2800/3800 и 2900/3900 ISR. Производительность – 95 Мб/с, количество туннелей шифрования – до 500.

Клиент безопасности Bel VPN Client предназначен для защиты индивидуального (удаленного) пользователя. Поставляется в виде программного дистрибутива под MS Windows XP, Vista. Настройка политики безопасности клиента по доступу к защищенной сети производится на шлюзе безопасности Bel VPN Gate.

Основные достоинства и преимущества Bel VPN продуктов

Надежность. Обеспечивается детектирование отказа и автоматический переход на резервный шлюз с переносом IP-адресов отказавшего шлюза на резервное устройство.

Качество сетевого обслуживания (QoS) с использованием механизмов:

– оптимизации производительности и управления уровнем загрузки процессора;
– мэппирования ToS;
– «прозрачной» пересинхронизации ключей;
– приоритетной обработки голосового трафика;
– сброс избыточного трафика данных при перегрузке;
– классификации IKE (приоритет IKE-сессии при установлении соединения);
– классификация трафика.

Интегрированный межсетевой экран:

– пакетная фильтрация с контролем состояния соединения;
– независимые наборы правил фильтрации для входящего и исходящего трафика;

– управление правилами фильтрации выполняется в командах маршрутизатора IOS (ACL).

Достижения и результаты

В январе 2010 года «С-Терра Бел» при содействии Посольства Беларуси в России и МИД Республики Беларусь провела защищенную видеоконференцсвязь между Москвой и Минском для членов участвовавшей в работе «Инфофорума» белорусской делегации. Защищенная ВКС с сопредельным государством проводилась в республике впервые. При защите каналов связи использовались шлюзы безопасности Bel VPN Gate на базе сервера Sun (белорусская территория) и сетевого блока MCM с маршрутизатором Cisco ISR (российская территория).

В мае 2010 года «С-Терра Бел» и Cisco Systems представляют новое комбинированное – программное и аппаратное решение – AXP Bel VPN для обеспечения безопасности коммуникаций в распределенных сетях. В качестве аппаратной платформы используются сетевые блоки NME-APPRE-302-K9 в составе маршрутизаторов Cisco ISR первого и второго поколений.

В июне 2010 года «С-Терра Бел» награждается дипломом 6-го Евразийского форума информационной безопасности – «Инфофорум-Евразия» за «создание эффективных средств сетевой защиты информации на Евразийском пространстве».

В ноябре 2010 года компания «С-Терра Бел» достигает рекордной производительности в 2 Гб/с шифрования данных с использованием белорусской криптографии (ESP Cipher, пакеты UDP 1400 байт). Рекордный результат получен в результате тестирования шлюза безопасности Bel VPN Gate 3.0 под управлением ОС Solaris на аппаратной платформе Sun Fire X2270 M2 с использованием двух шестиядерных процессоров Intel® Xeon® X5670 с тактовой частотой 2,93 GHz.

Практическое применение

За прошедшие почти два с момента прохождения госэкпертизы и появления на рынке Bel VPN продукты прошли опытное тестирование во многих белорусских министерствах и ведомствах, и по результатам испытаний получали только положительные заключения. Продукты поставляются в некоторые ведомства, где уже применяются для защиты:

– межсетевого трафика и удаленного доступа в ведомственных АИС;
– спутниковой связи;
– ftp – трафика;
– IP-телефонии и голосовой связи;
– видеоконференцсвязи;
– службы доставки мгновенных сообщений on-line.

Планы по расширению и совершенствованию Bel VPN продуктов

1. Новые продукты:

– Bel VPN Server – программный комплекс для сетевой защиты серверов и пакетной фильтрации трафика сетевых узлов;

– Bel VPN Updater – программный продукт для удаленного обновления сервера безопасности Bel VPN Server и клиента безопасности Bel VPN Client.

2. Новые аппаратные платформы (менее производительные, но экономичные) и решения:

– Bel VPN Gate 1000-й серии – шлюз безопасности для защиты сетей малых офисов (от 10 до 50 компьютеров) с количеством туннелей шифрования до 100;

– для Bel VPN Gate 100-й серии – шлюза безопасности для защиты банкоматов и платежных терминалов;

– применение токенов (для аутентификации, хранения политик безопасности VPN клиента и шлюза).

3. Реализация криптостандартов:

– поддержка алгоритма СТБ 34.101.31-2011 (БЕЛТ);

– выработка имитовставки по ГОСТ 28147;

– переход на ПФОК на эллиптических кривых.

4. Доработка и совершенствование шлюза безопасности Bel VPN Gate:

– переход на новые версии ОС семейства Unix – Solaris 10, RHEL5, CentOS;

– добавление в функции межсетевого экрана:

– независимая фильтрация трафика на входящем и исходящем интерфейсе;

– классификация и маркировка трафика.

5. Доработка и совершенствование клиента безопасности Bel VPN Client:

– работа с Windows 7 (32bit и 64bit);

– разрыв соединений при извлечении токена – токен работает как «ключ»;

– хранение политик безопасности на токене – в этом случае не нужно переустанавливать клиент при изменении политики;

6. Сертификация шлюза безопасности Bel VPN Gate как аппаратно-программного комплекса – на базе наиболее востребованных аппаратных платформ.

Р.Ф.САФРОНОВ, В.К.ФИСЕНКО

МОДЕЛЬ НАРУШИТЕЛЯ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Общая классификация нарушителя

Модель нарушителя отражает его практические и теоретические возможности, полученные заранее знания, степень оснащенности и вооруженности, мотивации и решимости. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на причины с целью предотвращения самой попытки нарушения, либо точнее определить требования к системе защиты от данного вида нарушений или преступлений. В каждом случае, исходя из конкретной обстановки на объекте, может быть определена модель нарушителя, которая должна быть по возможности адекватна реальному нарушителю.

При общей классификации нарушителя выделяют:

– предположительную категорию лиц, к которым может принадлежать нарушитель;

– предположения о мотивах действий нарушителя, преследуемых нарушителем целях с учетом фактора демотивации;

– предположения о квалификации нарушителя и его технической оснащенности, используемых для совершения нарушения методах и средствах, вооружении;

– ограничения и предположения о характере возможных действий нарушителей, тактику действий, сценарное планирование развития событий;

– предположения о составе группы.

Для оценки последних удобно ввести следующую классификацию нарушителей:

– внешний, не имеющий санкционированного доступа на объект и совершающий свои действия извне;

– внутренний, имеющий доступ на объект (сотрудник объекта, командированный, посетитель и проч.);

– комбинированный: внешний, вступивший в сговор с внутренним путем подкупа, шантажа и пр.

Внутренним нарушителем может быть лицо из следующих категорий: работники объекта, имеющие непосредственный контакт с хранящимися ценностями, персонал, обслуживающий технические средства, – инженеры, техники; прочий персонал, имеющий доступ в здания и помещения; работники охраны; руководители разных уровней должностной иерархии. Посторонними нарушителями могут стать клиенты, посетители, приглашенные по какому-либо поводу; представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности объекта, любые лица за пределами контролируемой территории.

Для дальнейших расчетов выделяют самые опасные и наиболее профессионально подготовленные типы нарушителей. После выбора модели следует ответить на следующие основные вопросы:

– каковы цели нарушителя;

– какова его мотивация, и какие факторы могут ее снизить;

– какую тактику наиболее вероятно изберет нарушитель: силовой прорыв, скрытое или легальное проникновение;

– какие уязвимые участки объекта может использовать нарушитель;

– какие ключевые точки нарушитель изберет своей целью.

Модель нарушителя в рамках математической модели с графом действий

Граф действий составляется исходя из данных относительно планировки помещений и охраняемой территории, а также анализа способов, которыми можно преодолеть тот или иной опасный участок с учетом ресурсных затрат и рисков. Ниже перечислены краткие особенности графа действий:

– Граф по структуре «привязан» к планировке охраняемой территории.

– Граф ориентированный.

– Структура графа меняется от времени и зависит от действий нарушителя. Это динамический граф. При этом постоянно изменяются показатели пути и ограничения.

– Узлы обозначают ключевые точки местоположения нарушителя. Благодаря ним возможно ветвление. Т.к. узлы могут появляться и исчезать на графе (граф динамический), то возникает необходимость математически описать граф так, чтобы при изменении структуры графа не было алгоритмических сложностей изменить и его математическое представление под новую структуру.

– Дуги графа отображают единицы работы, которые нарушитель выполняет, переходя от одного узла к следующему. Дуга может обозначать возможности и маршруты перехода, а также способ преодоления элементарного участка. Если говорить о толковании смысла дуги, это, скорее, единица работы, нежели способ перехода по элементарному участку. Отдельные дуги могут появляться, исчезать. Прохождение тех или иных дуг предопределяет появление новых, т.к. это особенность динамического графа, которым является граф действий.

– Данный граф построить на этапах, предшествующих этапу непосредственного осуществления НСД, практически невозможно, т.к. структура графа постоянно меняется. Однако он хорошо подходит для описания математической модели реализации НСД из-за большей правдоподобности.

Что касается *модели нарушителя*

Поскольку граф действий основан на планировке, то можно провести аналогию между перемещением нарушителя по охраняемой территории и перемещением нарушителя по графу действий. Т.о. адаптация модели нарушителя под данную модель позволит обозначить его на плане местности, на графе действий и определить какую единицу работы тот выполняет.

В рамках программной модели реализации НСД нарушителя можно представить как сущность, имеющую следующие поля (Нарушитель будет представлен точкой.):

– узел или путевая точка (waypoint), где находится нарушитель;

– единица работы (геометрически заданная набором путевых точек), которую выполняет нарушитель;

– запас ресурсов, которыми может располагать нарушитель;

Для простоты будем считать, что ресурс у нарушителя один. Преодолевая ту или иную дугу, т.е. выполняя ту или иную единицу работы, нарушитель затрачивает часть ресурсов. При планировке и осуществлении НСД нарушитель отслеживает остаток своего ресурса и не предпринимает способов НСД, если они требуют ресурса больше, чем у него есть.

– если речь идет о группе нарушителей, то значение имеет, как могут нарушители взаимодействовать между собой (например, какие у них средства связи).

Поведение нарушителя на охраняемом объекте

Предполагается, что нарушитель хорошо знает охраняемую территорию, по которой он перемещается, куда и в какие помещения ему нужно проникнуть, возможные пути отступления и ухода с территории в случае завершения НСД или угрозы провала.

Как правило, на предыдущих этапах (в основном, на разработке вариантов и особенно тщательно на отработке оптимального варианта) нарушитель становится осведомленным, как ему вести себя и что делать в случае возникновения тех или иных незапланированных ситуаций.

При изменении ситуации нарушитель:

– Первым делом сообщает других членов команды об изменениях, при этом оперативно принимается решение, продолжать НСД или нет. В случае с нарушителем-одиночкой, нарушитель принимает решение сам в зависимости от того, насколько важным считается успешное выполнение операции и чем он рискует в случае провала. Критерий принятия решения в данной ситуации (особенно в случае непредвиденных ситуаций) – тема отдельной статьи.

– Если ситуация была незапланированной, но предвиденной, нарушитель действует согласно отработанным на предыдущих этапах алгоритмам. Грамотные нарушители всегда пытаются предусмотреть всевозможные ситуации заранее. Если угроза раскрытия миновала, нарушитель продолжает осуществлять НСД согласно запланированному сценарию поведения для данной ситуации. Зачастую для этого разрабатываются альтернативные варианты НСД с учетом изменений топологического графа до этапа реализации.

– Наибольший интерес представляет незапланированная и непредвиденная ситуация.

Данный случай происходит исключительно на этапе реализации НСД, сопровождается внезапным или очень быстрым и нестабильным изменением показателей на модельном графе действий или даже фрагмента графа в области охраняемой территории, где находится нарушитель. Примеров может быть много: сработала аварийная система, о существовании которой нарушитель не знал, заблокировались двери, отрезав нарушителю часть путей перемещения и, соответственно, сделав невозможным выполнение тех единиц работ, которые требуют быстрого преодоления этих преград. Ограничения для тех или иных дуг также претерпевают изменения.

В изменившихся условиях в рамках программной реализации нашей модели нарушитель должен заново рассчитать оптимальный путь от точки, где он сейчас находится к ключевой точке, куда ему следует попасть, чтобы выйти из опасной ситуации. В реальности, в условиях неопределенности и стресса, рассчитать мгновенно такой путь практически нереально.

В рамках же математической модели наибольшую вычислительную сложность представляется максимально быстрое определение вариантов поведения нарушителя, как например, определить варианты быстрого ухода с охраняемой территории при изменении ситуации.

Один нарушитель

Рассмотрим для простоты случай, когда НСД осуществляет один нарушитель. Т.о. мы уже избавляемся от ограничения на количество людей: там, где нельзя в одиночку

преодолеть элементарный участок, дуга просто не отмечается. Под данный случай попадает также и группа нарушителей, которые действуют как один нарушитель, т.е.: 1) одновременно преодолевают элементарный участок; 2) не «разбредаются» по локации, это вытекает из предыдущего пункта (на практике группа нарушителей все чаще разделяется; случаи действия группы нарушителей как единого целого – редкость, это лишь взято для упрощения); 3) материальный ресурс считается общим, в отличие от моделей, где каждый нарушитель имеет свой собственный запас ресурсов (боеприпасов, топлива, например).

Нарушитель осуществляет НСД из стартовой точки, при этом у него есть:

– Срок выполнения операции – это т.н. максимально допустимое время T (в начале операции $T = T_{пред}$), которое нарушитель должен затратить на всю операцию по НСД (с учетом вернуться обратно). Если нарушитель не уложится в данное время, то операция считается проваленной. Данное время отсчитывается от начального и может изменяться по мере продвижения нарушителя по локациям. При отсутствии внешних изменений, т.е. изменений показателей дуг модели графа НСД, данное время уменьшается на величину, затраченную на преодоление какого-либо опасного участка. Однако при наличии изменений в модели срок выполнения операции может уменьшиться гораздо быстрее.

– Ресурсы нарушителя – это может быть некий материальный (именно материальный, время и людские ресурсы не считаются) ресурс: оборудование, деньги, топливо, боеприпасы – все, что использует нарушитель для перемещения по охраняемому объекту, преодолению опасных участков и выполнению задания. Ресурсы, понятно, не могут изменяться не по воле нарушителя. Тем не менее, они расходуются при перемещении. Для простоты мы будем считать, что ресурс всего один. Стоимость – показатель дуги, обозначающий, сколько данного ресурса потребуется на преодоление данного элементарного участка данным способом. Если у нарушителя не хватает ресурса для перемещения по какой-либо дуге данным способом, значит он, понятно, не сможет осуществить НСД по данному пути, если в состав данного пути входила эта злополучная дуга. Провальной для нарушителя считается ситуация, когда он, будучи в каком-то узле, не может пройти ни по одной дуге из-за нехватки ресурсов.

При изменении ситуации нарушитель может знать о происшедших изменениях. Нарушитель принимает решение, продолжать операцию по осуществлению НСД или нет. Нарушитель в новых условиях должен снова определить оптимальный вариант НСД, при этом делая поправку на то, что начальный узел не тот узел, которого начался НСД, а тот, где находится нарушитель в данный момент после изменения обстановки. В программной реализации этим временем пренебрегают. В реальности при изменении обстановки нарушителю требуется порой порядочно времени, чтобы заново спланировать свой маршрут.

В случае если нарушитель не знает о произошедших изменениях, он будет продолжать движение по заранее определенному оптимальному маршруту на графе действий. Нарушитель, достигнув того участка, где граф действий изменился, обнаружит эти изменения.

Что касается обнаружения изменений на графе нарушителем, то можно для каждого узла (или даже для каждой путевой точки) задать таблицу видимости.

В.Е.ТОКАРЕВ

КОМПЛЕКСНАЯ ЗАЩИТА В КОРПОРАТИВНОЙ АИСС ОБЕСПЕЧЕНИЕМ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ФСБ И ФСТЭК РОССИИ ПО КЛАССАМ АК2/АК3 ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1. Сертифицированные платформы на базе продуктов Майкрософт

В последнее время, всё большую актуальность приобретает защита информации в корпоративных автоматизированных информационных системах (АИС) от внутреннего нарушителя. Среди угроз такого характера – неумышленная установка вредоносного ПО и вынос конфиденциальной информации, в том числе персональных данных на съёмных носителях. Эта тенденция носит глобальный характер, подтверждающаяся публикациями на популярном ресурсе Wiki Leaks в сети Интернет.

Учитывая полученные ФГУП «НТЦ «Атлас» результаты по сертификации продуктов Майкрософт, в настоящее время имеется линейка продуктов с интегрированными российскими средствами защиты информации (СЗИ) и средствами криптографической защиты информации (СКЗИ), позволяющая создавать **территориально распределённые защищённые АИС с обеспечением выполнения требований ФСБ и ФСТЭК России**, имеющие защиту от внутреннего нарушителя и соответствующие классу АК3 требований ФСБ России по защите от НСД в АИС, без потери функциональности.

Данные решения обеспечивают защиту информации от преднамеренных злоумышленных или ошибочных действий пользователей АИС, в том числе блокируют несанкционированную установку ПО и обеспечивают защиту от выноса из корпоративной АИС информации на отчуждаемых носителях.

Для сопряжения сетей с разной категорией доступа к информации используется ПАК «Атликс-Шлюз-К», реализующий технологию однонаправленной передачи файлов. Для защиты каналов связи используются программно – аппаратные комплексы «Атликс -VPN» и «Модуль - HSM».

Программные продукты корпорации Microsoft совместно с программным СЗИ Secure Pack Rus версии 2.0 обеспечивают защиту от НСД с использованием СКЗИ КриптоПро CSP 3.6.1, средством шифрования КриптоПро EFS и системой криптографической защита каналов связи КриптоПро IPSec. При этом обеспечивается корректная работа СКЗИ по классам КС2/КС3.

Для обеспечения выполнения требований по защите от НСД СЗИ Secure Pack Rus реализует, в частности, следующие основные функции по защите информации:

– реализация замкнутой программной среды (запрет исполнения неразрешенных программных приложений, в том числе скриптов);

– шифрование файлов на внешних и внутренних носителях;

– обеспечения контроля целостности ОС, СЗИ и СКЗИ;

– криптографическую защиту передаваемых по сети данных.

Следует отметить, что вышеуказанные платформы имеют также сертификаты ФСТЭК России.

2. Защищенный документооборот на базе продуктов Майкрософт

Сертифицированные продукты корпорации Майкрософт с российской криптографией являются базовыми компонентами для построения корпоративного документооборота в Российской Федерации. При этом сохраняется полная исходная функциональность и обеспечивается преемственность с существующими системами корпоративного документооборота, что позволяет сохранить ранее сделанные государством инвестиции и избежать дополнительных расходов на программное и аппаратное обеспечение, переобучение сотрудников и т.п.

3. Защищенные мобильные АРМ на базе Windows 7

В последнее время проявляется всё возрастающая заинтересованность в создании защищенного планшетного компьютера, позволяющего мобильному пользователю обрабатывать информацию ограниченного распространения, не содержащую сведений, составляющих государственную тайну.

Учитывая, что работы по сертификации ОС Microsoft Windows 7 находятся в стадии завершения, появляется реальная возможность создания защищенных по классам АК2/АК3 требований ФСБ России мобильных рабочих мест на базе планшетных компьютеров, работающих под управлением ОС Windows 7.

С учётом новых решений по защите информации, предлагаемых ФГУП НТЦ «Атлас», существенно расширяются возможности использования планшетов с одновременным предоставлением дополнительных удобств пользователю.

В обычном режиме планшет предоставляет возможность **свободного** серфинга в сети Интернет, социальных сетях, использования электронной почты и любах других сервисов Интернет, в том числе игр.

В защищённом режиме появляется возможность работы на этом планшете с конфиденциальной информацией, а также удалённой работы пользователя в корпоративной АИС. Эти возможности обеспечиваются:

– загрузкой доверенной ОС Windows 7 с внешнего «read-only» USB-носителя;

– использованием сертифицированных по требованиям ФСБ России СЗИ (защита от НСД) и СКЗИ (шифрование данных на диске, шифрование каналов связи).

Появление на рынке планшетных компьютеров от Apple инициировала бум мобильных устройств такого класса для использования вместо ноутбуков.

На наш взгляд, с точки зрения возможности создания защищённого мобильного АРМ, в настоящее время большую перспективу имеют планшеты на базе ОС Windows 7.

В.К.ФИСЕНКО, Е.П.МАКСИМОВИЧ

АТТЕСТАЦИЯ. ОБСЛЕДОВАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ И ХРАНЕНИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ И ИНФОРМАЦИОННЫХ ПОТОКОВ В РЕАЛЬНЫХ УСЛОВИЯХ ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ/ИНФОРМАЦИОННЫХ СИСТЕМ

1. Методика обследования технологического процесса

Технологический процесс обработки информации в объектах информатизации/информационных системах (ОИ/ИС) включает в себя следующие основные операции:

– прием и комплектовка первичных документов – проверка полноты и качества их заполнения, комплектовки и т. д.;

– подготовка машинных носителей и контроль за ними;

– ввод данных в ЭВМ;

– контроль, результаты которого выдаются на пульт управления, терминал. Различают визуальный и программный контроль, позволяющий отслеживать информацию на полноту ввода, нарушение структуры исходных данных, ошибки кодирования. При обнаружении ошибки производится исправление вводимых данных, корректировка и их повторный ввод;

– запись входной информации в исходные массивы;

– сортировка (при необходимости);

– обработка данных;

– обеспечение хранения данных;

– выдача информации;

Для обследования технологического операции Заявитель (Владелец) ОИ/ИС представляет:

– документ, содержащий описание принципов построения и описание телекоммуникаций ИС, описание топологии сетей, состава и характеристик используемых телекоммуникационных средств;

– Инструкцию по обеспечению защиты информации ОИ/ИС;

– Инструкцию пользователя;

– Инструкцию администратора безопасности.

Реализация операций технологического процесса определяется показателем: **степень успешности реализации операций.** При этом используется следующий **критерий принятия решений**: если результаты реализации конкретной операции технологического процесса, проведенной на аттестуемом ОИ/ИС в соответствии с указанными выше инструкциями, согласуются с ожидаемыми, то операция реализована. Степень успешности реализации определяет эксперт.

Для определения степени успешности реализации операции используется лингвистическая и количественная шкалы оценок (таблица 1).

Таблица 1 - Соответствие между лингвистической и интервальной шкалами оценок степени успешности реализации операций технологического процесса

Лингвистическая оценка степени соответствия	Интервал количественных оценок
Высокая степень успешности реализации операций	0,75 – 1,0
Допустимая степень успешности реализации операции	0,5 – 0,74
Средняя степень успешности реализации операции	0,25 – 0,49
Низкая степень успешности реализации операции	0,01 – 0,24

Совокупность оценок степени успешности реализации операций определяют качество технологического процесса.

Общая количественная оценка E^{TP} качества технологического процесса вычисляется по формуле:

$$E^{TP} = \frac{\sum_{l=1}^{n} E^{TPl}}{n}$$

где E^{TPl} – количественная оценка экспертом степени успешности реализации операции l, n – количество реальных операций, реализованных (с учетом приведенного выше перечня операций) в обследуемом технологическом процессе аттестуемого ОИ/ИС.

Лингвистическая оценка качества технологического процесса определяется на основании количественной оценки E^{TP} в соответствии с таблицей 1.

Экспертное заключение о качестве технологического процесса формируется на основе следующих правил:

– технологический процесс, общая количественная оценка E^{TP} которого находится в пределах 1,0-0,5, удовлетворяет требованиям качества;

– если количественная оценка E^{TP} находится в пределах 0,49 – 0,01, то созывается согласительное совещание с Заявителем, на котором принимается одно из следующих решений;

1) осуществить доработку реализации технологического процесса в течение периода аттестации и провести повторную его оценку в части проверки устранения выявленных недостатков;

2) в случае отказа Заявителя от доработки принимается решение в отказе выдачи аттестата соответствия.

2. Методика обследования информационных потоков

Информационный поток – это поток сообщений в устной, документной (бумажной, электронной) и других формах внутри ОИ/ИС либо между ОИ/ИС и внешней средой, предназначенный в основном для реализации определенных (управляющих, информационных, почтовых и т.д.) функций. По степени открытости и уровню значимости информационные потоки бывают открытые, закрытые, коммерческие, секретные (конфиденциальные), простые, заказные. Обследование потоков информации дает общее представление о функционировании ОИ/ИС и является первым шагом к оценке информационных потоков.

Для обследования информационных потоков ОИ/ИС Заявитель (Владелец) ОИ/ИС представляет комиссии по аттестации:

– отчет о проблемах качества реализации информационных потоков ОИ/ИС, выявленных в ходе предшествующего периода;

– нормативно-методические и организационно-распорядительные документы по созданию и применению обследуемой системы защиты информации ИС;

– перечни технических средств и программного обеспечения, используемых в системе защиты информации ИС, режимы обработки данных в ИС;

– описания технологических схем обработки и передачи данных (документов) в ИС.

– схемы передачи информации внутри ОИ/ИС, а также между ОИ/ИС и внешней средой;

– Инструкцию по обеспечению защиты информации ОИ/ИС в процессе ее передачи.

Обследование информационных потоков предполагается проводить по заранее разработанной программе, которая включает: изучение структуры и функций подразделений организации, участвующих в информационном обмене; составление перечня входящих и исходящих информационных потоков для каждого подразделения, а также регистрацию всех поступающих и выходящих сообщений; четкое определение процессов формирования и маршрутов движения данных; сбор сведений о типах и назначении передаваемой информации, показателях, содержащихся в конкретных передаваемых документах (сообщениях) и др.

Независимо от вида информационного потока основной целью его реализации является обеспечение надежности передачи информации как внутри ОИ/ИС, так и между ОИ/ИС и внешней средой. Поэтому в качестве **показателя** качества информационного потока целесообразно принять **надежность** его **реализации**.

При этом используется следующий **критерий принятия решений**: если по результатам проверки реализация информационных потоков соответствуют требованиям, сформулированным в представленной документации, то требования реализованы. Степень надежности реализации определяет эксперт.

Для определения степени надежности реализации информационных потоков используется лингвистическая и количественная шкалы оценок (таблица 2).

Совокупность оценок качества выполнения требований к информационным потокам определяет качество реализации информационных потоков в ОИ/ИС.

Общая количественная оценка E^{IF} качества реализации требований к информационным потокам вычисляется по формуле:

$$E^{IF} = \frac{\sum_{l=1}^{k} E^{IFl}}{k},$$

где E^{IFl} – количественная оценка экспертом степени успешности реализации требования l, k – количество требований к информационным потокам в предоставленной документации.

Таблица 2 – Соответствие между лингвистической и интервальной шкалами оценок надежности реализации информационного потока

Лингвистическая оценка надежности реализации	Интервал количественных оценок
Высокая степень надежности реализации	0,75 – 1,0
Допустимая степень надежности реализации	0,5 – 0,74
Средняя степень надежности реализации	0,25 – 0,49
Низкая степень надежности реализации	0,01 – 0,24

Лингвистическая оценка качества реализации требований к информационным потокам определяется на основании количественной оценки E^{IF} в соответствии с таблицей 2.

Экспертное заключение о качестве информационного потока формируется на основе следующих правил:

– информационные потоки, общая количественная оценка E^{IF} которых находится в пределах 1,0-0,5, удовлетворяют требованиям качества;

– если количественная оценка E^{IF} находится в пределах 0,49 – 0,01, то созывается согласительное совещание с Заявителем, на котором принимается одно из следующих решений:

1) осуществить доработку реализации информационных потоков в течение периода аттестации и провести повторную их оценку в части проверки устранения выявленных недостатков;

2) в случае отказа Заявителя от доработки принимается решение в отказе выдачи аттестата соответствия.

Г.В.ФРОЛОВ

К ВОПРОСУ О ТИПИЗАЦИИ И УНИФИКАЦИИ РАЗРАБОТКИ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В настоящее время можно выделить два основных практических подхода к обеспечению безопасности ИТ. В основе первого лежит нормативно-методологическая база образованная Руководящими документами Гостехкомиссии России, второго – ГОСТ Р ИСО/МЭК 15408-2002, являющийся Российским вариантом «Общих критериев» (ОК).

Первый подход содержит элементы типизации проектных и прикладных решений в области защиты информации, в основе которых лежит понятие «класс защищенности». Данный подход обладает несомненными преимуществами, такими как простота практического применения, высокая скорость разработки, применение опробованных проектных и прикладных решений. Однако имеется и существенный недостаток – он учитывает в основном задачи обеспечения конфиденциальности информации, оставляя без должного внимания вопросы обеспечения ее целостности и доступности. Поэтому его применение для разработки систем безопасности ИТ не соответствует современным требованиям.

С принятием в 2004 г. ГОСТ Р ИСО/МЭК 15408-2002 появился новый стандартизированный подход к разработке защищенных ИТ. Однако отсутствие в ОК конкретных типовых требований и критериев для различных типов систем информационных технологий вынуждает разработчиков проектировать системы безопасности «с нуля». При этом в отсутствии развитого методического обеспечения, каждый разработчик реализует свой, неформализованный метод решения поставленной задачи. Как результат, в большинстве сопровождение и модернизация систем безопасности без участия разработчиков невозможна. При этом процесс разработки является сложным и трудоемким.

Отсутствие развитого методического обеспечения обуславливает наличие большого числа неформализованных методов, не имеющих какого – либо серьезного научного обоснования.

В основу практических методов разработки защищенных ИТ могут быть положены принципы формирования алгоритмов, применяемых для решения задач распознавания и классификации, к которым, при некоторой идеализации, приводятся любые задачи принятия решений, в том числе и задачи разработки защищенных ИТ.

Предлагается основывать типовые решения в области защиты информации на технологии «перекрытия угроз».

В технологии «перекрытия угроз» рассматривается взаимодействие «области угроз», «защищаемой области» (ресурсов АС) и «системы защиты» (механизмов безопасности ИТ). Использование данной технологии при разработке системы защиты ИТ требует создания соответствующих моделей. На практике построение таких моделей затруднено, т. к. эти понятия недостаточно формализованы и систематизированы. В отсутствие универсального подхода к определению угроз и объектов защиты информационных технологий каждый разработчик реализует свой неформализованный метод их определения для каждой конкретной ИТ. При этом отсутствуют гарантии качества полученного результата и возможности его использования в других разработках.

На основе технологии «перекрытия угроз» возможны различные варианты реализации систем безопасности:

– непосредственная нейтрализация самих угроз;

– защита объектов;

– системы защиты с полным перекрытием угроз.

Для выбора варианта реализации системы приемлемого качества была применена методология оценки качества систем по следующим критериям: пригодности, оптимальности и превосходства.

Предлагается рассматривать следующие существенные свойства систем, отсутствие которых приводит к потере того качества, которое связывалось с информационной безопасностью ИТ:

– Типизация;

– Полнота;

– Реализуемость.

По показателям этих свойств производится оценка качества. Для характеристики свойств системы использованы качественные показатели, определяющие наличие (отсутствие) существенных свойств.

В результате анализа был сделан следующий вывод. Из всех перечисленных выше вариантов реализации систем безопасности все качественные характеристики обеспечиваются для систем с «полным перекрытием угроз». Необходимым условием для этого является определенность объектов защиты и угроз на уровне детализации, предложенном в данной работе.

В связи с этим первым этапом решения поставленной задачи было выделение объектов защиты в современных ИТ, классификация и описание множества угроз безопасности ИТ.

Описание защищенного состояния системы ИТ (S) можно представить в виде следующей схемы:

$$S_{ijnm} = \{ O_{i,} T_{ij,} C_{ijn,} F_{ijnm}\}$$

где O_i – множество структурных компонентов ИТ;

T_{ij} – множество угроз i-му структурному компоненту ИТ;

C_{ijn} – множество сервисов безопасности, противодействующих j-ой угрозе;

F_{ijnm} – множество требований по реализации n-го сервиса безопасности, противодействующего j-ой угрозе на i-й структурный компонент ИТ.

Схема S_{ijnm} может быть достигнута после выполнения цепочки процедур, которые можно представить в виде операторов - построения базы данных угроз (P_b), построения модели угроз (P_j), разработки системы мер по защите (P_n), построения профиля защиты (P_m):

$$P_b : \{T_{j,} DBJ\} => B_j$$

$$P_j : \{S_{i,} B_j\} => S_{ij}$$

$$P_n : \{S_{ij,} B_n\} => S_{ijn}$$

$$P_m : \{S_{ijn,} B_m\} => S_{ijnm}$$

где DBJ – инструментарий разработки БД, который должен позволять реализовать БД угроз на основе заданной классификации угроз T_j;

B_j – база данных угроз безопасности;

B_n – база данных мер противодействия угрозам (сервисов безопасности);

B_m – база данных требований безопасности;

S_i – множество структурных компонентов системы;

S_{ij} – модель угроз;

S_{ijn} – система мер противодействия.

Задача построения защищенной ИТ может быть сформулирована в виде оператора:

$$P_r : \{S_{i,} B_{j,} B_{n,} B_{m,} z\} => S_{ijnm}$$

где Z – множество задач, которое должно быть решено, для того, чтобы реализовать мероприятия по защите на заданном уровне доверия.

Каждую угрозу можно рассматривать как процедуру, осуществление которой приводит к ущербу ИТ. Ущерб предлагается выражать в категориях конфиденциальности, целостности и доступности. Кроме того, угрозы можно рассматривать как проявление факторов, воздействующих на защищаемую информацию по ГОСТ 51275-99. Согласно данному стандарту фактор-явление, действие, процесс, результатом которых может быть утечка, искажение, уничтожение, блокирование доступа к информации.

Задача построения таксономии угроз может быть выражена в виде оператора:

$$P_j : \{S_{i,} K_{il,} Fa_y \} => T_j$$

где K_{il} – категория ущерба i-го структурного компонента ИТ;

Fa_y – фактор, воздействующий на информацию.

Данное выражение позволяет сформулировать следующие принципы таксономии угроз:

Таксономия угроз должна соответствовать множеству структурных компонентов ИТ;

Таксономия угроз должна соответствовать категориям ущерба;

Таксономия угроз должна соответствовать таксономии факторов, воздействующих на защищаемую информацию.

Очевидно, что такое представление угроз закладывает возможность при реализации системы обеспечения безопасности ИТ решать такие задачи как:

– контроль возможностей системы защиты по противодействию угрозам на структурные компоненты ИТ,

– контроль возможного ущерба при реализации угроз,

– контроль возможностей системы защиты по противодействию негативному воздействию факторов, действующих на объект информатизации.

Задача разработки баз данных сервисов безопасности и требований безопасности может быть сформулирована в виде операторов:

$$P_n : \{T_n, DBN\} => B_n$$
$$P_m : \{T_m, DBM\} => B_m$$

где T_n и T_m – заданные классификации сервисов и требований безопасности,

DBN и DBM – инструментарии разработки баз данных.

Принципы таксономии сервисов и требований безопасности аналогичны принципам таксономии угроз.

Для требований безопасности дополнительно сформулирован еще один принцип таксономии: таксономия требований безопасности должна соответствовать множеству сервисов безопасности. В приложении к разработке базы данных требований безопасности этот принцип означает, что каждому сервису безопасности должно соответствовать множество требований по его реализации.

В качестве объектов защиты ИТ выделены:

– технические средства ИТ (ТС);

– программные средства ИТ (ПС);

– каналы связи (КС);

– данные (Д);

– технологический процесс (ТП).

В основу определения угроз безопасности ИТ положена идея взаимоувязывания угроз с объектами защиты ИТ, что предполагает наличие пяти классов угроз, соответствующих выделенным объектам защиты ИТ. Описание угроз безопасности должно обеспечить возможность идентификации угроз безопасности в среде функционирования ИТ различных масштабов, архитектуры и области применения, т.е. описанные угрозы должны быть типовыми. Для этого предлагается описывать угрозы на уровне детализации, соответствующем пяти выделенным структурным компонентам ИТ.

Помимо построения моделей угроз и защищаемой области разработчик защищенной ИТ описывает множество мер противодействия, которые должны перекрыть пути осуществления угроз безопасности к защищаемым объектам. Как правило, угроза может быть реализована несколькими способами, поэтому следует говорить о множестве путей осуществления, связанных с угрозой безопасности ИТ. Отсюда следует, что каждой угрозе должны быть сопоставлены соответствующие множества мер противодействия. Так как в нашем случае описываются типовые угрозы ИТ, то им можно сопоставить типовые меры противодействия.

Наиболее важным моментом при использовании технологий, основанных на использовании типовых решений, является базовое определение типового элемента.

Для решения данной задачи систему защиты ИТ предлагается трактовать как совокупность сервисов (услуг) безопасности, предоставляемых прикладной подсистеме ИТ. В этом случае сервис рассматривается, как способность системы безопасности ИТ реализовать определенную типовую меру противодействия угрозе. Следовательно, для

противодействия угрозе должно быть реализовано множество типовых сервисов безопасности, соответствующее множеству типовых мер противодействия.

Таким образом, система защиты ИТ представляет собой совокупность сервисов безопасности, которые могут быть реализованы в среде функционирования ИТ, в самой ИТ (путем использования защищенных средств ИТ) или средствами защиты информации.

Предлагаемый подход обеспечивает полное перекрытие угроз, т. к. каждому классу объектов соответствует весь перечень возможных угроз, как для всего класса объектов, так и для каждого объекта в классе.

Так как каждой угрозе поставлен в соответствие перечень сервисов безопасности, обеспечивающих полное перекрытие конкретной угрозы, то все множество сервисов безопасности обеспечивает полное перекрытие множества всех угроз.

Каждому типовому сервису безопасности сопоставлены множества требований безопасности. Эти множества разработаны на основе каталога требований безопасности, содержащегося в ОК.

Из подхода к моделированию системы безопасности ИТ как совокупности типовых сервисов безопасности следует, что сервисный подход целесообразно применить и к описанию прикладных решений в области защиты информации. Средство ИТ или средство защиты, реализующее типовой сервис безопасности в данном случае можно рассматривать как типовое. Для оценки способности средств ИТ или средств защиты информации реализовывать сервисы безопасности, каждому сервису безопасности сопоставлены множества требований безопасности, разработанные на основании каталога функциональных требований безопасности ОК.

РАЗДЕЛ 5
ТЕХНИЧЕСКИЕ ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

Г.А.ГРУДЕЦКИЙ, И.В.СТРИЖАК

ИСПОЛЬЗОВАНИЕ НАВИГАЦИОННОГО ПРИЕМНИКА В КОМПЛЕКСЕ РАДИОМОНИТОРИНГА И ПЕЛЕНГАЦИИ.

В последнее время с развитием техники и электроники широкое развитие получили различные системы радиосвязи, системы передачи информации и другие радиотехнические устройства, которые в некоторых случаях могут являться источниками несанкционированных излучений (ИНИ). Данными источниками могут быть как самодельные (радиолюбительские), так и промышленно изготовленные системы и устройства.

Для борьбы с такими устройствами применяются системы радиомониторинга (определение частоты сигнала и мощности) и пеленгации (определение направления и местоположения). Данные системы производят выявление ИНИ и, в последующем, определение его местоположения. Системы можно разделить на стационарные, мобильные или комплексные (стационарные и передвижные). Стационарные системы представляют собой сооружения, обладающие соответствующей инфраструктурой и располагающиеся в определенных точках на местности. Они включают в себя большие антенные системы, позволяющие обеспечить хорошую чувствительность сигнала и высокое частотное разрешение. Недостатком таких сооружений является их высокая стоимость, а также для выполнения функций пеленга источников излучений, сооружений должно быть достаточное количество.

Передвижные системы представляют собой транспортные средства, которые оснащены необходимым оборудованием с антенной системой. Достоинствами таких систем являются мобильность (некоторые системы позволяют вести радиомониторинг и пеленг в движении), высокая скорость нахождения источника излучения и относительно невысокая стоимость. Недостатками данных систем являются низкая чувствительность по уровню сигналов и ограниченное частотное разрешение (низкие частотные диапазоны требуют громоздких антенных систем).

Комбинированные системы состоят из стационарных систем и дополняются подвижными системами, которые участвуют в уточнении места расположения источника излучения на местности.

В настоящее время при пеленгации источника излучения недостаточно знать направление на источник (угол пеленга), однако, необходимо знать точные координаты источника, которые должны быть отображены на карте местности.

Алгоритм функционирования комбинированной системы для нахождения источника излучения можно разбить на следующие этапы:

– сканирование частотного диапазона;

– выявление ИНИ по определенным признакам;

– определение направления на ИНИ (пеленг) стационарными системами;

– вычисление зоны нахождения ИНИ по данным пеленга стационарных систем;

– определение координат ИНИ с помощью мобильной системы (получение данных координат от навигационной спутниковой системы).

Спутниковые навигационные системы (СНС) в настоящее время получили широкое распространение во всем мире в разнообразных отраслях науки и техники.

В мире существует несколько основных спутниковых систем, созданных ведущими мировыми державами, которые являются лидерами в области разработки космической техники. Страны, создавшие спутниковые системы, в первую очередь решают проблемы покрытия навигационной системой своей территории для выполнения своих государственных задач в области обороны, науки и техники. Страны, которые не имеют собственных навигационных систем, вынуждены ориентироваться на системы соседних государств. Среди навигационных систем хочется отметить ГЛОНАСС (российская навигационная система) и GPS (навигационная система США). Спутниковая навигационная система GPS покрывает почти всю территорию земного шара. Второй по покрытию является система ГЛОНАСС, которая еще полностью не развернута в связи с недостаточным количеством спутников, также разворачивают свои системы Евросоюз и Китай. Современные спутниковые навигационные приемники могут поддерживать несколько разных спутниковых навигационных систем. На территории Республики Беларусь уверенно принимаются спутниковые навигационные системы ГЛОНАСС и GPS, поэтому при использовании навигационных систем необходимо ориентироваться на прием сигналов от этих системы.

Для приема сигналов СНС потребителями используются навигационные приемники. Одним из них является приемник ЗАО «КБ Навис». Из навигационных приемников, работающих по открытым гражданским кодам и выпускаемых серийно, был выбран СН-4706. Данный приемник обладает хорошими техническими и технологическими параметрами.

Основные достоинства данного приемника:

– поддержка (СНС) ГЛОНАСС/GPS;

– стандартные протоколы (NMEA,BINR) навигационных данных;

– стандартные интерфейсы передачи данных (RS-232);

– хорошие параметры по точности и времени получения данных в режимах «теплого и холодного старта»;

– небольшие габариты и поверхностный монтаж;

– требуется минимальное количество дополнительных элементов для работы.

В системе радиомониторинга и пеленга навигационный приемник входит в состав модуля «Навигатора».

Функциональная схема «Навигатора» состоит из следующих частей:

– навигационный приемник СН-4706;

– микропроцессор;

– контролер RS-232/USB;

– электронный компас;

– стабилизаторы питания.

Навигационный приемник выполняет следующие функции:

– получение данных от СНС (ГЛОНАСС/GPS);

– определение координат местоположения по данным СНС (ГЛОНАСС/GPS);

– формирование меток времени;

– выдача данных в формате двух протоколов NMEA, BINR по интерфейсу RS-232.

Микропроцессор производит настройку и инициализацию навигационного приемника.

Контролер RS-232/USB производит преобразование интерфейсов для последующей передачи данных в ЭВМ.

Электронный компас осуществляет выдачу угловых данных на северный магнитный полюс, используется для привязки данных направления пеленга к карте.

Стабилизаторы питания формируют необходимые по уровню напряжения для работы навигационного приемника и других частей модуля.

Кроме элементов модуля для работы навигационного приемника используется внешняя активная антенна рекомендованная производителем приемника.

При работе навигационного приемника данные передаются в ЭВМ. Программа производит обработку данных, устанавливает на электронной карте маркер (привязка к карте) в соответствии с координатами, определенными навигационным приемником, также на карту наносится направление пеленга (угол пеленга) на ИНИ. При перемещении мобильного пеленгатора или при использовании данных от другого пеленгатора (угол пеленга) на этот ИНИ производится расчет зоны возможного нахождения излучения. Данные используются от многих стационарных станций пеленга, точность при этом будет выше, а зона нахождения источника излучения меньше по площади. Пересечение линий пеленга на карте дает точку нахождения ИНИ, которая представляется также в виде координат, вычисленных по пересечению линий пеленга. На точность вычисления точки влияют следующие факторы:

– погрешность определения угла пеленга, которая обусловлена различными факторами, а именно, такими как физическое распространение радиоволн в пространстве (дифракция, интерференция, …);

– ошибки данных определения места навигационным приемником;

– ошибки привязки угловых величин к карте (погрешность компаса);

Существенное влияние в данных погрешностях вносит природа распространения радиоволн. Радиоволна не всегда приходит в приемное устройство пеленгатора по кратчайшему пути, причиной этому являются препятствия на пути радиоволн, которые они и огибают при распространении в пространстве. Данная проблема наиболее актуальна в городе с высотными зданиями и возможные пути решения - это подъем приемных антенн и перемещение пеленгатора к месту вероятного излучения источника. При приближении к источнику, сигнал, приходящий от источника, становится больше переотраженного сигнала приходящего с других сторон.

Ошибки определения места навигационным приемником можно разбить на категории:

– ошибки системы;

– ошибки, связанные с распространением навигационного сигнала;

– ошибки приемной аппаратуры.

Для повышения точности получаемых координат используется глобальная система дифференциальных поправок WAAS/EGNOS. Система дифференциальных поправок состоит из наземных станций и геостационарных спутников, которые позволяют скорректировать ионосферные задержки.

Таким образом, навигационный приемник с комплектом программного обеспечения и электронными картами в автоматическом режиме определяет место расположения ИНИ, освобождая при этом оператора от этих действий. Навигационные системы также можно использовать для ведения наблюдения за перемещением объекта с источником излучения (закладкой) на карте местности.

Благодаря использованию навигационных приемников существенно повышается эффективность использования систем пеленгации ИНИ. Приемники также позволяют существенно сократить время определения источника и своевременно реагировать на их действия.

В.А.ДМИТРИЕВ, О.Ю.КОНДРАХИН

ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ СВЕРХКОРОТКИХ (СВЕРХШИРОКОПОЛОСНЫХ) ЭЛЕКТРОМАГНИТНЫХ ИМПУЛЬСОВ

Актуальность задач защиты информации от утечки по техническим каналам несомненна и занимает ведущее место в общем ряду существующих в области безопасности информации проблем. Ряд современных, в первую очередь технических реалий, заставляет по-новому взглянуть на каналы утечки информации. В частности, это связано со стремительным развитием и широким распространением миниатюрных технических средств обработки информации. Дорогостоящие предварительные проверки объектов информатизации на наличие средств съема информации теряют смысл в случае проноса такой аппаратуры непосредственно на объект. А обнаружение подобных устройств при вносе практически невозможно в силу специфики применения технических средств обнаружения устройств съема.

Сложность обнаружения современных миниатюрных технических средств обработки информации заключается в том, что, с одной стороны, требуется аппаратура, позволяющая регистрировать очень слабое электромагнитное излучение работающего миниатюрного технического средства обработки информации. С другой стороны, она не должна реагировать на промышленные помехи и на излучения других приборов, которые могут быть значительными. Причем частотный диапазон, характер и форма электромагнитных колебаний от миниатюрного технического средства обработки информации и от источников помех могут во многом совпадать. Кроме того, профессиональные миниатюрные технические средства обработки информации имеют весьма серьезные конструктивные и схемотехнические методы защиты узлов, подверженных действию помех.

Принципиально по-новому решается задача защиты информации от ее несанкционированного прослушивания и перехвата в радиосвязи с сверхкороткими (сверхширокополосными) импульсами. При этом речь идет не о кодировании передаваемой информации, а о том, что часто затруднено обнаружение самого факта передачи информации. Это достигается за счет очень низкой спектральной плотности излучаемого сигнала, что и обеспечивает очень высокий уровень их энергетической скрытности (см., например, [1]). Кроме того, даже в случае обнаружения самого сигнала оценка его параметров (передаваемой информации) без знания вида передаваемого сигнала и его параметров в этих условиях становится нерешаемой задачей.

В настоящее время в развитии телекоммуникационных технологий наблюдается интенсивное освоение сверхкоротких (сверхширополосных) электромагнитных импульсов, длительность которых составляет от 0,2 до 1,0 наносекунды, а частота занимает сверхширокополосный интервал в несколько гигагерц. Сверхкороткие (сверхширокополосные) электромагнитные импульсы удовлетворяют условию [2]

$$0.01 < \mu < 0.2,$$

$$\mu = \frac{\Delta f}{f_o} = 2\frac{f_{max} - f_{min}}{f_{max} + f_{min}},$$

где Δf – ширина полосы сигнала,

f_0, f_{min}, f_{max} – центральная, минимальная и максимальная частоты.

При воздействии сверхкоротких (сверхширокополосных) электромагнитных импульсов на технические средства обработки информации наводятся сигналы, нарушающие функционирование таких технических средств. Поражающее действие сверхкоротких (сверхширокополосных) электромагнитных импульсов в помещении существенно возрастает. Это вызвано отражениями сигналов от стен и переизлучениями от металлических

конструкций, что создает дополнительный вклад в суммарную энергию воздействия. Благодаря сверхширокополосности, затухание сверхкоротких электромагнитных импульсов в различных средах оказывается достаточно незначительным, поскольку их подавление обычно происходит не во всем диапазоне. Поэтому сверхкороткие (сверхширокополосные) электромагнитные импульсы могут использоваться в блокираторах технических средств обработки информации.

Спектральная мощность этих сигналов очень мала. Сигнал как бы "размыт" и напоминает обычный шумовой фон. Для традиционных средств связи он не доступен не только к приему, но даже и к определению самого факта своего существования.

Для защиты информации от ее утечки по техническим каналам может использоваться генератор шумоподобного сверхширокополосного сигнала, располагаемый вблизи технического средства обработки информации в качестве передатчика сигналов противодействия, а именно:

− устройств подслушивания радио- и телефонных переговоров;

− устройств дистанционного съема информации с технических средств обработки информации;

− постановки помех переносным радиостанциям.

Литература

1. Цветнов В.В., Демин В.П., Куприянов А.И. Радиоэлектронная борьба: радиомаскировка и помехозащита − М.: МАИ, 1999, 240 с.

2. Лазоренко О.В., Черногор Л.Ф. Сверхширокополосные сигналы и физические процессы. 1. Основные понятия, модели и методы описания // Радиофизика и радиоастрономия. – 2008. − № 2. – С. 166-194.

В.Т.ЕРОФЕЕНКО, Г.Ч.ШУШКЕВИЧ

ЭКРАНИРОВАНИЕ ТЕХНИЧЕСКИХ УСТРОЙСТВ В КОМПЛЕКСНОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Введение. Передача и обработка информации в средствах вычислительной техники (СВТ) основывается на использовании электромагнитных процессов в электронных элементах техники. Электрические токи и заряды в сосредоточенных электродах возбуждают побочные электромагнитные излучения (ПЭМИ), которые распространяются в окружающее пространство, охватывают некоторые области вокруг источника и затухают при удалении от СВТ. Такое поле является носителем информационных сигналов, обрабатываемых в СВТ, и, одновременно, каналом утечки информации. При наличии измерительной техники напряженность электрического поля, большая, чем некоторое значение $\vec{E}_{изм}$, измеряется и может быть использована для доступа к конфиденциальной информации [1]. Помимо ПЭМИ в пространстве распространяются электромагнитные шумы с уровнем электрической напряженности $\vec{E}_{шум}$. В результате зона перехвата $D_{зп}^{ист}$ определяется областью пространства, в которой $\left|\vec{E}_{пэми}\right| > E_{кр} = \max(\vec{E}_{изм}, \vec{E}_{шум})$. Поверхность в пространстве $S_{кр}$, задаваемая уравнением $\left|\vec{E}_{пэми}\right| = E_{кр}$, охватывает область $D_{зп}^{ист}$ вокруг источника. При установке экранов вблизи СВТ область $D_{зп}^{ист}$ уменьшается и деформируется в область $D_{зп}^{экр}$.

Лазерный принтер является одним из устройств СВТ, который преобразует электронную информацию в информацию на бумажном носителе. Основой представления информации на принтере служит строка, состоящая из 600-1200 пикселей на дюйм длины

строки. Луч лазера, сканируя строку, последовательно снимает электрический заряд с пикселей в соответствии с рисунком. Информация о рисунке поступает на электрод лазера в виде последовательности импульсов электрического тока. В свою очередь, импульсы тока, чередующиеся с определенной частотой, возбуждают в спектральном разложении электрическое поле (ПЭМИ), которое заполняет область $D_{зп}^{ист}$ вокруг принтера и может быть использовано для перехвата изображения. В данной работе электрод лазера моделируется электрическим диполем, который колеблется с круговой частотой ω. Поле диполя экранируется тонкой незамкнутой сферической оболочкой, выполненной из магнитодиэлектрического проводящего материала.

Постановка задачи. В пространстве R^3 с диэлектрической проницаемостью ε_0 и магнитной проницаемостью μ_0 расположена полупрозрачная тонкостенная незамкнутая сферическая оболочка Γ_Δ толщины Δ (рис.1). Оболочка Γ_Δ выполнена из материала с электромагнитными параметрами ε, μ, γ: ε – диэлектрическая проницаемость, μ – магнитная проницаемость, γ – удельная электрическая проводимость. Она расположена на поверхности сферы Γ_1 радиуса a, круговое отверстие имеет угол раствора θ_0. Оболочку Γ_Δ заменим на идеальную поверхность $\Gamma = \left\{ r = a, \theta_0 \le \theta \le \pi,\ 0 \le \varphi \le 2\pi \right\}$.

В пространстве распространяется первичное низкочастотное электрическое поле с электрическим потенциалом u_0, колеблющимся с круговой частотой ω. Для электрического потенциала $u_1 = u_0 + u_1'$ поля внутри сферической поверхности и для потенциала u_2 вне поверхности Γ_1 сформулируем краевую задачу экранирования со специальными граничными условиями на поверхности экрана Γ [2]:

$$\Delta u_1' = 0, \quad 0 \le r < a, \qquad \Delta u_2 = 0, \quad r > a; \tag{1}$$

$$u_1\big|_{\Gamma_1 \setminus \Gamma} = u_2\big|_{\Gamma_1 \setminus \Gamma}, \qquad \left.\frac{\partial u_1}{\partial \vec{n}}\right|_{\Gamma_1 \setminus \Gamma} = \left.\frac{\partial u_2}{\partial \vec{n}}\right|_{\Gamma_1 \setminus \Gamma}, \quad 0 \le \theta < \theta_0; \tag{2}$$

$$u_1\big|_\Gamma = u_2\big|_\Gamma + V, \quad V - \text{const}, \quad \left.\frac{\partial (u_2 - u_1)}{\partial \vec{n}}\right|_\Gamma = -apF(u_2 + u_1)\big|_\Gamma, \quad \theta_0 < \theta \le \pi, \tag{3}$$

где $\vec{n} = \vec{e}_r$ – внешний нормальный единичный вектор к поверхностям Γ, $\Gamma_1 \setminus \Gamma$,

$$F(u) = -\frac{1}{r^2}\frac{\partial}{\partial r}\left(r^2 \frac{\partial u}{\partial r}\right), \quad p = \frac{\varepsilon' \delta}{2\varepsilon_0 a}, \quad \delta = \frac{2}{k} \operatorname{tg} \frac{k\Delta}{2}, \quad k = \omega\sqrt{\varepsilon' \mu}; \quad 0 \le \arg k < \pi,$$

$$\varepsilon' = \varepsilon + i\frac{\gamma}{\omega},$$

при чем потенциал u_2 должен удовлетворять условию на бесконечности

$$u_2(M) \to 0 \quad \text{при} \quad M \to \infty. \tag{4}$$

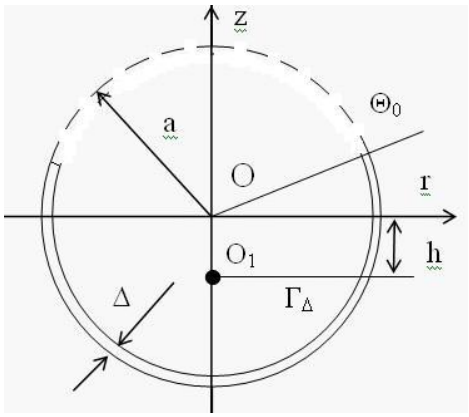


Рис 1. Геометрия задачи

Решение краевой задачи. Представим решение задачи (1)–(4) в виде суперпозиции по базисным решениям уравнения Лапласа в сферической системе координат так, чтобы выполнялось условие на бесконечности (4):

$$u_1' = \sum_{n=0}^{\infty} x_n \left(r/a\right)^n P_n\left(\cos\theta\right), \quad 0 \le r < a, \qquad u_2 = \sum_{n=0}^{\infty} y_n \left(a/r\right)^{n+1} P_n\left(\cos\theta\right), \quad r > a, \qquad (5)$$

где x_n, y_n – неизвестные коэффициенты, подлежащие определению; $P_n\left(\cos\theta\right)$ – полиномы Лежандра.

В качестве первичного электрического поля возьмем поле электрического диполя, ориентированного вдоль оси Oz и расположенного в точке $O_1(0,0,-h)$ внутри сферы Γ_1:

$$u_0 = \frac{p}{4\pi\varepsilon_0}\frac{\cos\theta_1}{r_1^2} = \overline{p}\frac{1}{r_1^2}P_1(\cos\theta_1), \quad \overline{p} = \frac{p}{4\pi\varepsilon_0},$$

где p – электрический момент, $\{r_1, \theta_1, \varphi\}$ – сферические координаты с началом в точке O_1. Полярность диполя меняется с частотой f, $\omega = 2\pi f$ – круговая частота.

Потенциал этого поля в окрестности сферической оболочки представим в виде ряда:

$$u_0 = \sum_{n=0}^{\infty} b_n \left(a/r\right)^{n+1} P_n\left(\cos\theta\right), \quad r > h, \qquad b_0 = 0, \qquad b_n = (-1)^{n+1}\frac{\overline{p}\,n}{a^2}\left(h/a\right)^{n-1}, n \ge 1. \quad (6)$$

Учитывая представления (5), (6) и выполняя граничные условия (2), (3) с учетом разложения

$$f(\theta) = \begin{cases} 0, & 0 \le \theta < \theta_0, \\ V, & \theta_0 < \theta \le \pi \end{cases} = \sum_{n=0}^{\infty} f_n P_n(\cos\theta),$$

получим соотношение между коэффициентами x_n, y_n:

$$x_n = f_n + y_n - b_n,$$

где $f_0 = 0{,}5V(1+\cos\theta_0)$ $\qquad f_n = \dfrac{2n+1}{2n(n+1)} V \sin\theta_0 P_n^1(\cos\theta_0), \quad n \ge 1,$

и парные сумматорные уравнения по полиномам Лежандра вида:

$$\begin{cases} \displaystyle\sum_{n=0}^{\infty}\left(1-g_n\right) T_n P_n\left(\cos\theta\right) = \sum_{n=0}^{\infty}\left(\alpha_n b_n + \beta_n f_n\right) P_n\left(\cos\theta\right), & 0 \le \theta < \theta_0, \\ \displaystyle\sum_{n=0}^{\infty}\left(2n+1\right) T_n P_n\left(\cos\theta\right) = 0, & \theta_0 < \theta \le \pi, \end{cases} \qquad (7)$$

где $\alpha_n = n(n+1)(2n+1)p^2/\Delta_n$, $\beta_n = n(n+1)p^2/2\Delta_n$, $\Delta_n = 2n+1+2n(n+1)p$,

$$g_n = \frac{2n+1-p/2}{2n+1+2n(n+1)p}, \quad (2n+1)T_n = \Delta_n y_n - (2n+1)b_n + n(1+(n+1)p)f_n,\ n = 0,1,\ldots .$$

Если ввести в рассмотрение новую функцию $\varphi(t)$ по формуле

$$T_n = \int_0^{\theta_0} \varphi(t)\cos(n+0,5)t\,dt, \quad n = 0,1,2,\ldots,$$

то парные сумматорные уравнения (7) можно преобразовать к регулярному интегральному уравнению Фредгольма второго рода [3]

$$\varphi(x) - \int_0^{\theta_0} K(x,t)\varphi(t)dt = G(x), \quad 0 \le x \le \theta_0, \tag{8}$$

где $K(x,t) = K_0(x,t) + K_1(x,t)$, $K_0(x,t) = (\mathrm{lnctg}((x+t)/4) + \mathrm{lnctg}(|x-t|/4))/\pi p$,

$$K_1(x,t) = \sum_{n=0}^{\infty} d_n C_n(x,t)/\pi, \quad C_n(x,t) = \cos(n+0,5)t\cos(n+0,5)x,$$

$$d_n = \frac{2-(2n+1)(p+4/p)}{(2n+1)(2n+1+2n(n+1)p)}, \quad G(x) = \frac{2}{\pi}\sum_{n=0}^{\infty}(\alpha_n b_n + \beta_n f_n)\cos(n+0,5)x .$$

Поверхности уровней электрического поля вне оболочки. Реальное электрическое поле вне оболочки Γ_1 определяется формулой

$$\vec{E}_2 = \mathrm{Re}(-\mathrm{grad}\,u_2 \exp(-i\omega t)) = Y_1(r,\theta,\bar{t})\vec{e}_r + Y_2(r,\theta,\bar{t})\vec{e}_\theta,$$

$$Y_1(r,\theta,\bar{t}) = a^{-1}\sum_{n=1}^{\infty}(n+1)\bar{y}_n(a/r)^{n+2}P_n(\cos\theta), \quad Y_2(r,\theta,\bar{t}) = -a^{-1}\sum_{n=1}^{\infty}\bar{y}_n(a/r)^{n+2}P_n^1(\cos\theta), \tag{9}$$

$$\bar{y}_n = \mathrm{Re}(y_n \exp(-2\pi i\bar{t})), \quad 0 \le \bar{t} \le 1, \quad \bar{t} = t/T - \text{безразмерное время.}$$

Поверхности уровня вторичного поля определяются уравнением

$$|\vec{E}_2| = \sqrt{Y_1^2(r,\theta,\bar{t}) + Y_2^2(r,\theta,\bar{t})} = E_{const},$$

а первичного –

$$|\vec{E}_0| = \sqrt{B_1^2(r,\theta,\bar{t}) + B_2^2(r,\theta,\bar{t})} = E_{const}.$$

Величины $B_1(r,\theta,\bar{t})$, $B_2(r,\theta,\bar{t})$ вычисляются по формулам (9), заменив $\bar{y}_n$ на b_n.

Если диполь находится в центре сферы, то

$$|\vec{E}_0| = |\bar{p}|\sqrt{1+3\cos^2\theta}\cos(2\pi\bar{t})/r^3.$$

При $\bar{t} = 0$ рассмотрим уравнение $|\bar{p}|\sqrt{1+3\cos^2\theta}/r^3 = E_{kp}$. Из этого уравнения находим r:

$$r = \sqrt[6]{|\bar{p}|^2(1+3\cos^2\theta)/E_{kp}^2} \quad \text{или} \quad r = \sqrt[3]{2\bar{p}/E_{kp}} \quad \text{при} \quad \theta = 0. \tag{10}$$

Поверхность, задаваемая уравнением (10), охватывает зону $D_{зп}^{ист}$, внутри которой может быть осуществлен перехват информации на частоте ω при отсутствии экрана Γ. В случае присутствия экрана Γ опасная зона $D_{зп}^{экр}$ ограничена поверхностью

$$\sqrt{Y_1^2\left(r,\theta,\overline{t}\right)+Y_2^2\left(r,\theta,\overline{t}\right)}=E_{кр}\,. \qquad (11)$$

В уравнении (11) $\overline{t}$ выбираем из условия, что область $D_{зп}^{экр}$ максимальна.

Для некоторых геометрических параметров экрана проведен вычислительный эксперимент, при этом полагалось, что $E_{изм}=10^{-8}$ В/м, момент электрического диполя $p=4/9\cdot10^{-14}$ Кл$\cdot$м.

Литература

1. Бузов, Г.А. Защита от утечки информации по техническим каналам / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая линия – Телеком, 2005. – 416 с.

2. Ерофеенко, В.Т. Аналитическое моделирование в электродинамике / В.Т.Ерофеенко, И.С. Козловская. – Мн.: БГУ, 2010. – 303 с.

3. Шушкевич, Г.Ч. Расчет электростатических полей методом парных, тройных уравнений с использованием теорем сложения / Г.Ч.Шушкевич. – Гродно: ГрГУ, 1999. – 237 с.

В.К.ЖЕЛЕЗНЯК

КОМЛЕКС ИЗМЕРИТЕЛЬНЫЙ ПРОГРАММНО-АППАРАТНЫЙ «ФИЛИН-А»

В «Концепции национальной безопасности Республики Беларусь» на государственном уровне сформулированы стратегические цели системного формирования и реализации национальной безопасности по различным направлениям. В частности, приоритетным направлением (п. 54) является совершенствование нормативной и правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности... Кроме того, активно продолжиться разработка и внедрение современных методов и средств защиты информации…»

В Республике Беларусь интенсивно развиваются информационные технологии. Информационные технологии основаны на сведениях (знаниях), циркулирующих между объектами, и обеспечивают их эффективное сигнальное формирование, высококачественную передачу с высокой производительностью и большой гибкостью. Информационные технологии реализуются компьютерными и автоматизированными системами. Автоматизированная система (АС) – автоматизированный целенаправленный комплекс программно-аппаратных средств, предназначенных для обработки информации, физическую среду передачи информационных массивов, формирование управляющих решений для точной оценки состояния функционирования и функционально-допускового контроля АС. На информационно технологическом уровне обеспечивается защищенность от НСД к информации с обеспечением достоверности, конфиденциальности, сохранности, целостности, а также техническая защита информации от ПЭМИН.

Важнейшей составной частью массивов информации является семантическая, определяемая ее содержательностью первичного и вторичного речевого и видео-сигнала, преобразованного для визуального наблюдения и регистрации, а также преобразованные в цифровую или знаковую форму.

Оценка защиты информации от утечки по техническим каналам связана с измерительной информацией, информационный параметр которой с заданной степенью точности функционально связан с информационными параметрами сигнала и должен измеряться с достаточно высокой точностью.

На примере семантической информации рассмотрена защита и ее оценка. Речевой сигнал может представляться первичным (аналоговым), вторичным (преобразованный в электрический сигнал, цифровым, преобразованного из аналогового сигнала для передачи по каналу связи).

Исследование каналов утечки возможно системным методом. Системный метод исследований определяет:

– множество элементов каждой системы, взаимосвязь которых обуславливает целостное свойство этого множества;

– выявляет множество связей и отношений внутри систем и связи с внешней средой.

Процесс исследования сложной системы, включающей три модели, соединенные в единое целое, позволяет установить каналы утечки информации. Первая модель включает каналы утечки информации (КУИ) аналогового речевого сигнала, вторая модель устанавливает каналы утечки информации речевой информации, преобразованную в цифровую форму. Возможно выделить в отдельную модель каналы утечки при взаимном воздействии первой модели на вторую и наоборот. Третья модель формируется для оценки параметров измерительной информации, обусловленных прохождением их через КУИ, обусловленных речевым сигналом.

На основании модели разработан комплекс измерительный программно-аппаратный (КИПА) «ФИЛИН-А» в виде локальной измерительной схемы, заменяющей несколько приборов (генератор сигналов низкочастотный, селективный вольтметр, осциллограф, нановольтметр). Измеряет величину разборчивости речи по слабым сигналам в шумах высокого уровня в соответствии с требованиями нормативно-методических документов по противодействию акустической речевой разведке. Обеспечивает полноту оценки объекта. Высокая точность измерений, производительность, воспроизводимость результатов. Комплекс удобен в эксплуатации. Измерительные преобразователи помехозащищены. Акустические системы практически не излучают магнитные и электрические поля (по уровню излучения соответствуют требованиям 1 категории на расстоянии 1 м.).

Основные технические характеристики КИПА «ФИЛИН-А»:

– чувствительность магнитного преобразователя не хуже 0,5 мкА·м$^{-1}$·Гц$^{-0,5}$;

– чувствительность электрического преобразователя не хуже 0,5 мкВ·м$^{-1}$·Гц$^{-0,5}$;

– чувствительность микрофона – 2,4мВ·Па$^{-1}$;

– чувствительность вибропреобразователя – 109 мВ·м$^{-1}$·с^{2};

– динамический диапазон не мене 100 дБ;

– чувствительность микрофонного усилителя – 5,0 нВ·Гц$^{-0,5}$;

– чувствительность по акустическому полю – 2·10^{-5} мВ·Па$^{-1}$;

– чувствительность по виброакустическому полю – 10^{-6} м·с$^{-2}$;

– число одновременно анализируемых каналов – 2;

– ширина полосы анализа – 0,025..1 Гц;

– время измерения на одной полосе – 1..40 с.;

– погрешность измерения действующего значения сигнала – ±5,0%.

Комплекс «ФИЛИН-А» предназначен для контроля и оценки в реальном масштабе времени возможных каналов утечки речевой информации по НЧ и ВЧ полям и их наводкам на цепи, уходящие из защищаемых помещений (ЗП), а также находящиеся в этом ЗП ОТСС и ВТСС. Специальный комплекс «ФИЛИН-А» обеспечивает контроль и оценку выполнения норм противодействия акустической речевой разведке на объектах 1, 2, 3 категорий в соответствии с требованиями нормативно-методических документов по противодействию акустической речевой разведке (НМД АРР).

Принцип работы «ФИЛИН-А» основан на измерении слабых сигналов в шумах высокого уровня в виде физических полей либо наведенных токов и/или напряжений. Из-за сложности алгоритма и высокой требуемой точности генерации и измерения сигналов, обработка осуществляется согласованным фильтром в цифровой форме ресурсами

шумомера-анализатора и ПЭВМ (Note Book). Программное обеспечение позволяет получить результаты измерения и обработки сигналов в виде разборчивости речи и отношения сигнал/шум в двадцати третьоктавных полосах. Комплекс предназначен для применения в качестве специализированного измерительного прибора в силовых ведомствах Республики Беларусь, Банках, таможенных службах и т.д.

Комплекс «ФИЛИН-А» является локальной измерительной схемой. Это позволяет обеспечить его производительность примерно в 200 раз выше по сравнению с неавтоматизированными системами.

Рис. 1 – Комплекс измерительный программно-аппаратный «ФИЛИН-А»

В.К.ЖЕЛЕЗНЯК, К.Я.РАХАНОВ, Д.С.РЯБЕНКО

АНАЛИЗ ИЗМЕРИТЕЛЬНЫХ СИГНАЛОВ ДЛЯ АВТОМАТИЗИРОВАННОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ АНАЛОГОВОЙ И ЦИФРОВОЙ РЕЧИ

Актуальным является защита информации (ЗИ) и контроль её защищенности с высокой точностью в реальном масштабе времени. Системы оценки защищенности должны быть автоматизированными, устойчивыми, оптимальными по заданному критерию (рациональными).

Задача заключается в том, чтобы многокритериальную оценку представить однокритериальной. Таким критерием целесообразно выбрать величину разборчивости речи для каналов утечки информации (КУИ) речевых сигналов. Преимущества однокритериального показателя:

– сравнение 1…n КУИ по величине разборчивости речи;

– выбор наилучшей альтернативы для достижения максимального качества ЗИ;

– установление весового коэффициента 1…n КУИ путем сопоставления величины разборчивости речевого сигнала в КУИ;

– оценка эффективности принятых мер ЗИ;

– определение параметров сигналов, искаженных помехами или средой распространения.

По достигнутым значениям нормируемого показателя (разборчивость речи) оценивают альтернативы и выбирают, наилучшую для достижения должного качества ЗИ и максимальной эффективности мер ЗИ.

Обоснование выбора измерительного сигнала для выявления КУИ, присущих речевому сигналу, с учетом факторов, влияющих на точность оценки величины разборчивости речи и принятых мер ЗИ зависит от:

– диапазона частот речевого сигнала;

– количества полос разбиения и ширины полосы сигнала;

– диапазона частот измерительного сигнала;

– наличия согласованного фильтра для речевого сигнала и оптимального приемника для сигнала при воздействии влияющих факторов и в первую очередь шумов и помех;

– возможности оценки слабых сигналов в шумах высокого уровня в КУИ, присущих речевому сигналу;

– уровня измерительного сигнала;

– алгоритма оценки разборчивости с учетом отличий русской речи;

– оптимальности по быстродействию обработки и представления результатов оценки защищенности либо принятых мер ЗИ.

Шумовой сигнал в качестве измерительного не адекватен речевому, не обладает оптимальностью обнаружения в условиях воздействующих факторов (например, шумы высокого уровня, искусственные помехи).

Метрологические характеристики для шумового сигнала не установлены, несмотря на то, что некоторые его характеристики возможно измерить шумомером. Основные параметры речевого и шумового сигналов значительно различаются.

Гармонический сигнал научно обоснован в качестве измерительного на базе корреляционной теории разборчивости речи [1] и апробирован в СИА «К6-6», «ФИЛИН-А». Высокая селективность средств измерений и измерительного сигнала решает задачу достоверного выявления всех видов КУИ (акустического, виброакустического, ПЭМИН, электроакустического, ВЧ- при подключении СИА к выходу НЧ-приемника).

Учитывая факторы, что спектральная характеристика речевого сигнала зависит от частоты, кривая чувствительности уха неравномерна, спектральная плотность фонового шума экспоненциально спадает от нижних частот, распространение речевого сигнала зависит от затухания среды распространения. Среда распространения включает прохождение речевого сигнала через элементы конструкции помещения (окна, двери), инженерные элементы (воздуховоды, системы отопления, газоводоснабжение и др.).

Эти факторы обусловливают погрешность оценки защищенности без учета АЧХ КУИ [1]. При этом использование гармонического измерительного сигнала на средних частотах полос равной разборчивости либо на средних частотах 1/3-октавных полос, и хуже того, на средних частотах октавных полос, допускает увеличение погрешности в КУИ с явно выраженными неравномерностями АЧХ в измеряемом диапазоне частот. Это в полной мере относиться к электроакустическому каналу.

Среди множества сложных сигналов преимуществами обладает ЛЧМ-сигнал, который позволяет расширить возможность оценки защищенности речи. Использование ЛЧМ-сигнала позволяет контролировать всю полосу частот октавы (1/3-октавы, полосы равной разборчивости), а не только отдельная точка на оси частот, в отличие от гармонического.

Для решения задачи оценивания параметров сигналов сложной частотно-временной структурой предлагается использовать технику совместных частотно-временных описаний

сигналов [2]. Среди множества форм частотно-временных описаний предпочтение отдается функции плотности распределения сигнальной энергии Вигнера:

$$Pw(f,t) = \int_{-\infty}^{\infty} Z_a^*(t-\tau/2) Z_a(t+\tau/2) \exp(-j2\pi f\tau) d\tau ,$$

где $Z_a(t) = Z(t) + j\widetilde{Z}(t)$ - есть аналитический сигнал, $\widetilde{Z}(t)$ - преобразование Гильберта действительного сигнала $Z(t)$, * - знак комплексного сопряжения.

Главное достоинство распределения Вигнера состоит в том, что она обладает свойством максимальной локализации сигнальной энергии, что позволяет измерять параметры сигнала на интервале частот [3]. Оценки параметров сигнала, полученные с помощью плотности распределения Вигнера являются устойчивыми даже при высоком уровне помех.

Для определения информационных показателей, гарантирующих защищенность цифровой речи, выбрана модель двоичного симметричного канала (ДСК).

Основной характеристикой ДСК является вероятность ошибки P [4]:

$$P = Q\left(-\sqrt{2 \cdot E_s / N_0}\right),$$

где E_s – энергия сигнала, N_0 – спектральная плотность шума, Q (x) – функция, определяемая по формуле интеграла вероятности

$$Q(x) = 1/2\pi \cdot \int_x^{\infty} e^{-\frac{t^2}{2}} dt ,$$

Для симметричного дискретного канала пропускная способность канала C_N в битах на один отсчет вычисляется [5]:

$$C_N = \frac{W}{N}\left[\log_2 M + P_0 \log_2 \frac{P_0}{M-1} + (1-P_0)\log_2(1-P_0)\right],$$

где P – вероятность ошибочного приема N – мерного сигнала в M – позиционной системе, W – ширина полосы частот.

Пропускная способность ДСК C определяется по формуле [5]:

$$R_{\max} = C = W\left[1 + P\log_2 P + (1-P)\log_2(1-P)\right], \qquad (1)$$

Для многократной ФМ с m_c позициями вероятность ошибочной регистрации $P_{0ФМ}$ определяется выражением

$$P_{0ФМ} = \left(1/\log_2 m_c\right)\left[1 - \Phi\left(\sqrt{2}q \sin \pi/m_c\right)\right].$$

Заключение

Многокритериальную задачу выделения измерительных сигналов в каналах утечки информации и представления результатов оценки предложено представлять однокритериальной. Критерием оценки защищенности предложена нормативная величина разборчивости речи.

В качестве измерительного для оценки разборчивости речи с высокой точностью в реальном масштабе времени предложен сигнал линейной частотной модуляции (ЛЧМ). Анализ шумового, гармонического сигналов показал преимущества ЛЧМ-сигнала.

Для оценки информационных показателей, определяющих защищенность цифровых и аналоговых речевых сигналов по единому критерию, получены выражения, которые позволяют реализовать СИА.

Литература

1. Железняк, В.К. Защита информации от утечки по техническим каналам: учебное пособие. – СПб.: ГУАП, 2006. –188 с.

2. Алексеев, А.А., Кириллов, А.Б. Технический анализ сигналов и распознавание радиоизлучений. – СПб.: ВАС, 1998.–368 с.

3. Дворников, С.В. Теоретические основы синтеза билинейных распределений. – СПб.: Изд-во Политехн. ун-та, 2007. 268 с.

4. Зюко, А.Г., Финк, Л.М., Кловский Д.Д. Теория передачи сигналов. // Под ред. М.В., Назарова. – М.: Связь. 1980.

5. Зюко, А.Г. и др. Помехоустойчивость и эффективность систем передачи информации. – М.: Радио и связь. – 1985.

В.К.ЖЕЛЕЗНЯК, К.Я.РАХАНОВ, Д.С.РЯБЕНКО
В.В.БУСЛЮК, С.И.ВОРОНЧУК, И.В.ЛЕШКЕВИЧ
С.С.ДЕРЕЧЕННИК

МЕТОДИКА ОЦЕНКИ ДЛЯ ОПЕРАТИВНОГО КОНТРОЛЯ ИСТОЧНИКОВ ШУМОВОГО СИГНАЛА

Эффективность любой информационной системы оценивают интегральным и частными показателями, одним из которых является степень защиты информации (ЗИ) информационной системы.

Степень защиты информации определяют её мерой, которая устанавливает полноту выделения и оценки существенных факторов, формирующих технические требования к параметрам ЗИ. Мера ЗИ зависит от рационального использования ресурсов, выделенных на ЗИ. Требования к ЗИ определяются функциональным назначением, структурой и параметрами информационной системы. Методы и средства ЗИ формируют с учетом особенностей эксплуатации объекта информатизации, ценности информации, выделяемых сигналов (видео-, речевой, передача данных, простые, сложные), обрабатываемых на объекте.

Разрушение каналов утечки информации (КУИ) со скрытым функционированием информационной системы обеспечивают схемно-конструктивными решениями и средствами ЗИ. Схемно-конструктивные решения реализуют взаимную компенсацию информационных полей рассеивания, срыв паразитных генераций, ослабление информационных мультипликативных ВЧ-излучений, их локализацией и рассогласованием среды распространения.

Важным является разрушение КУИ активными способами – путем маскирования информационных и демаскирующих параметров сигналов маскирующими помехами. Активные методы ЗИ основаны на формировании преднамеренных шумов, обладающих необходимой эффективностью по заданному критерию эффективности, выбор которого обоснован в [1].

Маскирующие помехи, сформированные непосредственно из сигнала (видео-, речевой), наиболее адаптированы к его параметрам [2]. В качестве источников генерации преднамеренных маскирующих шумов широко распространены шумовые диоды.

Основные параметры и характеристики помехи определяются источниками генерации преднамеренных маскирующих шумов, а усилительные каскады формируют частотный диапазон, при необходимости ограничивая его. Необходимые коррекции вводятся для регулировки напряжения, мощности выходных сигналов, согласования с нагрузкой, выполнения измерительных и контролирующих функций параметров и характеристик.

Целью исследования является оценка основных параметров диодов-генераторов шума серии ND 100, а также возможность использования их в качестве источника сигнала для генераторов маскирующего шума речевого и видеоканалов, линий передачи данных.

Технические характеристики диодов-генераторов шума представлены в таблице 1.

Таблица 1 – Технические характеристики диодов серии ND 100

Тип	Постоянное напряжение $U_{ш}$, при токе 100 мкА	Спектральная плотность напряжения шума S_U, мкВ / $\sqrt{Гц}$	Граничная частота $F_{гр}$, МГц при токе 50 мкА, не менее	Неравномерность спектральной плотности напряжения шума, δS_U, дБ при токе 50мкА, не более
ND-101L	7.0 – 11.0	70	0.1	4.0
ND-102L	7.0 – 11.0	50	0.5	4.0
ND-103L	6.0 – 9.0	30	1.0	3.0
ND-104L	6.0 – 9.0	3.0	3.0	3.0

Оценка основных параметров указанных источников шума выполнялась по приведенной ниже методике. С помощью измерительного АЦП производится преобразование аналогового шумового сигнала в дискретную форму для записи его на ПЭВМ с целью последующей оценки параметров. Время выборки при этом составляет не менее 5 секунд, частота дискретизации – не менее 400 кГц, что позволяет анализировать сигналы с частотой до 200 кГц. С целью устранения искажений, установлен фильтр нижних частот, через который пропускается входной аналоговый сигнал. Частота среза такого фильтра равна половине частоты дискретизации. Дискретные отсчеты сигнала записываются в 24-разрядном двоичном коде, представляющего цифровую форму исходного сигнала в ограниченной полосе. Фрагмент такого шумового сигнала представлен на рисунке 1.

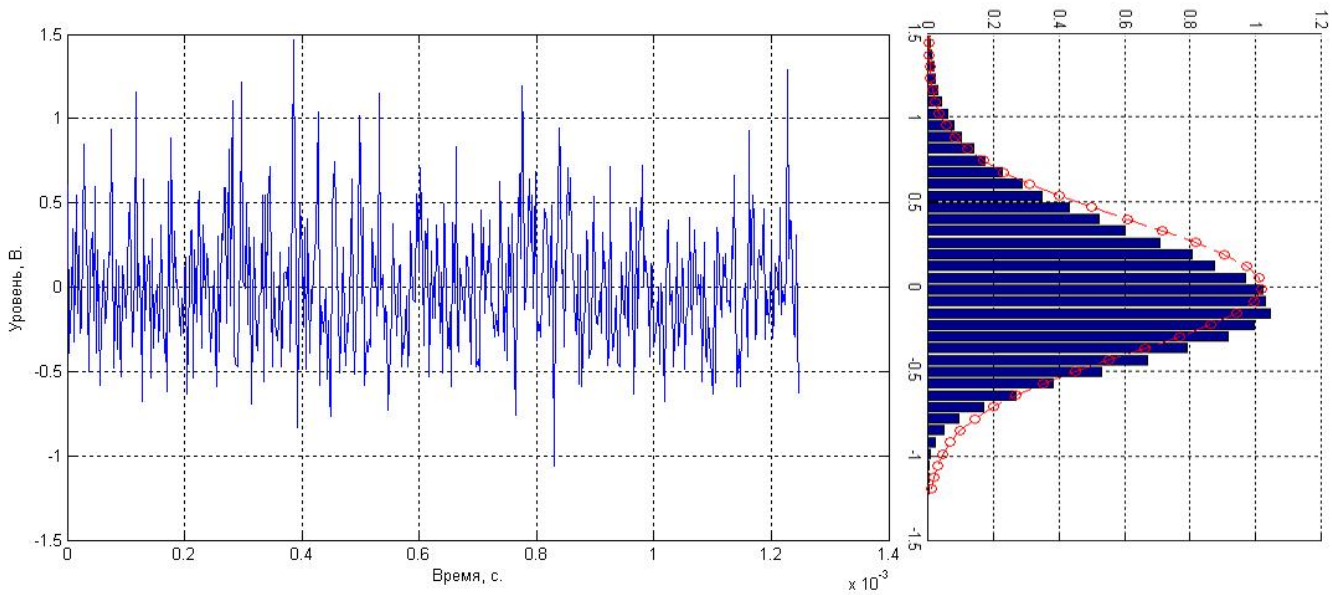


Рис. 1. Фрагмент шумового сигнала и плотность распределения его вероятности

Обобщенные характеристики шумового сигнала получены инструментально-расчетными методами. Высокая точность полученных исходных данных для расчета параметров гарантируются использованием измерительного АЦП, метрологические параметры которого аттестованы. Необходимые данные шумовых сигналов получены с помощью пакета прикладных программ MATLAB.

Обработка данных выполнена в соответствии с [3]. Оцениваемыми параметрами являлись:

– энтропийный коэффициент качества шумового сигнала (не менее 0,95);

– автокорреляционная функция (обобщенная характеристика представлена на рисунке 2);

– среднеквадратическая частота шумового сигнала (автокорреляционная функция и среднеквадратичная частота характеризуют отсутствие гармонических составляющих в спектре);

– распределение плотности вероятности шума подчинено закону Гаусса (показано с использованием критерия согласия χ^2 при уровне значимости 0,05);

– пик-фактор шумового сигнала (вверх, вниз – не менее 3);

– спектральная плотность мощности шумового сигнала равномерна в заявленных диапазонах частот.

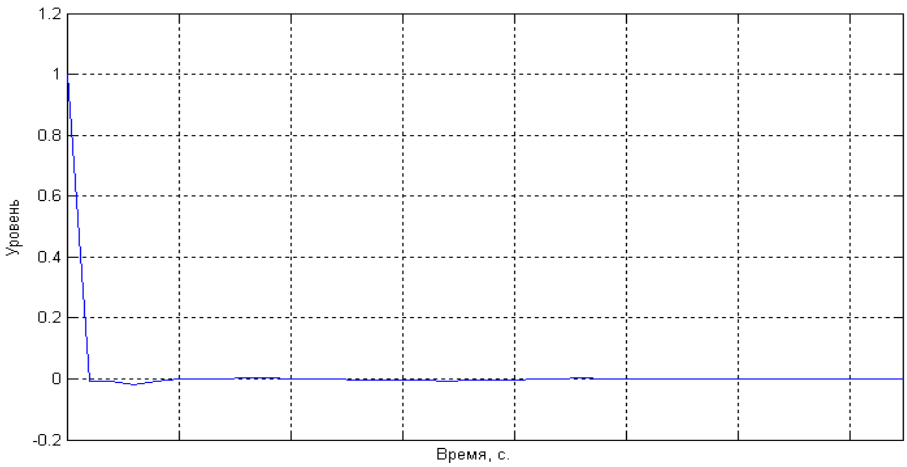


Рис. 2. Обобщенная автокорреляционная функция сигналов шумовых диодов

Выводы

В результате исследования установлены:

– высокая устойчивость метрологических параметров и характеристик (воспроизводимость результатов);

– контролепригодность параметров;

– исследованные диоды-генераторы шума превосходят известные ранее по ряду параметров (уровень излучения, неравномерность АЧХ в рабочем диапазоне частот, разброс характеристик при воздействующих факторах);

– энтропийный коэффициент качества шума, как основной параметр, приближается к единице.

На основании полученных данных достоверно показано, что диоды-генераторы шума серии ND 100 в полной мере применимы в качестве источников шумовых сигналов в генераторах маскирующего шума. Образцы таких диодов апробированы в некоторых генераторах маскирующего шума и обеспечили высокие характеристики последних.

Литература

1. Железняк, В.К. Защита информации от утечки по техническим каналам: учебное пособие. ГУАП. – СПб., 2006. –188 с.

2. Железняк, В.К., Карасев, Р.С. Автоматизированная оценка маскирующего шума в речевом диапазоне частот. // Информационные системы и технологии (IST 2009): материалы V Международной конференции-форума (Минск, 16-17 ноября 2009 г.). – В 2-х ч. – Ч2. / редкол.: Н.И. Листопад [и др.]. – Минск: А.Н. Вараксин, 2009. – С.42–46.

3. Кузнецов, В.А., Ялунина, Г.В. Общая метрология. – М.: ИПК Издательство стандартов. 2001. – 272 с.

4. Буслюк, В.В., Ворончук, С.И., Лешкевич, И.В., Дереченник, С.С. Кремниевые диоды-генераторы шума серии ND 100 для криптографических систем // Комплексная защита информации: материалы XIV Межд. конференции. – Минск, 2009. – С. 61–63.

В.А.КАРАСЬ

СПОСОБЫ ЗАЩИТЫ USB ФЛЭШ-НАКОПИТЕЛЕЙ ОТ УТЕЧКИ ИНФОРМАЦИИ

Применение внешних носителей информации, в частности, USB флеш-накопителей (далее – флеш-накопитель), приводит к проблеме защиты информации. Флеш-накопители являются одним из каналов утечки информации. Большинство пользователей, использующие флеш-накопители, хранят на них не только информацию личного пользования, но и информацию ограниченного использования. Утечка или уничтожение данных, хранящихся на флеш-накопителе, может привести к нанесению ущерба.

При использовании флеш-накопителя происходит его подключение к разным ПЭВМ, что представляет дополнительную угрозу распространения шпионского программного обеспечения и вредоносного программного кода. Данная канал распространения вредоносного программного кода является самым значимым.

Средств противодействия угрозам при использовании флеш-накопителей известно много, однако наиболее адекватную и надежную защиту в состоянии обеспечить только система контроля использования внешних устройств, в числе функций которой обязательно должны присутствовать: ведение журнала аудита событий безопасности; мониторинг действий пользователей; "теневое" копирование; шифрование данных, передаваемых на USB флеш-накопитель. Однако есть и другой выход – использование специализированных USB флеш-накопителей информации.

В докладе рассматриваются каналы утечки информации с USB флеш-накопителей и способы их защиты, методы и средства предотвращения утечек информации с USB флеш-накопителей, приводятся рекомендации по использованию специализированных USB накопителей на объектах информатизации разных категорий.

А.И.КОХАН

СОВРЕМЕННЫЕ МЕТОДЫ ВЕРИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Надежность и безопасность – наиболее важные требования к программному обеспечению (ПО) в случаях его применения на наиболее важных стратегических объектах:

электростанциях, банковских системах, в промышленности, для защиты конфиденциальной и секретной информации. Ошибка функционирования такого ПО может привести к угрозе для жизни или к тяжелым экономическим последствиям.

Для получения обоснованных гарантий относительно надежности и безопасности ПО, применяют имитационное моделирование и тестирование, которые включают в себя ввод определенных исходных данных и наблюдение за полученными результатами. Кроме того, в отдельных случаях применяют дедуктивный анализ, подразумевающий применение аксиом и правил вывода для доказательства правильности функционирования системы.

Однако имитационное моделирование и тестирование не всегда является достаточной мерой для подтверждения правильности функционирования ПО. Например, практически невозможно охватить тестированием все состояния ПО, если оно представляет собой распределенную или реактивную систему, состоящую из множества компонентов, функционирующих одновременно и конкурирующих за общие ресурсы. В то же время применение дедуктивного анализа требует слишком много времени, и он может быть осуществлен только экспертами, обладающими знаниями в области логического вывода и немалый практический опыт [1].

Таким образом, для проверки правильности функционирования описанных выше распределенных, реактивных систем необходимо в дополнение к уже существующим применять дополнительные меры. Такими мерами является применение верификации ПО, в частности современный метод проверки на модели. Для указанных систем применение этого метода должно быть выполнено до этапа тестирования.

Существуют «классический» и «современный» подходы к верификации ПО посредством проверки на модели. «Классический» подход подразумевает применение процедуры верификации на этапе проектирования ПО, в то время как «современный» подход предполагает анализ ПО после этапа реализации (написания исходных текстов ПО) [2].

Важным преимуществом «современного» подхода, кроме того, что он может быть применен к уже разработанному ПО, является масштабируемость. В случае изменения исходных текстов ПО (выхода новой версии), требуется незначительное изменение построенной модели, и, как следствие, минимальных затрат по времени для проведения повторной верификации. Рассмотрим ниже этот подход подробнее.

Процесс верификации начинается с определения области ее применения, и построения абстрактной модели M функционирования ПО таким образом, что в модель включаются все существенные (относительно набора проверяемых свойств) детали, и все несущественные опускаются. Процесс исключения несущественных свойств обычно включает следующие действия:

а) все инструкции, не связанные с рассматриваемыми свойствами, заменяются пустой инструкцией;

б) все исходы ветвей, не связанных с рассматриваемыми свойствами, рассматриваются как равновероятные [3].

Набор проверяемых свойств задается при помощи формул временной логики (как правило, LTL или CTL*). Формулы временной логики могут являться формализацией таких подлежащих проверке свойств, как, например, «событие X всегда предшествует событию Y», «последовательность событий X, Y, Z не может произойти», «в любом бесконечном исполнении процесса событие X происходит бесконечно часто».

Формулы временной логики могут быть использованы для проверки отсутствия таких проблем, характерных для распределенных систем, как:

а) взаимная блокировка процессов (deadlock);

б) активная блокировка процессов (livelock);

в) состояние гонки (race condition) [4].

Для проверки того, что модель M, заданная при помощи структуры Крипке, обладает некоторым свойством φ, заданным при помощи формул временной логики LTL, то есть, $M \models \varphi$, можно выполнить следующие действия:

а) преобразование структуры Крипке M в автомат Бюхи A(M);

б) преобразование отрицания формулы LTL φ в автомат Бюхи A(not φ);

в) вычисление произведения $A = A(M) \otimes A(\text{not } \varphi)$.

Если для полученного в результате автомата Бюхи A выполнено $L(A) = \varnothing$, то есть множество слов, которые принимает автомат, пусто, то $M \models \varphi$.

Общая схема верификации представлена на рисунке 1. В настоящее время существует широкий выбор ПО, позволяющего автоматизировать все необходимые действия, за исключением:

а) преобразования произвольного исходного кода ПО в модель;

б) составления формул временной логики;

в) анализа результатов.

Примером свободно распространяемого ПО для автоматизации задач верификации является SPIN. Входными данными являются модель M и формулы LTL φ (в общем случае, любое ω-регулярное свойство), заданные при помощи языка PROMELA, специально разработанного для представления систем процессов, исполняемых параллельно и взаимодействующих между собой. Выходными данными являются результаты верификации: в случае, если формула φ не соответствует модели M, выдается последовательность действий, приводящая к несоответствию. Эти данные можно использовать для устранения ошибок: таким образом, SPIN может выступать как средство диагностики и отладки.

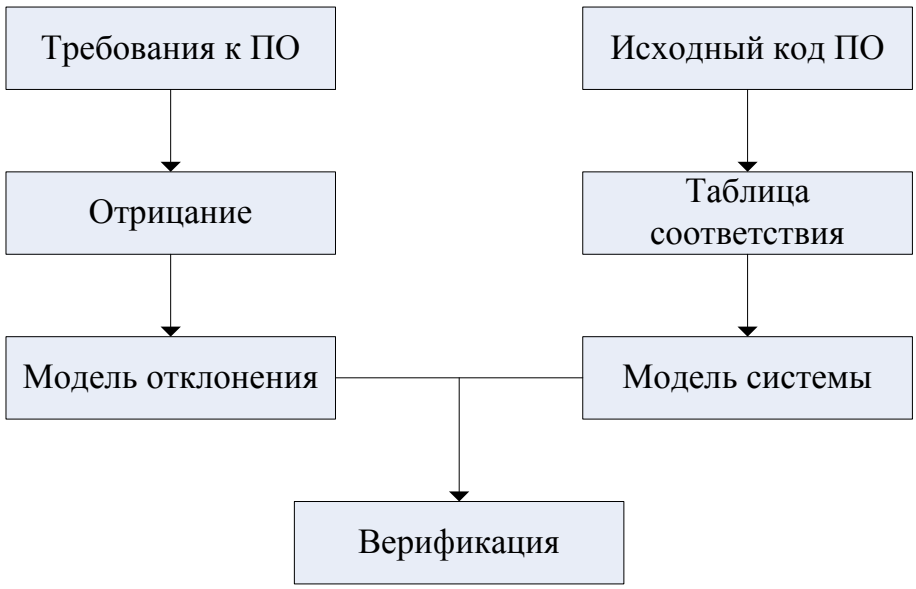


Рисунок 1 – Общая схема верификации

Этап перевода исходного кода ПО в описание модели M не может быть выполнен автоматически для произвольного ПО, но может быть автоматизирован для каждого конкретного случая. Это может быть выполнено путем составления таблицы отношений, которая каждой инструкции из исходных текстов ПО ставит в соответствие выражение, описывающее модель M. Далее эта таблица считывается специальной программой (парсером), которая и генерирует описание модели. Подробнее о построении таблицы соответствия см. [5].

Программный комплекс, состоящий из ПО для автоматизации верификации (SPIN), таблицы соответствия и программы считывания, является достаточным для проведения верификации, причем этот процесс характеризуется невысокими затратами и высокой эффективностью.

Подводя итоги, можно сказать, что верификация является дополнительной мерой гарантии надежности ПО, применяемого в критически важных сферах. Если ПО представляет собой сложную систему, состоящую из нескольких компонентов, функционирующих одновременно, то проведение верификации дает дополнительные гарантии относительно тех или иных свойств ПО. Процесс верификации путем проверки на модели проводится до этапа тестирования ПО.

В случае, если верификация не проводилась на этапе проектирования ПО, она должна проводится после того, как будут готовы исходные коды программы, или на этапе их доработки. Практический метод применения верификации в этом случае описан выше в данной работе.

Верификация посредством проверки на модели должна быть обязательным этапом проверки правильности функционирования сложных распределенных, реактивных систем, надежность которых является критическим параметром, поскольку этот метод характеризуется невысокими затратами по сравнению с дедуктивным анализом, и в то же время позволяет обнаруживать некорректное функционирование ПО в тех случаях, когда это крайне сложно сделать при помощи имитационного моделирования и тестирования.

Литература

1. Кларк, Э.М. Верификация моделей программ / Э.М. Кларк, О. Грамберг, Д. Пелед. – М.: Издательство Московского центра непрерывного математического образования, 2002 – 416 с.

2. Ruys T., Holzmann G. Advanced SPIN Tutorial [Электрон. ресурс] – 11 февраля 2011. – Режим доступа: http://spinroot.com/spin/Doc/Spin_tutorial_2004.pdf

3. Holzmann G., Smith M. Automating Software Feature Verification [Электрон. ресурс] – 1 марта 2011. – Режим доступа: http://spinroot.com/gerard/pdf/bltj2000.pdf

4. Parker D. Probabilistic Model Checking [Электрон. ресурс] – 5 марта 2011. – Режим доступа: http://www.prismmodelchecker.org/lectures/pmc/17-omega%20regular.pdf

5. Holzmann G., Smith M. A Practical Method for Verifying Event-Driven Software [Электрон. ресурс] – 25 марта 2011. – Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/download? doi=10.1.1.69.4722&rep=rep1&type=pdf

Э.Г.ЛАЗАРЕВИЧ, Д.Д.ГОЛОДЮК, Ю.И.СЕМАК

ЗАЩИТА ВИРТУАЛЬНОГО КОМПОНЕНТА НА ВСЕХ СТАДИЯХ ЖИЗНЕННОГО ЦИКЛА ОБРАЗЦОВ ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ

Тенденции развития современного промышленного производства показывают, что проблемы обеспечения качества и конкурентоспособности высокотехнологичной наукоемкой продукции, включающей вооружение и военную технику (ВВТ), невозможно решить без применения современных информационных технологий. Наибольшую известность приобрели компьютерные технологии информационной поддержки и автоматизации процессов разработки, производства, сбыта и эксплуатации высокотехнологической продукции, основанные на системном подходе к описанию ее жизненного цикла (CALS или ИПИ-технологии).

Основным строительным блоком при реализации стратегии ИПИ-технологий в процессе создания отечественных систем вооружения являются стандарты. Для этих целей в Республике Беларусь международные стандарты по новейшим информационным технологиям пока не нашли широкого применения. Это вызывает принципиальные трудности для информационной поддержки изделий ВВТ на протяжении жизненного цикла (ЖЦ), ***их защиты, как интеллектуальной собственности, так и как конфиденциальной информации***.

Данная проблема актуальна для создания всех видов ВВТ. В стенах государственного учреждения «Научно-исследовательский институт Вооруженных Сил Республики Беларусь» (ГУ «НИИ ВС РБ») была разработана концепция виртуальной электронной компонентной базы (ВЭКБ). Данная концепция обеспечивает перевод радиоэлектронной аппаратуры современных и перспективных образцов вооружения на элементную базу пятого поколения, основной составной частью которой будут являются виртуальные компоненты (VC – Virtual Component) (рис. 1).

Виртуальный компонент приобретает реальность в виде IP-блоков. Другими словами IP-блоки представляют собой программную или физическую реализацию VC на соответствующем уровне (этапе) проектирования. Виртуальные компоненты представляют собой полезную информацию об изделии, накапливающуюся с течением времени.

Виртуальный компонент – это проектный блок, специально созданный с целью повторного использования, который был разработан и сертифицирован для максимального повторного использования [2].

В настоящее время VC представляет собой вербальные описания, алгоритмы, математические модели различных уровней проектирования (системного, функционального) компонентов ВВТ или продукции двойного назначения, которые помимо того, что информационно не поддержаны ***и не защищены***, как объекты интеллектуальной собственности, так и как конфиденциальная информация, влияющая на обороноспособность государства.

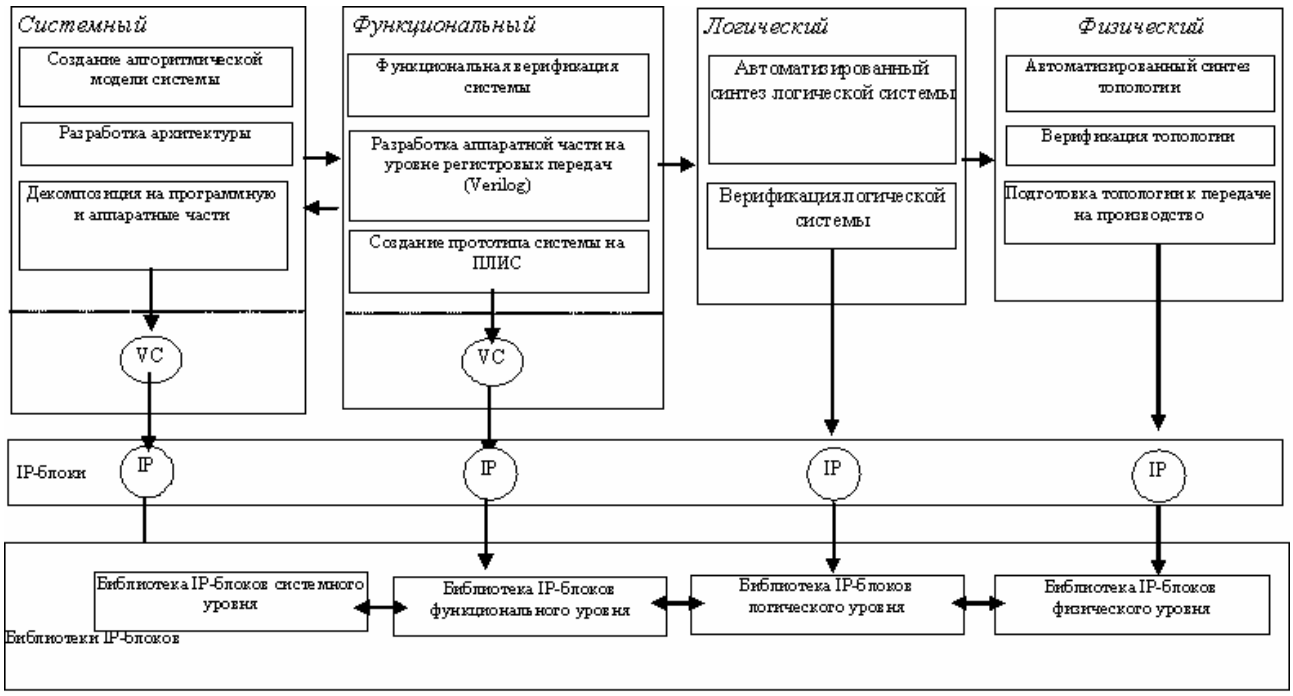


Рисунок 1. Уровни проектирования виртуальных компонентов

Проведенный анализ показывает, что целью промышленного и военного шпионажа были и будут новейшие технологии в области разработки ВВТ. Переход отечественной промышленности от традиционных технологий разработки, производства и эксплуатации

наукоемкой продукции к использованию современных информационных технологий, приведет к утечке наукоемкой информации. Незащищенность VC в области разработки ВВТ приведет к снижению уровня обороноспособности государства.

Для решения этой проблемы потребуется реализация комплекса мероприятий, включающих: структурно-организационные, экономические, методологические, военно-технические и нормативно-правовые мероприятия.

Литература

1. Ковшов, А.Н., Назаров, Ю.Ф., Ибрагимов, И.М., Никифоров, А.Д. Информационная поддержка жизненного цикла изделий машиностроения: принципы, системы и технологии CALS/ИПИ: учебное пособие для студентов высших учебных заведений. – Москва: Издательский центр «Академия» 2007. - 304 с.

2. Немудров В. Системы-на-кристале. Проектирование и развитие. – М.: Техносфера, 2004. – 216 с.

3. Бронин Е.И., Вермишев Ю.Х. Информационная инфраструктура разрабатывающего предприятия//Информационные технологии в проектировании и производстве. 1999. – № 2.

Л.М.ЛЫНЬКОВ, А.А.КАЗЕКА, Т.В.БОРБОТЬКО, О.В.БОЙПРАВ

ВЛИЯНИЕ ВОДОСОДЕРЖАЩИХ ЭКРАНИРУЮЩИХ МАТЕРИАЛОВ НА ОСЛАБЛЕНИЕ ИЗЛУЧЕНИЯ ГЕНЕРАТОРОВ ЭЛЕКТРОМАГНИТНОГО ШУМА

Работа средств вычислительной техники (СВТ) сопровождается побочными электромагнитными излучениями и наводками (ПЭМИН), посредством которых образуется электромагнитный канал утечки информации. Защита информации от утечки по данным каналам в ряде случаев осуществляется с помощью генераторов электромагнитного шума (ГЭМШ), которые излучают в эфир широкополосный сигнал с уровнем, превышающим уровень ПЭМИН СВТ. Недостатком применения ГЭМШ является негативное влияние их излучений на организм человека. В связи с этим существует необходимость защиты операторов СВТ от излучения ГЭМШ, которая может быть реализована посредством использования экранирующих конструкций, располагаемых между источником ЭМИ и рабочими местами персонала [1]. Эти конструкции могут изготавливаться из различных материалов (проводящих и диэлектрических материалов и т.д.) и иметь различную структуру поверхности (равномерную либо с геометрическими неоднородностями в виде шипов, конусов, пирамид).

В рамках данной работы в частотном диапазоне 0,3–1 ГГц проведены исследования эффективности экранирования ГЭМШ влагосодержащим машинно-вязаным полотном, стеклопакетом, заполненным водным раствором хлорида натрия и биологическим объектом (тело человека). Исследования выполняли в три этапа. На первом этапе осуществлялось измерение уровня электромагнитного фона в помещении, на втором – измерение уровня излучений ГЭМШ, на третьем – измерение уровня излучений ГЭМШ, который экранировался вышеуказанными образцами.

Для проведения измерений использовалась антенна с узкой диаграммой направленности, которая устанавливалась от ГЭМШ на расстоянии не ближе трех длин волн, что позволило сократить время обнаружения максимальных значений уровня ЭМИ.

Принцип работы измерительной системы основан на определении уровня электрической и магнитной составляющих электромагнитного поля и передачи полученных результатов на персональный компьютер оператора. Специальное программное обеспечение SCANF позволило автоматизировать процесс измерения, а также процессы обработки,

визуализации и сохранения его результатов [2]. Для общей оценки эффективности экранирования ЭМИ в разработанном программном модуле специально предусмотрено вычисление средней спектральной плотности мощности сигнала.

На рис. 1–3 представлены частотные зависимости уровня ЭМИ, прошедшего через каждый из исследованных образцов.

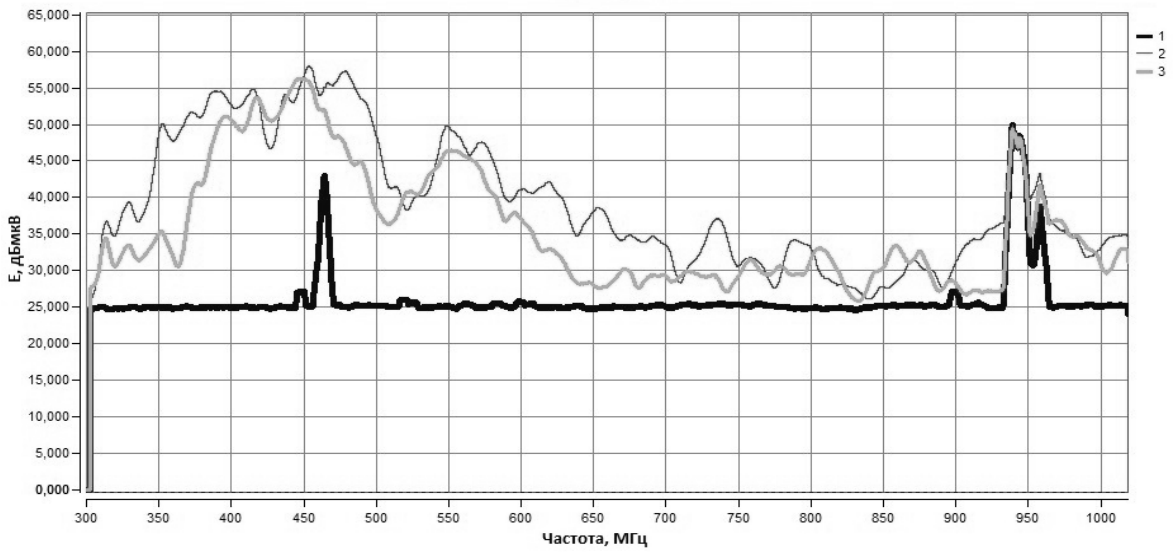


Рис. 1. Частотные зависимости уровня ЭМИ:

1 – электромагнитный фон помещения, 2 – ГЭМШ, 3 – экран – биологический объект (тело человека)

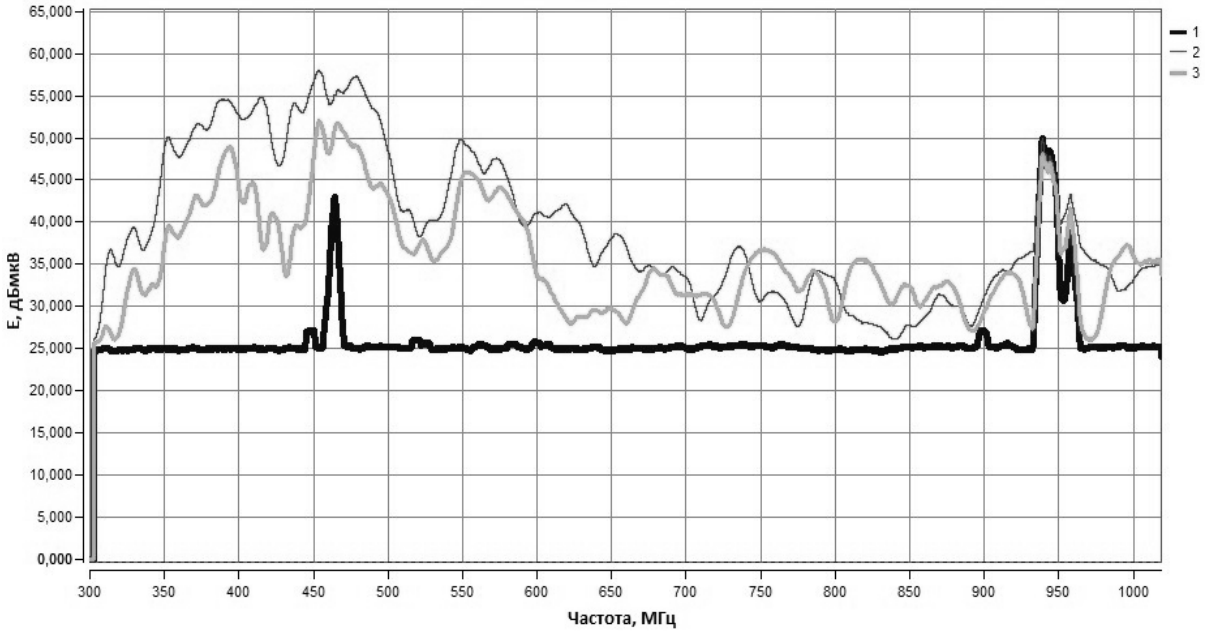


Рис. 2. Частотные зависимости уровня ЭМИ:

1 – электромагнитный фона помещения, 2 – ГЭМШ, 3 – экран - влагосодержащее машинно-вязаное полотно

Установлено, что в диапазоне частот 0,3–1 ГГц средняя мощность спектра электромагнитного фона в помещении, в котором проводились исследования, составляет $3{,}32 \cdot 10^{-10}$ $В^2/Гц$, средняя мощность спектра ГЭМШ – $5{,}55 \cdot 10^{-8}$ $В^2/Гц$, средняя мощность

спектра ЭМИ ГЭМШ, прошедшего через тело человека – $2{,}52 \cdot 10^{-8}$ $В^2$/Гц, средняя мощность спектра ЭМИ ГЭМШ, прошедшего через влагосодержащее машинно-вязаное полотно – $8{,}62 \cdot 10^{-9}$ $В^2$/Гц, средняя мощность спектра ЭМИ ГЭМШ, прошедшего через стеклопакет, заполненный водным раствором хлорида натрия – $4{,}1 \cdot 10^{-8}$ $В^2$/Гц.

Поглощение ЭМИ водой обусловлено различными механизмами. При воздействии на полярные диэлектрики ЭМИ радиочастотного диапазона появляется дипольная поляризация, приводящая к повышению диэлектрической проницаемости, а значит, и к повышению диэлектрических потерь энергии ЭМИ. В области релаксационной дисперсии, когда диполи не успевают переориентироваться за полупериод изменения электрического поля, возникают релаксационные потери энергии [3].

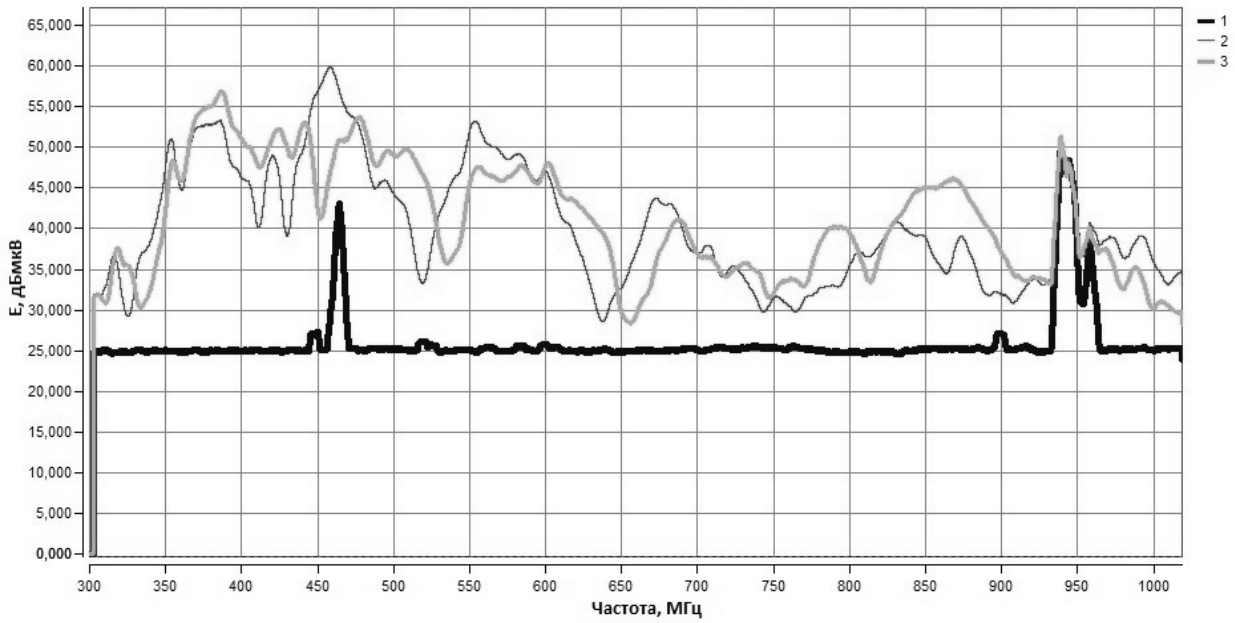


Рис. 2. Частотные зависимости уровня ЭМИ:

1 – электромагнитный фон помещения, 2 – ГЭМШ, 3 – экран - стеклопакет, заполненный водным раствором хлорида натрия

Таким образом, следует отметить, что для защиты операторов СВТ от ЭМИ ГЭМШ целесообразно применять экранирующие конструкции на основе машинно-вязаных полотен, пропитанных водой либо водным раствором, эффективно снижающих уровень излучений в полосе частот 0,3–1 ГГц.

Литература

1. Казека, А.А. Экраны электромагнитного излучения для защиты персонала от излучения генераторов электромагнитного шума / А.А. Казека, М.В. Жалковский, Т.В. Борботько // Технические средства защиты информации: материалы VIII Белорусско-российской науч.-тех. конф., Минск, 24–28 мая 2010 г. / БГУИР, Минск; редкол.: В.Ф. Голиков [и др.]. – Минск, 2010. – С. 104.

2. Казека, А.А. Защита от побочного электромагнитного излучения персонального компьютера / А.А. Казека, А.М. Прудник // Инженерный вестник. 2010. №2(30). С. 49–51.

3. Прохоров, А.М. Физический энциклопедический словарь/ Гл. ред. А.М.. Прохоров. – М: Советская энциклопедия, 1988. Т. 1. – 704 с.

А.Ф.МЕЛЬНИК

О НЕКОТОРЫХ ВОПРОСАХ ВЛИЯНИЯ УСЛОВИЙ ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ НА ИХ РЕЗУЛЬТАТЫ

Как известно, результатом проведения специальных исследований (СИ) средств вычислительной техники (СВТ), предназначенных для обработки защищаемой информации, является рассчитанное по действующим методикам значение радиуса R_2 зоны 2 вокруг СВТ, на границе которой и за ее пределами отношение пикового значения напряженности электромагнитного поля (ЭМП) побочных электромагнитных излучений (ПЭМИ) к среднеквадратичному значению напряженности шума (помехи) не превышает нормированного значения Δ [1]. При этом считается, что СВТ защищены от перехвата ПЭМИ средствами радиоразведки, расположенными за пределами зоны 2.

Соответственно, размер зоны 2 определяет минимальную контролируемую зону вокруг СВТ, установленных на объекте, а также необходимость применения технических средств защиты информации в зависимости от условий расположения объекта.

В связи с этим особое значение приобретают вопросы обеспечения достоверности и воспроизводимости результатов СИ. При проведении СИ должны использоваться средства измерения, имеющие свидетельство о метрологической поверке, а специалистам необходимо учитывать и правильно применять целый ряд параметров, влияющих на результаты исследований (выбор тестового режима, полосы пропускания измерительного приемника, типа детектора, вида представления информации и т.п.). Корректность задания этих параметров, отражаемых в протоколах СИ, можно при необходимости проверить при осуществлении контроля достоверности результатов СИ.

Тем не менее, даже при абсолютно корректной установке требуемых параметров и режимов на практике бывают случаи значительных расхождений результатов СИ однотипных (и даже одинаковых) СВТ, проведенных различными организациями. При этом основным фактором, влияющим на результаты измерений, становится степень соответствия закона ослабления электромагнитного поля в помещении для проведения СИ некоторой усредненной стандартной функции ослабления поля, принятой в методиках [1 - 3].

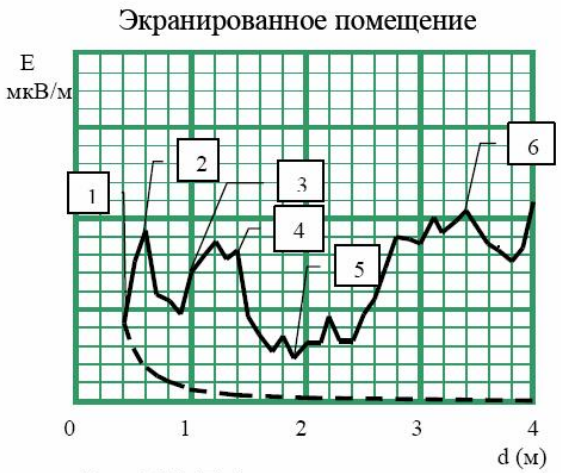
Для количественной оценки влияния закона ослабления электромагнитного поля в помещениях на результаты СИ были проведены исследования затухания ЭМП ПЭМИ от персонального компьютера (ПК) в зависимости от расстояния d от ПК до измерительной антенны в двух помещениях без радиопоглощающего покрытия, предназначенных для проведения СИ (экранированном, а также неэкранированном с металлическим фальшполом). Габаритные размеры экранированного помещения – 10 м (длина) × 9 м (ширина) × 3 м (высота), площадь 90 м^2 . Габаритные размеры неэкранированного помещения – 18 м (длина) × 10 м (ширина) × 5,5 м (высота), площадь 180 м^2.

ПК устанавливался в центральной зоне помещения, задавался тестовый режим проверки видеотракта «точка через точку» и проводились измерения электрической компоненты ЭМП ПЭМИ при горизонтальной и вертикальной поляризации приемной антенны для различных расстояниях d (начиная с расстояния $d = 0{,}4$ м) с шагом 0,1 м.

На рисунках 1-4 в виде графиков приведены некоторые характерные результаты измерений напряженности ЭМП ПЭМИ для различных частот F_N гармоник тестового сигнала, которые привели в итоге к весьма значительному расхождению результатов расчета радиуса R_2. Графики представляют собой зависимость напряженности ЭМП $E\left(мкВ/м\right)$ от расстояния $d\left(м\right)$. В отмеченных на графиках контрольных точках был проведен расчет значений радиуса зоны R_2 при размещении приемной антенны в этих точках. Границы ближней и дальней зон обозначены L_1 и L_2 соответственно.

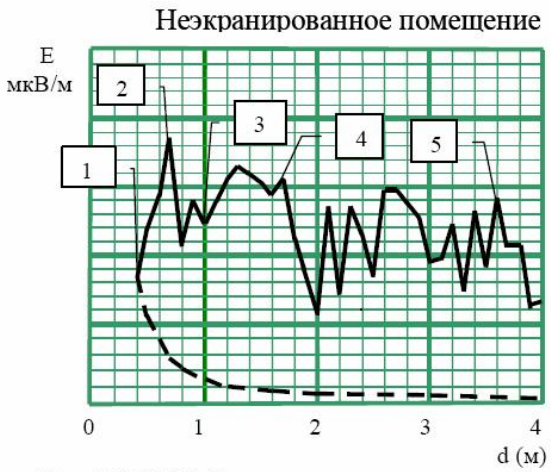
После каждой пары графиков в таблицах 1- 4 приведены результаты расчета значений радиуса R_2 зоны 2 в обозначенных на графиках точках, выполненного в полном соответствии со сборником методических материалов 1977 года (с проведением более точных расчетов).

На рисунках 1- 4 график реального распределения напряженности ЭМП ПЭМИ в зависимости от расстояния изображен сплошной линией, а график расчетного распределения (соответствует принятой в методиках СИ усредненной стандартной функции ослабления ЭМП, измеренного при расстоянии до измерительной антенны $d = 0{,}4$ м) - пунктирной линией.



F_N = 243 МГц (горизонтальная поляризация),
L_1 = 0,20 м, L_2 = 3,70 м

Рисунок 1



F_N = 748,3 МГц (горизонтальная поляризация),
L_1 = 0,06 м, L_2 = 1,20 м

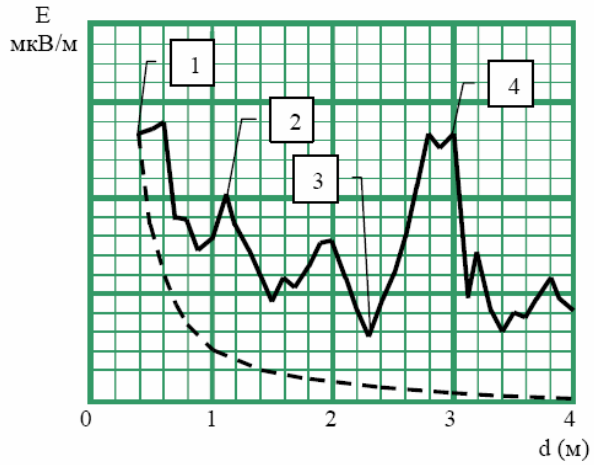
Рисунок 2

Таблица 1 – Значения R_2 в контрольных точках графика (рисунок 1)

Номер контрольной точки	1	2	3	4	5	6
Расстояние до антенны d (м)	0,4	0,6	1,0	1,4	1,9	3,4
Рассчитанное значение R_2 (м)	1,90	12,00	21,50	63,80	24,20	267,00

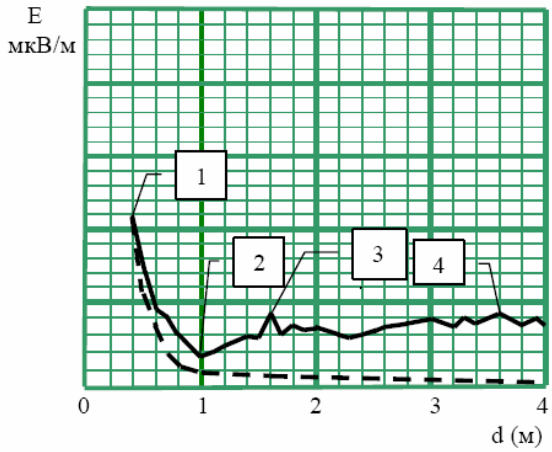
Таблица 2 – Значения R_2 в контрольных точках графика (рисунок 2)

Номер контрольной точки	1	2	3	4	5
Расстояние до антенны d (м)	0,4	0,7	1,0	1,7	3,6
Рассчитанное значение R_2 (м)	0,50	7,60	5,20	-	-



F_N = 243 МГц (вертикальная поляризация),
L_1 = 0,20 м, L_2 = 3,70 м

Рисунок 3



F_N = 39,4 МГц (вертикальная поляризация),
L_1 = 1,22 м, L_2 = 22,84 м

Рисунок 4

Таблица 3 – Значения R_2 в контрольных точках графика (рисунок 3)

Номер контрольной точки	1	2	3	4
Расстояние до антенны d (м)	0,4	1,1	2,3	3,0
Рассчитанное значение R_2 (м)	5,90	26,50	44,00	258,80

Таблица 4 – Значения R_2 в контрольных точках графика (рисунок 4)

Номер контрольной точки	1	2	3	4
Расстояние до антенны d (м)	0,4	1,0	1,6	3,6
Рассчитанное значение R_2 (м)	1,60	0,50	4,00	8,70

Как видно из таблиц 1-4 максимальная разница в полученных значениях радиуса R_2 зоны 2 при измерении ПЭМИ в разных точках помещений при полном соблюдении всех требований методики расчета весьма существенна (в 140 раз для экранированного и почти в 18 раз для неэкранированного помещения). Причиной этого является значительная интерференция электромагнитных волн ПЭМИ в помещениях за счет отражений от ограждающих конструкций, особенно в экранированном помещении, ограждающие конструкции которого отражают практически 100 % энергии падающих на них электромагнитных волн. В результате закон убывания напряженности ЭМП с ростом расстояния от источника излучения не является монотонным, характерным для условий свободного пространства.

По результатам эксперимента можно сделать вывод о необходимости стандартизации условий проведения СИ в части количественной оценки затухания ЭМП и аттестации помещений, предназначенных для СИ. Одним из вариантов может быть использование опыта проведения сертификационных испытаний радиоэлектронных изделий на соответствие нормам по электромагнитной совместимости (ЭМС), которые в соответствии с [4, 5] должны проводиться на аттестованных измерительных площадках. Известно, что

строительство и аттестация измерительной площадки и, в особенности, экранированной безэховой камеры, связаны со значительными затратами, однако существующую проблему, влияющую на обеспечение достоверности и воспроизводимости результатов СИ, надо решать.

Литература

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. М.: Горячая линия – Телеком, 2005 – 416 с.

2. Суворов П.А., Кондратьев А.В., Белихов С.Н. Некоторые особенности поля побочного электромагнитного излучения технических средств, обрабатывающих конфиденциальную информацию. // «Специальная техника», № 2, 2004.

3. Вихлянцев С.П., Петров В.В., Симонов М.В., Андриенко А.А. Определение границ ближней и дальней зоны при измерениях ПЭМИ, // «Конфидент», № 4-5, 2002.

4. СИСПР 16-1: Требования к аппаратуре для измерения радиопомех и помехоустойчивости и методы измерений

5. СТБ ГОСТ Р 51320-2001 Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний технических средств – источников индустриальных радиопомех.

И.В.МУРИНОВ, С.В.ХОДЯКОВ, С.М.КИРИЕНКО

К ВОПРОСУ ОПРЕДЕЛЕНИЯ ПЕЛЕНГА В МОБИЛЬНОЙ СИСТЕМЕ РАДИОМОНИТОРИНГА

Одной из задач, решаемых системой радиомониторинга «Беседь», является локализация источника радиоизлучения на местности. Для решения этой задачи система используется в мобильном варианте и содержит пеленгаторную антенну, модули, выполняющие функции приёмного устройства, навигации, цифровой обработки сигналов, коммутации и управления. Для осуществления пеленга в системе применён цифровой метод обработки информационных сигналов, реализуемый соответствующим программным обеспечением.

Программное обеспечение системы содержит алгоритмы, осуществляющие обработку выходных сигналов приёмного устройства после их аналого-цифрового преобразования, а также настройку и общее управление системой в режиме пеленга и отображение его результатов на электронной карте. В системе также используются вспомогательные программные модули, необходимые для проверки её работоспособности.

Сложность осуществления пеленга в городских условиях с помощью одиночной станции радиоконтроля [1,2] обусловила включение в систему алгоритмов, реализующих квазистационарный метод и метод автоматического вычисления координат источников в движении.

В докладе представлено описание математической модели использованного в системе квазидоплеровского метода определения пеленга, в соответствии с которым была создана его программная модель. Данная модель была необходима и применялась при исследовании эффективности различных математических алгоритмов, разрабатывавшихся для вычисления расчётного угла пеленга. Модель позволяет имитировать для заданного пеленга информационные сигналы пеленгаторной антенны и сигналы пеленгационных приёмников, а также контролировать все этапы обработки этих сигналов в процессе вычисления пеленга. Кроме имитации в программной модели предусмотрена возможность использовать результаты оцифровки сигналов, которые были сформированы пеленгационными

приёмниками в процессе пеленга реального источника радиосигнала и сохранены вспомогательным программным модулем системы в виде файлов данных.

Программная модель пеленгатора предоставила возможность оперативно оценивать работоспособность и эффективность алгоритмов пеленга. Это сделало целенаправленным и упростило процесс разработки программного обеспечения системы в части пеленга.

Литература

1. Ашихмин А.В., Козьмин В.А., Рембовский А.М. Наземные мобильные комплексы радиоконтроля и пеленгования. - Специальная техника, 2002, специальный выпуск.

2. Глазнев А.А., Козьмин В.А., Литвинов Г.В., Шадрин И.А. Многостанционные системы радиоконтроля и определения местоположения источников радиоизлучения - Специальная техника, 2002, специальный выпуск.

А.М.ПРУДНИК, С.Н.ПЕТРОВ, В.Б.СОКОЛОВ,
Т.В.БОРБОТЬКО, Л.М.ЛЫНЬКОВ

КОНСТРУКЦИИ ПАНЕЛЕЙ ДЛЯ ЭЛЕКТРОМАГНИТНО-АКУСТИЧЕСКОЙ ЗАЩИТЫ ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ

Для защиты выделенных помещений от утечки речевой информации по акустическим каналам в настоящее время широко используется метод активного зашумления, реализуемый за счет применения генераторов акустического шума (белый, окрашенный шум, речеподобная помеха). Недостатком такого метода является воздействие акустического шума, создаваемого в воздушном пространстве защищаемого помещения на человека. Данный недостаток исключается при использовании пассивных методов защиты, в частности звукоизоляции. Широко применяемые сегодня звукоизоляционные материалы обладают рядом недостатков, основными из которых являются: значительная толщина конструкции, сложность ее монтажа и высокая стоимость. Особый интерес представляет разработка материалов и конструкций устройств защиты на их основе для одновременного блокирования электромагнитного и акустического каналов утечки информации. Практическое применение таких средств защиты позволит экономически обосновать реализацию пассивных методов защиты информации.

Целью настоящей работы была создание пассивных средств защиты информации от утечки по электромагнитным и акустическим каналам для использования их в выделенных помещениях. Реализация поставленной цели возможна за счет создания средств защиты, имеющих многослойную конструкцию, где каждый из слоев выполняется из различных типов материалов с необходимыми звукоизолирующими и экранирующими характеристиками.

Исследования экранирующих характеристик созданных панелей электромагнитно-акустической защиты проводили в диапазоне частот 0,009-120 ГГц. Для чего указанный диапазон был разделен на ряд поддиапазонов. В более низкочастотной области в качестве средств измерений использовался анализатор спектра Agilent E4407B, в высокочастотной – панорамные измерители КСВН и ослабления с необходимой антенной техникой [1]. Для измерения звукоизоляции акустического шума использовался анализатор акустического шума “Маном-4/2” [2].

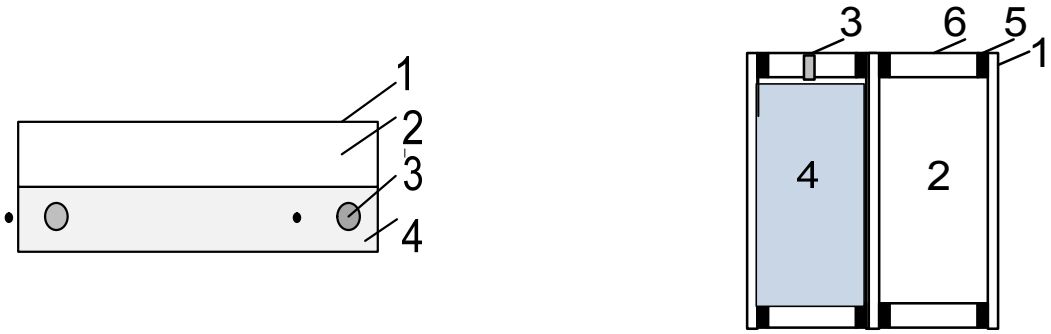
Разработанная конструкция панели для закрепления на стенах защищаемого помещения состоит из двух листов стекломагнезита толщиной 4 мм, между которыми размещается слой резинобитумной мастики толщиной 4 мм, покрытый слоем алюминиевой

фольги. Соединение слоев между собой обеспечивается за счет их склеивания в процессе производства.

Предложенная конструкция обеспечивает подавление акустических волн не менее 20 дБ в диапазоне частот 160 – 8000 Гц, за счет использования материалов с различными акустическими сопротивлениями и ослабление электромагнитных волн не менее 25 дБ в диапазоне частот 0,009 - 120 ГГц, что обусловлено применением фольгированного слоя резинобитумной мастики заполненной углеродным наполнителем (до 10%).

Применение стекломагнезита [3] позволяет обеспечить огнестойкость конструкции до 800°С, а так же возможность ее различных видов отделки путем покраски, оклейки обоями, облицовки плиткой и т.д. Экранирующие и звукоизолирующие характеристики панели выдерживаются в соответствие вышеуказанным значением в температурном диапазоне от минус 50°С до плюс 50°С, а также при использовании в условиях повышенной влажности (относительная влажность воздуха 98% при температуре плюс 25°С).

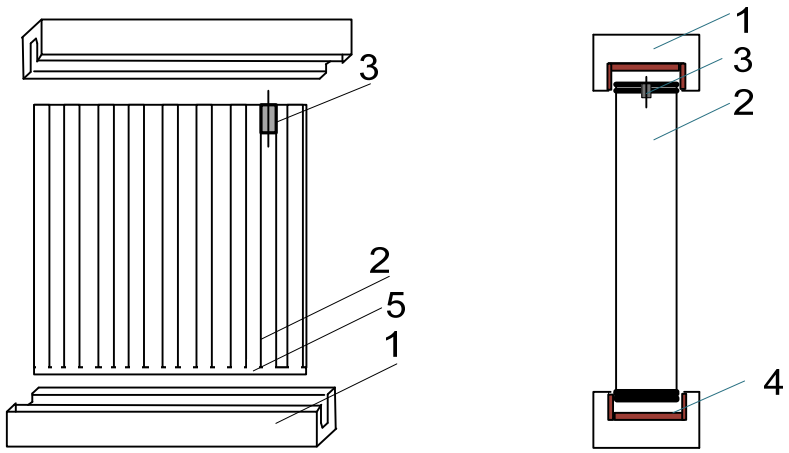
Для монтажа в оконных проемах разработана конструкция оптически прозрачной панели электромагнитно-акустической защиты выполняемой на основе стеклопакета [4]. Такая конструкция содержит три стекла толщиной 4 мм, отстоящих одно от другого на расстояние 6 мм и образующих две камеры. Одна камера заполнена водным раствором хлорида натрия и высокомолекулярных спиртов (рисунок 1), вторая – воздухом, что позволяет обеспечить ослабление звуковой волны до 70 дБ в диапазоне частот 160 – 8000 Гц при одновременном ослаблении электромагнитного излучения до 30 дБ за счет механизмов дипольных и релаксационных потерь в жидкости.



1 – стекло; 2 - камера, заполненная воздухом; 3 – капилляр для заполнения камеры водным раствором; 4 – камера, заполненная водным раствором; 5 – клей-герметик; 6 – дистанционная планка

Рисунок 1 – Схематичное изображение конструкции панели электромагнитно-акустической защиты на основе стеклопакета

Снижение массы и увеличение прочности таких конструкций возможно за счет использования полимерных материалов, например сотового поликарбоната [5] (рисунок 2), что позволяет в три раза снизить массу (при сопоставимых толщинах и площадях). Панель из сотового поликарбоната толщиной 10 мм, заполненная водным раствором хлорида натрия, обладает ослаблением электромагнитного излучения до 28 дБ, при звукоизоляции воздушного шума до 40 дБ.



1 – рама; 2 – панель сотового поликарбоната; 3 - штуцер; 4 – герметик;
5 – канал, соединяющий ячейки панели

Рисунок 2 - Схематичное изображение конструкции панели электромагнитно-акустической защиты на основе сотового поликарбоната

Срок службы разработанных панелей электромагнитно-акустической защиты определяется сроками службы составных частей, надежностью клеевого соединения и составляет, согласно проведенным расчетам, не менее 5 лет.

Все вышерассмотренные конструкции позволяют обеспечить комплексную защиту информации в выделенном помещении от утечки по акустическому и электромагнитному каналам.

Литература

1. Богуш, В.А. Электромагнитные излучения. Методы и средства защиты / В.А. Богуш [и др.] ; под ред. Л.М. Лынькова. – Минск : Бестпринт, 2003. – 406 с.

2. Пулко Т.А. Пассивные технические средства обеспечения информационной безопасности от утечки по электромагнитному, оптическому и акустическому каналам / Т.А. Пулко [и др.]; под общ. ред. Л.М. Лынькова. – Минск: Бестпринт, 2010. – 225 с.

3. ТУ 5742-001-79255329-2007. Листы стекломагнезитовые. Ростов-на-Дону: ГОУВПО “Ростовский государственный университет”, 2007. – 29 с.

4. Интегрированная защитная панель : пат. 3904 Респ. Беларусь, МПК7 H 01 Q 17/00, E 06 B 5/00 / Л.М. Лыньков, Т.В. Борботько, С.Н. Петров ; заявитель Учреждение образования “Белорусский государственный университет информатики и радиоэлектроники”. – № u20070115 ; заявл. 15.02.07 ; опубл. 04.07.07 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2007. – № 5 – С. 230.

5. Сотовый поликарбонат. [Электронный ресурс]. – 2010. – Режим доступа: http://www.sadovnik.by/catalog2.php?id=761&cat=42. – Дата доступа: 12.03.2011.

П.И.САВКОВ, А.В.ДЕМИДОВ

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ В ИНТЕРЕСАХ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Информационные системы (ИС) являются сложными техническими комплексами и оснащаются разнообразными программными средствами, образующими функциональное или прикладное (ФПО) и системное (СПО) программное обеспечение. Программные комплексы (ПК) является наиболее развитой по структуре и функциональным связям составной частью ИС.

Специфика применения ИС в условиях несанкционированных (НСВ) и непреднамеренных (НПВ) программных воздействий обусловливает особые требования, предъявляемые к надежности функционирования ПК ИС. Нарушение работоспособности ПК может привести к потере отдельных функций ИС или задержке их выполнения, искажению информации или управляющих воздействий. Задача по противодействию НСВ и НПВ возлагается на комплекс средств безопасности (КСБ) ИС.

Возможность для реализации НСВ и НПВ обусловлена наличием в ПК уязвимостей. Под уязвимостью понимается возникающее в результате ошибок или особенностей проектирования, программирования, эксплуатации или постороннего вмешательства (модификации в ходе эксплуатации) расширение возможностей доступа либо за счет роста функциональных возможностей прикладных программ, которые не запрещаются средствами защиты, либо за счет сокращения возможностей самих средств защиты. Возникшее в результате уязвимости расширение возможностей по доступу не обязательно будет противоречить политике безопасности ПК. Таким образом, возможно осуществление вредоносных воздействий, не нарушающих политику безопасности, но несущих угрозу информационной системе [1].

В связи с принципиальной ограниченностью существующих технологий обнаружения и блокирования вредоносных программных воздействий, повышение устойчивости функционирования ПК в условиях успешных НСВ и НПВ является необходимым требованием для КСБ ИС.

Разработка программного обеспечения, нечувствительного к определенным типам ошибок и искажений, считается более перспективным направлением по сравнению с разработкой безошибочных программ [2]. Повышение устойчивости ПК к ошибкам достигается за счет введения избыточности (резервирования), ограниченного обслуживания и изоляции ошибок [3].

Рассмотрим схему КСБ ПК с точки зрения обеспечения устойчивости функционирования. Процессы с одинаковым уровнем привилегий функционируют в рамках одной среды безопасности КСБ. Компрометация или отказ любого из процессов в соответствии с позицией «крайнего пессимизма» предполагает отказ всех остальных процессов. Используя подходы теории надежности к построению моделей надежности, можно представить КСБ ПК в виде системы с последовательно-параллельной структурой из $N = S \cup U$ объектов ИТ, где S – множество привилегированных служб s_i, $i = \overline{1,m}$, которые составляют доверенную вычислительную базу ИС, а U – множество прикладных приложений уровня пользователя u_j, $j = \overline{1,k}$.

КСБ включает средства безопасности (СБ) объектов ИТ, входящих в состав ПК, и обеспечивает: а) защиту от НСВ и НПВ элементов u_j на элементы s_i; б) защиту от НСВ и НПВ элементов u_j на другие элементы множества U. Следует отметить, что КСБ ПК не предусматривает защиту от НСВ и НПВ элементов s_i на другие элементы множества S, а также на элементы u_j множества U.

Один из ключевых подходов решения задачи повышения устойчивости функционирования ПК может основываться на парадигме «Гарантоспособные (надежные и безопасные) системы из ненадежных компонентов» (Dependable Systems out of Undependable Components – DSooUDC). В качестве такого компонента КСБ для программной реализации методов повышения устойчивости функционирования ПК в различных работах предлагаются технология виртуализации [4,5,6].

Термин «виртуализация» имеет довольно широкое толкование и в общем случае означает отделение логического процесса от физического способа его реализации. Отсюда понятно, что виртуализация — это одна из ключевых концептуальных идей в сфере ИТ. В упрощенном виде она подразумевает, что пользователь отделен от реальных вычислительных процессов и работает с ними в удобном для себя виде, а не в том, в каком они происходят на самом деле.

Основная цель использования виртуализации состоит в повышении эффективности использования ИТ и снижении затрат, связанных с приобретением и эксплуатацией программных и аппаратных средств. Можно сказать, что с точки зрения надежной эксплуатации программного обеспечения, идеальный вариант — это использование отдельного компьютера под каждое приложение и работа в монопольном режиме. Но такая организация явно неоптимальна с точки зрения затрат на технику. Отсюда возникает задача использовать один компьютер для работы нескольких разных программ.

В принципе поддержка многопользовательского и многозадачного режимов — это функция любой современной ОС. Применение дополнительных средств виртуализации обусловлено необходимостью одновременной работы нескольких, в том числе разнородных, операционных сред и недостаточным уровнем изоляции приложений с одинаковым уровнем привилегий.

Применение технологий виртуализации позволяет реализовать подходы к повышению устойчивости ПК к отказам, а именно ограниченное обслуживание, изоляцию ошибок и резервирование.

Перенос выполнения большинства привилегированных процессов на уровень пользователя при виртуализации снижает их полномочия (особенно по доступу к аппаратным ресурсам) и ограничивает их возможности по реализации НСВ и НПВ на другие компоненты ПК.

Создание для компонентов ПК с одинаковым уровнем полномочий изолированных виртуальных окружений обеспечивает снижение влияния отказа отдельного компонента ПК на другие компоненты системы. Такой подход позволяет повысить эффективность использования имеющейся ИТ-инфраструктуры за счет параллельного выполнения критически важных приложений – объектов ИТ и формирования вокруг них отдельных сред безопасности.

Отделение объектов виртуализации от физической инфраструктуры ИС в соответствии с принципом инкапсуляции создает возможность для их резервирования путем построения виртуальных кластерных систем. Это позволяет управлять интенсивностью восстановления работоспособности ПК в условиях отказов, увеличить допустимое время на принятие решения персоналом ИС по реагированию на НСВ (НПВ), а также обеспечить динамическую реконфигурацию ИТ-инфраструктуры в соответствии с условиями обстановки.

Литература

1. Зегжда Д.П. Принципы и методы создания защищенных систем обработки информации [Электронный ресурс] : Дис. … док-ра техн. наук : 05.13.19. – М.: РГБ, 2003.

2. Черкесов Г.Н. Надежность аппаратно-программных комплексов.– СПб.:Питер, 2005.

3. Майерс. Г. Надежность программного обеспечения. - М.: Мир, 1980.

4. Таненбаум Э., Босс Х. Можем ли мы сделать операционные системы надежными и безопасными [Электронный ресурс]. – Режим доступа: http://www.citforum.ru.

5. Золотарёв С.В. LynxSecure: время операционных систем реального времени в MILS-архитектуре пришло [Электронный ресурс]. – Режим доступа: http://www.rtsoft.ru.

6. Rutkowska J. Qubes OS Architecture. – Режим доступа: http://qubes-os.org.

А.А.ТЕПЛЯКОВ, Е.А.ФЕДОРОВ, В.А.КРУК

ОПЫТ РАЗРАБОТКИ ШИРОКОПОЛОСНЫХ ГЕНЕРАТОРОВ ШУМА

ПЭМИ ПК представлен колебаниями в достаточно широком диапазоне частот от единиц мегагерц и до нескольких гигагерц. Диаграмма направленности побочного электромагнитного излучения ПК не имеет ярко выраженного максимума, взаиморасположение составных частей ПК отличается большим количеством вариантов. Поляризация излучений ПК, как правило, линейная и определяется взаиморасположением соединительных проводов и отдельных блоков. Соединительные неэкранированные провода и кабели являются главным фактором возникновения ПЭМИ [1].

Для защиты от утечки по каналам ПЭМИ можно использовать пассивные (экранирование и уменьшение энергии защищаемого сигнала) и активные методы (зашумление). Первые из них чрезвычайно дороги, вторые же имеют ограничения, связанные с трудностями генерации мощных широкополосных сигналов и влияние этих сигналов на окружающую среду. Одним из решений, позволяющих получить мощный широкополосный шумовой сигнал, является использование генераторов основанных на эффекте хаоса, создаваемого связанными генераторами на основе нелинейных элементов[2]. Предлагаемые решения позволяют получить мощный шумовой сигнал в широкой полосе частот. Недостатком этого решения являлась высокая рассеиваемая (тепловая) мощность, что приводит к необходимости применения радиаторов с большой излучающей поверхностью, ухудшающей массогабаритные параметры устройства или вентиляторов, приводящих к снижению надежности устройств за счет механической компоненты- вентилятора. В качестве нелинейных элементов используются мощные СВЧ транзисторы с граничной частотой 2-3 ГГц, что ограничивает верхнюю частоту генерируемого сигнала и одновременно увеличивает количество выделяемого тепла.

В результате проведенных экспериментов, было выявлено, что увеличение числа нелинейных элементов, включенных параллельно двух до восьми, понижает коллекторное напряжение, при котором система переходит в режим генерации шумового сигнала с 8 до 3В. Применение же транзисторов с граничной частотой 6-7 ГГц позволяет расширить полосу генерируемого сигнала до 4-5 ГГц и уменьшить количество выделяемого тепла до уровня, рассеиваемого печатной платой. Вид полученного шумового сигнала, измеренный в разных диапазонах частот, приведен на рис.1 и рис.2.

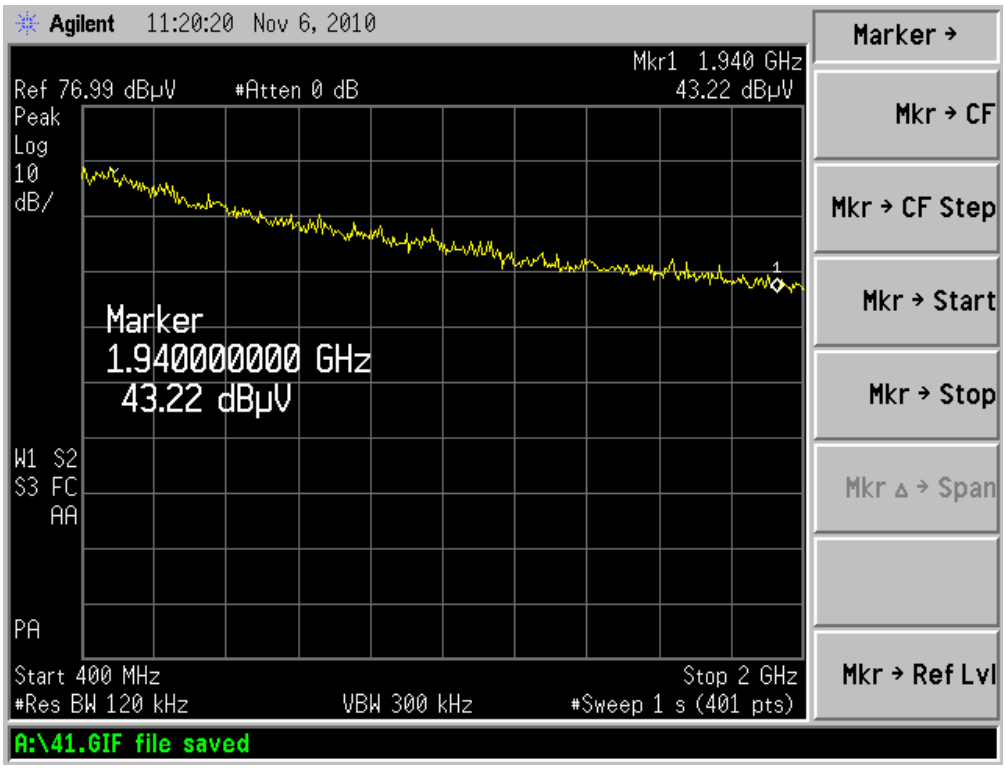


Рис.1

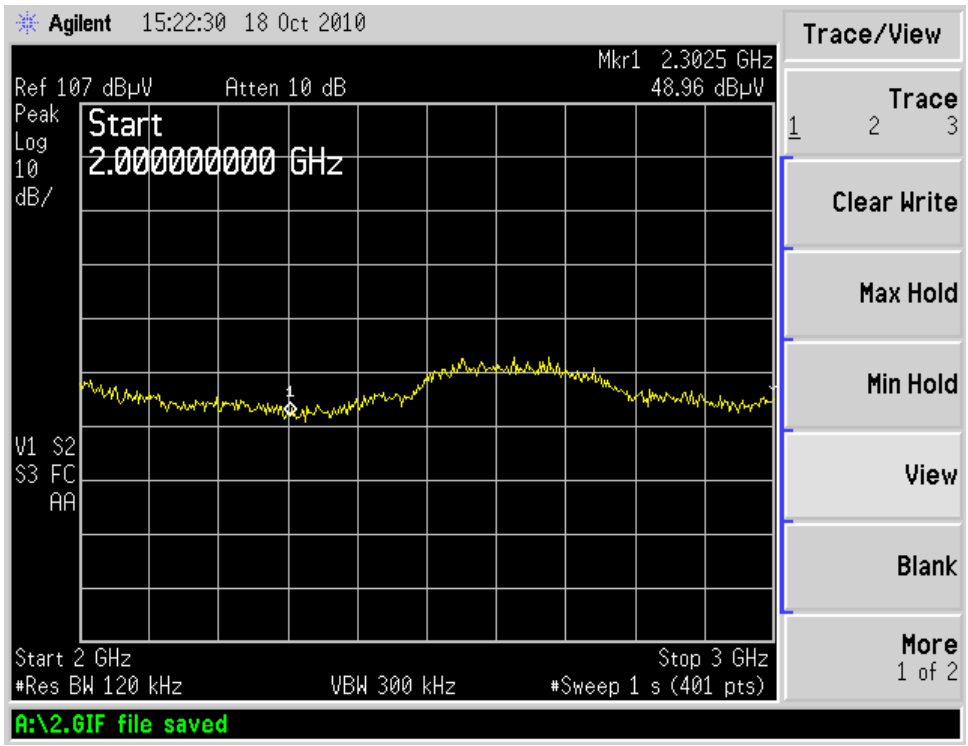


Рис.2

Литература

1. Бойцев О.М. Утечка информации через побочные электромагнитные излучения. Сетевые решения. №4 2007.

2. Иванов В.П. Сверхширокополосные генераторы шума и их практическое применение. Успехи современной радиоэлектроники. №1, 2008 г.

А.Г.ФИЛИППОВИЧ

ЭЛЕКТРОДИНАМИЧЕСКОЕ МОДЕЛИРОВАНИЕ КАНАЛА ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ПЭВМ

В настоящее время основным средством обработки информации во всех сферах деятельности общества является ПЭВМ. Часто характер обрабатываемой информации в средствах вычислительной техники предъявляет повышенные требования к защищённости ПЭВМ от различного рода угроз информационной безопасности. Одним из основных каналов утечки информации в средствах вычислительной техники являются каналы побочных электромагнитных излучений [1]. Их образование связано с тем, что в средствах вычислительной техники информация обрабатывается и передаётся с помощью электрических сигналов, циркулирующих в аппаратных устройствах и интерфейсах средств вычислительной техники. Указанные электрические сигналы являются источниками электромагнитных полей, излучаемыми ПЭВМ. Как показывают исследования [1-5], информация, передаваемая побочными электромагнитными излучениями, может быть перехвачена средствами разведки на расстояниях десятков и сотен метров, и зачастую этого расстояния достаточно для установки средств разведки. В этой связи видится необходимым осуществлять оценку опасности побочных электромагнитных излучений ПЭВМ до начала обработки информации с целью определения необходимых мероприятий для защиты информации.

Как правило, защищённость информации, обрабатываемой ПЭВМ, от утечки по каналам побочных электромагнитных излучений определяется таким параметром, как отношение сигнала к шуму на входе приёмного устройства средства разведки [1,6]:

$$q = \frac{U_c \sqrt{\dfrac{\Delta F}{2F_T}}}{U_{ø}(\Delta F)}, \qquad (1)$$

где U_c – напряжение сигнала на входе разведывательного приёмника, $U_{ø}(\Delta F)$ – напряжение шумов на входе разведывательного приёмника, измеренное в полосе частот ΔF, ΔF – ширина спектра тестового сигнала, $F_{\dot{O}}$ – тактовая частота тестового сигнала. Напряжение тестового сигнала на входе разведывательного приёмника для электрической и магнитной составляющих электромагнитного поля рассчитывается по формулам [6]:

$$U_{ci} \approx \frac{h_a}{2}\sqrt{\sum_{\Delta F_i}\left(\frac{E_{cj}}{V_j(R)}\right)^2}, \quad U_{ci} \approx \frac{h_a}{2}\sqrt{\sum_{\Delta F_i}\left(\frac{\rho H_{cj}}{V_j(R)}\right)^2}, \qquad (2)$$

где E_{cj}, ρH_{cj} – напряжённости электрической и магнитной составляющих электромагнитного поля тестового сигнала на j-й частоте в частотном интервале ΔF_i в точке проведения измерений соответственно, h_a – действующая высота антенны разведывательного приёмника, $V_j(R)$ – коэффициент затухания электромагнитного поля, R – расстояние от средства вычислительной техники.

В общем случае расчёт коэффициента затухания электромагнитного поля ПЭМИ $V_j(R)$ представляет собой сложную задачу. Сложность расчёта коэффициента $V_j(R)$ обусловлена двумя причинами: широким частотным диапазоном ПЭМИ и близостью точки измерения к источнику электромагнитного излучения ПЭМИ. Вследствие этих причин точка

проведения измерений может находиться в ближней, промежуточной или дальней зонах излучения ПЭМИ.

В настоящее время для расчёта коэффициента затухания электромагнитного поля ПЭМИ, как правило, пользуются формулами, справедливыми для элементарных электрических или магнитных излучателей [1]. Такой подход справедлив для частот ниже 300 МГц, когда длина волны ПЭМИ существенно превышает геометрические размеры источника излучения. Как показывают исследования, на более высоких частотах использование моделей элементарных электрических излучателей может привести к существенным погрешностям в определении параметров эффективности защиты информации. Эффективно в смысле точности решения и времени расчёта на ЭВМ указанная задача может быть решена на основе интегрального представления векторов напряжённостей электрического и магнитного полей [7]:

$$\begin{aligned}\vec{E}(M_0) = \oint_S \{ & \left[gradG(M,M_0), \left[\vec{n}, \vec{E}(M)\right]\right] - i\omega\mu_a G(M,M_0)\left[\vec{H}(M), \vec{n}\right] - \\ & - \left(\vec{n}, \vec{E}(M)\right) gradG(M,M_0) \} ds + \int_V \vec{F}^e_{cm}(M) G(M_0,M) dv \\ \vec{H}(M_0) = \oint_S \{ & \left[gradG(M,M_0), \left[\vec{n}, \vec{H}(M)\right]\right] + i\omega\varepsilon_a G(M,M_0)\left[\vec{E}(M), \vec{n}\right] - \\ & - \left(\vec{n}, \vec{H}(M)\right) gradG(M,M_0) \} ds + \int_V \vec{F}^m_{cm}(M) G(M_0,M) dv\end{aligned} \qquad (3)$$

где $\vec{E}, \vec{H}$ – вектора напряжённостей электрического и магнитного полей, $G = \frac{e^{-ikr}}{4\pi r}$ – функция Грина свободного пространства, делённая на 4π, r – расстояние между точкой наблюдения и интегрирования, M – точка интегрирования, M_0 – точка наблюдения, ε_a, μ_a – абсолютные электрическая и магнитная проницаемости среды, $\vec{n}$ – вектор нормали к поверхности S, ω – круговая частота, F^e_{cm} и F^m_{cm} – функции сторонних источников поля.

На основании выражения (3) была разработана математическая модель электромагнитного поля ПЭМИ, образуемыми в результате работы ПЭВМ. Результаты моделирования хорошо согласуются с экспериментальными исследованиями. Полученная модель может быть использована для оценки защищённости ПЭВМ от утечки по каналам ПЭМИ.

Литература

1. А.Г. Пятачков, «Защита информации, обрабатываемой вычислительной техникой, от утечки по техническим каналам», Москва, 2007 г. – 196 стр.

2. W. van Eck, «Electromagnetic radiation from video display units: an eavesdropping risk?», Computers&Security, №4, 1985, стр. 269-286.

3. M.G. Kuhn, «Compromising emanations: eavesdropping risks of computer displays», Technical report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, 2003.

4. H. Tanaka, O. Takizawa, A. Yamamura, «A trial of the interception of display image using emanation of electromagnetic wave», Journal of the Institute of Image Electronics Engineers of Japan, vol. 34, №2, 2005, стр. 213-223.

5. H. Tanaka, O. Takizawa, A. Yamamura, «Evaluation and improvement of the tempest fonts», Information security applications, vol. 3325, Springer Berlin/Heidelbers, 2005, стр. 457-469

6. А.А. Хорев, «Оценка эффективности защиты средств вычислительной техники от утечки информации по техническим каналам», Специальная техника, №4, стр. 56-64, №5, стр. 40-51, 2007.

7. Вычислительные методы в электродинамике, под ред. Р. Митры./ пер. с анг. под ред. Бурштейна Э.Л. – М.: Мир, 1977.

В.А.ФУНТИКОВ, А.И.ИВАНОВ

ОЦЕНКА «НАНО» И «ПИКО» ВЕРОЯТНОСТЕЙ ЗАВИСИМЫХ СОБЫТИЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА МАЛЫХ ТЕСТОВЫХ ВЫБОРКАХ ПО ГОСТ Р 52633.3

В настоящее время Россия в рамках технического комитета «Защита информации» (ТК №362) активно ведет работы по созданию пакета национальных стандартов, регламентирующих требования к средствам биометрической аутентификации личности, обеспечивающих конфиденциальность, анонимность, обезличенность массового оборота персональных биометрических данных. Одним из наиболее важных стандартов является ГОСТ Р 52633.3 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».

Значимость этого стандарта обусловлена тем, что доверие к той или иной технологии (в том числе к технологии высоконадежной биометрико-нейросетевой аутентификации) определяется наличием сертификатов соответствия требованиям национальных и международных стандартов. В свою очередь тестирование нейросетевых преобразователей биометрия-код (ПБК) является достаточно сложной научно-технической задачей из-за высоких значений стойкости ПБК к атакам подбора. Процедуры тестирования по ГОСТ Р 52633.3, с одной стороны позволяют получать достоверные численные оценки стойкости к атакам подбора ПБК, а с другой стороны отказаться от использования больших и сверхбольших баз биометрических образов «Чужой».При решении задачи тестирования ПБК предполагается, что выходные коды нейросетевого ПБК в пространстве расстояний Хэмминга от кода «Свой» могут быть описаны биномиальным законом зависимых (связанных между собой) событий.

Известен классический закон распределения плотностей вероятности независимых событий соответствующий численному эксперименту по схеме Бернулли. Применительно к ПБК в рамках гипотезы независимости разрядов выходного кода длиной – n, злоумышленник сможет угадать k разрядов кода «Свой» с вероятностью описываемой классическим биномиальным законом:

$$P(k,n,P(.)) = \left[\frac{n!}{k!\cdot(n-k)!}\right]\cdot\{P(.)\}^{k}\cdot\{1-P(.)\}^{n-k}, \qquad (1)$$

где P(k) – вероятность угадывания k разрядов выходного кода длиной – n;

P(.) – показатель асимметрии использованной в опытах Бернулли единственной монеты. P(.) либо совпадает с вероятностью появления состояний «0», если состояние «0» для асимметричной монеты наиболее вероятно, либо совпадает с вероятностью появления состояний «1», если состояние «1» для асимметричной монеты наиболее вероятно.

Очевидно, что можно усложнить схему Бернулли и последовательно бросать некоторую последовательность асимметричных меченных номером монет (каждая монета имеет свой номер последовательного бросания). Кроме того, каждая из монет обладает собственной асимметрией, но последовательность поочередного бросания монет всегда одна и та же. Эта ситуация соответствует разной стабильности состояний в каждом из разрядов биометрического кода и приводит к следующей модификации классической записи:

$$P(k,n,P(.)) = \left[\frac{n!}{k!\cdot(n-k)!}\right]\cdot\{\prod_{i=1}^{k}P_i(.)\}\cdot\prod_{j=1}^{n-k}\{1-P_j(.)\}, \qquad (2),$$

где $P_i(.)$ - показатель асимметрии одной из угаданных монет;

$P_j(.)$ - показатель асимметрии одной из неугаданных монет.

Для того чтобы вернуться к привычной степенной форме записи биномиального закона, следует использовать среднее геометрическое соответствующих показателей асимметрии:

$$P(k,n,P(\,.\,)) = \left[\frac{n!}{k!\cdot(n-k)!}\right]\cdot\{\Theta(P_i(.)\}^k\cdot\left\{\Theta(1-P_j(\,.\,))\right\}^{n-k}, \qquad (2a),$$

где $\Theta(\,.\,)$ - оператор вычисления среднего геометрического.

Модифицированная схема Бернулли с разными монетами усложняется еще сильнее, если бросать монеты не независимо, а зависимо (горстью). Тогда их состояния после падения оказываются зависимыми (коррелированными). В этом случае функция распределения значений оказывается четырехмерной, причем четвертой переменной оказывается значение математического ожидания модулей парных коэффициентов корреляции - $E(|r|)$ между случайно выбранными разрядами выходных кодов ПБК. В общем виде зависимость от корреляционных связей может быть описана следующим образом:

$$P(k,n,\Theta(\,.\,),E(|r|)) = \left[\frac{n!\cdot f_1(E(|r|)}{k!\cdot(n-k)!}\right]\cdot\{\Theta(P_i(.)\}^{k\cdot f_2(E(|r|))}\cdot\left\{\Theta(1-P_j(\,.\,))\right\}^{(n-k)\cdot f_3(E(|r|)} \qquad (3),$$

где $f_1(.),\ f_2(.), f_3(.)$ - три одномерные функции переменной - $E(|r|)$.

Нейросетевые преобразователи биометрия-код, видимо, являются первым искусственным объектом, для описания которого нельзя пользоваться упрощенной схемой Бернулли, приводящей к появлению биномиального закона независимых данных (1). Однако точного аналитического описания более сложного биномиального закона зависимых данных с разной асимметрией в каждом разряде биометрического кода (3) пока нет. На данный момент имеются только результаты имитационного моделирования распределения расстояний Хэмминга для различных значений одинаковых коэффициентов парной корреляции – r.

Примеры изменения кривых плотностей распределения для ПБК с равновероятными состояниями «0» и «1» во всех разрядах выходных кодов для интервала изменения коэффициентов парной корреляции от 0.0 до 0.5 приведены на рисунке 1.

Примеры изменения кривых плотностей распределения для ПБК с равновероятными состояниями «0» и «1» во всех разрядах выходных кодов для интервала изменения коэффициентов парной корреляции от 0.5 до 0.92 приведены на рисунке 2.

Основной проблемой при создании ГОСТ Р 52633.3 являлось то, что аналитическое четырехмерное описание биномиального закона зависимых данных (3) пока отсутствует и необходимо создать процедуры неявной оценки вероятностей ошибок второго рода ПБК. Для этой цели новый стандарт рекомендует использовать базу из 10 000 тестовых биометрических образов «Чужой». Такой размер тестовой базы примерно в 1 000 000 раз меньше, чем требуется для примитивного тестирования последовательной подстановкой всех имеющихся тестовых образов.

Для того чтобы достоверно оценить «нано» и «пико» вероятности редких зависимых (коррелированных) событий биометрической аутентификации, ГОСТ Р 52633.3 предлагает использовать генетический алгоритм подбора биометрических образов «Чужой», наиболее похожих на образ «Свой». Генетический алгоритм подбора иллюстрируется рисунком 3. В нулевом поколении выбираются наиболее близкие образы «Чужой» к образу «Свой». Далее выбранные образы скрещиваются между собой и из образов родителей получаются образы – потомки. Процедура скрещивания двух рукописных образов родителей «*знамя*» и «*Север*» иллюстрируется рисунком 4. При скрещивании образов-родителей используются процедуры морфинга, определенные в стандарте ГОСТ Р 52633.2-2010.

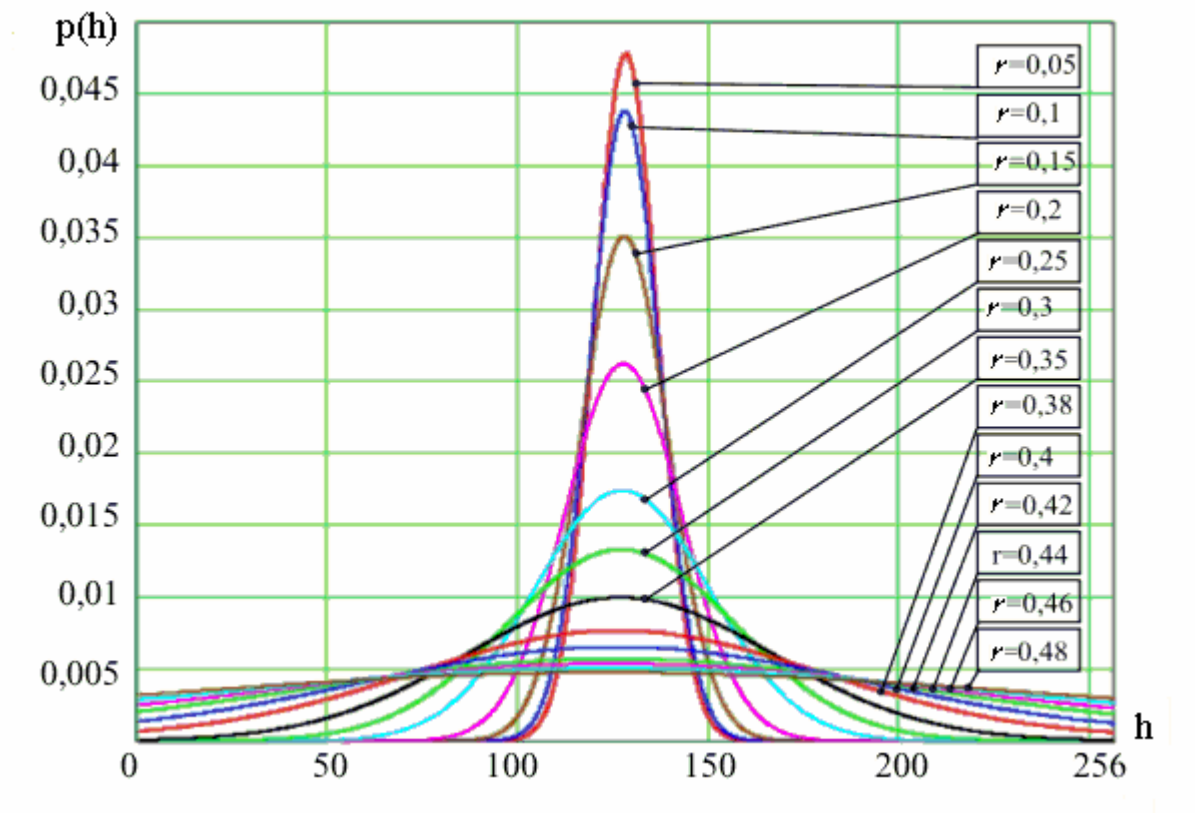


Рис. 1. Изменение плотности распределения значений меры Хэмминга образов «Чужой» для значений модуля коэффициентов парных корреляций от r=0.05 до r=0.48

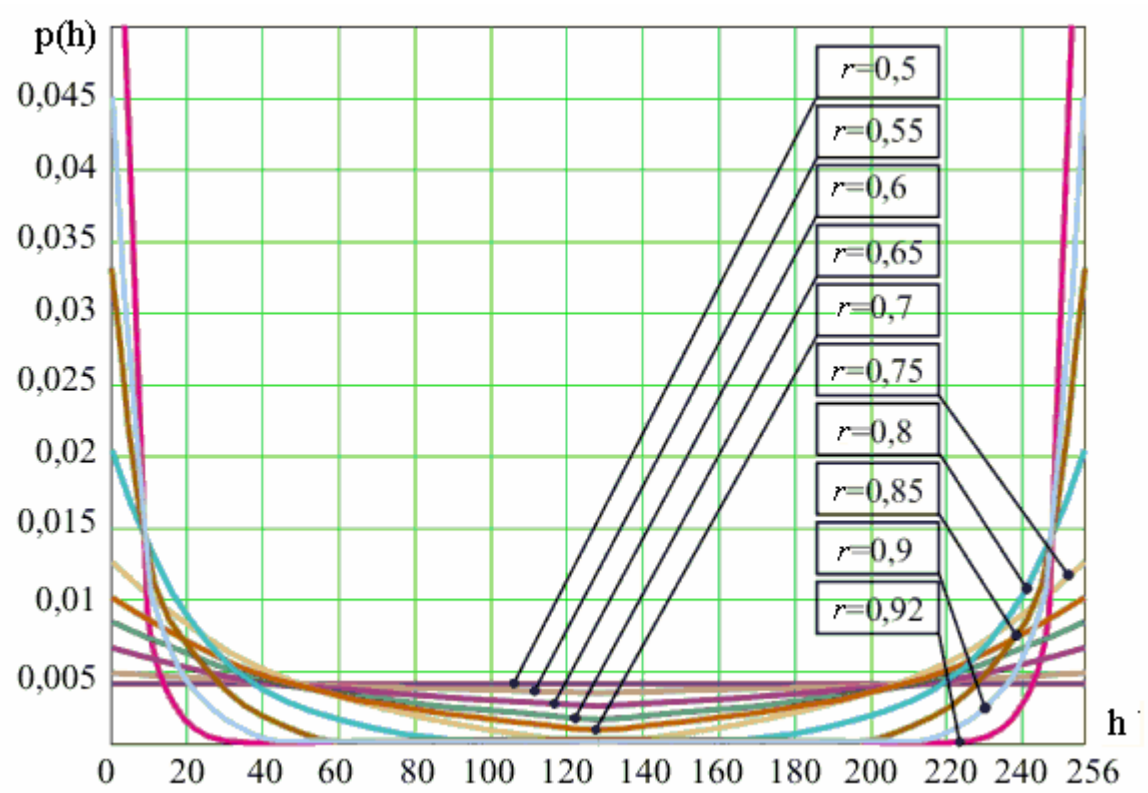


Рис. 2. Изменение плотности распределения значений меры Хэмминга образов «Чужой» для значений модуля коэффициентов парных корреляций от r=0.5 до r=0.92

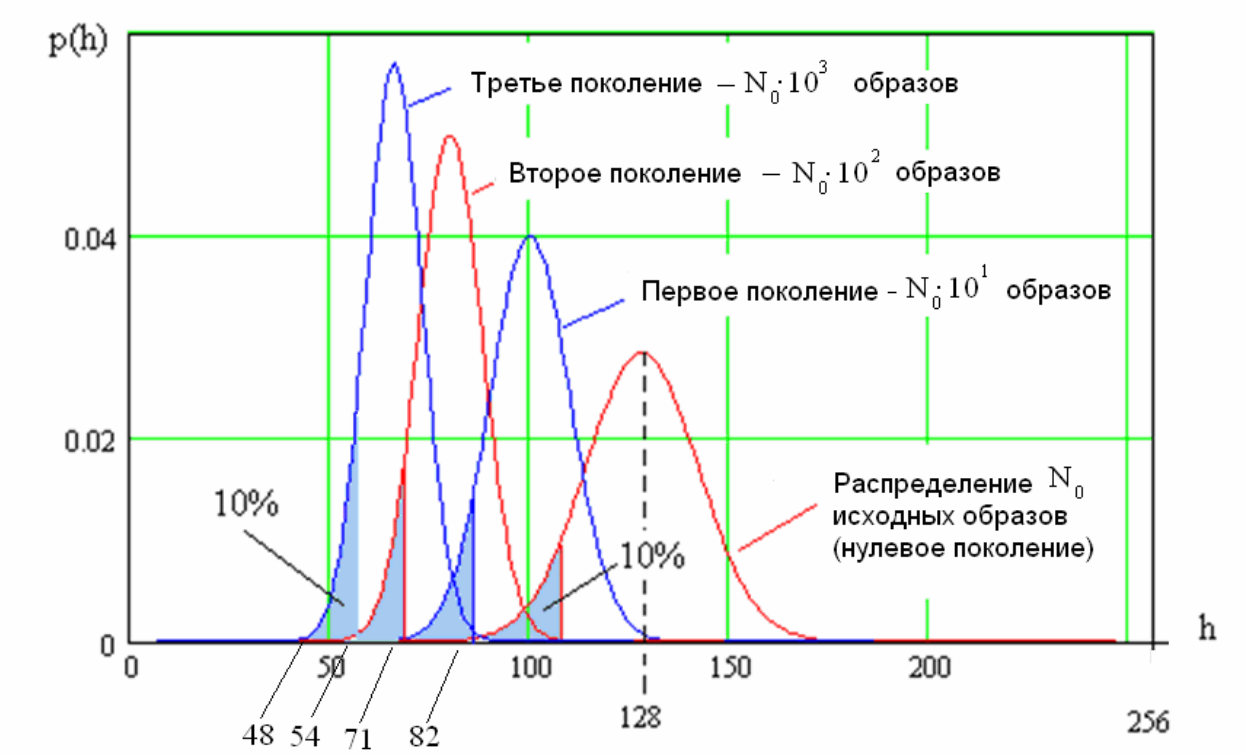


Рис. 3. Изменение плотности распределения расстояний Хэмминга для четырех поколений генетического подбора

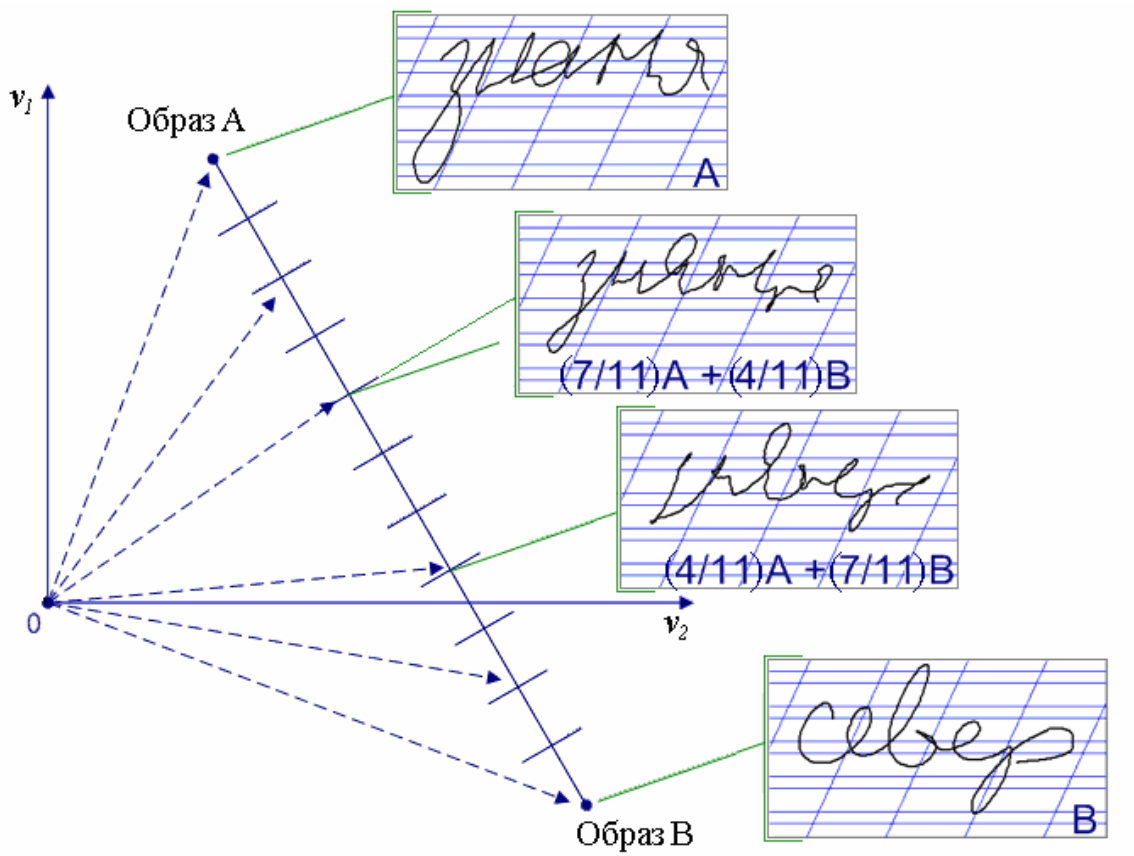


Рис. 4. Скрещивание двух образов-родителей и получение двух образов-потомков путем морфинга по ГОСТ Р 52633.2-2010

Описанной выше процедурой генетического подбора удается подобрать (синтезировать) биометрические образы «Чужой», дающие коды отклики ПБК, совпадающие с кодом «Свой» от 70% до 90%. Фактически имеется эффективная процедура компрометации образа «Свой», если выходной код ПБК для образа «Свой» известен.

Следующим этапом тестирования ГОСТ Р 52633.3 рекомендует осуществлять случайный подбор уже почти полностью скомпрометированного биометрического образа «Свой». Случайный подбор осуществляется по блок-схеме, приведенной на рисунке 5.

При этом типе тестирования большинство биометрических параметров (100%-a%) заимствуется от образа «Свой», а меньшее число биометрических параметров (a%) заимствуется от генератора псевдослучайных данных, имитирующего множество образов «Все Чужие». Тестирование по блок-схеме рисунка 5 повторяют многократно, случайно выбирая скомпрометированные и неизвестные параметры биометрического образа «Свой». Результаты тестирования усредняют.

Оценку стойкости обученного нейросетевого ПБК далее осуществляют путем умножения числа примеров образов «Чужой», потраченных на частичную компрометацию биометрического образа «Свой», на среднее число примеров образов «Чужой», потраченных на подбор уже почти полностью скомпрометированного образа «Свой» по блок-схеме рисунка 5.

В конечном итоге по процедурам ГОСТ Р 52633.3 удается оценивать «нано» и «пико» вероятности зависимых событий биометрической аутентификации, находящиеся в интервале вероятностей от $P_2 \approx 10^{-9}$ до $P_2 \approx 10^{-12}$ на тестовых базах, состоящих всего из 10 000 естественных биометрических образов «Чужой». При этом используются обычные средства вычислительной техники с обычными показателями производительности и обычными показателями размеров памяти.

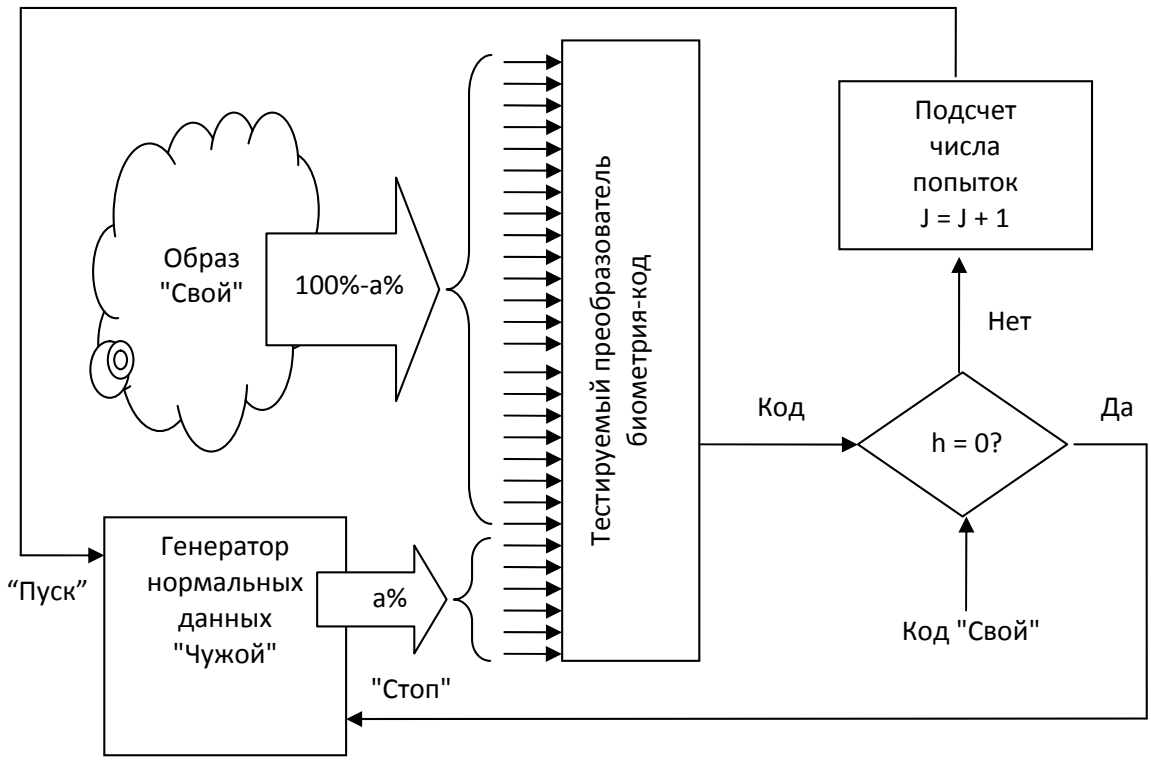


Рис. 5. Блок-схема тестирования остаточной стойкости почти полностью скомпрометированного биометрического образа

Д.М.ШЕЛАКОВ

ВОПРОСЫ, ВОЗНИКАЮЩИЕ В ХОДЕ ПРОВЕДЕНИЕ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ ТЕХНИЧЕСКИХ СРЕДСТВ В УСЛОВИЯХ ПРОГРЕССА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В условиях стремительного научно-технического прогресса во многих сферах жизнедеятельности человека, а особенно в области информационных технологий, вопросы, связанные с обеспечением технической защиты информации требуют постоянного переосмысления и дополнительных проработок.

Исходя из принципов организации технической защиты информации известно, что для защиты информации ограниченного распространения, обрабатываемой с помощью средств вычислительной техники, применяются различные организационные и технические мероприятия, конечная цель которых - достижение желаемого уровня защищенности информационных объектов.

Одним из обстоятельств, препятствующим поддержанию высокого уровня защищенности информационных объектов, обрабатывающих закрытую информацию, является постоянное совершенствование информационных технологий, внедрение новых интерфейсов передачи информации, в том числе и между составными элементами технических средств обработки информации (ТСОИ). Данный «естественный» процесс развития технологий вызывает дополнительные трудности в вопросах технической защиты информации и требует пристального внимания специалистов. В современном, динамично меняющемся мире постоянно возникает необходимость в применении новых, современных ТСОИ, использование которых ранее рассматривалось нецелесообразным и сложно исполнимым (организация конференцсвязи, удаленного мониторинга, распределенных вычислительных сетей, подвижных центров и т.д.). Однако желание обновления парка вычислительной техники или организации необходимых вычислительных систем не может и не должно «упираться» в возможности организаций, ответственных за обеспечение технической защиты информации.

Необходимо отметить, что одной из важнейших составляющих мероприятий по обеспечению технической защиты информации выступает проведение специальных исследований ТСОИ (лабораторных или объектовых) на предмет выявления технических каналов утечки защищаемой информации (ПЭМИН, каналы утечки по отходящим коммуникациям гальванически связанных ТСОИ, каналы неравномерного потребления тока). Именно по результатам специальных исследований устанавливаются значения опасных сигналов, определяющие дальнейшие мероприятия по технической защите информации.

В соответствии с требованиями технических нормативных правовых актов до начала проведения специальных исследований необходимо детально изучить техническое описание и принципиальные схемы испытуемых ТСОИ, а также рассмотреть возможные режимы работы, так как в составе любого цифрового устройства одновременно работают десятки схем, узлов, блоков. Без знания частоты информационного сигнала проведение специальных исследований затруднительно. Именно поэтому измерение параметров ПЭМИН производятся во всех режимах функционирования ТСОИ, максимально приближенных к реальным условиям их эксплуатации.

Основным методом, используемым при проведении специальных исследований, является задание «идеализированного» режима работы устройства, при котором формируются тестовые сигналы, позволяющие произвести поиск и оценку наиболее «опасного» сигнала.

Для обнаружения тестовых сигналов в общей совокупности принимаемых измерительной аппаратурой сигналов используются различные признаки, облегчающие

процесс распознавания (совпадение частот обнаруженных гармоник и интервалов между ними с расчетными значениями, изменение формы сигнала на выходе измерительного приемника при изменении параметров тестовых сигналов и т.д.). При этом применяют ряд методик для генерации тестовых режимов испытуемых технических средств, когда длительность и амплитуда информационных импульсов совпадают с параметрами рабочего режима, но формируется последовательность из серии импульсов. Это условие связано с методикой расчета результатов специальных исследований: тактовая частота информационных сигналов и значения суммирования частотных составляющих должны быть установлены экспериментально, иначе расчет результатов становится трудноразрешимой задачей.

Появление и дальнейшее внедрение новых интерфейсов передачи данных влечет за собой проблему установления показателей и норм оценки уровня защищенности ТСОИ, в которых планируется использовать или уже используются новейшие способы передачи данных. Все это приводит к состоянию, когда злоумышленник, имеющий доступ к технической документации или, участвовавший в разработке изделия, находится в более выгодной позиции по отношению к организации, отвечающей за техническую защиту.

К сожалению, быть готовыми не всегда означает иметь возможность своевременно и в достаточной мере обеспечивать защиту информационных объектов. Большинство устройств, входящих в состав ТСОИ, являются устройствами с последовательным кодированием данных (видеоподсистема, накопители на жестких и гибких дисках, различные устройства считывания и записи на компакт диски, клавиатура, последовательные COM и USB порты, принтеры и т.д.), но имеют параллельные интерфейсы обмена данными.

Небольшой пример. В настоящее время, максимально широкое распространение имеет 15-контактный интерфейс подключения монитора D-Sub HD15, более известный как «VGA разъем». За протяженный период времени эксплуатации данного интерфейса накоплен большой опыт оценки всех возможных рисков и способов их снижения (доработка стандартных кабелей, выпуск специально изготовленных экранированных кабелей, специальных разъемов и т.д.). Имеется хорошо отлаженная методика проверки ТСОИ, использующих интерфейс D-Sub HD15.

В настоящее время наличие в ТСОИ интерфейса DVI не является чем-то необычным, а значит, большинство пользователей имеют возможность его использовать. На данный момент известно три вида цифрового видеоинтерфейса (DVI-A, DVI-I, DVI-D), отличающиеся параметрами сигналов не только от D-Sub и HDMI, но и между собой: пропускной способностью, минимальными и максимальными тактовыми частотами, режимами вывода информации на монитор.

Так же присутствуют потенциальные угрозы при внедрении новых интерфейсов обмена данных как между составными элементами ТСОИ, так и в информационных вычислительных сетях (как проводных, так и беспроводных).

Следовательно, при проведении специальных исследований специалист должен обладать весьма обширными знаниями не только в теоретических аспектах, но и иметь богатый опыт работы с различными типами устройств. Необходимо учитывать, в каком режиме организована передача данных и знать параметры и характеристики сигналов, т.к. без точного знания длительности импульса, частоты следования импульсов в пакете, частоты следования пакетов, невозможно правильно рассчитать требуемые показатели защищенности.

Конечно, есть простой метод разрешения проблем применения новых, не изученных технологий – запрет на их использование. Это приемлемо лишь в случаях переизбыточности желаний заказчика, когда отсутствует прямая необходимость в использовании новейших технологий для решения простых задач, а, следовательно, не является панацеей от всего нового и незнакомого.

Прогресс технологий ставит ряд актуальных задач: сбор данных по всему многообразию новых интерфейсов, установление их основных параметров и режимов передачи сигналов, исследование новых изделий, совершенствование методик измерений, пересмотр норм, применяемых для оценки защищенности ТСОИ, и, самое главное, постоянное поддержание квалификационного уровня специалистов в области защиты информации.

Литература

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки по техническим каналам: Учебное пособие. - М.: Горячая линия - Телеком, 2005. – 416с.: ил.

Ю.К.ЯЗОВ, А.И.ИВАНОВ

РАЗРАБОТКА АБСОЛЮТНО УСТОЙЧИВОГО АЛГОРИТМА АВТОМАТИЧЕСКОГО ОБУЧЕНИЯ НЕЙРОННОЙ СЕТИ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИЯ-КОД ДЛЯ ГОСТ Р 52633.5

В настоящее время Россия в рамках технического комитета «Защита информации» (ТК №362) активно ведет работы по созданию пакета национальных стандартов, регламентирующих требования к средствам биометрической аутентификации личности, обеспечивающих конфиденциальность, анонимность, обезличенность массового оборота персональных биометрических данных. Одним из наиболее важных стандартов является ГОСТ Р 52633.5 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».

Значимость этого стандарта обусловлена тем, что обучение нейросетевого преобразователя биометрия-код является опасной процедурой, так как построено на знании кода «Свой» и использовании нескольких примеров биометрического образа «Свой». Компрометация этих данных приводит к тому, что биометрическое средство аутентификации перестает быть высоконадежным и характеризуется только остаточной стойкостью к атакам подбора скомпрометированного биометрического образа. В связи с этой угрозой обучение не должно проводиться в присутствии третьих лиц. По требованиям базового национального стандарта ГОСТ Р 52633.0-2006 нейронная сеть преобразователя биометрия-код должна обучаться автоматически, после обучения исходные данные (код «Свой» и примеры образа «Свой») должны уничтожаться.

По требованиям ГОСТ Р 52633.0-2006 обучение нейросетевого преобразователя биометрия-код (ПБК) должно выполняться таким образом, чтобы каждый i-ый пример образа «Свой» после его преобразования в вектор контролируемых биометрических параметров - $\overline{v}_i$, давал на выходах ПБК одинаковые коды - $\overline{c}$:

$$\begin{bmatrix} \text{ПБК} \\ N \times n \end{bmatrix} \cdot \overline{v}_i = \overline{c} \qquad (1),$$

где $\begin{bmatrix} \text{ПБК} \\ N \times n \end{bmatrix}$ - матрица нелинейных функционалов ПБК размерности (N×n), осуществляющих нелинейную нейросетевую обработку вектора из N непрерывных биометрических параметров - $\overline{v}_i$ по их преобразованию в код $\overline{c}$, состоящий из n разрядов.

В том случае, если на входы нейросетевого ПБК будут подаваться случайные вектора биометрических образов «Чужой» - $\bar{\xi}_i$, то на каждый i-ый вектор ПБК должен откликаться случайным кодом - $\bar{z}_i$:

$$\begin{bmatrix} \text{ПБК} \\ N \times n \end{bmatrix} \cdot \bar{\xi}_i = \bar{z}_i \qquad (2).$$

Фактически нейросетевой ПБК осуществляет сжатие практически до нуля собственной энтропии биометрического образа «Свой» (в выражении (1) $\bar{c}$ = constant), а для биометрических образов «Чужой» нейросетевой ПБК производит существенное усиление энтропии до величины примерно в 5 раз меньше предельного значения энтропии.

Для того чтобы одновременно выполнить условия (1) и (2), необходимо уметь строить специальные автоматы обучения нейронов нейронных сетей ПБК. На рисунке 1 дана блок-схема работы автомата обучения одного нейрона.

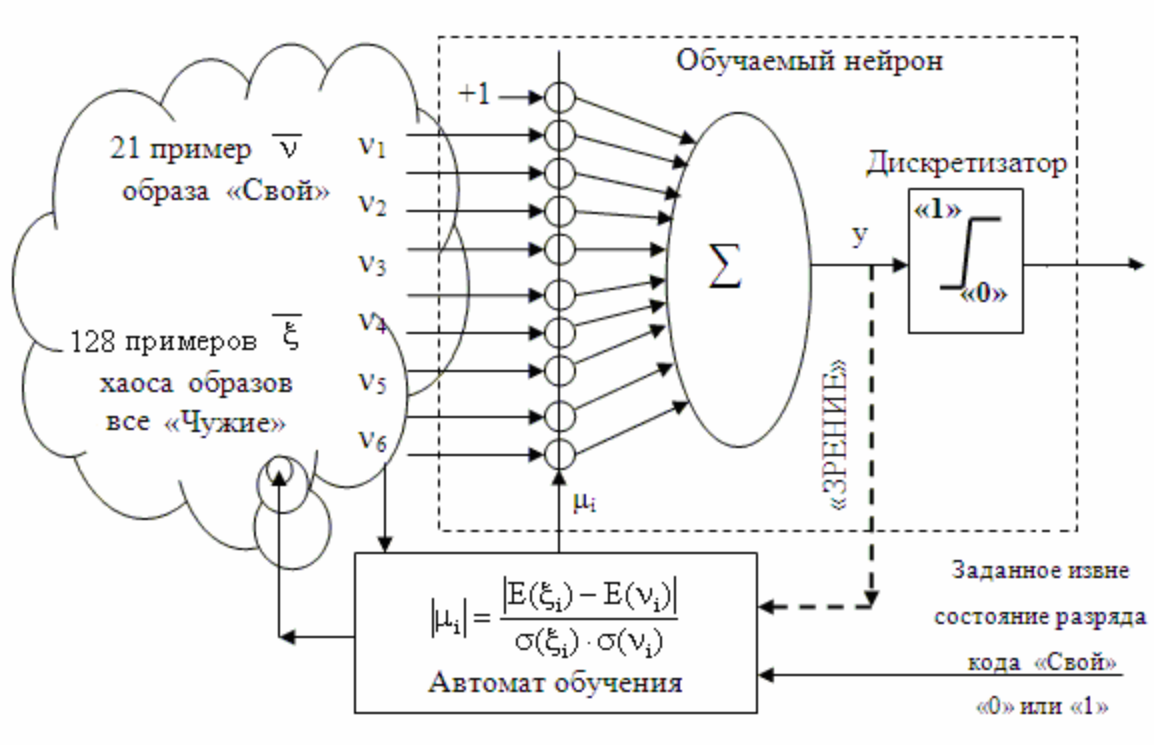


Рис. 1. Блок-схема автоматического обучения одного нейрона нейросети ПБК

Одной из основных особенностей алгоритма обучения, рекомендуемого ГОСТ Р 52633.5, является то, что нелинейная функция нейрона осуществляет переключение состояния «0» в состояние «1» в точке математического ожидания откликов образов все «Чужие» - $E(y(\bar{\xi}))$. Это нейросетевое решение показано на рисунке 2 утолщенной линией. В отличие от обычных нейросетевых решений (тонкая линия рисунка 2) оно позволяет сделать атаку «поиска близнецов» неэффективной.

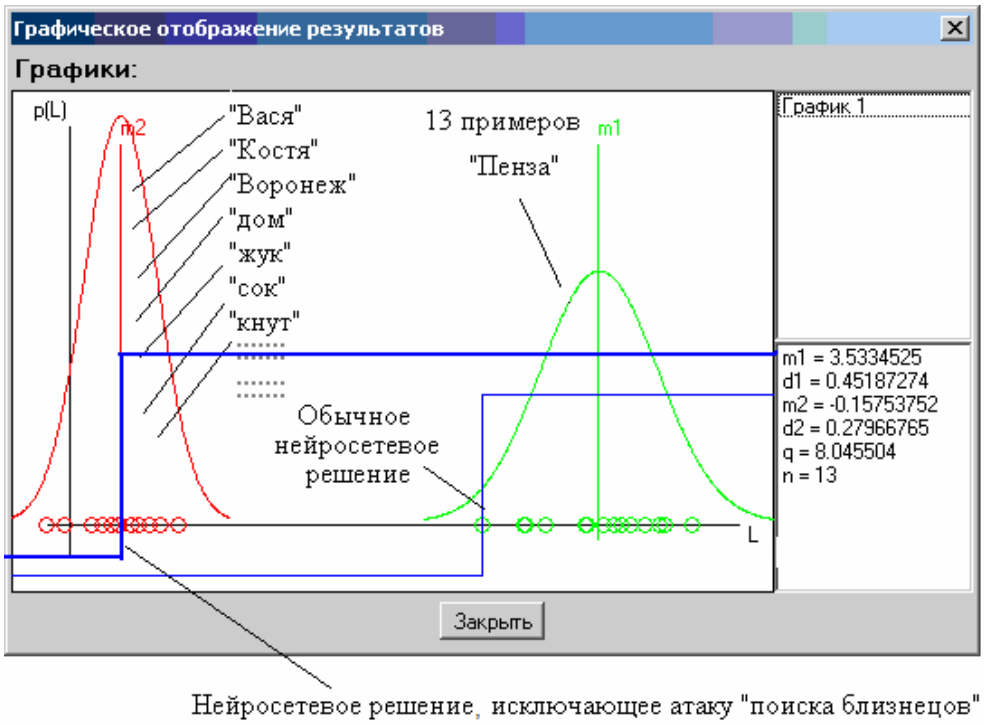


Рис. 2. Два варианта нейросетевых решений (обычное решение – тонкая линия) и решение по ГОСТ Р 52633.5 (утолщенная линия)

Из рисунка 2 видно, что обычное нейросетевое решение дает состояние «1» для образов «Свой» и состояние «0» для образов «Чужие». ГОСТ Р 52633.5 требует отказаться от такого подхода к решению задачи и требует добиваться равновероятного состояния «0» и «1» для множества образов «Все Чужие».

Казалось бы, что происходит катастрофическое ухудшение качества принимаемых нейронной сетью решений, так как каждый разряд выходного кода ПБК ошибается с вероятностью 0.5 (ошибочно принимает биометрический образ «Чужой» за образ «Свой»). На самом деле катастрофы не происходит из-за выполнения условия (2), по которому выходные коды ПБК должны быть слабо коррелированными. При полном отсутствии корреляционных связей выходных кодов длиной 256 бит мы имеем фантастически малое значение вероятностей ошибок второго рода:

$$P_2 = 0.5^{256} \approx 10^{-77} \quad (3).$$

К сожалению, полного уничтожения корреляционных связей между разрядами выходных кодов - $\bar{z}_i$ добиться не удается. В связи с этим ГОСТ Р 52633.0-2006 допускает наличие парных корреляционных связей между разрядами выходных кодов ПБК (допустимо наличие корреляционных связей, математическое ожидание модулей которых не превышает 0.15). В предельном случае, $E(|r|) = 0.15$, в показателе выражения (3) появляется поправочный коэффициент $\beta \approx 0.1$:

$$P_2 = 0.5^{\beta \cdot 256} \approx 0.5^{0.1 \cdot 256} \approx 0.5^{26} \approx 10^{-8} \quad (3а).$$

Наличие корреляционных связей в выходных кодах «Чужой» ПБК несомненно ослабляет биометрическую защиту, однако ее стойкость к атакам подбора на уровне 10^8 попыток оказывается вполне приемлемой для коммерческих приложений.

Еще одной важной особенностью ГОСТ Р 52633.5 является то, что он рекомендует отказаться от итерационных алгоритмов обучения искусственной нейронной сети ПБК. На сегодняшний день известно несколько сотен итерационных алгоритмов обучения нейронных сетей, однако все они теряют устойчивость при увеличении числа входов у нейронов или при

снижении качества входных биометрических данных. Пример утраты устойчивости автоматом обучения приведен на рисунке 3.

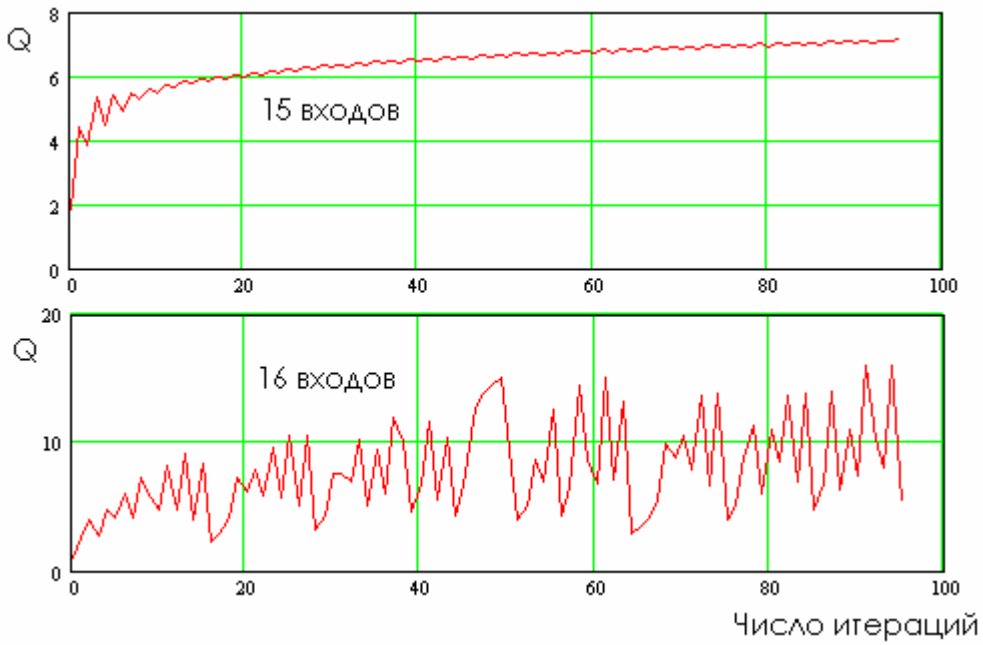


Рис. 3. Утрата устойчивости автоматом итерационного обучения при увеличении числа входов, обучаемого нейрона

Кривые рисунка 3 построены по результатам обучения нейрона с 15 и 16 входами на одних и тех же 13 примерах образа «Свой» и 128 примерах разных образов «Чужие». Обучение велось в среде имитационного моделирования «НейроУчитель» (разработка Пензенского государственного университета). Из рисунка 3 видно, что при 15 входах у обучаемого нейрона качество его выходных решений практически монотонно увеличивается на всех 100 итерациях. При увеличении числа входов у обучаемого нейрона до 16 происходит утрата монотонности итерационного обучения (нижняя часть рисунка 3). Фактически процесс обучения теряет устойчивость, и, соответственно, у разработчиков автоматов обучения нейронов возникают значительные трудности.

Обычно для итерационных алгоритмов обучения число примеров в обучающей выборке должно примерно совпадать с числом входов у обучаемого нейрона. Если это условие не выполняется, то автомат итерационного обучения начинает оптимизировать ошибки представления биометрического образа «Свой» конечной выборкой примеров этого образа. Повысить устойчивость автомата итерационного обучения (вернуться к монотонному росту качества обучения на каждой следующей итерации) всегда можно через увеличение примеров образа «Свой» в обучающей выборке.

Еще одной причиной утраты устойчивости процедуры обучения является снижение качества входных биометрических данных (показатель качества биометрических данных определен в ГОСТ Р 52633.1-2009). При плохом качестве входных данных срыв устойчивости происходит при меньшем числе входов у обучаемого нейрона. Эта ситуация отображена на рисунке 4.

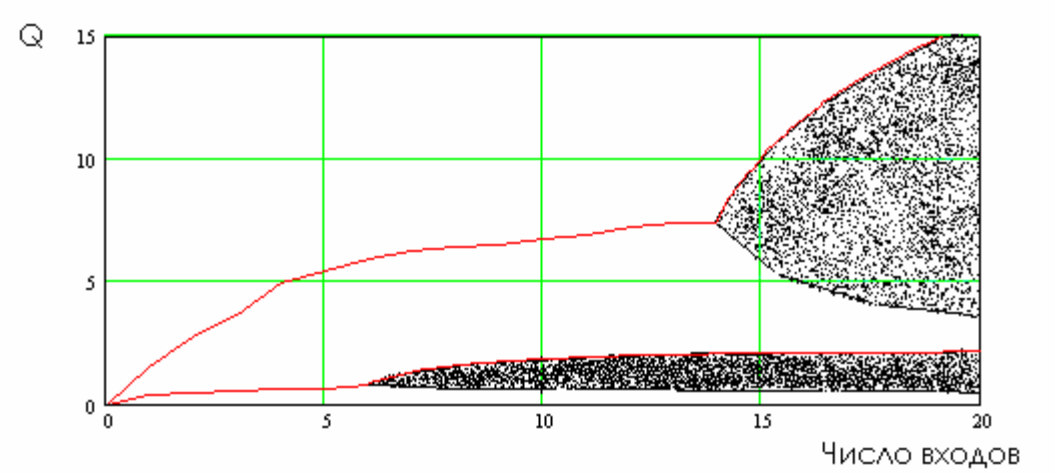


Рис. 4. Связь положения точки утраты устойчивости обучения (точки бифуркации) с числом входов нейрона и качеством входных (выходных) биометрических данных

В верхней части рисунка 4 отображена ситуация, соответствующая процессам рисунка 3. При хорошем входном качестве 13-ти примеров образа «Свой» итерационное обучение является устойчивым для 1, 2,…, 13 входов обучаемого нейрона. Однако уже при 14 входах происходит утрата устойчивости обучения. При 15 входах нейрона ложные экстремумы функционала качества уже хорошо наблюдаемы (показаны в верхней части рисунка 3).

В нижней части рисунка 4 отображена ситуация обучения нейрона на 13-ти примерах образа «Свой» с биометрическими данными плохого качества. Из рисунка следует, что качество обучения нейрона на плохих данных оказывается хуже. При этом срыв устойчивости обучения происходит уже при 6 входах обучаемого нейрона.

В связи с отмеченной выше закономерностью ГОСТ Р 52633.5 требует отказаться от использования итерационных алгоритмов обучения (на рисунке 1 обратная связь с выхода сумматора нейрона на вход автомата обучения показана пунктиром).

Новый стандарт рекомендует использовать прямое вычисление модулей весовых коэффициентов через привлечение математических ожиданий и среднеквадратических отклонений биометрических параметров:

$$|\mu_i| = \frac{|E(\xi_i) - E(\nu_i)|}{\sigma(\xi_i) \cdot \sigma(\nu_i)} \quad (4).$$

Знак при весовом коэффициенте (4) выбирается автоматически, исходя из соотношения $E(\xi_i), E(\nu_i)$ и требуемого выходного состояния «0» или «1» при воздействии на нейрон образами «Свой». Из-за того, что алгоритм обучения по ГОСТ Р 52633.5 исключает итерационный поиск весовых коэффициентов нейронов, процедуры обучения нейронных сетей становятся рекордно быстрыми и устойчивыми. Снимается также проблема обучения многослойных нейронных сетей (число слоев нейронов у обучаемых нейронных сетей может быть любым), однако стандарт рассматривает только однослойные и двухслойные нейронные сети. Нейронные сети с тремя и более слоями нейронов являются избыточными, и для их применения необходимо специальное обоснование.

В конечном итоге алгоритм обучения по ГОСТ Р 52633.5 позволяет экспоненциально снижать вероятности ошибок второго рода, увеличивая число учитываемых биометрических параметров. Графики связи вероятности ошибок второго рода и числа учитываемых биометрических параметров приведены на рисунке 5.

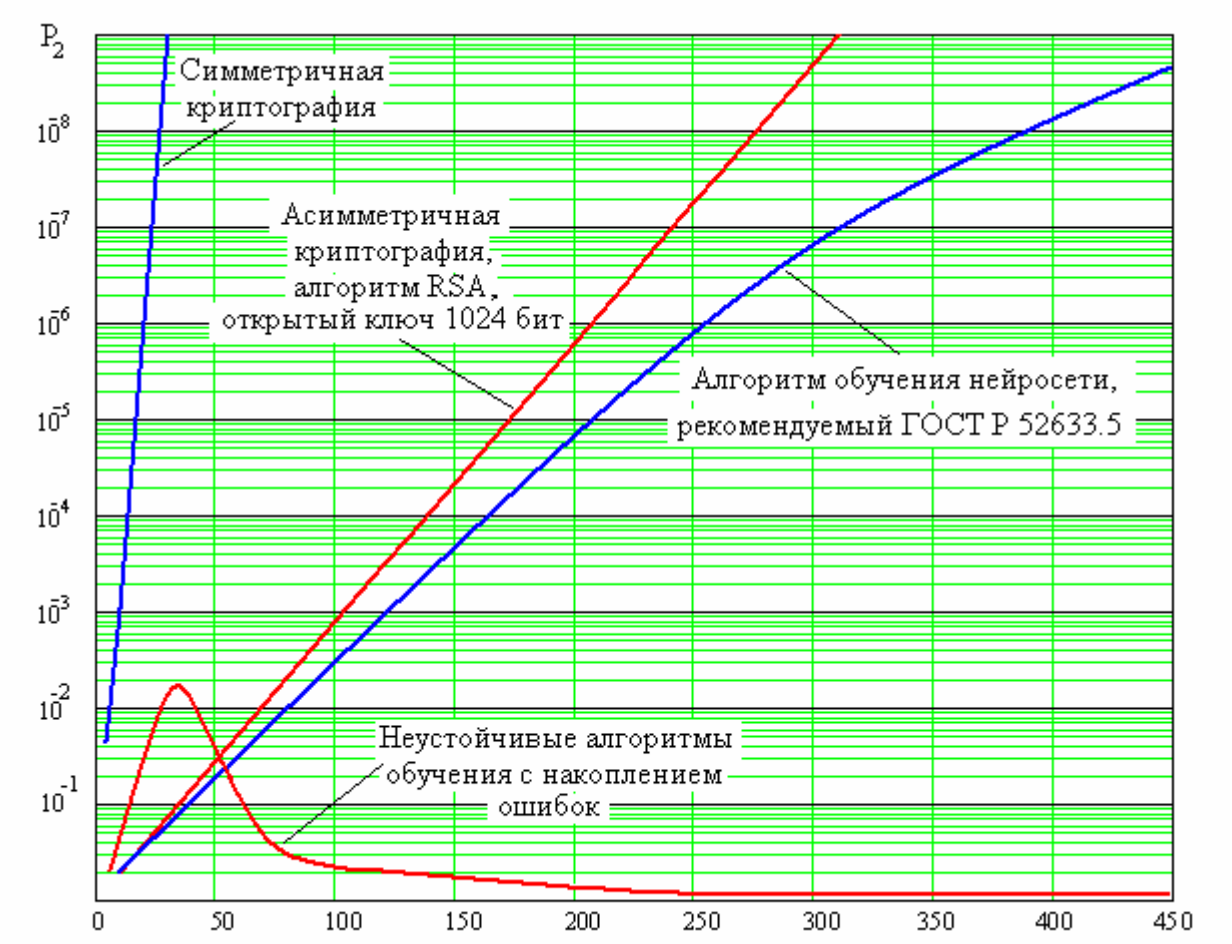


Рис. 5. Зависимости роста качества принимаемого решения (снижения вероятности ошибок второго рода – P_2), как функция длины вектора анализируемых параметров

Из рисунка 5 видно, что для малого числа хороших биометрических параметров рекомендуемый стандартом алгоритм обучения проигрывает обычным итерационным алгоритмам. При большом числе биометрических параметров ситуация становится обратной, становится выгодным использовать новые алгоритмы обучения.

РАЗДЕЛ 6
ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.П.БАТУРА, Л.М.ЛЫНЬКОВ, Т.В.БОРБОТЬКО

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ НА БАЗЕ БЕЛОРУССКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

В Белорусском государственном университете информатики и радиоэлектроники накоплен некоторый опыт подготовки специалистов различного уровня в сфере информационной безопасности.

С 2001 г. открыто несколько учебных инженерных специальностей:

1. 1-38 02 03 «Техническое обеспечение безопасности» – подготовка инженеров-электромехаников умеющих выполнять анализ потенциальных каналов утечки информации, наличие которых обусловлено применением технических средств шпионажа и утечкой информации посредством компьютерных сетей, а так же выбор наиболее оптимальных способов их защиты;

2. 1-98 01 02 «Защита информации в телекоммуникациях» – подготовка специалистов по двум квалификациям (специалист по защите информации, инженер по телекоммуникациям) обладающих теоретическими знаниями и практическими навыками исследования, разработки и сопровождения специальных и технических средств защиты и обработки информации в телекоммуникационных системах, способных выполнить оперативные задания, связанных с обеспечением контроля технических средств и механизмов системы защиты информации, проведением аттестации и сертификации защищаемых объектов, помещений, технических средств, программ и алгоритмов на предмет соответствия нормативным требованиям технической защиты информации;

3. 1-39 01 04 «Радиоэлектронная защита информации» – подготовка инженеров по радиоэлектроники со специальными знаниями в области построения защищенных радиоэлектронных программно-аппаратных систем и устройств радионаблюдения, радиоэлектронной борьбы и криптологии, а также инженерно-технических средств;

4. 1-39 03 01 «Электронные системы безопасности» – подготовка инженеров-проектировщиков, способных проводить комплексное проектирование электронных систем безопасности, включающее определение угроз и рисков для защищаемого объекта, разрабатывать принципы обеспечения защиты и общую структурную схему системы безопасности, определение наиболее эффективных каналов передачи сигналов, выбор промышленно выпускаемых электронных и других технических устройств, совместно решающих задачу по обеспечению безопасности объекта.

С 2001 года введен единый для всех инженерных специальностей курс “Основы защиты информации и управление интеллектуальной собственностью”, который содержит основные сведения по правовому, организационно-техническому и криптографическому обеспечению информационной безопасности информационно-коммуникационных систем кредитно-финансовых и других специальных организаций.

С 2007 года в БГУИР обучается ежегодно не менее 35 магистрантов дневной и заочной форм обучения по специальности 1-98 80 01 “Методы и системы защиты, информационная безопасность”. С 2010 года начата подготовка магистрантов дневной

формы обучения на английском языке. Проведен набор 2010 года общей численностью 8 человек – граждане Ирака, Ирана, Нигерии и Туркменистана. Учебный план обучающихся включает изучение курсов обеспечивающих специальную инженерную подготовку, таких как «Цифровые и микропроцессорные устройства средств измерений», «Теория кодирования» и «Научные основы создания перспективных технологий изготовления радиоэлектронных средств», а так же дисциплины специальности «Организационно-правовое и методологическое обеспечение безопасности», «Защита информации в банковских технологиях», «Методы и средства защиты объектов связи от несанкционированного доступа», «Криптографическая защита информации», «Современные телекоммуникационные технологии и защита информации в телекоммуникационных сетях», «Проектирование и эксплуатация защищенных технических объектов» и «Технические средства обнаружения и подавления каналов утечки информации». Темы магистерских работ посвящены разработке технических и программно-аппаратных средств защиты информации.

В БГУИР ведется подготовка в аспирантуре по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность», функционирует Совет по защите диссертаций по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность». Проводится ежегодная Белорусско-Российская научно-техническая конференция «Технические средства защиты информации» (г. Браслав), отдельные доклады в виде статей публикуются в журнале «Доклады БГУИР».

На базе Института информационных технологий и кафедры защиты информации БГУИР проводятся ежегодные курсы повышения квалификации по темам: «Защита информации в телекоммуникационных и автоматизированных системах», «Применение методов и средств криптографической защиты информации, в том числе электронной цифровой подписи», «Основы безопасности сетей» и др. С начала 2011 г проведено обучение 5 групп (30 человек) специалистов с высшим образованием из различных организаций.

М.А.ВУС

ИНФОРМАТИКА – ОСНОВА ОБРАЗОВАНИЯ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

(Заметки с Первого Всероссийского Съезда учителей информатики)

Опубликованные результаты исследования об уровне компьютерных навыков населения в возрасте 16–74 лет, приведенные Высшей школой экономики, свидетельствуют, что в России - при очень низкой технической оснащенности большинства населения – очень высокий уровень овладения компьютерными знаниями у оставшегося меньшинства. Это означает, что потенциал России по-прежнему не исчерпан, умы не перевелись. Второй же момент заключается в том, что эти знания меньшинства могут так и остаться втуне, если не будет подтянут уровень всех остальных.
[http://www.ng.ru/education/2011-03-29/8_informatics.html]

I. Традиция Всероссийских съездов учителей, которая начиналась в начале прошлого столетия как особый феномен учительского диалога, в 21 веке обрела новую актуальность. Проведя в октябре 2010 г. Всероссийский съезд учителей математики Московский государственный университет имени М.В. Ломоносова возродил традиции проведения Съездов школьных учителей-предметников. Первые два Всероссийских съезда преподавателей математики, как известно, были проведены еще в начале XX века в дореволюционной России. Почти столетие спустя учителя математики собирались в 2000 г. в Дубне, но то была Всероссийская конференция «Математика и общество. Математическое образование на рубеже веков».

Всероссийские съезды учителей заявлены как один из проектов утвержденной председателем Правительства России В.В. Путиным Программы развития Московского государственного университета. Это - инструмент включения школы в процессы инновационного развития страны. Уникальной чертой съездов, проводящихся в МГУ, является соединение на одной площадке учительского и вузовского сообщества с лидерами отраслевых и профессиональных организаций.

Возрожденные Съезды учителей рассматриваются сегодня не только как инструмент объединения усилий средней и высшей школы, но и преследуют цель восстановления статуса учителя, включения школы в процессы инновационного развития страны. Их цель - посредством диалога школьного учителя и вузовского преподавателя достичь согласования качества образования, наполнения его содержания научным дыханием и пониманием высоких интеллектуальных стандартов, которые должны быть едиными для школы и вуза. Выступая на математическом съезде в Год Учителя, ректор МГУ академик В.А. Садовничий особо подчеркнул роль учителя, приведя такой исторический пример: *«Отец-основатель кибернетики Янош фон Нейман и лауреат Нобелевской премии по физике Юджин Вигнер в школе учились у одного учителя математики – Ласло Ратца. Вот что значит Учитель!»*.

II. ***24-26 марта 2011 г. в МГУ прошел Всероссийский Съезд учителей информатики.*** На Съезде, собравшем почти тысячу делегатов из 71 субъекта Российской Федерации, а также представителей Белоруссии, Азербайджана, Казахстана, Киргизии и Туркменистана, прошло широкое обсуждение состояния и перспектив развития школьного образования в области информатики и информационно-коммуникационных технологий в контексте основных принципов Национальной образовательной инициативы «Наша новая школа». В работе Съезда приняли участие учителя школ, преподаватели вузов, научные работники, специалисты по педагогике и методике преподавания информатики и ИКТ, руководители образовательных учреждений, ректоры вузов, представители органов управления образованием и ИТ-индустрии.

Открыли Съезд ректор МГУ им. М.В. Ломоносова академик В.А. Садовничий и Министр образования и науки РФ А.А. Фурсенко. В своих докладах они обратили внимание на роль информатики для страны, для становления и воспитания личности гражданина, а также на необходимость повышения качества обучения и привлечения различных общественных и профессиональных организаций для совместной работы. В выступлениях участников Съезда (на заседаниях которого было заслушано около сотни докладов), в дискуссиях на круглых столах был дан анализ 25-летнего опыта преподавания общеобразовательного курса информатики в отечественной школе, оценка современных проблем школьной информатики и обсуждены перспективы развития предмета в свете формирования глобального информационного общества, в связи с переходом к новым образовательным стандартам.

Академик В.А. Садовничий в своем докладе отметил, что информатика – самая молодая из школьных дисциплин и в тоже время из всех школьных предметов информатика, наверное, развивается и изменяется быстрее всех. В 1985 г. во всех общеобразовательных школах был введён курс «Основы информатики и вычислительной техники». (Справедливости ради необходимо отметить, что первый опыт обучения школьников программированию на ЭВМ относится еще к началу 1960-х гг. В начале этого года отметил свое 50-летие широко известный успехами своих учеников далеко за его пределами Санкт-Петербурга Физико-математический лицей № 239.)

Введение предмета информатика шло непросто – не было ни подготовленных учителей, ни компьютерных классов. Ныне предмет, изучаемый в школе, именуется «Информатика и ИКТ». И сегодня, спустя двадцать пять лет, перед учителями информатики стоят проблемы, которые требуют своего решения. Это – и содержание преподавания информатики, и учебная литература, и соотнесение школьной программы с вузовской

подготовкой и требованиями работодателей, и выбор языков программирования, и техническое обслуживание персональных компьютеров в школе, и многие другие вопросы. С интересным пленарным докладом «Информатика в школе: вызовы времени» в первый день работы Съезда выступил абсолютный победитель Всероссийского конкурса «Учитель года России» Д.Д. Гущин, рассказавший о тех проблемах, с которыми сталкивается учитель информатики в своей повседневной работе. Его выступление неоднократно прерывалось одобрительными аплодисментами зала.

Программа работы Съезда была очень насыщенной. Пленарные заседания проходили в прекрасно оборудованном Актовом зале Интеллектуального центра – фундаментальной библиотеке МГУ. Вторая половина дня работы Съезда была организована на факультете вычислительной математики и технической кибернетики в виде тематических секций и круглых столов. На каких принципах строить углубленное изучение информатики? Почему обучение информатики должно стать непрерывным? Как преподавать информатику интересно и увлекательно для школьников и студентов? Какие языки программирования должны изучаться в школе? Этим и другим вопросам были посвящены тематические секции и круглые столы по различным аспектам современного образования в области информатики и информационных технологий.

III. С самого начала своего становления в качестве школьного учебного предмета информатика ставила задачу развития мышления: школьного, алгоритмического, операционного, логического. В ходе двадцатипятилетнего развития школьной информатики она двигалась от преимущественного изучения алгоритмики (включая её «безмашинный» вариант) к преимущественному освоению компьютерных технологий. Это было связано как с совершенствованием цифровых технологий, расширением области их применения, так и с улучшением оснащения школ компьютерной техникой. Если в середине 80-х гг. XX века все старшеклассники изучали основы алгоритмизации и программирования, то сейчас в базисном учебном плане предусмотрена инвариантность обучения информатике в зависимости от выбранного профильного направления.

В последние годы становится все более модным компетентностный подход к образованию. В этой связи не следует забывать, что среди ключевых компетентностей в современном информационном обществе особую роль играет компетентность в области информационных и коммуникационных технологий. Трудно представить себе современного специалиста любой неинформационной сферы деятельности, не владеющего компьютерными технологиями на уровне профессионального пользователя.

Еще один из пионеров-родоначальников школьной информатики академик А.П. Ершов (которому сегодня исполнилось бы 80 лет) сформулировал компетенции, которые следует формировать у выпускников школы.

Это: - умение строить информационные модели для описания объектов и систем;

– умение планировать структуру действий, необходимых для достижения цели при помощи фиксированного набора средств;

– умение организовать поиск информации, нужной для решения поставленной задачи;

– умение структурировать общение в соответствии с компетенцией сторон;

– приобретение навыка обращения к компьютеру при решении задач из разных предметных областей;

– умение использовать информационно-сетевые средства, позволяющие работать с удаленными информационными фондами и участвовать в диалоговых и коллективных видах деятельности;

– освоение технических навыков взаимодействия с компьютером, в частности, в организации обмена информацией между компьютером и современной цифровой мультимедийной периферийной аппаратурой.

После принятия в 1993 г. «Закона об образовании», провозгласившего концепцию образовательных стандартов, изменилась парадигма компьютерной грамотности: от программирования к пользовательскому уровню работы на персональном компьютере. Еще в 1995 г. Решением Коллегии Минобразования РФ были рекомендованы три этапа сквозного (с 1 по 11 классы) изучения информатики, однако это прогрессивный посыл не получил своего развития на практике.

Цели обучения информатике много шире и разнообразнее, чем это принято считать. Изучение информатики является важным звеном в формировании научной картины мира. Одной из основных задач курса информатики и информационно-коммуникационных технологий является подготовка творческих учащихся к жизни в информационном обществе. На практике же сегодня имеет место множество разных проблем. В их числе, например, такие как цифровое неравенство участников образовательного процесса, проблемы с учебниками, когда часть информации в них устаревает еще до выхода из типографии, и др. Развивающий потенциал информатики как учебной дисциплины реализуется недостаточно эффективным образом. Недостаточна поддержка информатизации образовательного процесса со стороны органов управления образованием. К тому же в первоначальном проекте федерального государственного образовательного стандарта (ФГОС) второго поколения информатика чуть было вообще не исчезла из федерального образовательного компонента?!

Проект нового ФГОС, обсуждение которого вызвало жаркие споры в обществе, сократил до одного часа в неделю изучение информационных технологий и предмета информатики. В версиях проекта ФГОС от 15.02.2011 г. (и доработанной от 19.04.) для полной средней школы информатика объединена в одну предметную область с математикой и, как большинство общеобразовательных предметов, является дисциплиной по выбору. Но из-за установленных ограничений на включение в учебный план 1-2 предметов из одной предметной области «*информатика по определению оказывается вне игры, поскольку для сдачи обязательного ЕГЭ по математике нужно учить алгебру и геометрию, а информатика – третий лишний*».

IV. Ректор МГУ академик В.А. Садовничий в своем докладе отметил исключительную стратегическую важность информационных технологий для современной жизни и постоянно ускоряющийся темп их изменений. При этом он особо подчеркнул, что информационные технологии сегодня реально вторгаются в сферу социальных отношений: «*Если раньше воспитание шло в режиме ребёнок – взрослый, то теперь компьютер, Интернет стал еще одним значимым так сказать «взрослым», от которого ребёнок тоже, хотим мы этого или не хотим, учится жизни*». В процессе школьной практики, необходимо готовить учащихся к грамотному, современному информационному поведению в условиях информационной избыточности глобальной среды Интернета.

Главную цель российской образовательной политики – обеспечение современного качества образования – невозможно достичь без включения инновационных идей, технологий и проектов в образовательный процесс. Современное образование должно учить мыслить, находить нестандартные решения в разных ситуациях и отстаивать собственную позицию. В то же время постоянно растет потребность страны в специалистах – профессионалах в области информационно-коммуникационных технологий, а не только в грамотных пользователях.

Последнее обстоятельство с необходимостью возвращает нас от пользовательской информатики к фундаментальной. Тем более что информатика имеет очень большое и все возрастающее число междисциплинарных связей, причем как на уровне понятийного аппарата, так и на уровне инструментария. Можно сказать, что она представляет собой «метадисциплину», которая обладает общенаучным языком. Из этого следует, что информатика во всё большей степени должна становится базовой школьной дисциплиной –

такой, как физика и математика. Она должна давать основы фундаментальных научных знаний в связи с их приложениями в окружающем мире. При этом динамичность предметной области должна отражаться на развитии учебного предмета и, в первую очередь, на его фундаментальном содержании. Так, многие выступающие отмечали также, что при изучении как правовых, так и профессиональных дисциплин следует усилить внимание вопросам информационной безопасности. В существующих условиях, при минимуме отводимых на эти вопросы часов, формирование компетенции учащихся в области информационной безопасности становится практически нереализованным.

Выступавшие на Съезде подчеркивали, что сокращение количества часов, отводимых учебными планами на изучение информатики и ИКТ, отрицательно влияет на качество образования по всем школьным предметам. А отсутствие ЕГЭ по информатике в перечне обязательных вступительных испытаний в вузах, готовящих ИТ-специалистов, оказывает прямое негативное влияние на качество образования в области информатики. В то же время в одном из докладов была дана образная оценка: «*ЕГЭ – это взятка, которую правительство дало населению за то, что не сумело или не захотело обеспечить достойный средний уровень школьного образования*».

Информатика сегодня обеспечивает научную базу для формирования глобального информационного общества, основанного на знаниях. И в качестве фундаментальной науки стала важной составляющей всей системы научного познания. Главную цель российской образовательной политики – обеспечение современного качества образования – невозможно достичь без включения инновационных идей, технологий и проектов в образовательный процесс. В этой связи особенно необходимо дальнейшее развитие сложившейся системы работы с одаренными в области информатики детьми, развитие системы олимпиад и конкурсов школьников.

В России идет переход к информационному обществу. Перед образованием этот переход ставит значительные проблемы. Современное образование должно учить мыслить, находить нестандартные решения в разных ситуациях и отстаивать собственную позицию. Среди прозвучавших пленарных докладов исключительно интересными и содержательными в познавательном плане оказались доклады председателя секции «Прикладная математика и информатика» Отделения математических наук РАН, заведующего кафедрой «математических методов прогнозирования» факультета ВМК МГУ академика Ю.И. Журавлёва «Методы обработки плохо формализованной информации» и директора Института прикладной математики РАН, члена-корреспондента Б.Н. Четверухина «Высокопроизводительные вычисления – основа информационных технологий». Авторы докладов, блестяще проиллюстрировали роль информатики как основы образования в информационном обществе. Эпиграфом к их докладам могли бы послужить слова французского поэта Поля Валери: «*Если бы логик всегда должен был оставаться логически мыслящей личностью, он бы не стал и не мог бы стать логиком; и если поэт всегда будет только поэтом, без малейшей склонности абстрагировать и рассуждать, никакого следа в поэзии он не оставит*».

V. В принятой резолюции Съезд подчеркнул, что информатика: представляет собой стратегически важное направление науки и практики, жизненно необходимое для развития экономики, промышленности, высоких технологий, обеспечения национальной безопасности, профессионального образования всех уровней и подготовки научных кадров.

Образование в области информатики есть важнейший и необходимый компонент развития личности, представляющий собой основу интеллектуального и творческого развития, подготовки к условиям жизни и деятельности в информационном обществе, представляет собой стратегический ресурс инновационного развития России в условиях модернизации, что многократно доказано отечественным и всемирным историческим опытом.

Съезд выразил обеспокоенность несоблюдением, в части преподавания информатики в средней школе, одного из фундаментальных принципов образовательной деятельности – единого образовательного пространства – и отсутствием условий для его формирования, а также обратил внимание на недопустимый факт отсутствия в новых стандартах начального и основного общего образования и в проекте ФГОС от 15.02.2011 г. для старшей школы информатики как самостоятельного и обязательного для изучения общеобразовательного предмета. В то же время в принятой резолюции отмечено, что «*нельзя сводить информатику только к изучению программных продуктов, однако, обучать компьютерным технологиям может и должен именно учитель информатики*».

Съезд обратился к Министерству образования и науки РФ с просьбой:

1) включить информатику и ИКТ в систему общего образования как самостоятельный и обязательный предмет, изучаемый на базовом и профильном уровне;

2) обеспечить непрерывность и преемственность изучения общеобразовательного курса информатики и ИКТ на всех ступенях школьного образования, начиная со второго класса.

Опубликованный на сайте Минобрнауки России (15.04.2011г.), представленный Президиумом Российской академии образования, проект Федерального государственного образовательного стандарта среднего (полного) общего образования учел рекомендацию Съезда в отношении представления дисциплины «Информатика» в обязательной части основной образовательной программы. Казалось бы, авторитетное мнение Всероссийского съезда преподавателей информатики учтено. Вместе с тем версия проекта ФГОС, «доработанная» Институтом стратегических исследований в образовании РАО, которая была обнародована 19.04.2011г., с упорством достойным лучшего применения, изобретает новый интегрированный образовательного предмет «математика и информатика». И эта версия «рекомендована группой мониторинга доработки стандартов общего образования при Совете Минобрнауки России по федеральным государственным образовательным стандартам». Чье же мнение окажется весомее?!

Всероссийский съезд преподавателей информатики отметил в своей резолюции обязательность при разработке и утверждении новых образовательных стандартов проведения предварительного конкурса концепций с обеспечением широкой профессиональной экспертизы и общественного обсуждения. В этой связи Съезд призвал преподавателей и ученых в области информатики принять активное участие в открытом обсуждении проектов закона «Об образовании в РФ» и ФГОС и выразить свою профессиональную позицию.

Съезд высказался в пользу целесообразности создания постоянно действующей Ассоциации учителей и преподавателей информатики.

Н.В.ДЕЕВА, С.В.ПИЩИК, Н.В.САВЕЛЬЕВА

О ПОДГОТОВКЕ IT-СПЕЦИАЛИСТОВ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

С проникновением информационных технологий во все сферы жизни возрастают и требования к защищенности IT-систем, сохранности и безопасности данных. Тематика информационной безопасности чрезвычайно актуальна для предприятий и организаций, работающих во всех сферах экономики. Банки, мобильные операторы, крупные предприятия, частные компании - первые лица, заинтересованные в вопросах информационной безопасности, которые не только осознают необходимость в безопасности информационных систем, но и способны делать практические шаги в данном направлении, рассматривая

инвестиции в безопасность не как затраты, а как инвестиции в сохранность бизнеса. Но, к сожалению, вследствие низкой получаемой прибыли многие белорусские организации сегодня вынуждены смотреть на обеспечение компьютерной безопасности скорее как на роскошь.

На сегодняшний день уровень развития компьютерной безопасности в Беларуси сравнительно с другими странами весьма слаб. Главной причиной этому вполне может быть отсутствие в стране крупных IT-корпораций. О недостаточном уровне развития компьютерной безопасности в стране свидетельствует и относительная бедность законодательной базы. Для решения вопросов в сфере IT в настоящее время в Беларуси руководствуются всего двумя основными документами:

1. Статьи 349-355 Уголовного Кодекса Республики Беларусь (Раздел XII. Преступления против информационной безопасности. Глава 31. Преступления против информационной безопасности) [1];
2. Закон Республики Беларусь «Об информации, информатизации и защите информации» от 10.11.2008 No.455-З [2].

Тем не менее, почва к обеспечению нормативно-правовой документацией различных направлений компьютерной безопасности в стране постепенно возделывается. В последнее годы этим вопросам со стороны государства начало уделяться большее внимание. В частности, об использовании сети Интернет были приняты следующие законодательные акты:

– О мерах по совершенствованию использования национального сегмента сети Интернет (Указ Президента Республики Беларусь от 01.02.2010 №. 60 [3], см. также комментарий к Указу Президента Республики Беларусь от 01.02.2010 № 60 [4]);

– О некоторых вопросах совершенствования использования национального сегмента глобальной компьютерной сети Интернет (Постановление Совета Министров Республики Беларусь от 29.04.2010 № 644 [5]).

Для сравнения, в Республике Индия, где действует много крупных IT-компаний, законодательная база в области IT развита больше, более детально описываются вариации преступлений в сфере высоких технологий. К сожалению, по сравнению с другими преступлениями, определения компьютерных преступлений во многих случаях остаются весьма расплывчатыми, и нарушителей привлекают к ответственности, в основном, за потенциальный вред, а не фактический.

В Беларуси на данный момент действительно есть большая потребность в подготовке высококвалифицированных специалистов в области компьютерной безопасности, особенно актуальным этот вопрос встаёт после определения одним из векторов развития нашей страны информатизации Беларуси и развитие IT-индустрии [6]. Документальным подтверждением этому может служить одобрение Советом Министров Беларуси Национальной программы ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011-2015 годы [7].

Уже работающие специалисты в сфере компьютерной безопасности, как правило, вынуждены были готовиться самостоятельно, в свободное от основной работы время, без какого-либо вектора. Поэтому у многих из них знания точечны, рассеянны, не имеют комплексности. Более того, готовиться зачастую приходилось на обрывках информации из Интернет, поскольку ни книг по компьютерной безопасности, ни какой-либо учебно-методической литературы, особенно на русском языке, не издавалось. Последнее послужило одной из главных причин того, что квалификация существующих специалистов порой даже не позволяет определить, случился ли инцидент несанкционированного доступа в принципе, если информация была всего лишь скопирована или прочитана, но не модифицирована или уничтожена. Как правило, такие инциденты могут быть зафиксированы (или может быть сделано предположение об их возникновении) только в случае использования этой информации и вытекающих очевидных последствий её использования.

Необходимость комплексной подготовки специалистов в сфере защиты информации, а также развития научной и учебной базы в этом направлении в нашей стране (с учётом специфики наших производств и менталитета населения) очевидна.

В данный момент белорусские вузы могут осуществлять подготовку по специальности «Компьютерная безопасность» (1-98 01 01) по двум направлениям: “математические методы и программные системы” (- 01) и “радиофизические методы и программно-технические средства” (- 02) со специализациями «Математические методы защиты информации», «Анализ безопасности компьютерных систем», «Защищенные информационные системы», «Программно-аппаратные методы защиты информации», «Безопасность автоматизированных систем обработки информации и управления», «Комплексное обеспечение информационной безопасности телекоммуникационных и информационных систем», «Программно-технические средства и системы защиты информации», «Интеллектуальные технологии защиты информационных систем», «Моделирование и анализ информационных систем». К сожалению, подготовка по специальности «Компьютерная безопасность» осуществляется пока только в трёх вузах Беларуси: БГУ (с 2002 года), ГрГУ (с 2010, а с 2005 на специальность «Программное обеспечение информационных технологий» со специализацией «Системы обеспечения безопасности данных»), ПГУ (с 2009 года), а также БГУИР по направлению 1-98 01 02 «Защита информации в телекоммуникациях». Основная масса выпускников данной специальности поступят на рынок только через несколько лет, а дефицит в высококвалифицированных кадрах имеется уже сейчас. Одним из эффективных решений, например, может быть организация последипломного образования в форме курсов повышения квалификации для действующих специалистов, а также подготовка/переподготовка кадров.

В соответствии с Меморандумом о взаимопонимании между Республикой Беларусь и Республикой Индия, подписанным 17 сентября 2009 года, на базе государственного учреждения «Администрация Парка высоких технологий» и 4-х белорусских вузов уже в 2011 году создан белорусско-индийский учебный центр в области информационно-коммуникационных технологий имени Раджива Ганди. Учебный центр нацелен на обеспечение подготовки и переподготовки специалистов в области информационных технологий, в том числе и по компьютерной безопасности. Причём предлагаемые центром формы проведения занятий удобны для работающих слушателей: очно-заочное обучение, дистанционное обучение, консультирование и индивидуальные занятия, возможность индивидуального подбора учебной программы для группы.

Для работы в белорусско-индийском учебном центре восемь белорусских специалистов были направлены на полугодовую стажировку в Индию, трое из которых обучались по специальности "Diploma in Information System and Cyber Security". Обучение проходило в тренировочной школе (учебном центре) C-DAC (Centre for Development of Advanced Computing) и для обучающихся по компьютерной безопасности предполагало изучение следующих дисциплин: Fundamental of computers and networks; Concepts of Operating System and Administration; C and Data Structures; Database Security Issues; Network Defense and Countermeasures; Auditing, Securing standards and Best Practices; Concepts of Information and Security System; Cyber Forensics; Public Key Infrastructure and Biometrics Concepts and Planning; Ethical Hacking & Cyber Laws. Около половины из названных дисциплин, будучи основополагающими для специалиста в области компьютерной безопасности, к сожалению, отсутствуют в белорусских учебных программах или включены в качестве небольших разделов.

В рамках стажировки занятия проходили в хорошо оборудованных аудиториях и проводились высококвалифицированными специалистами, работающими в крупных IT-компаниях (Hewlett Packard, Microsoft, Oracle и др.). Обучающимся давалась возможность работать с разнообразными программными продуктами, ориентированными на обеспечение

информационной безопасности и анализ ее уровня. Глубина погружения в материал была достаточной, чтобы развивать любую из перечисленных дисциплин для преподавания в Беларуси.

Специалисты, работающие в сфере IT-безопасности, вынуждены непрерывно повышать уровень своих знаний, так как информационные технологии развиваются стремительно, и практически ежедневно появляются новые угрозы. От знаний и умений специалистов по информационной безопасности зависит надежность защиты от компьютерных угроз.

Вопрос подготовки специалистов в области компьютерной безопасности можно рассматривать в системе двух составляющих: комплексная подготовка узкоспециализированного специалиста и поддержка квалификации (переобучение) готового IT-специалиста в сфере безопасности. Первую составляющую разумно обеспечивать вузами Республики по соответствующей специальности с привлечением практикующих специалистов и квалифицированных тренеров. Вторая составляющая может поддерживаться тренировочными или учебными центрами, одним из которых может выступать белорусско-индийский учебный центр, который обеспечит информационную и практическую поддержку для уже готовых специалистов или переподготовку IT-специалистов.

Кроме того, необычайно важно разработать и внедрить комплексные обучающие курсы по компьютерной безопасности, ориентированные как на белорусскую, так и на зарубежную IT-аудиторию в вузах Республики. Так, ряд разработанных краткосрочных курсов уже преподается в рамках учебного процесса УО «Витебский государственный университет им. П. М. Машерова» на математическом факультете и факультете повышения квалификации и переподготовки кадров, а также в УО «Брестский государственный университет им. А. С. Пушкина» на математическом факультете и в УО «Гродненский государственный университет имени Янки Купалы» на факультете математики и информатики.

Литература

1. Уголовный Кодекс Республики Беларусь [Электронный ресурс]. - Режим доступа: http://pravo.kulichki.com/vip/uk/. - Дата доступа: 28.03.2011.
2. Закон Республики Беларусь «Об информации, информатизации и защите информации» от 10 ноября 2008 г. № 455-З [Электронный ресурс]. - Режим доступа: http://pravo.by/webnpa/text.asp?RN=h10800455. - Дата доступа: 20.03.2011.
3. Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» [Электронный ресурс]. - Режим доступа: http://pravo.by/webnpa/text.asp?RN=P31000060 - Дата доступа: 27.03.2011.
4. Комментарий к Указу № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» [Электронный ресурс]. - Режим доступа: http://president.gov.by/press83050.html- Дата доступа: 30.03.2011.
5. Постановление Совета Министров Республики Беларусь от 29 апреля 2010 г. № 644 «О некоторых вопросах совершенствования использования национального сегмента глобальной компьютерной сети Интернет» [Электронный ресурс]. - Режим доступа: http://pravo.by/webnpa/text.asp?RN=C21000644 - Дата доступа: 23.03.2011.
6. А.Лукашенко: <Беларусь не должна отстать от прогресса в области связи и информационных технологий> //12.06.2006 [Электронный ресурс]. - Режим доступа: http://www.ctv.by/news/~news=1668 - Дата доступа: 30.03.2011.
7. Президиум Совета Министров Беларуси одобрил Национальную программу ускоренного развития услуг в сфере ИКТ //1.03.2011 [Электронный ресурс]. - Режим доступа: http://government.gov.by/ru/rus_dayevents20110301.html Дата доступа: 23.03.2011.

А.М.КАДАН, Е.Н.ЛИВАК

ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ В ГРОДНЕНСКОМ ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ

Современное общество - глобальное информационное общество, в котором фактически любая деятельность опирается на использование информационных услуг и технологий, а информационные ресурсы превращаются в важный стратегический товар. В Республике Беларусь ориентация на современное информационное общество и развитие рынка информационных услуг провозглашена одним из государственных приоритетов [1]. К сожалению, в силу непреодолимых глобальных законов диалектического развития, положительные составляющие процесса информатизации неотделимы от ее негативных аспектов. В связи с этим остро стоит вопрос защиты информации, защиты информационных ресурсов и услуг, разработки защищенного программного обеспечения.

Свидетельством признания этих проблем является формирование и развитие специфического сегмента информационной сферы – системы информационной безопасности в целом и одной из ее составляющих – компьютерной безопасности. Особое значение в связи с этим в современных условиях приобретает развитие системы подготовки и переподготовки кадров в области защиты информации.

Руководствуясь государственными стратегическими приоритетами и современным состоянием рынка труда, Гродненский государственный университет (далее - ГрГУ) уделяет пристальное внимание совершенствованию системы подготовки квалифицированных специалистов в области информационных технологий.

В настоящее время университет осуществляет подготовку программистов и ИТ-специалистов по 9 специальностям, три из которых открыты за последние несколько лет, в том числе специальность «Компьютерная безопасность».

Подготовка по специализации 1-40 01 01-04 «Системы обеспечения безопасности данных»

В 2005 году в рамках подготовки студентов по специальности 1-40 01 01 «Программное обеспечение информационных технологий» была начата подготовка по специализации 1-40 01 01-04 «Системы обеспечения безопасности данных». В настоящее время ГрГУ – единственный в республике вуз, который осуществляет подготовку по данной специализации.

Необходимо отметить, что дисциплины, связанные с компьютерной безопасностью и защитой данных, читались студентам факультета и раньше. Так, спецкурс «Методы защиты компьютерной информации» для специальности 1-40 01 01 читался, начиная с 1998 года. Также давнюю историю имеют спецкурсы «Сетевая ОС UNIX и администрирование сети», «Администрирование локальных сетей и обеспечение их безопасности», в которых вопросам компьютерной безопасности уделялось значительное внимание.

При открытии специализации с учетом опыта изучения российских стандартов 2-го поколения специальностей 075200 Компьютерная безопасность, 075300 Организация и технология защиты информации, 075400 Комплексная защита объектов информатизации, 075500 Комплексное обеспечение информационной безопасности автоматизированных систем, 075600 Информационная безопасность телекоммуникационных систем авторами была разработана система спецкурсов, которая учитывала требования совместной подготовки по всем имеющимся на факультете специализациям специальности «Программное обеспечение информационных технологий» и включала дисциплины следующих направлений:

– по разработке программного обеспечения – Java-технологии, технологии разработки Интернет-приложений – «Разработка платформенно-независимых приложений», «Специализированные языки разметки документов»;

– по безопасности информационных систем – «Основы информационной безопасности», «Методы защиты компьютерной информации», «Безопасность электронного бизнеса», «Методы криптографической защиты информации»;

– по обеспечению безопасности компьютерных систем на платформах Unix / Linux и Microsoft Windows – «Сетевая ОС UNIX и администрирование сети», «Защита в операционных системах», «Планирование и поддержка работы в операционных системах семейства Microsoft Windows Server»;

– по обеспечению безопасности компьютерных сетей и сетевых информационных систем – «Администрирование локальных сетей и обеспечение их безопасности», «Управление безопасностью локальных сетевых технологий», «Обеспечение безопасности глобальных сетевых технологий», «Безопасность технических средств сетевых коммуникаций».

Также в рамках обязательного компонента учебного плана специальности «Программное обеспечение информационных технологий» студенты изучают дисциплину «Защита информационных ресурсов, компьютерных систем и сетей».

Согласно требованиям к содержанию курсовых и дипломных работ и регламенту их защиты, студенты, проходящие специализацию «Системы обеспечения безопасности данных», обязаны отражать требования компьютерной безопасности своих проектов в тексте дипломной / курсовой записки и при прохождении процедуры публичной защиты.

Начиная с 2007-2008 учебного года, в рамках специализации подготовлено 48 выпускников. Анализ знаний и компетенций выпускников по специализации «Системы обеспечения безопасности данных» показывает, что они обладают необходимыми профессионально-специализированными компетенциями – способны использовать современные технологии программирования для разработки защищенного программного обеспечения; проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей; учитывать требования современных стандартов по безопасности компьютерных систем; осваивать современные среды разработки программного обеспечения и новые образцы программных средств защиты.

Основные сложности дальнейшего их трудоустройства связаны с отсутствием в штатном расписании большинства организаций региона должностей, связанных с профессиональной деятельностью в области компьютерной безопасности, и пассивностью работодателей.

Выпускники факультета также имеют возможность продолжить образование в рамках магистратуры по специальности 1-40 08 03 «Вычислительные машины и системы». Среди специальных дисциплин магистратуры - курсы «Управление безопасностью компьютерных систем», «Методы защиты компьютерной информации».

Следует отметить, что при распределении студентов по специализациям в начале 3-го курса (с учетом их пожеланий), специализацию «Системы обеспечения безопасности данных» выбирают, как правило, потенциально сильные и более подготовленные студенты. Основной их аргумент – «мы хотим учиться тому, что не сможем изучить самостоятельно».

Подготовка по специальности 1-98 01 01-01 Компьютерная безопасность (математические методы и программные системы)

Подготовка по специальности 1-98 01 01-01 Компьютерная безопасность (математические методы и программные системы), специализация 1-98 01 01-01 03 Защищенные информационные системы открыта в 2010 году в соответствии с «Программой развития подготовки специалистов в области информационных технологий в Учреждении образования «Гродненский государственный университет имени Янки Купалы» на 2009-2012

годы», разработанной с учетом Концепции подготовки и переподготовки специалистов в области информационных технологий в региональном вузе [2]. Изучение перспективной потребности в специалистах с высшим образованием по специальности Компьютерная безопасность в Гродненской области на 2010-2015 годы показывает ее устойчивый рост.

В 2010-2011 учебном году осуществлен первый набор на специальность Компьютерная безопасность. Подготовка студентов ведется в рамках типового учебного плана Белорусского государственного университета (регистрационный № Р 98-065 ДП/уч., от 13.03.2009).

Для объединения и координации усилий специалистов в области компьютерной безопасности в октябре 2010 года на факультете математики и информатики ГрГУ была создана кафедра системного программирования и компьютерной безопасности (СПиКБ). В настоящее время кафедра обеспечивает подготовку 30 студентов 1 курса специальности «Компьютерная безопасность» и 64 студентов 3-5 курсов специализации «Системы обеспечения безопасности данных» специальности «Программное обеспечение информационных технологий».

Как необходимое условие для обеспечения подготовки востребованных специалистов авторы рассматривают участие организаций-потребителей кадров, ИТ-компаний региона, резидентов ПВТ в подготовке специалистов по компьютерной безопасности: в оценке потребностей в специалистах; формировании целевого заказа; участии в учебном процессе (разработке программ спецкурсов, исследовательских работах, производственных практиках, дипломном проектировании). Несомненно, что ключевую роль в этом может сыграть предполагаемое открытие в Гродно филиалов ПВТ и ГП «НИИ ТЗИ».

Важным моментом в подготовке студентов в области компьютерной безопасности, по мнению авторов, является сотрудничество факультета математики и информатики с системой Сетевых Академий Cisco (Локальная Академия Cisco открыта в ГрГУ в мае 2007 г.). Заслуженным авторитетом у студентов факультета пользуются курсы Академии по программе CCNA, учебный материал которых предполагает знакомство с методами защиты информации в компьютерных сетях, изучение защищенных сетевых протоколов и технических устройств обеспечения сетевой безопасности. В 2009 г. Академия Cisco при ГрГУ получила статус Региональной Академии, что позволяет в ее структуре готовить преподавателей факультета к работе в качестве инструкторов программы CCNA.

Планы и перспективы подготовки специалистов по компьютерной безопасности

С марта 2011 года при кафедре системного программирования и компьютерной безопасности ГрГУ начал работу научно-практический семинар «Технологии безопасности 21 века», в рамках которого планируется представление достижений современной науки в области компьютерной безопасности авторитетными специалистами РБ и других стран.

В апреле-мае 2011 года на базе ГрГУ впервые в республике будет проведена олимпиада для студентов и школьников по криптографии и защите информации.

В 2013 году планируется открытие специализированной учебной лаборатории для обеспечения учебных занятий по специальным дисциплинам.

Интересные перспективы открывает ориентация учебного процесса на использование проектных методов обучения. Это позволит организовать работу над совместными учебными проектами, где роль специалиста по компьютерной безопасности в проектной группе будет соответствовать современным требованиям и важности задач разработки защищенных систем и приложений.

Важное место уделяется совершенствованию системы дополнительного образования и переподготовки в области компьютерной безопасности специалистов Гродненского региона, в обеспечении которых задействован потенциал преподавателей кафедры системного программирования и компьютерной безопасности.

В ближайших планах факультета – внедрение новых программ Академии Cisco в учебный процесс. С этой целью в 2010 г. проведено сертифицированное обучение преподавателей по программе CCNA Security. Также от имени ГрГУ в программу TEMPUS заявлен проект «Higher Education Network for Innovative Studies of Networking Curricula», предполагающий адаптацию учебных программ Cisco, в том числе по CCNA Security и CCNP, в учебные программы вузов стран СНГ.

Литература

1. О Стратегии развития информационного общества в Республике Беларусь на период до 2015 года и плане первоочередных мер по реализации Стратегии развития информационного общества в Республике Беларусь на 2010 год / Постановление Совета Министров Республики Беларусь 9 августа 2010 г. № 1174. - [Электронный ресурс]. - http://pravo.by/webnpa/text.asp?RN=C21001174. – Доступ 29.03.2011.

2. Ровба, Е.А. Проблемы подготовки и переподготовки IT-специалистов в региональном вузе / Е.А. Ровба, В.К. Бойко, А.М. Кадан, Е.Н. Ливак // Современные информационные компьютерные технологии: сб. науч. ст. В 2 ч. Ч. 1. - / ГрГУ им. Я. Купалы; редкол.: Е.А. Ровба, А.М. Кадан (отв. ред.) [и др.]. – Гродно: ГрГУ, 2008. – С. 153-156.

Р.А.КАШЕВСКАЯ

КАДРОВЫЙ АСПЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стремительное развитие новых информационных технологий коренным образом изменило процессы функционирования как общества в целом, так и отдельных его структурных элементов. Особенно динамично развивается сфера информатизации процессов управления, основанных на производстве и потреблении информации, что формирует условия для эффективного функционирования самих организаций.

С учетом стратегического характера информационных ресурсов и приоритетного развития информационного сектора экономики многим государствам удалось сделать колоссальный рывок в экономическом, правовом и социальном развитии. При этом концепция создания и обеспечения системы информационной безопасности белорусских организаций приобретает все более актуальное и приоритетное значение и занимает ключевые позиции при принятии управленческих решений.

Следует отметить, что система информационной безопасности организации должна представлять собой единый механизм мобилизации и наиболее оптимального управления корпоративными ресурсами с целью наиболее эффективного их использования и обеспечения устойчивого функционирования конкретной организации, активного противодействия многочисленным негативным влияниям и иным отрицательным воздействиям.

Наиболее значимой частью информационных ресурсов является документированная конфиденциальная информация, которая постоянно оказывает влияние на все сферы деятельности организаций, с помощью которой формируется эффективность и стабильность бизнес-процессов. Объективные условия рыночной конкуренции ставят задачи защиты этого ресурса и число первоочередных и требуют новых решений в вопросах информационной безопасности. На наш взгляд, основой решения проблемы информационной безопасности должна стать последовательная кадровая политика, отвечающая всем современным требованиям по подбору, унификации деятельности персонала, всестороннему контролю их деятельности, формированию у работников положительной мотивации труда. Решение этих

вопросов становится сегодня значимым условием информационной безопасности организации и защиты сведений, составляющих государственную и коммерческую тайну.

Существенной составляющей информационной безопасности организации является профессиональная безопасность, которая может быть определена как совокупность действий по обеспечению оптимального уровня деятельности организации посредством тесной взаимосвязи интеллектуального и кадрового ресурсов. Очевидно, что без надежных и квалифицированных специалистов организации невозможно выжить и победить в конкурентной борьбе. Ведь работники не только являются основным активом организации, но и главным источником потенциальных угроз для нее. В связи с этим обеспечение комплекса мер по предотвращению рисков и опасностей, связанных с личностью человека, с его деятельностью, важнейшая задача кадровой службы организации. Недостаточный квалификационный уровень персонала организации и низкая отдача труда работников могут быть вызваны, в том числе, и ошибками в планировании и управлении персоналом организации, недостаточным материальным стимулированием результатов труда.

Профессиональная составляющая информационной безопасности строится на качественном подборе и стимулировании кадров, на четком распределении служебных обязанностей в соответствии с локальными нормативными правовыми актами. Положительные результаты в организациях дает внедрение системы внутриорганизационного контроля, которая включает в себя отбор персонала посредством современных методов и средств, продуманную и экономически обоснованную систему вознаграждения и карьерного роста, создание такого морально-психологического климата в трудовом коллективе, который благоприятствует совместной работе персонала.

Система трудовой мотивации – еще один действенный инструмент, позволяющий, с одной стороны, на основе управляющего воздействия на ценностные факторы побуждать и стимулировать работников развивать свой интеллектуальный и трудовой потенциал, а с другой – содействовать инновационному преобразованию организации через мотивацию развития персонала.

Практика показывает, что мотивация труда и лояльность организации всегда обусловлены множеством переплетающихся мотивов. Например, одному работнику важен высокий заработок, другому – карьерный рост, третьему – социальная защищенность, четвертому – престиж или возможность заниматься творческой работой. Неудовлетворенный или обиженный сотрудник сродни взрывному устройству замедленного действия, которое в определенный момент обязательно сработает.

Дальнейшее совершенствование правового регулирования отношений, касающихся персонала организации, должно осуществляться прежде всего с учетом Концепции государственной кадровой политики Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 18 июля 2001 г. № 399 (Национальный реестр правовых актов Республики Беларусь, 2001 г., № 68, 1/2863).

Принятие Концепции государственной кадровой политики, которой обусловлено необходимостью реализации стратегического курса на формирование социально ориентированной рыночной экономики, более глубокой интеграции страны в мировую экономическую систему, совершенствования механизма управления обществом на основе сочетания методов государственного и рыночного регулирования, использования современных организационных, информационных, социальных и политических технологий.

Согласно Концепции государственной кадровой политики основными направлениями государственной кадровой политики в Республике Беларусь являются:

формирование современных требований к кадрам различных сфер деятельности и уровней управления;

подбор кадров с учетом их профессиональных и нравственно-психологических качеств;

формирование действенного резерва руководящих кадров и организация планомерной работы с ним;

совершенствование форм и методов оценки деятельности кадров;

мотивация эффективного труда, рациональное использование кадров, создание благоприятных условий для их работы и профессиональной карьеры;

совершенствование системы подготовки, переподготовки и повышения квалификации кадров.

Достижение целей, задач и приоритетов государственной кадровой политики требует совершенствования механизма ее реализации, в частности, нормативно-правового, организационно-методического, информационного, материально-технического, финансового обеспечения.

В современных условиях функционирования нашего государства для субъектов малого и среднего предпринимательства необходим контингент высококлассных кадров с новым экономическим мышлением, глубоким пониманием и знанием прогрессивных методов хозяйствования и правовых основ его ведения, навыками использования современных информационных технологий и работы в условиях демократизации, самоуправления и рыночных отношений. От их уровня компетентности, дисциплины и профессиональной этики зависит эффективное развитие организаций, а также укрепление их престижа и авторитета в обществе.

Достижение указанной цели возможно лишь на основе выработки и реализации государственной кадровой политики, направленной на содействие создания и развития системы подготовки, повышения квалификации и переподготовки кадров для субъектов малого и среднего предпринимательства, адекватной сегодняшним социально-экономическим реалиям.

Обеспечение постоянного соответствия уровня профессиональной компетенции персонала организации требованиям развития экономики и социальной сферы для наиболее эффективного достижения принимаемых целей возможно при активном внимании к таким факторам как:

ясное целепологание и четкое программирование всех сторон деятельности на всех уровнях управления;

постоянное накопление профессиональной компетентности;

регулярная обратная связь, оценка деятельности;

формирование эффективной системы мотивации для работников организации;

поощрение обновления знаний.

Развитие персонала – это не самоцель. Не имеет смысла развивать персонал, если сотрудники не имеют возможности реализовать свои возросшие способности. Необходимо помнить, что способности, по всей видимости, будут применяться на практике только тогда, когда для этого будут реальные возможности.

Проблема управления государством кадровым потенциалом, как весомой составляющей информационной безопасности любой белорусской организации состоит в том, чтобы выработать такие теоретические основы – принципы, механизмы и технологии, которые бы создали самые благоприятные условия для реализации творческого начала человека, задавали единые правила игры для всех субъектов кадровой политики. В основе этих теоретических постулатов должен лежать анализ объективно протекающих процессов в сфере человеческой практики, человеческой деятельности. Цель при этом должна быть одна: обеспечить максимальное приращение кадрового потенциала и рационально им распорядиться в интересах динамичного развития всего общества в целом.

О.Ю.КОНДРАХИН

УЧЕБНО-МЕТОДИЧЕСКОЕ НАПРАВЛЕНИЕ СОВЕРШЕНСТВОВАНИЯ ПРОЦЕССА ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Состояние информационной безопасности определяют не только вопросы подготовки специалистов в высших учебных заведениях, но и переподготовки (повышения квалификации) специалистов, обслуживающих информационные технологии.

Вопросам повышения квалификации специалистов в области защиты государственных секретов в Республике Беларусь уделяется достаточно мало внимания. В настоящее время, как правило, учебные заведения, осуществляющие подготовку студентов по информационной безопасности, не занимаются повышением квалификации в области защиты государственных секретов, в том числе защиты от утечки информации по техническим каналам.

Концепция совершенствования процесса обучения в этом направлении предусматривает решение следующих задач: формирование правовой культуры в области информационных технологий, корректировка существующих учебных программ, введение новых учебных дисциплин. Для отражения современных достижений в области защиты информации необходимо регулярно пересматривать содержание специальных учебных дисциплин. Несбалансированность учебной программы бросается в глаза при прохождении производственных практик студентов старших курсов высших учебных заведений. За десятки часов рассмотреть вопросы технических каналов утечки информации возможно только поверхностно, не вдаваясь в подробности. Полностью отсутствуют вопросы, посвященные нормативно-правовой базе, практических занятий, наличия наглядных пособий средств защиты информации и применимости в реальных условиях эксплуатации. В настоящее время целесообразно дополнить учебные программы подготовки специалистов в области информационной безопасности практическими занятиями.

Целью учебных программ должно являться обеспечение повышения квалификации руководителей служб и подразделений верхнего и среднего уровней, руководителей подразделений по защите информации, ответственных за состояние информационной безопасности в организации, аналитикам, экспертам и консультантам по компьютерной безопасности; администраторам безопасности, контроля и управления безопасностью, ответственным за сопровождение и администрирование средств защиты информации; специалистам, ответственным за разработку нормативно-методических и организационно-распорядительных документов по вопросам защиты информации, менеджерам, ответственным за работу с персоналом по вопросам обеспечения информационной безопасности организаций.

Основными целями подготовки, переподготовки и повышения квалификации специалистов в области защиты информации являются обеспечение постоянного приобретения ими знаний в области теории и практики защиты информации, идеологии, экономики, права, совершенствование управленческих умений и навыков, позволяющих успешно выполнять служебные обязанности. Подготовка, переподготовка и повышение квалификации кадров должна строиться на принципах системности, обязательности, дифференцированного подхода, перспективности. Для обеспечения непрерывного роста профессионального уровня руководящих работников, назначаемых на новые должности, руководителями государственных органов (организаций) должно предусматриваться обязательное повышение их квалификации. Ведущими государственными высшими учебными заведениями в системе подготовки, переподготовки и повышения квалификации в области защиты информации являются БГУ, БГУИР, БНТУ, Академия управления при Президенте Республики Беларусь, Институт повышения квалификации и переподготовки

руководителей и специалистов промышленности «Кадры индустрии». Подготовка, переподготовка и повышение квалификации должна осуществляться на основе государственного заказа. В государственный заказ должен включаться перечень специальностей и специализаций, а также категорий обучающихся, число слушателей, необходимое финансирование.

В настоящее время наблюдается диспропорция в подготовке кадров для защиты государственных секретов. В ВУЗах Республики Беларусь осуществляется подготовка специалистов по защите информации в телекоммуникациях, по расследованию компьютерных преступлений, с изложением основ теории защиты информации и т.д. Понятно, что досконально изучить вопросы, связанные с технической защитой информации не представляется возможным. Один из подходов организации эффективного повышения квалификации является привлечение высококвалифицированных специалистов по защите информации. Однако, в настоящее время, они практически не знакомы с особенностями учебных программ. Учебные программы не согласовываются с заинтересованными структурами.

В идеальном случае решение такой проблемы видится в открытии специализированного центра повышения квалификации. Одними из учреждений, обеспечивающих повышение квалификации в области информационной безопасности (в т.ч. специалистов в области технической защиты информации), являются Негосударственное образовательное учреждение «Центр повышения квалификации специалистов по технической защите информации» при Государственном научном исследовательском испытательном институте проблем технической защиты информации ФСТЭК России, Национальный технический университет Украины (НТУУ) «КПИ». Еще в 1994 году на базе НТУУ «КПИ» был создан научный учебно-методический центр повышения квалификации специалистов по вопросам защиты секретной информации и технической защиты информации, переименованный позднее в специальные курсы последипломного образования в области защиты информации с ограниченным доступом.

Проведение кадровой политики в области защиты информации имеет немаловажное, решающее значение при сохранении секретов. Умение правильно руководить сотрудниками, подбирать квалифицированно кадры, обеспечить защиту информации ценится очень высоко. В области подготовленности кадров по вопросам защиты информации Соединенные Штаты являются одной из передовых стран. Этот вопрос решается на государственном уровне, и деятельность служб безопасности контролируются президентом. Поэтому тот положительный опыт, который по этим вопросам можно использовать у нас в стране, очень ценен. Используя опыт США, в нашей стране создаются кафедры и центры повышения квалификации.

Задача, которая сейчас стоит перед этими учреждениями - подготовка кадров широкого профиля по комплексной защите информации с узкой специализацией по одному из направлений защиты информации. Каждый специалист в области защиты информации должен понимать всю важность решаемой им проблемы, осознавать свою ответственность перед обществом.

Немаловажное значение имеет психологический аспект. В Соединенных Штатах при приеме сотрудника в службу безопасности досконально изучается его характер, окружение, прошлое, семья и др. Помимо простого анкетирования, проводится ряд тестов на профессиональную пригодность, определяются положительные и отрицательные черты характера, иногда проводится даже графологическая экспертиза. Таким образом, возможность попадания в службу безопасности лиц, несоответствующих данной профессии исключается практически совсем.

Большое воздействие на сотрудника имеет материальное обеспечение. При хорошей зарплате сотрудников на предприятии существует меньшая вероятность хищения информации, представляющей ценность для конкурентов.

Руководствуясь положительным опытом зарубежных стран, в Беларуси можно создать четкую и отлаженную систему организации работы с кадрами, способную защитить государственные секреты.

Учитывая важность своевременного повышения квалификации специалистов в области информационной безопасности, необходимость обеспечения единых подходов при выполнении программ Союзного государства актуальным становится вопрос взаимного сотрудничества и обмена опытом.

Е.Н.ЛИВАК

ФОРМИРОВАНИЕ БАЗОВЫХ ЗНАНИЙ И КОМПЕТЕНЦИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ БУДУЩИХ ПРОГРАММИСТОВ

В системе подготовки студентов по специальности 1-40 01 01 Программное обеспечение информационных технологий в Гродненском государственном университете имени Янки Купалы (далее – ГрГУ) особое внимание уделяется формированию знаний и компетенций студентов в области защиты информации.

В 1998 году автором была разработана специальная дисциплина (спецкурс) «Методы защиты информационных систем». С тех пор содержание дисциплины постоянно обновлялось и совершенствовалось, а сама дисциплина с течением времени была переименована в «Методы защиты компьютерной информации». Сегодня эта дисциплина является дисциплиной, в рамках которой формируются базовые знания и компетенции в области защиты информации будущих IT-специалистов, разработчиков программного обеспечения. Спецкурс изучают студенты 3 курса двух специализаций 1-40 01 01-01 «Компьютерные системы и Интернет-технологии» и 1-40 01 01-04 «Системы обеспечения безопасности данных».

Основная направленность и тематика

Основная задача специальной дисциплины – сформировать фундаментальные знания и компетенции студентов в области обеспечения безопасности программ и данных, ознакомить с современными подходами, методами, алгоритмами и механизмами защиты компьютерной информации.

Содержание дисциплины предполагает изучение следующих основных модулей

– теория современных компьютерных вирусов;

– традиционные методы защиты данных и компьютерных программ от нелегального использования и модификации; методы идентификации программных продуктов;

– алгоритмы, системы и стандарты криптографической защиты информации;

– методы компьютерной стеганографии;

– методы защиты программ от исследования;

– методы взлома механизмов защиты;

– методы программно-аппаратной защиты;

– методы охраны авторских прав разработчиков программного обеспечения; современные технологии лицензирования локального и сетевого программного обеспечения;

– юридические аспекты защиты программных продуктов от нелегального использования;

– технологии защиты интеллектуальной собственности в Internet.

Ниже представлено обоснование предложенной автором тематики.

Компьютерные вирусы получили чрезвычайно широкое распространение, а многие из них наносят значительный экономический ущерб работе компьютерных систем. Поэтому

студентам необходимо разбираться в теории компьютерных вирусов, знать способы их распространения, технологии внедрения вирусов в заражаемые объекты, современные форматы исполняемых файлов, способы маскировки вирусов, принципы внедрения и активизации сетевых червей, угрозы проникновения в компьютерную систему троянцев.

Необходимо также знать и понимать правила, которые требуется соблюдать для предотвращения внедрения вируса в компьютерную систему, а также методы, которые позволяют быстрее обнаруживать наличие вируса, для того, чтобы остановить его распространение. В случае проявления вирусом своих агрессивных свойств необходимо уметь восстанавливать пораженные объекты.

Студенты должны овладеть методикой использования современных антивирусных средств. На рынке программного обеспечения доступно большое количество антивирусных средств, каждое из которых имеет свои достоинства и недостатки. Необходимо уметь обосновать выбор и правильно сконфигурировать инструмент для работы в конкретной вычислительной системе.

К сожалению, современные вирусы используют такие методы маскировки, которые позволяют им быть незамеченными антивирусными средствами. Поэтому студентам необходимо владеть основными навыками ручного обнаружения и удаления вируса, а также восстановления поврежденной информации. Методы восстановления объектов заражения вирусами и системы в целом практически аналогичны методам восстановления работоспособности компьютера в случае аварии или сбоя, поэтому названные методы предлагается рассматривать параллельно.

Большое внимание при изучении спецкурса уделяется криптографическим методам, которые многими специалистами признаются универсальными и надежными. Студенты изучают базовые и современные алгоритмы шифрования; государственные стандарты в области криптографии и практические реализации криптосистем. Обсуждается стойкость алгоритмов симметричного и асимметричного шифрования, особое внимание уделяется ошибкам в практических реализациях. Изучается также особый раздел криптографии – алгоритмы и схемы формирования и проверки электронной цифровой подписи. Параллельно изучаются защищенные функции хэширования и области их применения.

Особое место в содержании спецкурса занимают современные технологии безопасности – технологии стеганографической защиты данных, компьютерных программ и мультимедийной продукции. Автор согласна со специалистами: «на базе компьютерной стеганографии, являющейся одной из технологий информационной безопасности XXI века, возможна разработка новых, более эффективных нетрадиционных методов обеспечения информационной безопасности» [1, с. 71].

В настоящее время широко используются на практике и многими пользователями признаются надежным средством системы программно-аппаратной защиты. В основном такие системы − привилегия корпоративных заказчиков, именно поэтому на рынке ПО с каждым годом растет количество применяемых электронных ключей и других аппаратных средств защиты. Поэтому при изучении базовых методов защиты студенты знакомятся и с принципами работы систем программно-аппаратной защиты, изучают конкретные реализации таких систем.

Программист, владеющий методами технической защиты, несомненно, должен владеть технологиями взлома механизмов защит для того, чтобы, во-первых, не повторять ошибки существующих систем и, во-вторых, создавать более эффективные и надежные механизмы. Поэтому в спецкурсе рассматриваются основные идеи, приемы, алгоритмы и технологии, позволяющие снимать, обходить или взламывать программную защиту. Для взлома механизма защиты нарушителю, прежде всего, необходимо найти в программном модуле защитный механизм и понять логику его работы, то есть исследовать программу. Поэтому противодействие попыткам запуска и/или исполнения защищенной программы

рекомендуется сопровождать механизмами, предотвращающими возможность исследования программы, в том числе и зарегистрированных (законных) копий.

Разработчик механизмов защиты также должен быть хорошо знаком с инструментарием современных взломщиков и учитывать возможности существующих средств исследования программ (отладчиков, дизассемблеров, просмотрщиков) при проектировании механизмов и систем защиты программ и данных.

В настоящее время в компьютерной индустрии, в области программного обеспечения остро стоит вопрос о защите программных продуктов от нелегального использования и модификации. Кроме того, на современном этапе развития глобальных информационных технологий остро стоит вопрос об охране объектов интеллектуальной собственности в Internet. Поэтому в спецкурсе уделяется внимание вопросам, связанным с защитой прав авторов (владельцев) компьютерных программ и других объектов, распространяемых и/или опубликованных в сети Internet.

Авторские права охраняются специальными законами, как на национальном, так и на международном уровне. Республика Беларусь имеет современное законодательство об авторском праве. При изучении спецкурса рассматриваются наиболее существенные для разработчиков программных продуктов положения законодательства об авторском праве: права авторов компьютерных программ; положения о воспроизведении компьютерных программ; положения законодательства о соавторстве; положения об авторском праве на служебные произведения; положения о защите нарушенных прав автора. Изучаются также нюансы регистрации компьютерных программ и норм патентного права.

Таким образом, содержание специального курса отражает современный взгляд на методы обеспечения компьютерной безопасности и действительно позволяет ознакомить слушателей на базовом уровне с традиционными и современными подходами, методами, алгоритмами и механизмами защиты компьютерной информации.

Учебно-методическое обеспечение и инновационные формы обучения и контроля

Учебно-методическим обеспечением спецдисциплины являются разработанные автором учебные пособия [2, 3, 4] и электронный учебно-методический комплекс (УМК) [5, 6]. Обратим внимание, что УМК адаптирован для доступа в двух режимах: 1) использование на локальном компьютере, 2) доступ посредством сети Internet и, соответственно, имеет две формы представления. В настоящее время УМК доступен по адресу http://mf.grsu.by/UchProc/livak/discipline_zachita.htm. А локальная версия УМК включает также и вспомогательные средства обучения − презентации избранных лекций.

Авторская инновационная форма самостоятельной работы студентов под управлением преподавателя − углубленное изучение студентами одной из тем предметной области (по выбору студента), не вошедших в тематику лекционного курса или вошедших в ограниченном объеме. Для обеспечения такой формы работы в УМК включены аннотированные темы для углубленного самостоятельного изучения. В качестве контроля результатов обучения предлагается индивидуальное собеседование студента с преподавателем по исследуемой тематике.

Помимо традиционного экзамена автором используются такие формы контроля как совместное со студентом тестирование разработанных механизмов защиты; групповая работа по настройке и изучению функциональных возможностей систем. Большой интерес у студентов вызывает выполнение заданий, включающих взлом механизмов защиты, реализованных товарищами, с оценкой мощности предложенного механизма и указанием товарищу на слабые места защиты.

В рамках дисциплины активно используется также проектный метод обучения, предусматривающий работу студентов в проектных группах, проведение коллективной творческой работы.

Литература

1. Барсуков В.С., Водолазкий В.В. Современные технологии безопасности. М.: «Нолидж», 2000. − 496 с.

2. Ливак, Е.Н. Защита информации: Учебное пособие. В 4 ч. Ч.1. Компьютерные вирусы. − Гродно, ГрГУ, 1997 − 100 с.

3. Ливак Е.Н. Защита информации: Учебное пособие. В 4-х ч. Ч.2 − Как лечить компьютер. − Гродно, ГрГУ, 1998 − 95 с.

4. Ливак, Е.Н. Защита информации: Учеб. пособие: В 4 ч. Ч.3. Защита авторских прав в области программного обеспечения. − Гродно, ГрГУ, 2000. − 109 с.

5. Ливак, Е. Н. Методы защиты компьютерной информации: Учебно-методический комплекс [Электронный ресурс]: Гродненск. гос. ун-т им. Я. Купалы. − 2008. − 1 электр. компакт диск (CD-R). − 228 с. − Библиогр.: с.222-228 (89 назв.) − Рус. − Деп. в ГУ «БелИСА» 21.04.2008 № Д200818.

6. Ливак Е.Н. Компоненты, содержание и особенности электронного учебно-методического комплекса «Методы защиты компьютерной информации» // Современные информационные компьютерные технологии: сб. науч. ст. В 2 ч. Ч. 2 / ГрГУ им. Я.Купалы; редкол.: А.М. Кадан (отв. ред) [и др.]. – Гродно: ГрГУ, 2008 – С. 341-343.

Н.В.МЕДВЕДЕВ

ИННОВАЦИОННОЕ ОБРАЗОВАНИЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ И США

Обеспечение информационной безопасности (ИБ) является важной международной проблемой. Ценные и значимые информационные ресурсы могут стать жертвами атак хакеров, кибертеррористов, инсайдеров, социально-политических организаций определенного толка, расположенных по всему миру. Атаки на информационные системы и сети обострялись в течение последних нескольких лет. Критические элементы национальной инфраструктуры (например, электрические сети, ГЭС, химические и ядерные установки, системы трубопроводов, объекты здравоохранения), а также правительственные организации, предприятия и финансовые учреждения уязвимы для кибернетических атак, которые могут вызвать разрушительные последствия.

РФ и США стоят на технологически передовых позициях в указанном аспекте и находятся среди 10 лучших стран по противодействию вредоносной киберактивности. Обе страны имеют серьезный дефицит специалистов, которые адекватно подготовлены не только для понимания рисков нарушения информационной безопасности, разработки политики ИБ, осуществления контроля безопасности и анализа инцидентов, но и в понимании мотивов такой деятельности. Информационная безопасность является междисциплинарной областью и включает в себя несколько дисциплин: теоретическую информатику, компьютерные науки, уголовное и гражданское право, судебную медицину, математику, системный и схемотехнический анализ и синтез, деловое администрирование, психологию (список далеко не полон). Существует необходимость интеграции подходов к дисциплинам в области ИБ в разных странах для адекватного международного сотрудничества. Совсем недавно правительства России и США провели активную совместную работу по решению этой проблемы.

Образовательные системы двух стран имеют свои уникальные достоинства. Российское образование, базирующееся на лучших традициях советской высшей школы, имеет преимущество в фундаментальных физико-математических науках, признаваемое

США. В то же время имеется определенное преимущество США в области прикладных наук и деловом администрировании. Одновременно существуют идеологические различия у людей, имеющих дело с понятиями конфиденциальности и информационной безопасности. Совместная деятельность с целью разработки учебных программ по России и Соединенным Штатам поможет в привлечении сильных сторон этих двух стран при подготовке специалистов по информационной безопасности и окажет помощь в сокращении идеологических различий.

Различия в вопросах коммуникации, языка, ресурсов и культуры, создают очевидные препятствия для такой деятельности. Однако эти барьеры преодолимы. Официальное соглашение, подписанное Министрами образования США и РФ, привело к разработке совместного проекта, в котором участвуют МГТУ имени Н. Э. Баумана и Университет штата Нью-Йорк (State University of New York).

В рамках проекта, стартовавшего в ноябре 2010 года, предусмотрена совместная разработка ряда электронных курсов дистанционного образования в области ИБ; прошедшим обучение предполагается выдавать соответствующий сертификат, признанный двумя странами. В настоящее время происходит активный обмен знаниями между двумя университетами, идет совместная разработка учебных программ и контента в формате дистанционного обучения. Студенты из двух стран будут заниматься совместно с использованием работы через интернет-форумы. Они также примут участие в летней 4-недельной практике по изучению языка для студентов МГТУ в Олбани, а для студентов SUNY в Москве.

Первоначальный список курсов совместного проекта приведен ниже:

– Математические методы в задачах ИБ;
– Теоретические основы ИБ;
– Анализ информационных рисков;
– Технологии реализации ИБ;
– Разработка политик ИБ;
– Экспертиза компьютерной безопасности;
– Психология ИБ;
– Шифрование и кодирование информации.

Каждый курс создается в двуязычном варианте.

Е.А.СВИРСКИЙ, В.Н.ШАЛИМА

О ПОВЫШЕНИИ КОМПЕТЕНТНОСТИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗАКОН ГАРДНЕРА: 85 процентов людей любой профессии некомпетентны.
Джон Гарднер

Основное достоинство специалиста по информационной безопасности – это его компетентность в области защиты информации. Очевидно, что компетентность специалиста базируется на знаниях, навыках и опыте. Что когда и где можно получить.

Классически процессы повышения уровней компетентности осуществляются следующим образом:

знания можно получить только в учреждениях образования: университеты, институты, учреждения переподготовки кадров и повышения квалификации;

навыки – частично в учреждения образования, но в основном на рабочих местах или на различных курсах по изучению и освоению конкретных систем, проводимых как самими производителями систем, так и аккредитованными учебными центрами;

опыт только в результате производственной и/или исследовательской деятельности.

Процессы формирования специалиста, его компетентности, достаточно трудоемки и растянуты во времени. Классическая схема подготовки специалистов давала неплохие результаты только в зрелых отраслях с установившимися технологическими процессами. Для инновационных отраслей, к которым относится отрасль информационных технологий, в том числе, и одно из ее наиболее динамично развивающихся направлений защита информации, такая схема формирования компетентности специалистов становится неприемлемой. В инновационных отраслях знания устаревают очень быстро и часто конкретные знания по специальности, полученные в учебном заведении, оказываются ненужными, поскольку технологии ушли вперед.

Внедрение информационных технологий во все сферы деятельности общества резко повысило темпы обработки информации и создания новых знаний во всех отраслях. Учреждения образования чаще всего не в состоянии обновлять учебные программы такими же темпами в силу многих факторов, например, отсутствие достаточных финансовых ресурсов для модернизации материальной базы учебных процессов, отсутствие доступа к новейшим технологиям, недостаточная квалификация преподавательского персонала и т.п.

В таких условиях при подготовке специалистов по информационной безопасности необходима большая дифференциация процессов получения знаний. Поскольку классические университеты не в состоянии угнаться за темпами развития технологий, то они должны сконцентрировать основное внимание на предоставлении базовых, фундаментальных знаний по специальности, освоении основных теорий информационных технологий и т.п., а также то, что, очевидно, является самым главным научить своих студентов учиться и дальше.

Таким образом, первое образование должно стать платформой, на которой можно формировать все последующие специализации через систему переподготовки кадров и повышения квалификации. Система формирования специалиста остается той же – базовое университетское образование, система переподготовки и повышения квалификации, только должны сместиться акценты. Необходимо ускорить время достижения специалистом уровня компетентности, позволяющего самостоятельно принимать решения и организовывать деятельность в сфере его полномочий. А это означает, что основные навыки по специализации он должен получить в системе переподготовки кадров и повышения квалификации. Здесь же он должен получить и определенную долю опыта работы по специальности. Как этого достичь?

Это возможно сделать, если пойти по пути создания центров компетентности при организации переподготовки кадров и повышения квалификации. Штатные преподаватели системы переподготовки кадров и повышения квалификации в полной мере не могут дать навыков и опыта в силу тех же причин, что и преподаватели базового образования. В центр компетентности кроме учреждения образования должны входить структуры, владеющие актуальными знаниями, навыками и опытом работы в сфере защиты информационных ресурсов и информационных технологий. К таким, очевидно, можно отнести центры реагирования на компьютерные инциденты, структуры, осуществляющие аудит информационной безопасности, исследовательские центры, структуры, выполняющие работы по построению и обслуживанию систем защиты информации и т.п. Естественно, в центре компетентности должны присутствовать и органы государственного управления и иные структуры, обеспечивающие государственной регулирование в этой сфере.

РЕЗОЛЮЦИЯ XVI НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

«КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ»

С 17 по 20 мая 2011 г. в г. Гродно состоялась очередная XVI научно-практическая конференции «Комплексная защита информации» как мероприятие Союзного государства. Организаторы конференции – Парламентское Собрание Союза Беларуси и России, Постоянный Комитет Союзного государства, аппарат Совета Безопасности Российской Федерации, Оперативно-аналитический центр при Президенте Республики Беларусь, Федеральная служба по техническому и экспортному контролю Российской Федерации, Межрегиональная общественная организация «Ассоциация защиты информации». В работе конференции приняли участие около 200 ученых и специалистов Беларуси и России.

На пленарных заседаниях и круглых столах было заслушано и обсуждено более 130 докладов ученых, специалистов, представителей государственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных направлений, осуществлялся обмен опытом по вопросам использования информационных и коммуникационных технологий в различных сферах жизни общества и государства.

Совместно с конференцией Парламентским Собранием Союза Беларуси и России проведен семинар «Безопасность информационного пространства Союзного государства».

В ходе проведения конференции на пленарных заседаниях обсуждались следующие вопросы:

1. Основы безопасности информационного пространства Союзного государства и государств-участников.
2. Организационно-правовое обеспечение безопасности субъектов информационных отношений.
3. Современные методы, технологии и средства защиты информации.
4. Подготовка специалистов в области защиты информации.

На круглых столах участники конференции обменялись опытом по следующим проблемам:

1. Нормативные правовые аспекты обеспечения информационной безопасности общества.
2. Обеспечение информационной безопасности и противодействие киберпреступности в сети Интернет.
3. Создание защищенных объектов информационных технологий.
4. Вопросы криптографической защиты информации.
5. Технические вопросы защиты информации. Защита критически важных объектов информационно-коммуникационной инфраструктуры.

На конференции подведены итоги практической деятельности государственных органов, организаций и предприятий России и Беларуси по выполнению программ Союзного государства в области информационных технологий и защиты общих информационных ресурсов государств-участников.

Участники конференции обменялись опытом исследований, разработки и внедрения теоретических, методологических, нормативных, организационно-технических, правовых и гуманитарных вопросов обеспечения информационной безопасности.

Программа круглых столов содержательная и насыщенная. Наибольший интерес вызывали вопросы обеспечения безопасности использования Интернета в современных условиях, а также защита критически важных объектов информационно-коммуникационной инфраструктуры.

Участники конференции считают, что обеспечение безопасности информационно-технологической сферы, наряду с формированием информационных ресурсов, в настоящее время по-прежнему является одним из основных направлений развития Союзного государства.

Полагаем, что придание Советом Министров Союзного государства конференции «Комплексная защита информации» статуса ежегодного мероприятия Союзного государства служит дальнейшему укреплению сотрудничества Беларуси и России в данной сфере на благо наших народов.

Участники конференции постановили:

1. Одобрить работу XVI научно-практической конференции «Комплексная защита информации» в целом как актуального и важного шага по консолидации усилий научной и деловой общественности, представителей органов власти и государственного управления Союзного государства и государств-участников для разработки современных подходов и поиска путей повышения эффективности защиты информации и обеспечения информационной безопасности личности, общества, государства.

2. Поддержать предложение о формировании новой программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011-2015 годы с учетом современных рисков и угроз информационной безопасности.

3. Обратиться в Постоянный Комитет Союзного государства и Парламентское Собрание Союза Беларуси и России с предложением проработать вопрос об учреждении Премии Союзного государства для молодых ученых в области информационной безопасности.

4. Провести XVII научно-практическую конференцию «Комплексная защита информации» в 2012 г. в Российской Федерации. Просить Постоянный Комитет Союзного государства сформировать рабочую группу для подготовки и осуществления организационных мероприятий.

5. Проинформировать руководство Постоянного Комитета Союзного государства и Парламентского Собрания Союза Беларуси и России об итогах XVI научно-практической конференции «Комплексная защита информации» и ее предложениях.

Принята на пленарном заседании
20 мая 2011 года
г. Гродно

ФОТОРЕПОРТАЖ С XVI НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ»

Участники 16-й научно-практической конференции «Комплексная защита информации» и семинара «Безопасность информационного пространства Союзного государства» Парламентского Собрания Союза Беларуси и России возлагают венок к монументу в честь советских воинов, погибших при освобождении Гродно от немецко-фашистских захватчиков

Встреча участников конференции и семинара в Гродненском государственном университете имени Янки Купалы

Открытие конференции в актовом зале Гродненского государственного университета имени Янки Купалы

Председатель Комиссии Парламентского Собрания Союза Беларуси и России по безопасности, обороне и борьбе с преступностью Ванькович А.С.

Председатель Государственного комитета по науке и технологиям Республики Беларусь Войтов И.В.

Участники конференции на пленарном заседании в день открытия конференции 17 мая 2011 года

Заместитель Государственного секретаря – член Постоянного Комитета Союзного государства Дубинский Ю.М. вручает медаль «За сотрудничество» заместителю начальника Оперативно-аналитического центра при Президенте Республики Беларусь Капариху С.Н. за организацию подготовки конференции

Заместитель Государственного секретаря – член Постоянного Комитета Союзного государства Дубинский Ю.М. вручает медаль «За сотрудничество» директору Государственного предприятия «НИИ ТЗИ» Картелю В.Ф. за организацию подготовки конференции

Участники круглого стола «Вопросы создания защищенных объектов информационных технологий»

Участники 16-й научно-практической конференции «Комплексная защита информации»

СОДЕРЖАНИЕ