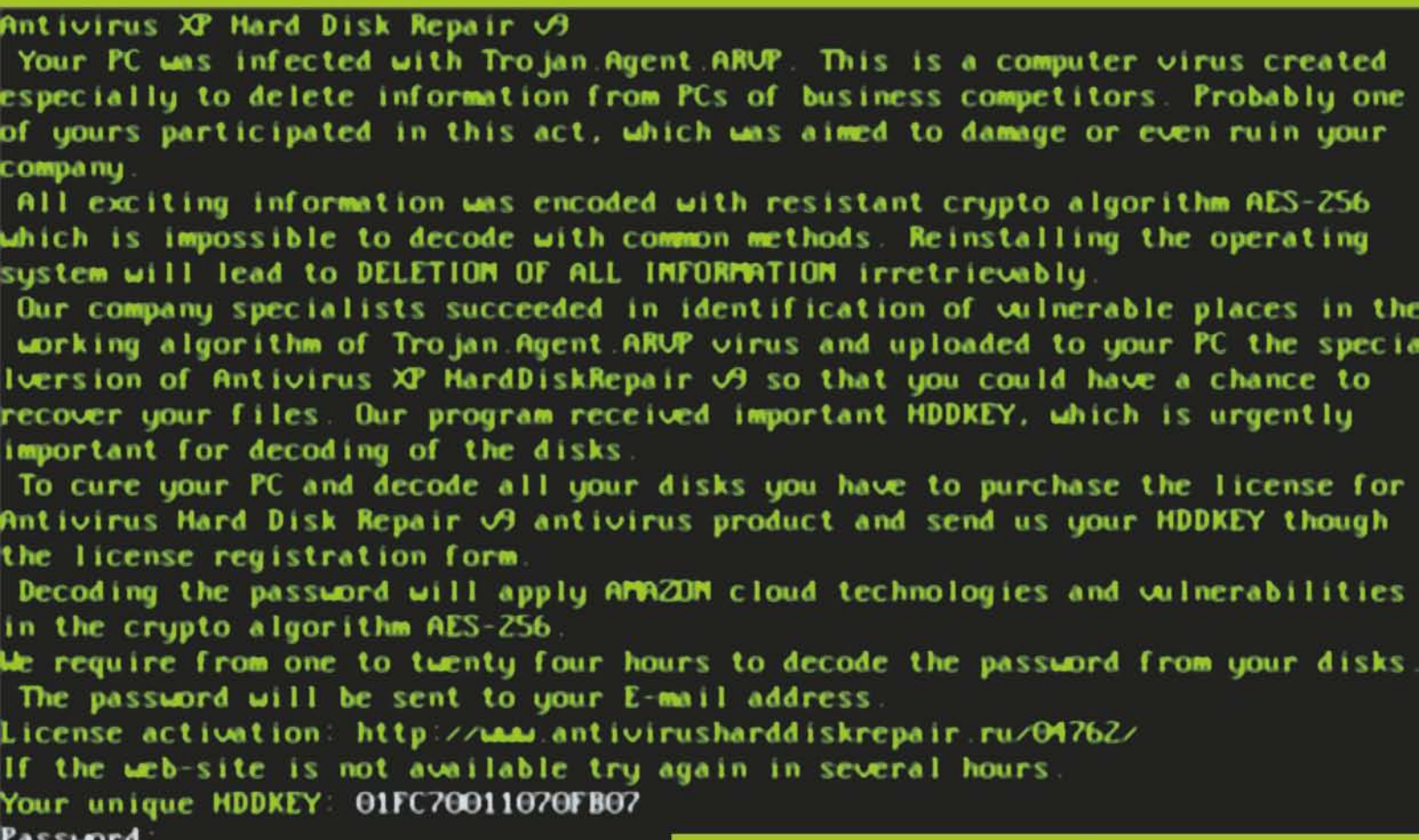
Журнал для руководителей предприятий и специалистов отрасли безопасности

№2 (29)
март-апрель
2013

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ



специальный номер
Информационная безопасность

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

СРЕДСТВА И СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

AXIOM

Не требует доказательств

Оборудование видеонаблюдения

ОДО “Сфератрэйд”
ул. Машиностроителей 29-117, Минск 220118 Беларусь
www.axiom.by

Velcom: +375 29 641 50 50
МТС: + 375 29 541 50 50
Тел/факс: +375 17 341 50 50

УНН100972915

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ, №2 (29)–2013
В НОМЕРЕ:

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

СРЕДСТВА И СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ

СПРАВОЧНАЯ ИНФОРМАЦИЯ

«ТЕХНОЛОГИИ БЕЗОПАСНОСТИ»
Производственно-практический журнал
№2 (29), март-апрель, 2013

Периодичность выхода: 1 раз в 2 месяца

Учредитель и издатель:
ООО «АэркомБел»

Главный редактор:
Сергей Адамович Драгун

Над номером работали:
Лисенкова Анна
Карпук Мария

Журнал зарегистрирован
в Министерстве информации
Республики Беларусь
Свидетельство о регистрации
№ 846 от 10.12.2009

Адрес редакции:
220073, г. Минск, ул. Гусовского, 6,
оф. 2.15.2
Тел./факс: (017) 290-84-05

Отдел рекламы:
Тел./факс: (017) (017) 290-84-05,
256-10-35, 256-10-47
e-mail: info@aercom.by
www.aercom.by

Отдел подписки:
Тел./факс: (017) 290-84-05
e-mail: podpiska@aercom.by

Подписка через РУП «Белпочта»:
01248 — для индивидуальных
подписчиков;
012482 — для предприятий и организаций.

Цена 59500 бел. руб. без НДС,
на основании п. 3.12 ст. 286
Особенной части Налогового Кодекса
Республики Беларусь

Подписано в печать — 21.03.2013 г.
Формат: 60x90 1/8
Бумага офсетная
Гарнитура Myriad Pro. Печать офсетная
Усл. печ. л. 5,5; Уч.-изд.л. 5,9
Тираж: 800 экз.
Заказ _____

Отпечатано в типографии
ООО «Юстмаж»

Адрес типографии: г. Минск,
ул. Калиновского, д.6, Г 4/К, комн. 201
Лиц. ЛП №02330/0552734 от 31.12.2009,
Министерство информации РБ

ISSN 2221-8661

Сегмент информационной безопасности в Беларуси демонстрирует взрывной рост и, соответственно, увеличение бюджетов. Предпосылки роста – процесс информатизации в стране и подверженность общемировым рискам информационной безопасности. Лидерами по применению продуктов и внедрению технических средств являются государственные ведомства, крупный корпоративный сектор и банковская отрасль.

Для банков информационная безопасность становится особо актуальной, т.к. её обеспечение стимулируется не только реальными угрозами, но и принятием государственных программ по развитию систем безналичных платежей с использованием карточек и средств электронных платежей на 2013-2016 гг. Безналичный денежный оборот в сферах розничной торговли и услуг в Беларуси к 2016 году планируется увеличить примерно в четыре раза – до 50%.

Мы работаем над созданием национальных информационных площадок для консолидации профессионального сообщества, на которых будет происходить обмен информацией, повышение квалификации, общение между участниками сегментов, регуляторами и пр. специалистами отрасли безопасности. В 2013 году состоятся тематические выставки-форумы под брэндом «Центр безопасности»:

- 5 июня 2013, состоится выставка-форум по тематике – «Инженерно-техническая безопасность»;
- в ноябре 2013, состоится выставка-форум по тематике – «Методы и системы защиты информации, информационная безопасность».

Подробнее на сайте cb.aercom.by

Учитывая специализацию данного номера, ранее запланированные материалы будут размещены в №3, май-июнь, 2013.

С уважением, Драгун Сергей Адамович,
главный редактор журнала.

21-24 мая 2013 года в г. Бресте
состоится ежегодное мероприятие Союзного государства
- XVIII научно-практическая конференция «Комплексная защита информации»

Постоянный Комитет Союзного государства, Парламентское Собрание Союза Беларуси и России при участии аппарата Совета Безопасности Российской Федерации, Оперативно-аналитического центра при Президенте Республики Беларусь, Федеральной службы по техническому и экспортному контролю Российской Федерации приглашает ученых, специалистов, представителей государственных органов и практических работников в области обеспечения информационной безопасности принять участие в ежегодном мероприятии для обмена опытом по вопросам использования информационных и коммуникационных технологий в различных сферах жизни общества и государства.

«Актуальные вопросы безопасности информационного пространства государств-участников Союзного государства»

создание защищенных объектов информационных технологий;
техническая защита информации;
нормативно-правовые аспекты обеспечения информационной безопасности;
государственные системы управления открытыми ключами;
государственные системы идентификации и аутентификации;
математика и безопасность информационных технологий;
подготовка специалистов в области информационной безопасности.

Организатор: НИИТЗИ, подробнее http://niitzi.by
Информационный партнер: журнал «Технологии безопасности»

Ноябрь, 2013
1 национальная выставка-форум

«Методы и системы защиты информации, информационная безопасность»

Центр безопасности

новейшие технологии
проблемно-ориентированные решения
семинары с участием регуляторов, экспертов-практиков из других стран

aercom.by

Защита информации – важнейшая составляющая безопасности Союзного государства

Картель Владимир Федорович,
директор Государственного предприятия «НИИ ТЗИ».

Бакун Виктор Николаевич,
начальник сектора Государственного предприятия «НИИ ТЗИ».

В условиях непрерывного совершенствования информационных технологий, обусловленного решением всё более сложных и масштабных задач во всех сферах жизнедеятельности человека, возрастает зависимость государства и общества от состояния обеспечения безопасности информационных ресурсов.

Рост объема информационных ресурсов за последнее десятилетие и интенсивное развитие информационных технологий закономерно влекут за собой повышение опасности угроз безопасности информации, связанных с деятельностью иностранных спецслужб, преступных сообществ и отдельных лиц в сферах государственного управления, банковской деятельности, функционирования критически важных систем информационной инфраструктуры и в других сферах.

В этой связи, одним из основных направлений деятельности в области укрепления информационной безопасности государств является решение задач по предупреждению и нейтрализации угроз безопасности информации.

Для совершенствования единого научно-технического обеспечения защиты общих информационных ресурсов Беларуси и России, Союзным государством более 10 лет осуществляется деятельность по реализации программ и других мероприятий по укреплению информационной безопасности участников Союзного государства.

Общие информационные ресурсы Беларуси и России содержат информационные системы, обеспечивающие деятельность Союзного государства в военно-техническом сотрудничестве и обороне, таможенном и экспортном контроле, эксплуатации топливно-энергетического комплекса, взаимодействия правоохранительных органов и в других областях.

Важной частью общих информационных ресурсов является информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну Российской Федерации или государственные секреты Республики Беларусь, которая включает в себя сведения, составляющие коммерческую, служебную и иные виды тайн.

Значительную долю общих информационных ресурсов Беларуси и России составляют критически важные системы информационной инфраструктуры, обеспечивающие функционирование жизненно важных элементов инфраструктуры Союзного государства. В ходе совместной деятельности Республики Беларусь и Российской Федерации может функционировать более 20 таких систем, к числу которых относятся: системы управления движением железнодорожного транспорта, географические и навигационные системы, финансово-кредитные и другие системы.

Деструктивные информационные воздействия на критически важные системы информационной инфраструктуры могут привести к значительному экономическому ущербу и другим негативным последствиям в различных сферах жизнедеятельности Союзного государства (нарушению функционирования систем государственного управления, систем управления жизнеобеспечением городов и населенных пунктов, систем управления движением транспорта, систем управления потенциально опасными объектами).

Для решения проблем защиты общих информационных ресурсов в период с 2000 по 2010 годы были выполнены программы «Защита общих информационных ресурсов Беларуси и России» и «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006 2010 годы». В результате выполнения указанных программ были разработаны:

- основы единой научно-технической политики по защите общих информационных ресурсов Беларуси и России;
- единая российско-белорусская система документов, регламентирующих деятельность по обеспечению защиты общих информационных ресурсов Беларуси и России от информационных угроз;
- информационно-техническая система защиты общих информационных ресурсов Беларуси и России от информационных угроз;
- система документов, регламентирующих деятельность по обеспечению безопасности информации на критически важных объектах информационно-телекоммуникационной инфраструктуры и контроля эффективности этих мероприятий;
- информационно-техническая система контроля безопасности информации на критически важных объектах информационно-телекоммуникационной инфраструктуры;
- перспективные технологии защиты общих информационных ресурсов Беларуси и России: от утечки по техническим каналам; от несанкционированного доступа; от компьютерных атак и вирусов на основе криптографических методов;
- аппаратные, программные и программно-аппаратные средства,

обеспечивающие эффективное решение отдельных задач защиты информации;

- единые образовательные стандарты в области защиты информации.

Полученные в период с 2000 по 2010 годы результаты позволили создать базовые условия для формирования и совершенствования системы защиты общих информационных ресурсов Беларуси и России; предотвращения ущерба от реализации информационных угроз; производства конкурентоспособных средств защиты информации.

Наиболее важное значение для защиты общих информационных ресурсов имеют проведенные исследования по организации мониторинга состояния обеспечения безопасности на критически важных трансграничных системах информационно-телекоммуникационной инфраструктуры Союзного государства, проведению контроля на критически важных объектах, по информационному обмену между национальными органами контроля; создание опытного образца 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; разработка специального программного обеспечения контроля эффективности защиты распределенных информационных ресурсов от воздействия компьютерных атак.

Был получен ценный опыт решения задач по защите информации, сформированный с участием более 30 научно-исследовательских организаций Республики Беларусь и Российской Федерации.

В настоящее время совершенствование единого научно-технического обеспечения защиты общих информационных ресурсов Беларуси и России осуществляется путем реализации программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011-2015 годы.

В ходе реализации программы решаются задачи по разработке на основе высоких технологий необходимых научно-технических решений для реализации мер по предупреждению и нейтрализации угроз безопасности информации в критически важных системах информационной инфраструктуры и создания на основе высоких технологий необходимых научно-технических и нормативно-методических условий для реализации мер по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты), при использовании высоких технологий её обработки.

Для решения этих задач выполняется комплекс научно-исследовательских и опытно-конструкторских работ, включающий: анализ и оценку защищенности типовых критически важных систем информационной инфраструктуры от угроз безопасности информации; разработку с использованием высоких технологий методов и средств оценки защищенности критически важных систем информационной инфраструктуры от угроз безопасности информации; разработку методов и средств тестирования локальных компьютерных сетей критически важных систем информационной инфраструктуры с целью выявления скрытых каналов передачи данных; анализ состояния и перспектив развития информационных технологий, оценку уровня защищенности информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты), от угроз безопасности информации; разработку перспективных способов и средств защиты информации при реализации наукоёмких технологий обработки информации, создании доверенных сред при распределённой обработке информации с использованием информационно-телекоммуникационной среды общего пользования; разработку эффективных способов и систем аутентификации и разграничения доступа. Кроме того, программой предусмотрено решение задач по формированию межгосударственной системы стандартов в области защиты общих информационных ресурсов; обоснования и разработки основных направлений дальнейших исследований по совершенствованию системы защиты общих информационных ресурсов Беларуси и России.

В ходе выполнения программы Союзному государству будут предоставлены механизмы, разработанные на принципиально новых и высокоэффективных технических и организационных решениях, позволяющие осуществлять эффективное нормативно-правовое и организационное регулирование деятельности государственных субъектов Беларуси и России в области защиты информации; будут разработаны направления и способы обеспечения безопасного функционирования критически важных систем информационной инфраструктуры и объектов информатизации органов государственного управления Союзного государства; будут сохранены достигнутые в ходе совместной работы и получат дальнейшее развитие научно-технический и технологический потенциалы Беларуси и России в сфере обеспечения безопасности информации.

Реализация программы ведется по следующим направлениям:

- разработка системы взглядов на обеспечение защиты информации в распределённых информационно-вычислительных системах на основе Grid-технологий и сетей связи общего пользования, макетов информационно-вычислительных комплексов (систем) на основе Grid-технологий и требования по защите информации при реализации наукоёмких технологий её обработки;

- разработка рекомендаций по созданию доверенных сред при распределённой обработке информации с использованием информационно-телекоммуникационной среды общего пользования;

- создание макетов (опытных образцов) перспективных средств высоконадежной аутентификации и разграничения доступа;

- разработка методического и программного обеспечения мероприятий по контролю защищенности информации в критически важных системах информационной инфраструктуры от деструктивных информационных воздействий, методы и средства тестирования локальных вычислительных сетей указанных систем с целью выявления скрытых каналов утечки информации;

- разработка алгоритмического и программного обеспечения инфраструктуры открытых ключей на информационном пространстве Союзного государства;

- разработка методического документа в области защиты информации ограниченного доступа, не составляющей государственную тайну (государственные секреты), и требований к средствам защиты информации;

Продолжение на стр. 9 →

Создание систем защиты информации – задача для системного интегратора

Барановский Олег Константинович, заместитель начальника по науке центра испытаний средств защиты информации и аттестации объектов информатизации Государственного предприятия «НИИ ТЗИ»

Справка ТБ

Образование высшее, радиофизик, в 1998 г. закончил Белорусский Государственный Университет. Имеет академическую степень магистра естественных наук, кандидат физико-математических наук. Опыт работы в области защиты информации с 1998 года по настоящее время.

Согласно Стратегии развития информационного общества в Республике Беларусь, утвержденной постановлением Совета Министров Республики Беларусь от 9 августа 2010 г. № 1174, до 2015 г. планируется завершить работу по формированию базовых компонентов национальной информационно-коммуникационной инфраструктуры:

– общегосударственная автоматизированная информационная система, интегрирующая государственные информационные ресурсы в целях предоставления электронных услуг;

– государственная система управления открытыми ключами;

– система идентификации физических и юридических лиц;

– система формирования и хранения государственных информационных ресурсов, используемых при оказании электронных услуг, включая регистр населения, на основе которого создается единая система идентификации граждан;

– платежный шлюз в интеграции с единым расчетным информационным пространством, посредством которого будут осуществляться платежные трансакции через портал общегосударственной автоматизированной информационной системы;

– единая защищенная среда информационного взаимодействия республиканских органов государственного управления.

Стоит упомянуть, что согласно Указу Президента Республики Беларусь от 4 апреля 2013 года № 157 «О внесении изменений и дополнений в некоторые указы Президента Республики Беларусь», до 1 января 2015 г. внедрение систем электронного документооборота поручено государственным органам и иным государственным организациям, подчиненным (подотчетным) президенту, Совету Республики и Палате представителей, Конституционному, Верховному и Высшему Хозяйственному Судам, Комитету госконтроля, Генпрокуратуре, Аппарату Совета Министров, республиканским органам государственного правления и иным государственным организациям, подчиненным правительству, областным и Минскому горисполкомам, а до 1 января 2016 г. – государственным органам и организациям, хозяйственным обществам, в отношении которых Республика Беларусь либо административно-территориальная единица, обладая акциями (долями в уставных фондах), может определять решения, принимаемые этими хозяйственными обществами.

При этом важнейшим из факторов успеха реализации Стратегии является укрепление доверия и безопасности используемых информационно-коммуникационных технологий. Достигнуть успеха в столь короткие сроки в условиях необходимости снижения затрат на приобретение (разработку, модернизацию) средств и систем информатизации можно только с применением единых, апробированных практикой подходов и методов в области обеспечения информационной безопасности.

В связи с этим, в настоящее время стоит задача технического обеспечения (перевооружения) субъектов информационных отношений для подключения к создаваемым интегрирующим системам. Кроме того, создание (модернизация) систем защиты информации владельцами отдельных информационных систем, систем электронного документооборота и других систем, включаемых в единую защищенную среду, является обязательным элементом обеспечения информационной безопасности республики в целом.

В настоящее время при создании систем защиты информации руководствуются постановлением Совета Министров Республики Беларусь от 26 мая 2009 г. № 675 «О некоторых вопросах защиты информации». Владелец создаваемой (модернизируемой) системы вправе выбирать правовые, организационные или технические меры для обеспечения защиты информации. Однако Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, который вступает в силу через шесть месяцев после его официального опубликования, четко регламентируются условия выбора мер технической и (или) криптографической защиты информации в зависимости от типа объекта защиты и вида угроз.

Оказание услуг по проектированию и разработке систем защиты информации в Республике Беларусь является лицензируемым видом деятельности. И это правильно для информационных систем с государственной формой собственности, а также обрабатывающих информацию, распространение и (или) предоставление которой ограничивается государством. На рынке республики в данном секторе работает ряд компаний и организаций. Однако лицензиатов, предлагающих весь спектр работ от аудита информационной безопасности и разработки требований защиты информации до выдачи аттестата соответствия на систему защиты информации, можно пересчитать по пальцам, а имеющих опыт работы с органами

государственного управления – единицы.

Для получения положительного результата системный интегратор уже на стадии обследования обязан привлекать специалистов, которые будут проводить мероприятия по аттестации системы защиты информации. Все еще существует практика, когда за создание системы защиты информации берется компания, не имеющая лицензии на оказание услуг по аттестации систем защиты информации, а для выполнения этих работ привлекает на конечном этапе другую организацию. В связи с отсутствием опыта у первой, аттестующей организации, приходится перерабатывать документацию на создаваемую систему защиты для приведения ее в соответствие с законодательством Республики Беларусь. В конечном счете, комплексное решение по защите информации часто экономически неэффективно.

Для выполнения работ по созданию (модернизации) систем защиты информации необходимо привлекать зарекомендовавших себя лицензиатов.

Как правило, работы по созданию (модернизации) систем защиты информации включают следующие этапы:

– комплексное обследование (аудит) информационной безопасности организации и защищаемой системы;

– разработка (пересмотр) политики информационной безопасности организации;

– техническое проектирование системы защиты информации;

– разработка (корректировка) нормативной, организационно-распорядительной и эксплуатационной документации, документации для аттестации системы защиты информации;

– реализация предложенных технических решений, внедрение организационных мер;

– аттестация системы защиты информации.

Для оптимизации предлагаемых решений каждый этап должен проводиться при непосредственном участии заказчика. В рамках комплексного обследования (аудита) информационной безопасности совместно выполняются следующие работы:

– анализ структуры, состава, принципов функционирования информационной системы и существующей системы защиты информации (при наличии);

– категорирование ресурсов (технические, программные, аппаратно-программные средства, обрабатываемая информация);

– анализ имеющихся нормативных и организационно-распорядительных документов по эксплуатации информационной системы и системы защиты информации.

Результаты комплексного обследования (аудита) позволяют выработать основные принципы управления информационной безопасностью организации.

Далее на основе выработанных положений политики информационной безопасности и требований нормативных правовых актов, в том числе технических нормативных правовых актов Республики Беларусь, разрабатываются решения по системе защите информации в форме технического проекта.

Реализация предложенных технических решений, внедрение организационных мер включает также:

– разработка и оформление технической документации на поставку средств защиты информации для комплектования системы защиты информации (технических, программных, аппаратно-программных средств);

– поставка и испытания (сертификационные, в рамках государственной экспертизы) средств защиты информации.

Типовой комплект документации, предоставляемый заказчику по окончании аттестации системы защиты информации, в соответствии с нормативными правовыми актами Республики Беларусь включает:

– техническое задание на создание (модернизацию) системы защиты информации (при необходимости);

– политика информационной безопасности организации;

– технический проект (пояснительная записка, содержащая сравнительный анализ и обоснование выбора основных решений по защите информации, спецификация средств защиты информации);

– задание по безопасности и протокол его оценки;

– рабочая документация;

– документация для аттестации;

– эксплуатационная документация, нормативная, организационно-распорядительная документация;

– протоколы и акты приемочных и аттестационных испытаний;

– сертификаты или экспертные заключения на средства защиты информации;

– аттестат соответствия.

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации» имеет большой опыт работы в части создания и аттестации систем защиты информации государственных информационных систем, а также информационных систем, обрабатывающих информацию, распространение и (или) предоставление которой ограничено. Предприятие, как системный интегратор, специализируется на выполнении полного спектра работ по созданию защищенных информационных систем в интересах министерств, ведомств и организаций Республики Беларусь.

Предприятие имеет специальные разрешения (лицензии) Оперативно-аналитического центра при Президенте Республики Беларусь, Комитета государственной безопасности, Министерства внутренних дел, Государственного военно-промышленного комитета, Министерства юстиции на право осуществления целого ряда направлений деятельности в области технической защиты информации. На государственном предприятии «НИИ ТЗИ» разработана, внедрена и эффективно функционирует система менеджмента качества в соответствии с требованиями стандарта СТБ ISO 9001-2009, подтвержденная в Национальной системе соответствия сертификатом. Качество работ обеспечивается за счет строгого соблюдения требований технических нормативных правовых актов и методических документов республики и предприятия.

За последние годы государственным предприятием «НИИ ТЗИ» выполнен ряд работ для таких государственных органов, как: Государственный секретариат Совета безопасности Республики Беларусь, Администрация Президента Республики Беларусь, Оперативно-аналитический центр при Президенте Республики Беларусь, Комитет государственной безопасности, Следственный комитет, Министерство обороны, Государственный пограничный комитет, Министерство внутренних дел, Министерство финансов, Департамент финансовых расследований Комитета государственного контроля Республики Беларусь и др. ■

О кадровых аспектах обеспечения качества управления АЭС

Крюкова Эмма Петровна,
ведущий научный сотрудник НИИ ТЗИ, к.т.н.

В 1996 году МАГАТЭ разработало серию стандартов и руководств Q1–Q14, посвященных обеспечению качества АЭС. Документы устанавливали десять основных требований по разработке и выполнению всесторонней программы обеспечения качества в ходе определения местоположения, проектирования, создания, эксплуатации и вывода из эксплуатации оборудования, связанных с безопасностью АЭС. Они отражали опыт промышленности и текущее понимание требований обеспечения качества, необходимые для достижения безопасного, надежного и эффективного использования ядерной энергии, управления и обработки радиоактивных материалов [1].

Основные требования документов представлены в трех функциональных категориях «управление-эффективность-оценка». Цель требований безопасности состояла в том, чтобы обеспечить требования и правила по реализации эффективной системы управления, которая:

– интегрирует все аспекты управления ядерными установками и мероприятиями, включая безопасность, здоровье, экологию, охрану, качественные и экономические требования взаимосвязанным образом;

– обеспечивает непрерывное совершенствование;

– описывает планируемые и систематические мероприятия, необходимые для обеспечения соответствующей уверенности в том, что все эти требования могут быть удовлетворены;

– поддерживает рост и совершенствование культуры организации и культуры безопасности.

Положения, касающиеся таких вопросов, как ревизия и подготовка персонала, в этой редакции были расширены для придания им всеобъемлющего характера и обеспечения большей четкости в их применении. В документе и связанных с ним руководствах по безопасности, касающихся обеспечения качества, подчеркивается, что руководители, непосредственные исполнители и контролеры, оценивающие работу, – все вносят свой вклад в обеспечение качества и безопасности АЭС. Основанный на адекватности выполняемой работы подход к обеспечению качества способствует изменению распространенного ошибочного представления о том, что обеспечение качества состоит только в выполнении формальных требований.

МАГАТЭ провело сравнение требований ИСО 9001:2000 с требованиями стандарта 50-C/SG-Q. Сравнение показало, что документы МАГАТЭ используют подход «сверху-вниз», который сосредотачивается на том, чтобы соответствовать полностью требованиям безопасности АЭС, персонала и общества в целом. В стандарте ИСО 9001 используется подход «снизу-вверх», который сосредотачивается на удовлетворении определенных требований непосредственного потребителя.

Сравнение показало, что цели документов различны, хотя их нельзя назвать несовместимыми. Требования стандарта ИСО 9001 отличаются в таких разделах, как программа обеспечения качества, обучение и квалификация персонала, проектирование и независимая проверка правильности проектных решений, независимость инспекций и испытаний [2].

МАГАТЭ пришло к выводу о необходимости дополнения требований ИСО 9001 для применения в рамках атомного надзора. В связи с этим возникла необходимость разработки соответствующих национальных стандартов. Первые стандарты такого рода были разработаны ранее ASME (американским Обществом инженеров-механиков) [3].

Стандарты ASME устанавливают требования и рекомендации для разработки и выполнения программы обеспечения качества на всех этапах жизненного цикла оборудования АЭС. Они отражают опыт промышленности и текущее понимание требований по обеспечению качества, необходимые для достижения безопасного, надежного и эффективного использования ядерной энергии, управления и обработки радиоактивных материалов.

Стандарты, сосредотачиваясь на достижении результатов, подчеркивают роль человека и управления производством в достижении качества, и способствуют приложению этих требований способом, совместимым с относительной важностью элемента или мероприятия.

В соответствии с идеологией NQA-1, для достижения нужного качества нужно определить необходимую работу, выполнить ее правильно с первого раза, соблюсти все имеющие силу требования, удовлетворить требования потребителей. При этом:

– персонал должен сам выявлять проблемы с качеством;

– проблемы требуют немедленных корректирующих действий или принятия быстрых временных компенсирующих мер (коррекция);

– выясняются и корректируются как случайные причины, так и общие (системные);

– контролируется эффективность корректирующих действий;

– недостатки самооценки рассматриваются как проблема качества.

Одним из важнейших критериев обеспечения качества АЭС является квалификация ее персонала, а важным критерием отбора персонала является отношение каждого его члена к безопасности (культура безопасности).

Комиссией по ядерной безопасности Канады (NSCA), в соответствии с «Законом о Ядерной безопасности и управлении» и инструкциями к нему, разработан Руководящий документ, определяющий требования к сертификации персонала, работающего на канадских АЭС в должностях (ролях), от которых напрямую зависит ядерная безопасность. Документ определяет требования, которым должны соответствовать специалисты, работающие или стремящиеся работать в различных должностях на ядерных предприятиях, и для которых необхо-

дим сертификат Канадской Комиссии по Ядерной безопасности (CNSC). Он также определяет требования к программам и процессам, поддерживающим сертификацию работающих, которые должны быть реализованы лицензиатом АЭС для обучения и проверки людей, являющихся соискателями или держателями сертификата CNSC.

В соответствии с принципами CNSC и международной практикой, за безопасную работу АЭС несут ответственность, в первую очередь, лица, имеющие лицензию на право эксплуатации АЭС. Следовательно, лицензиаты АЭС считаются полностью ответственными за обучение и тестирование своих работающих, обеспечивая гарантии, что они полностью квалифицированы для выполнения обязанностей в соответствии со своей ролью и современными нормативными требованиями.

CNSC требует гарантию, что каждый специалист, которого она сертифицирует, компетентен для выполнения обязанностей в соответствии с применяемой ролью. Этому служит режим контроля со стороны регулятора за программами и сертификационными экзаменами, основанными на комбинации соответствующих руководств регулятора и мероприятий по обеспечению соответствия.

В первую очередь, лицензиат АЭС должен установить и документально оформить эти требования для обучения и оценки квалификации лиц – соискателей сертификата на следующие должности на АЭС [4]:

– главный дозиметрист;
– оператор реактора;
– оператор нулевого модуля;
– начальник смены щита управления;
– начальник смены установки.

Современная система подготовки кадров для атомной энергетики базируется на принципах допуска к самостоятельной работе по управлению АЭС (управленческий и инженерный персонал) и к эксплуатации и ремонту оборудования (оперативный и ремонтный персонал) только подготовленного и аттестованного персонала.

Мировой опыт эксплуатации АЭС в условиях применения современных компьютерных технологий показывает, что недостатки в управлении безопасностью и многочисленные ошибки человека могут привести к событиям с существенными последствиями. Основные недостатки в действиях человека и управлении безопасностью можно описать через следующие события:

– недостаточное взаимодействие и усиление роли и обязанностей;
– отсутствие адекватной жесткой верификации;
– недостаточный анализ изменяющихся условий для тестирования;
– недостатки в планировании работ и управлении человеческими ресурсами;
– самоуспокоенность и самонадеянность в процессах верификации на всех стадиях подготовки и исполнения;
– недостаточная технологическая подготовка, недостатки в предпусковом инструктаже и оценке после проведения операции;
– многочисленные нарушения рабочих инструкций и процедур;
– недостатки в проектах и эксплуатационной документации.

Наиболее существенные корректирующие действия по повышению безопасности АЭС требуют четкого соотношения ролей и обязанностей, а также повышения внимания работающих и руководства к основным правилам эксплуатации и безопасности в ходе работ по обслуживанию. В последние годы, из-за изменений в деловой среде, управление и организационный фактор становятся более важными, оказывая влияние на эффективность работы отдельного человека. Изменения в управлении в организации могут оказать существенное влияние на ядерную безопасность.

Культура безопасности и опыт управления безопасностью являются спе-

---

← *Начало на стр. 5*

Защита информации – важнейшая составляющая безопасности Союзного государства

- разработка номенклатуры первоочередных межгосударственных стандартов в области защиты общих информационных ресурсов Беларуси и России.

Наиболее значимыми разработками текущей программы планируются создание современного высокоскоростного устройства криптографической защиты информационного обмена в вычислительных сетях; разработка программно-аппаратных комплексов доверенных центров обеспечения электронного документооборота и межгосударственной системы управления открытыми ключами.

Важнейшим мероприятием по совершенствованию единого научно-технического обеспечения защиты общих информационных ресурсов Беларуси и России является ежегодно проводимая научно-практическая конференция «Комплексная защита информации». В ходе конференции рассматриваются актуальные вопросы безопасности информационного пространства Союзного государства. Конференция поочередно проводится в Беларуси и России и является одним из мероприятий, поддерживаемых структурами Союзного государства, на котором освещается официальная политика двух государств по обеспечению их информационной безопасности. Очередная XVIII научно-практическая конференция «Комплексная защита информации» состоится 21-24 мая 2013 года в г. Бресте.

В работе конференции принимают участие передовые ученые, высококвалифицированные специалисты, представители ведущих организаций, осуществляющих деятельность в области защиты информации.

В ходе XVIII конференции будут рассмотрены актуальные вопросы безопасности информационного пространства Союзного государства. Планируется работа секций и круглых столов по следующим направлениям:

вопросы создания защищенных объектов информационных технологий; техническая защита информации; нормативно-правовые аспекты обеспечения информационной безопасности; государственные системы управления открытыми ключами; государственные системы идентификации и аутентификации; математика и безопасность информационных технологий; подготовка специалистов в области информационной безопасности.

Таким образом, проблема обеспечения безопасности информации в критически важных системах информационной инфраструктуры Союзного государства и совместный поиск эффективных решений по их защите осуществляется в ходе реализации программ Союзного государства. На ежегодно проводимых научно-практических конференциях производится выработка общих подходов к решению проблем защиты информации, участие в конференции ведущих ученых и специалистов стран участников Союзного государства позволяет прогнозировать и решать возникающие угрозы безопасности информации на уровне мировых тенденций развития технологий. ■

циальными атрибутами, которые необходимо принимать во внимание в процессе отбора и назначения персонала АЭС. При этом требования к опыту в различных странах разные: количество лет не столь важно, как качество опыта, компетентность организации, где был получен этот опыт или уровень ответственности, которым был наделен работник в период приобретения надлежащего опыта.

Одной из конкретных позиций, которые необходимо учитывать при отборе персонала на должности, связанные с безопасностью АЭС, помимо выполнения квалификационных требований и прохождения подготовки, являются психологические черты: навыки управления стрессом, способность распознавать отклонения в поведении коллег и подчиненных, самоконтроль, интуиция, положительные личные черты, необходимые для работы в коллективе и в стрессовых ситуациях [5].

Обеспечение безопасности АЭС, связанное с использованием компьютерной техники и противодействием кибернетическим угрозам, требует новых подходов к подготовке персонала, ответственного за функционирование компьютерных систем контроля и управления, относящихся к безопасности АЭС, и четкому распределению обязанностей каждого специалиста в этой области.

Общие цели предложенной в 2011 году МАГАТЭ Программы координированных исследований состоят в том, чтобы усилить возможности государств-членов МАГАТЭ в области оптимизации производительности и срока службы атомных электростанций посредством лучшего понимания технологий и управления в области кибернетической безопасности. Она включает создание соответствующих мер против умышленных актов, направленных против компьютерных систем контроля и управления АЭС. При этом отмечается, что решения, которые признаются хорошими для IT-систем, не всегда применимы к цифровым системам АЭС [6].

Для проведения системного анализа, инсталляции, модификации, обслуживания, контроля и/или интеграции компьютерных операционных систем, приложений, сетей и баз данных в технологические процессы АЭС, должна быть создана рабочая группа специалистов в области информационных технологий. Должности участников группы ранжируются от уровня исполнителей до уровня директора и охватывают несколько функциональных областей, включая программирование/анализ приложений, проектирование систем, анализ/проектирование сетей, анализ информационных технологий, специализированное оборудование и приложения, базы данных и безопасность.

Роли в этой рабочей группе включают следующие профессиональные классификации [7]:

– руководители компьютерных и информационных систем;

– специалисты по прикладному программному обеспечению компьютеров;

– специалисты по системному программному обеспечению компьютеров;

– программисты;

– специалисты по техническому обслуживанию компьютеров;

– специалисты по анализу компьютерных систем;

– администраторы баз данных;

– администраторы сети и компьютерных систем;

– специалисты по анализу сетевых систем и передаче данных.

В соответствии с требованиями МАГАТЭ, программа обеспечения качества АЭС должна включать формальные процедуры и правила определения требований к квалификации исполнителя любого задания, которое может потенциально повлиять на качество функционирования или безопасность оборудования АЭС. Эти требования включают необходимые знания, полученные через образование, программы начального и непрерывного обучения, записи о квалификации.

Анализ мирового опыта показал, что в качестве эксплуатирующего персонала на АЭС, как правило, работают сотрудники, имеющие высшее (бакалавр, магистр), среднее и среднее специальное образование. Необходимый опыт работы колеблется от одного до 10 лет, в зависимости от должности [8].

Персонал, обеспечивающий безопасность АЭС, фактически во всех странах с первых шагов проходит обучение практическим мерам управления безопасностью АЭС, и продолжает обучение, причем более 90 % обучаются на специальных имитаторах оборудования, моделирующих управление в критических ситуациях. Для новых предприятий доступен специальный имитатор щита, моделирующий всю область управления реактором даже на шаге ввода АЭС в действие. В работу стенда при обучении включаются и операции на щитах и вне щита управления (например, дистанционные пульты отключения, аварийные дизельные генераторы).

При оценке профессиональной компетентности персонала АЭС, от каждого требуются особо четкие знания инструкций и грамотных реакций человека на нештатные ситуации, что следует учитывать как положительное влияние действий человека на обеспечение безопасности АЭС. Будучи звеном компьютерной системы, оператор может стать преградой, предотвращающей отказ системы или ее компрометацию, что еще раз говорит о необходимости обеспечения его подготовленности и наличия практического опыта для работы с такими системами.

Ключевым пунктом программы обеспечения качества является компетентность персонала, работающего по контрактам, которая должна быть оценена через проверку существующей или запрашиваемой документации и отчетов, таких как: сертификаты, дипломы, отчеты о работе, краткие биографии, результаты оценок, отчеты об аналогичных работах, выполненных на другой АЭС и т.д.

Персонал подрядчиков категорируется следующим образом [9]:

– **персонал, работающий вне АЭС:** обычно результат работы – поставляемая услуга. В этом случае метод подтверждения компетентности является косвенным, через обеспечение качества (к такому персоналу относятся инженеры по сервисам, преподаватели и др.);

– **персонал, работающий на АЭС:** выполняет работу по техническому обслуживанию, по техническому контролю в процессе эксплуатации и др.;

– **персонал, работающий постоянно (больше года):** обычно обслуживает конкретные технологические позиции на АЭС (специалисты по техническому обслуживанию, охране, персонал столовых на территории предприятия и административно-хозяйственного отдела);

– **персонал, работающий кратковременно:** работает на АЭС в течение короткого периода времени при отключениях, возможно, в большинстве случаев без сопровождения, но не только (специалисты по перезагрузке топлива в атомном реакторе, по дозиметрии, разработке модификаций и др.);

– **инспекторы:** выполняет кратковременные задачи, без существенного риска и под непосредственным контролем (внешние аудиторы, административный персонал и т.д.);

– **сертифицированные специалисты:** специалисты, для которых необходимо официальное признание компетентности, позволяющей выполнить работу, обычно из местных органов власти или других официальных органов (инспекторы по сварке, неразрушающему контролю и др.);

– **персонал, подверженный радиации:** технический персонал по дозиметрии, инспекторы паровых генераторов и первичного цикла и др.

Принципы подтверждения компетентности персонала АЭС, работающего по контрактам, должны исходить из общей политики обеспечения качества и безопасности АЭС и из нормативных требований. Основной принцип обеспечения компетентности персонала, работающего по контракту – специалисты должны быть соответствующим образом оценены прежде, чем выполнить работу. Соответственно, компетентность персонала, работающего по контракту, должна быть формально оценена и зарегистрирована.

Конечная ответственность за обеспечение качества всех работ, выполняемых на АЭС, остается за эксплуатирующей организацией АЭС.

Выполнение определенных видов работ по контрактам осуществляется работниками (персоналом) эксплуатирующих организаций и организаций, выполняющих работы и (или) оказывающих услуги при осуществлении деятельности по использованию атомной энергии, при наличии у этих работников (персонала) разрешений на право ведения работ, выдаваемых уполномоченным государственным органом по регулированию безопасности при использовании атомной энергии [10].

Законодательство Российской Федерации предполагает как обязательную сертификацию (связанную с безопасностью жизни и охраной здоровья), так и добровольную сертификацию персонала [11].

При подборе персонала для Белорусской АЭС необходимо учесть мировой опыт организационного управления безопасностью АЭС. Для работы на ключевых должностях Белорусской АЭС планируется привлечь около 70 зарубежных специалистов, обладающих опытом работы на АЭС. В соответствии с генеральным контрактом на строительство АЭС в Беларуси, подготовка эксплуатационного персонала АЭС будет осуществляться российской стороной, и проводиться как в Беларуси, так и на строящихся и действующих АЭС в России [12].

Предполагается, что состав персонала для белорусской АЭС будет назначаться, исходя из структуры, установленной нормативными документами России. К персоналу, обеспечивающему нормальную эксплуатацию оборудования, систем и сооружений АЭС относятся [13]:

– работники по обеспечению: ядерной безопасности, радиационной безопасности пожарной безопасности, общей техники безопасности, всех вспомогательных технических услуг, нормальной работы систем теплоснабжения и подземных коммуникаций, нормальной работы систем вентиляции и кондиционирования, азотом, кислородом, гелием, сухим и влажным воздухом различных давлений;

– работники технической инспекции, по анализу надежности работы оборудования АЭС, режима и охраны, по подготовке кадров, по обращению с топливом и его хранению, по обращению с твердыми, жидкими и газообразными отходами, осуществляющие химический и радиохимический контроль, осуществляющие наблюдение за гидротехническими и другими сооружениями, а также зданиями, осуществляющие наладку и испытания оборудования атомной станции, по проведению периодической дезактивации оборудования и производственных помещений атомной станции, осуществляющие ведомственную поверку средств измерений.

Единый квалификационный справочник (ЕКС) должностей руководителей, специалистов и служащих России в общем виде описывает обязанности персонала АЭС, полномочия которого касаются использования средств автоматизации [14].

Содержание их должностных обязанностей приведено в таблице 1 (выдержки, касающиеся собственно профессиональных обязанностей). Анализ таблицы показывает, что в должностных обязанностях недостаточно четко прописывается иерархия ролей, профили ролей во многом перекрываются, что не позволяет четко разграничить ответственность каждого за безопасность компьютерных систем АЭС, важных для безопасности.

Ежегодно четыре белорусских вуза – БГУ, БНТУ, БГУИР и Международный государственный экологический университет имени А.Д. Сахарова – будут готовить около 220 специалистов в области ядерной энергетики – по управлению АЭС (управление и инженерный персонал), эксплуатации и ремонту оборудования (оперативные и ремонтные рабочие). Министерство образования планирует обеспечить системный подход к подготовке персонала. Министерство основывается на документах Международного агентства по атомной энергии (МАГАТЭ) и лучшей международной практике.

В стране будет налажена непрерывная и гибкая система подготовки персонала АЭС, сотрудников в соответствии с этапами ее строительства, пуска в эксплуатацию и дальнейшей эксплуатации. Схема подготовки кадров – профотбор, базовая подготовка (5-5,5 года) в отечественных вузах, специальная подготовка (0,5-3 года) за рубежом. Будет создан учебно-тренировочный центр АЭС [15].

При подготовке кадров должны учитываться требования МАГАТЭ к персоналу АЭС, а также использование национального и мирового опыта подготовки персонала для критически важных приложений, что уже находит отражение в создании национальных технических нормативных актов на основе руководств и стандартов МАГАТЭ и МЭК.

Опыт подбора и управления персоналом при решении задач обеспечения безопасности в области атомной энергетики целесообразно распространить на другие критически важные инфраструктуры. ■

Литература

1. IAEA, Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations, Code and Safety Guides, Safety Series No. 50-C/SGQ, IAEA, Vienna, Austria (1996);

2. Quality Standards. Safety Reports Series 22: Comparison between IAEA 50-C/SG-Q and ISO 9001;

3. Quality Assurance Program Requirements for Nuclear Facilities/with Addenda. NQA-1 – 1994;

4. Canadian Nuclear Safety Commission (CNSC) RD-204: Certification of Persons Working at Nuclear Power Plants 2012;

5. Набор, квалификация и подготовка персонала для атомных станций. МАГАТЭ. Серия норма безопасности. Руководство NS-G-2.8.Вена, 2005;

6. IAEA.Coordinated Research Programme (CRP), 2011;

7. Transitional Document – Career Group Description Occupational Family: Engineering and Technology Career Group: Information Technology Specialists. Statistical Reporting Canada;

8. "Кадровик. Кадровый менеджмент", 2009, N12. Подготовка кадров для эффективной работы АЭС;

9. IAEA TECDOC-1232 *Assuring the competence of nuclear power plant contractor personnel*. 2001;

10. Закон Республики Беларусь от 30 июля 2008 г. №426-з «Об использовании атомной энергии»;

11. Федеральный закон N184-ФЗ «О техническом регулировании», 2002;

12. http://www.belta.by/ru/all_news/economics/Belorusskuju-AES-budut-sovmestno-obsluzhivat-belorusskie-i-inostrannye-spetsialisty_i_628412.html;

13. Основные положения по подбору, подготовке, допуску к работе и контролю в процессе эксплуатации персонала атомных станций (ОПКП АЭС -90), Москва, 2000;

14. Министерство здравоохранения и социального развития Российской Федерации. Приказ от 3 октября 2005 г. №614 «Об утверждении тарифно-квалификационных характеристик профессий рабочих атомных электростанций. Приложение к Приказу Министерства здравоохранения и социального развития Российской Федерации от 10 декабря 2009 г. N977. Единый квалификационный справочник должностей руководителей, специалистов и служащих. Раздел «Квалификационные характеристики должностей работников организаций атомной энергетики»;

15 http://www.nestor.minsk.by/sn/2008/35/sn83504.html .

Таблица 1 Должностные обязанности персонала АЭС, полномочия которого касаются использования средств автоматизации	
Должность	Основные обязанности (выдержки)
Главный инженер АЭС	Является главным техническим руководителем на АЭС и несет ответственность за: – организацию работ по обеспечению ядерной безопасности; – общий технический уровень эксплуатации станции; – подготовку эксплуатационного персонала атомной станции. Эти обязанности расписываются далее по соответствующим специалистам и носят организационный характер.
Главный специалист АЭС	Определяет единую для атомной станции техническую политику по обеспечению экономичной, надежной и безопасной работы оборудования.
Главный приборист	Устройство и правила эксплуатации средств измерений и организации их ремонта; методы проведения исследований и разработок в области совершенствования метрологического обеспечения и средств измерений; отечественный и зарубежный опыт в области метрологического обеспечения производства.
Главный технолог АЭС	
Мастер по ремонту оборудования начальник группы (бюро), лаборатории …	Организует применение электронно-вычислительной техники, других средств автоматизации процессов исследований и разработок, выполняемых группой (бюро), лабораторией.
Начальник отдела АСУТП	После внедрения автоматизированной системы обеспечивает ее бесперебойное функционирование и принимает оперативные меры по устранению возникающих в процессе работы нарушений. Проводит работу по анализу отказов систем, разрабатывает мероприятия по повышению качества и надежности автоматизированных систем, расширению сферы применения, модернизации применяемых технических средств и программного обеспечения.
Начальник исследовательской группы	Организует применение электронно-вычислительной техники, других средств автоматизации процессов исследований и разработок, выполняемых группой (бюро), лабораторией. Организует применение электронно-вычислительной техники при проведении исследований и обработке результатов испытаний, разработку новых программ расчета.
Начальник НИО по комплексной защите информации	Проводит изучение и анализ технических средств, применяемых для получения информации, с учетом профиля работ организации и особенностей его дислокации.
Начальник НТО по комплексной защите информации	Организует рассмотрение проектов приказов и указаний по организации, стандартов организации, инструкций по комплексной защите информации, соответствующих разделов технологической и отчетной документации с целью оценки полноты предусмотренных в них требований и мероприятий по комплексной защите информации при производстве техники, проектировании, строительстве (реконструкции) и эксплуатации объектов организации, а также при проведении других работ.
Начальник ЭВМ	Обеспечивает эксплуатацию электронных машин и их устройств в соответствии с техническими условиями и нормами обслуживания, проведение необходимых тестовых проверок, профилактических осмотров, снижение трудоемкости и себестоимости обработки информации и выполнения вычислительных работ. Анализирует причины, вызывающие простои средств вычислительной техники и снижение качества обработки информации и выполнения вычислительных работ, участвует в разработке и внедрении мероприятий по устранению выявленных недостатков. Контролирует качество технического и ремонтного обслуживания. Участвует в приемке, монтаже и испытаниях вновь вводимого в эксплуатацию оборудования, в опытной проверке программного обеспечения. Контролирует своевременность внесения изменений и дополнений в программы и рабочие инструкции.
Руководитель группы … по комплексной защите информации	Проводит аналитические исследования по определению информации об организации и выполняемых работах, которая подлежит комплексной защите, на этапах разработки, производства, испытаний техники, проведения научно-исследовательских и опытно-конструкторских работ.
Руководитель группы … по комплексной защите информации	Выполняет работы по комплексной защите информации от утечки по техническим каналам при разработке, производстве и испытании продукции.
Администратор баз данных	Поддерживает в рабочем состоянии полный объем оперативной и накапливаемой информации базы данных, а также осуществляет защиту информации от несанкционированного доступа. Осваивает новые программные средства. Участвует в разработке мероприятий по совершенствованию процесса хранения и обработки информации с целью обеспечения требуемой достоверности результатов и минимизации времени расчетов. Обеспечивает обмен информацией с подразделениями организации в соответствии с установленным порядком (в том числе с использованием электронных сетей телекоммуникаций). Обеспечивает целостность, достоверность и сохранность циркулирующих в автоматизированной информационной системе данных.

Администратор вычислительной сети	Поддерживает бесперебойное функционирование вычислительной сети. Осуществляет поддержку функционирования баз данных вычислительной сети. Обеспечивает целостность данных, защиту их от несанкционированного доступа, регулирует права доступа пользователей вычислительной сети к ресурсам вычислительной сети. Выполняет установленные требования по резервному копированию данных вычислительной сети. Разрабатывает способы и методы организации доступа пользователей вычислительной сети к ее ресурсам. Ведет журналы, необходимые для нормального функционирования вычислительной сети.
Администратор информационной безопасности вычислительной сети	Обеспечивает информационную безопасность вычислительной сети. Разрабатывает правила эксплуатации вычислительной сети, определяет полномочия пользователей вычислительной сети по доступу к ресурсам вычислительной сети, осуществляет административную поддержку (настройку, контроль и оперативное реагирование на поступающие сигналы о нарушениях установленных правил доступа, анализ журналов регистрации событий безопасности и т.п.). Предотвращает несанкционированные модификации программного обеспечения, добавление новых функций, несанкционированный доступ к информации, аппаратуре и другим общим ресурсам вычислительной сети. Осуществляет сопровождение и, при необходимости, доработку внедренных программных средств по информационной защите. Разрабатывает программы для информационной защиты вычислительной сети и сетевых приложений. Разрабатывает способы и методы организации доступа пользователей вычислительной сети к ресурсам вычислительной сети. Ведет журналы, необходимые для нормального функционирования вычислительной сети. Информирует работников организации об уязвимых местах вычислительной сети, возможных путях несанкционированного доступа и воздействия на вычислительную сеть, известных компьютерных вирусах.
Инженер-конструктор-системотехник	Выполняет работу по проектированию и внедрению автоматизированных систем управления (АСУ) и автоматизированных систем контроля (АСК) различного назначения, кроме автоматизированных систем управления производством (АСУП).
Инженер-конструктор-схемотехник	Выполняет схемотехническую и системотехническую разработку электронных и радиотехнических устройств, приборов, автоматизированных систем контроля и управления технологическими процессами. Разрабатывает электрические схемы устройств управления на базе микропроцессорных средств, однокристальных электронно-вычислительных машин (ЭВМ) и микроЭВМ общего применения, устройств связи, согласующих устройств, используемых в составе автоматизированных систем. Разрабатывает и отрабатывает программное обеспечение входящих в состав устройств и систем технических средств и типовые программы управления объектами автоматизации. Проводит расчеты электронных и электрических схем.
Инженер по АСУТП	Выполняет работы по проектированию и внедрению автоматизированных систем управления технологическими процессами (АСУТП). Курирует работы по разработке программного и математического обеспечения, обеспечивает подготовку локальных программ для проверки отдельных информационных трактов АСУТП. Проводит работы по совершенствованию программных методов контроля оборудования АСУТП. Принимает участие в разработке и внедрении программных систем защиты информации. Вносит изменения в математическое обеспечение, направленные на совершенствование работы систем защиты и их надежности. Обеспечивает эксплуатацию программных систем защиты информации. Принимает участие в разборе причин срывов решения задач АСУТП. Организует оперативное устранение отказов и дефектов программного обеспечения подчиненным персоналом.
Инженер – системный программист	Определяет необходимые системные и программные средства для разработки и отладки прикладного программного обеспечения (ПО). Производит выбор операционной системы (ОС) и других системных компонентов, осуществляет подготовку задания на приобретение необходимой ОС на основе анализа задач, решаемых автоматизированной системой управления технологическими процессами (АСУТП), автоматизированной системой управления предприятием (АСУП), автоматизированной системой контроля (АСК), гибкими производственными системами (ГПС). Экспериментально проверяет реализацию алгоритмов контроля и управления программных средств ОС и пакетов прикладных программ. Производит доработку компонентов ОС по результатам эксперимента. Определяет объем и содержание тестовых примеров, обеспечивающих наиболее полную проверку соответствия ОС задачам, решаемым в АСУТП, АСУП, АСК, ГПС. Обеспечивает модернизацию стандартных конфигураций ОС, устройств, сетей, протоколов и программ. Поддерживает в рабочем состоянии полный объем оперативной, накапливаемой и хранимой информации, обеспечивает защиту от несанкционированного доступа к информационным ресурсам. Обеспечивает работу локальной вычислительной сети.
Приборист цеха	Обеспечивает работу средств измерений, испытаний, контроля и автоматики, средств автоматизированных систем управления (АСУ), их правильную эксплуатацию, своевременный ремонт и модернизацию.
Техник по автоматизированным системам управления технологическими процессами (техник-конструктор-системотехник)	Самостоятельно разрабатывает отдельные виды обеспечения простых систем управления или контроля на основании современных средств вычислительной техники, приборов и средств автоматизации. По заданию инженера-системотехника выполняет макетирование испытываемой системы и участвует в испытании макета. Принимает участие в наладке составных частей разрабатываемых систем и проведении их опытной эксплуатации. Готовит и проводит приемо-сдаточные и метрологические испытания разрабатываемых систем с оформлением протоколов испытаний.

Проблемы организации доверенных удостоверяющих центров инфраструктуры открытых ключей при построении национальных и межгосударственного пространства доверия для признания электронной цифровой подписи

Томина Галина Дмитриевна,
ведущий научный сотрудник Государственного предприятия «НИИ ТЗИ»

Комликов Дмитрий Александрович,
кандидат технических наук, начальник отдела Государственного предприятия «НИИ ТЗИ»

Юрьева Анна Владимировна,
старший научный сотрудник Государственного предприятия «НИИ ТЗИ»

Обеспечение взаимного признания электронной цифровой подписи (ЭЦП) при организации межведомственного взаимодействия, оказании государственных электронных услуг или обмене электронными документами в рамках национального сегмента доверия или при межгосударственном взаимодействии является актуальным и порождает ряд нерешенных на сегодняшний день проблем.

Основные принципы создания инфраструктуры открытых ключей изложены в международных рекомендациях X.842 [1], X.843 [2], RFC 5280 [3], кроме того в [1], [2] предъявлены требования к использованию, управлению, основным услугам доверенной третьей стороны (ДТС) и услугам по поддержке приложений ЭЦП.

Из наиболее известных моделей построения пространства доверенных УЦ можно выделить два подхода, базирующихся на принципе «топология сертификатов», описывающем схему определения отношений доверия в цепочке сертификатов, выданных различными УЦ:

– строго иерархическая, использующая проверку цепочки сертификатов, начиная с корневого узла и оканчивая локальным узлом УЦ;

– иерархическая по кросс-сертификатам, использующая двунаправленный граф и проверку цепочки сертификатов начиная с локального УЦ (выдавшего сертификат пользователя), а не с корневого узла.

Каждая из моделей имеет свои недостатки, основными из которых является возможность отказа в любом звене при использовании иерархической модели, либо потеря управляемости при использовании второй модели с кросс-сертификатами из-за недостатков в отслеживании изменения кросс-сертификатов.

В Республике Беларусь нормативно-правовым актом (НПА) [4] определена законность и порядок применения ЭЦП.

В [5] определена иерархическая модель построения государственной системы управления открытыми ключами (ГосСУОК) инфраструктуры открытых ключей. Однако при этом определяется также необходимость использования механизмов безопасного связывания уникальных имен субъектов взаимодействия открытых ключей, которые совместно с иерархической моделью решат задачи обеспечения аутентификации, конфиденциальности, целостности, подлинности и невозможности отказа от участия в обмене электронными документами и информацией в электронных коммуникационных средах Республики Беларусь. Согласно НПА [6] Республики Беларусь, для решения вышеуказанных задач должны использоваться аппаратные, аппаратно-программные средства, реализующие криптографические алгоритмы и использующие протоколы с открытыми ключами. Порядок функционирования ГосСУОК определен в [7].

При этом основными компонентами, реализующими услуги ГосСУОК, являются:

– корневой УЦ;

– подчиненные УЦ;

– регистрационные центры (РЦ);

– реестры сертификатов и списков отозванных сертификатов;

– архивы сертификатов и списков отозванных сертификатов.

Услуги, обеспечиваемые в иерархической модели корневым и подчиненными УЦ, регистрирующими центрами, реестрами и архивами рекомендованы в [1], [2], [3].

Национальный сегмент доверенных УЦ для организации национального пространства обращения ЭЦП и идентификации субъектов информационного обмена должен представлять единую службу управления ключами и сертификатами, которая обеспечит субъектам следующие основные сервисы:

– формирования запроса на издание сертификата;

– издания, распространения, отзыва сертификата;

– приостановления и возобновления действия сертификата;

– предоставления информации о статусе сертификата;

– хранения сертификата;

– поддержки реестра (базы данных), архива сертификатов и списков отозванных сертификатов;

– регистрации владельцев личных ключей (достоверное подтверждение принадлежности открытого ключа определенному юридическому или физическому лицу);

– выпуска и управления атрибутивными сертификатами (хранение дополнительной информации по разграничению доступа субъекта к ресурсу и уровня привилегий субъекта);

– хранения информации в архиве (долговременное хранение и управление электронными документами, карточками открытых ключей и другой информации);

– резервного хранения и восстановления ключей идентификации (шифрования);

– автоматического обновления сертификата;

– управления историями сертификата;

– онлайновой проверки статуса сертификата;

– электронного нотариата (заверение электронных документов и сертификатов);

– проставления меток времени;

– удостоверения формы внешнего представления электронного документа.

Однако для обеспечения межгосударственного (трансграничного) взаимодействия доверенных УЦ национального сегмента доверия с доверенными УЦ других государств необходимо, чтобы протоколы взаимодействия и услуги соответствовали международным рекомендациям. Например, услуга проверки сертификатов и ЭЦП, выданных доверенным УЦ других государств, должна быть настроена в соответствии с положениями ETSI TS 102231 v2.1.1 [8], определяющими использование однорангового списка TSL, который позволяет включить свои национальные корневые сертификаты в список вне привязки к модели национального головного (корневого) УЦ, так называемая браузерная модель, обеспечивающая кросс-сертификацию.

Фактически TSL представляет собой доверенный реестр, который может быть применен как в национальном сегменте доверенных УЦ, так и при межгосударственном (трансграничном) взаимодействии, а содержимым TSL являются актуальные кросс-сертификаты.

Согласно данной модели, национальный доверенный центр должен доверять актуальности корневых сертификатов в списке TSL. При проверке в электронном документе ЭЦП, национальный УЦ проверяет пришедший к нему сертификат пользователя, подписавшего электронный документ, на наличие в нем корневого сертификата из списка. В случае наличия корневого сертификата в TSL проверяется наличие сертификата пользователя в списке отозванных сертификатов по точке доступа к УЦ, выпустившего этот сертификат, далее проверяется ЭЦП электронного документа на корректность.

Существенной проблемой при межгосударственном (трансграничном) обмене электронными документами является ведение единой шкалы времени для служб национальных доверенных УЦ, объединенных пространством доверия. Уже в рамках национального сегмента доверия проведение мероприятий по созданию инфраструктуры точного времени включает в себя комплекс нормативных, организационных и технических мер по созданию элементов инфраструктуры (источников точного времени), их синхронизации с национальными системами точного времени и стандартизации методологии использования точного времени и штампов времени при включении в состав ЭЦП, квитанции и сообщения.

Второй существенной проблемой организации межгосударственного (трансграничного) обмена электронными документами является применение единой структуры сертификата и списков отозванных сертификатов. Так в Республике Беларусь формат сертификатов и списков отозванных сертификатов определен СТБ 34.101.19-2012, который соответствует международному документу X.509. В то же время приказом ФСБ России «Об утверждении требований к форме квалифицированного сертификата ключа проверки подписи» от 27.01.2012 г. № 23041 определены основные поля квалифицированного сертификата, которые являются дополнительными по отношению к стандарту, а рекомендации по заполнению этих полей в настоящее время отсутствуют.

Следовательно, необходимо при заключении соглашений и договоров по электронному межгосударственному (трансграничному) взаимодействию определить те вопросы, решение которых подлежит техническому регулированию путем принятия дополнительных (к стандартизированным) технических мер, а также принятия правовых мер в виде включения в договора условий по возмещению финансовых потерь в случае возникновения спорных ситуаций между субъектами хозяйствования страной, допустившей отклонение от стандартизованных технических мер.

Отсюда вытекает потребность в сертификации технических и программных решений, используемых при построении доверенных УЦ, аттестации доверенных УЦ на соответствие требованиям ТНПА в области защиты информации, а также вопросы аккредитации доверенных УЦ в национальном регулирующем органе власти и проведение контроля за соблюдением условий аккредитации поставщиком услуг.

Согласно [5], [7], субъектами взаимодействия в инфраструктуре открытых ключей Республики Беларусь могут быть:

– головной доверенный национальный УЦ, выпускающий самоподписанный корневой сертификат;

– подчиненные доверенные национальные УЦ, для которых сертификаты выпускает головной доверенный национальный УЦ;

– доверенные регистрационные центры, для которых сертификаты выпускают соответствующие подчиненные доверенные УЦ, в чьем ведении они находятся;

– конечные пользователи, для которых сертификаты выпускает тот подчиненный доверенный УЦ, в регистрационных центрах которого зарегистрированы конечные пользователи.

При этом [5], [7] уточняют, что субъектами сертификатов конечных пользователей могут быть не только физические лица, но и приложения, серверы (сервисы) и устройства. Заявителями по выдаче сертификата приложению, серверу или устройству должны выступать юридические лица, которые являются их владельцами.

В то же время [7] определяет, что осуществление выработки открытого ключа на базе личного ключа осуществляет владелец с использованием средств ЭЦП, имеющего сертификат соответствия. В соответствии с [6], в Республике Беларусь такие средства должны быть аппаратными или аппаратно-программными для выполнения требований по обеспечению безопасности.

Существующие на рынке ОС и криптопровайдеры осуществляют генерацию личных и открытых ключей программным способом, а также предоставляют услугу по выработке и проверке ЭЦП программным способом, что приводит к снижению уровня доверия к национальным пространствам, доверия других стран, законодательно не запрещающих такой подход.

Следовательно, при заключении межгосударственных соглашений и договоров необходимо согласовать политику применения сертификатов и пакет необходимых регламентов и инструкций. ■

Источники:

[1] X.842 Information technology – Security techniques – Guidelines for the use and management of trusted third party services;

[2] X.843 Information technology – Security techniques – Specification of TTP services to support the application of digital signatures;

[3] RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

[4] Закон Республики Беларусь от 28.12.2009 г. «Об электронном документе и электронной цифровой подписи»;

[5] Концепция развития государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, утвержденной Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 16.10.2012 г. №79;

[6] Положение о порядке организации криптографической защиты информации в государственных информационных системах, а также в информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено, утвержденное Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 25 мая 2012 года №46 «О некоторых мерах по реализации Указа Президента Республики Беларусь от 8 ноября 2011 года №515»;

[7] Положение о государственной системе управления открытыми ключами электронной цифровой подписи Республики Беларусь, утвержденное Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 16.10.2012 г. №79;

[8] ETSI TS 102231 v2.1.1 «Provision of harmonized Trust Service Provider information».

Аппаратные комплексы криптографической защиты информации

Милашенко Виктор Иванович,
начальник отдела государственного предприятия «НИИ ТЗИ»

Развитие информационного общества в Республике Беларусь сопровождается созданием и модернизацией информационных сетей и информационных сервисов на их основе. Укрепление доверия со стороны пользователей и обеспечение безопасности информационных технологий является одним из условий успешности данного процесса.

Применение сетей передачи данных общего пользования для обмена информацией, распространение и (или) предоставление которой ограничено, позволяет существенно снизить издержки по информатизации различных сфер деятельности государства и общества. В этой связи, обеспечение конфиденциальности передаваемой информации является важной задачей, при решении которой требуется использовать аппаратно-программные (аппаратные или технические) средства криптографической защиты информации.

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации» является разработчиком и поставщиком средств защиты информации, распространение и (или) предоставление которой ограничено, для ее передачи по сетям общего пользования.

Аппаратно-программный комплекс (АПК) криптографической защиты цифровых потоков Е1 «Авангард».

АПК «Авангард» предназначен для криптографической защиты конфиденциальной информации, передаваемой по цифровым каналам Е1 со скоростью до 2 Мбит/с.

АПК «Авангард» может применяться на следующих участках защищенной системы связи:

– соединение двух автоматических телефонных станций (АТС) по каналу Е1;

– связь между сегментами защищенной локальной вычислительной сети (Ethernet);

– объединение сетей передачи данных на базе маршрутизаторов, имеющих синхронный цифровой выход 64 – 2048 кбит/с (V.35).

Технические характеристики АПК «Авангард»	
Линейный (канальный) интерфейс	E1 (G.703/G.704) – DB-9F
Станционные (абонентские) интерфейсы	E1 (G.703/G.704) – DB-9F, V.35 – DB26F-HD, Ethernet – RJ45
Режимы работы по каналу E1	Unframed (2048 кбит/с), Framed, Fractional (nx64 кбит/с)
Интерфейсы управления	Ethernet, USB
Управление	Опционально в комплект поставки может включаться прикладное ПО управления для ПЭВМ для ОС Windows
Сигнализация внешняя (Авария, НСД, Звонок)	DB-15F-HD
Клавиатура, ЖКИ	Локальное управление
Алгоритм шифрования	ГОСТ 28147-89
Длина ключа	256 бит
Встроенная функция генерации и записи ключей	(опционально)
Питание	~100-220 В /50-60 Гц
Потребляемая мощность	не более 12 Вт
Габариты	484x285x44 мм
Масса	5 кг
Рабочая температура	0° … 50°С

АПК «Авангард» объединяет потоки информации, поступающие через три интерфейса (Е1, Ethernet, V.35), и обеспечивает криптографическую защиту согласно ГОСТ 28147-89 и целостность объединенного потока при его передаче по каналу Е1 (рисунок 1).

Управление АПК «Авангард» обеспечивается встроенными средствами или через сеть TCP/IP с помощью программного обеспечения удаленного администрирования.

Аппаратно-программное устройство IP-шифрования.

Аппаратно-программное устройство IP-шифрования (АПУ IP-шифрования) предназначено для криптографиче-

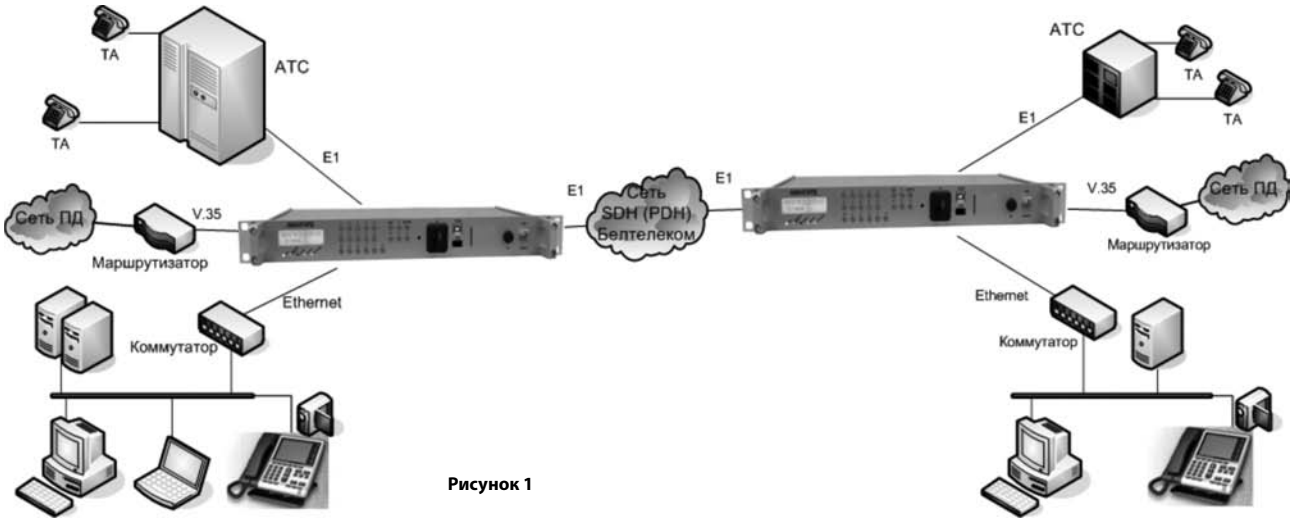


Рисунок 1

Технические характеристики АПУ IP-шифрования	
Скорость шифрования	200 Мбит/с
Скорость шифрования пакетов	50 000 пакетов/с
Количество туннелей	1024 шт.
Интерфейсы	1) 10/100 TX RJ 45 2) 100 FX Optical, LC
Управление с передней панели (клавиатура, ЖКИ)	да
Идентификация локального оператора	да
Электропитание	100-220 В/50-60 Гц (опция = 20-72 В)
Потребляемая мощность	менее 20 Вт
Масса	<8 кг (вместе с УВКП)
Рабочая температура	минус 10 – плюс 40°С

ской защиты информационного обмена между локальными сетями и/или отдельными станциями, взаимодействующими по протоколу IP через сети передачи данных по медным и оптическим кабелям со скоростью до 100 Мбит/с.

АПУ IP-шифрования обеспечивает:

– криптографическую защиту IP-пакетов методом полной инкапсуляции;

– прозрачное автоматическое шифрование/расшифрование информации с заданной стойкостью по алгоритму шифрования ГОСТ 28147-89 или СТБ 34.101.31-2011;

– контроль целостности пакетов данных – имитозащиту по ГОСТ 28147 89 или СТБ 34.101.31-2011;

– генерацию ключей для работы в сети с использованием датчика случайных чисел (ДСЧ) на основе физического источника шума;

– проверку целостности программного обеспечения криптомодулей с использованием алгоритма СТБ 1176.2-99 или СТБ П 34.101.45-2011;

– одновременную работу в сети не менее 1000 изделий (обеспечение одновременного функционирования не менее 1000 виртуальных каналов).

Схема типового применения АПУ IP-шифрования представлена на рисунке 2.

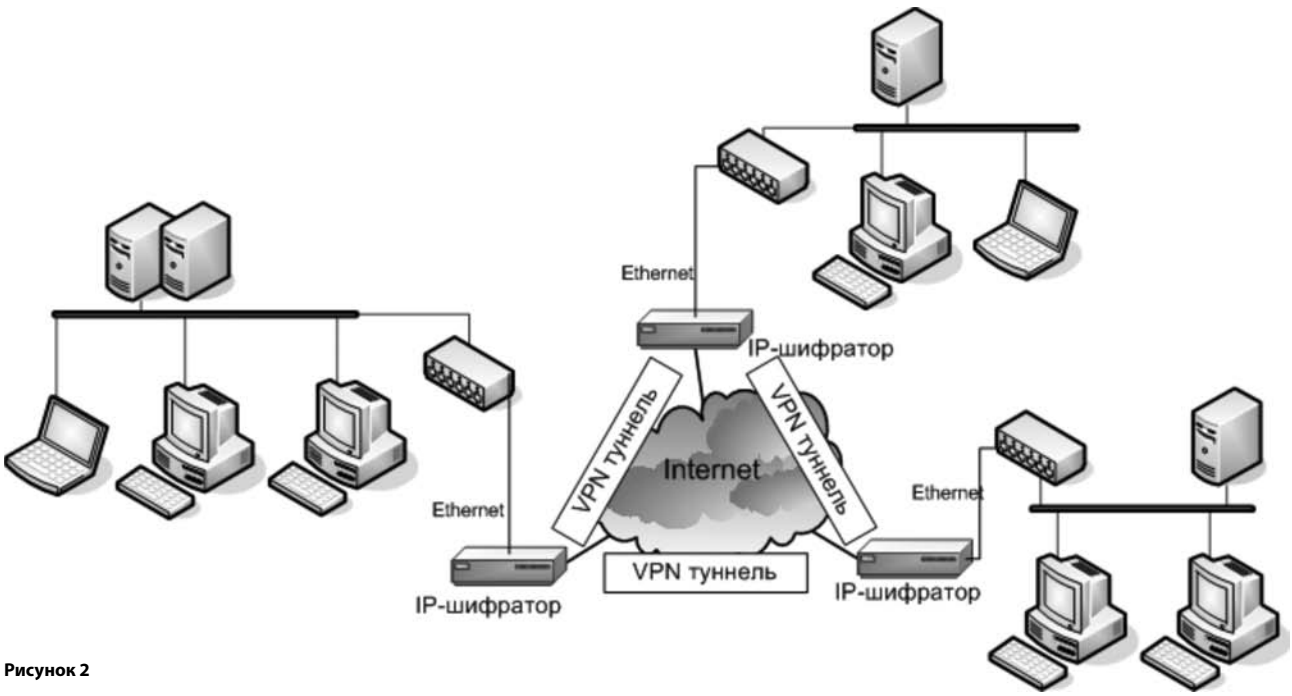
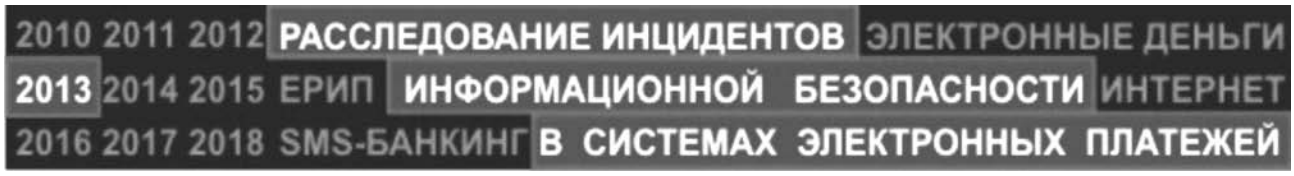


Рисунок 2



Опыт предотвращения мошенничества при проведении банковских транзакций

Расследования компьютерных преступлений и инцидентов информационной безопасности в системах электронных платежей в мировой практике относят к сложным задачам, которые приходится решать корпоративным службам безопасности и правоохранительным органам.

Национальный банк Республики Беларусь, Белорусский государственный университет информатики и радиоэлектроники и журнал «Технологии безопасности» 27 марта 2013 года провели научно-практический семинар «Расследование инцидентов информационной безопасности в системах электронных платежей». Специалисты из ведущих российских и белорусских компаний рассказали о практическом опыте в расследовании и предотвращении хищений в системах электронных платежей.

В ходе докладов и презентаций были рассмотрены юридические, организационные и технические моменты возникновения рисков. Были выделены основные зоны возникновения рисков, а также рассмотрены средства и методы защиты в дистанционном банковском обслуживании (ДБО) для юридических и физических лиц. Также обсуждались методы эффективного построения защиты карточек клиентов и внутренних процессов банка.

В рамках круглого стола участники семинара поделились практическим опытом реализации решений, позволяющих реагировать на инциденты в системах электронных платежей.

Участие в семинаре приняли руководители и специалисты служб информационной безопасности банков и финансовых компаний, государственных организаций. Общее количество участников составило более 100 человек.

Учитывая актуальность поднятых вопросов, планируется проведение еще одного семинара с углубленной проработкой вопросов обеспечения безопасности ДБО. В частности будут рассматриваться вопросы использования аппаратно-программных решений, применяемых на клиентской стороне с использованием ДБО. ■

Генеральный партнер мероприятия – «Доктор Веб», российский разработчик антивирусных программ и сервисов для предоставления услуг информационной защиты

Информационный партнер – компания «Андэк» специализируется на обеспечении безопасности бизнеса

Актуальность проведения мероприятий на тематику расследования инцидентов информационной безопасности в системах электронных платежей

Денисов Денис Валерьевич, главный специалист операционного управления системы «Расчет»

Справка ТБ

Денисов Денис Валерьевич, окончил факультет прикладной математики и информатики БГУ в 2007 году, специальность «Компьютерная безопасность». Руководил направлением информационной безопасности в службах безопасности ОАО «Белорусский Индустриальный Банк», ОАО «Банк Москва-Минск». Сейчас работает на должности главного специалиста операционного управления системы «Расчет» Главного управления единого расчетного и информационного пространства (ЕРИП) Национального банка Республики Беларусь, руководит направлением обеспечения безопасности системы «Расчет», является секретарем межведомственной Рабочей группы по противодействию мошенничеству в области электронных платежей.

Пожалуй, отправной точкой нового витка развития направления обеспечения банковской безопасности можно считать разбойное нападение 10.12.2009 г. на обменный пункт ЗАО "Абсолютбанк" в Минске. В ходе инцидента погибла 21-летняя кассир. После этого инцидента 24.12.2009 г. в Национальном банке Республики Беларусь с участием представителей органов государственного управления и руководителей банков состоялось совещание, на котором были приняты достаточно серьезные решения. По результатам совещания был составлен план мероприятий. В дальнейшем, в целях комплексного подхода к борьбе с преступностью, Указом Президента от 23.09.2010 г. №485 утверждена Государственная программа по борьбе с преступностью и коррупцией на 2010–2012 годы, в которой уже были учтены и мероприятия по результатам совещания в Национальном банке. Во исполнение решений п. 2.3 Плана мероприятий совещания в Национальном банке Республики Беларусь и п. 3.1.1.4 Государственной программы, распоряжением Председателя Правления Национального банка Республики Беларусь от 31.12.2010 года № 1056 была создана межведомственная рабочая группа по противодействию мошенничеству в области электронных платежей, в состав которой вошли представители Национального банка Республики Беларусь, крупнейших банков Республики Беларусь, Министерства внутренних дел Республики Беларусь, Следственного комитета Республики Беларусь, ОАО "Банковский процессинговый центр", ООО "VISA Украина", ООО "Мастеркард" (г. Москва). Результатом работы группы стал Свод рекомендаций, включивший в себя:

- рекомендации по организации взаимодействия между банками, процессинговыми центрами и органами Министерства внутренних дел в случае выявления мошенничества с банковскими платежными карточками;
- рекомендации по обеспечению безопасного функционирования программно-технической инфраструктуры банков, ОАО "Банковский процессинговый центр", ООО "Веб Пэй" и аналогичных организаций, участвующих в обработке интернет-транзакций с использованием банковских платежных карточек;
- рекомендации для оценки надежности интернет-магазинов, подключаемых белорусскими банками-эквайерами;
- рекомендации по противодействию мошенничеству при совершении расчетов в сети Интернет по банковским платежным карточкам;
- рекомендации банкам по оформлению документов, позволяющих подтверждать ущерб, причиненный резидентам иностранных государств в результате мошенничества в области интернет-эквайеринга на территории Республики Беларусь.

В дальнейшем, по распоряжению Первого заместителя Председателя Правления Национального банка Республики Беларусь Лузгина Н.В. от 13.11.2012 г. №484 были продолжены мероприятия по функционированию Рабочей группы по противодействию мошенничеству в области электронных платежей с целью дальнейшего анализа состояния и потребностей в данном направлении, также была дана оценка эффективности применения разработанного в 2011 году свода рекомендаций по противодействию мошенничеству в области электронных платежей и определены новые векторы работы группы. По итогам совещания было отмечено снижение количества преступлений в сфере незаконного оборота платежных карт в Республике Беларусь, а также высокая эффективность разработанных рекомендаций по организации взаимодействия между банками, процессинговыми центрами и органами Министерства внутренних дел в случае выявления мошенничества с банковскими платежными карточками.

По информации банков, некоторые из них внедрили механизмы микроплатежей. При совершении оплаты с использованием иностранной банковской платежной карточки платежный сервер осуществляет online авторизацию с использованием данной карты на случайную сумму от 0,5 до 2 USD. Держатель карты должен узнать сумму микроплатежа в банке-эмитенте платежной карты и ввести сумму микроплатежа для подтверждения совершения основной оплаты в течение одного часа. Если сумма микроплате-

жа совпадет с введенной держателем карты суммой, валидация карты считается успешной и платежный сервер осуществляет online авторизацию на основную сумму оплаты и формирует операцию отмены по микроплатежу. В случае, если держатель карты неправильно ввел сумму микроплатежа три раза или не ввел ее в течение часа, платежный сервер формирует операцию отмены по микроплатежу и не осуществляет online авторизацию на основную сумму оплаты. Также банки используют технологии Verified by VISA и MasterCard SecureCode, трехфакторную аутентификацию платежей интернет-банкинга 3D Secure. Совершенствуются методы фрод-мониторинга, устанавливаются блокировки на суммы снятия денежных средств, дополнительные методы подтверждения платежей в географически опасных станах мира (Таиланд, США и др.), иногда полностью запрещаются операции в некоторых странах, все больше карт выпускаются с микрочипами. ОАО "Банковский процессинговый центр" ежеквартально проверяет контент интернет-магазинов с эквайерингом белорусских банков согласно Своду рекомендаций. VISA и MasterCard предлагают все больше услуг по безопасному использованию банковских платежных карт: возможности геоблокировки, уведомления держателей карт об опасных транзакциях, когда параметры транзакции соответствуют определенным ограничениям по географии, сумме транзакции, по типу организаций торговли и сервиса, и наконец даже скоринговые интеллектуальные системы фрод-мониторинга.

В рамках деятельности рабочей группы был создан закрытый информационный ресурс, на котором специалисты по карточной безопасности банков и специалисты органов внутренних дел обмениваются контактной информацией и оперативно оповещают других участников о точках подтвержденной компрометации карт. Так, например, участники оперативно могут узнать, в каких устройствах и в какой промежуток времени производилось считывание карт скиммерами.

Национальным банком Республики Беларусь разработаны типовые памятки держателям карт. Указанные памятки имеются во всех отделениях банков, а также на официальных сайтах банков. С целью реализации государственной программы по повышению финансовой грамотности населения реализуется целый комплекс мероприятий с привлечением банков и средств массовой информации. Все больше банков перед операциями с банкоматами выдают оповещение клиентам с тем, чтобы они убедились в отсутствии скиммеров в банкомате и так далее.

Так, по сведениям Министерства внутренних дел Республики Беларусь, анализ оперативной обстановки на территории республики в 2012 году отражает тот факт, что количество преступлений в сфере незаконного оборота платежных карт снижается. Так, если за 9 месяцев 2011 года зарегистрировано 1528 преступлений, то за аналогичный период текущего – 1271, снижение составляет 16,8 %.

Если рассматривать структуру зарегистрированных преступлений, то подавляющее большинство совершено с использованием подлинных банковских платежных карт, но наибольшую общественную опасность представляют хищения, совершаемые с использованием поддельных карт, либо их реквизитов, а также с использованием специальных средств, предназначенных для несанкционированного копирования информации с магнитных полос банковских платежных карт.

Для объективной оценки состояния преступности следует иметь в виду, что в этой части официальная статистика не отражает реальное количество хищений, совершенных с использованием поддельных карт. Как правило, такие преступления совершаются в составе организованных групп, которые к моменту выявления и принятия решения о возбуждении уголовного дела уже совершили десятки и сотни эпизодов хищений, осуществили приготовление к совершению новых преступлений. При возбуждении уголовного дела в таких случаях, принимая во внимание наличие единого умысла на совершение ряда преступлений, следователь возбуждает одно уголовное дело. То есть на практике зачастую в одном уголовном деле расследуются сотни эпизодов хищений, объединенных единым умыслом, совершенных одними и теми же лицами из банкоматов, принадлежащих различным банкам, с использованием сотен банковских платежных карт, эмитированных различными банками.

Всего в 2012 году обезврежено 5 преступных групп (общей численностью 12 человек, в том числе 2 международные), специализировавшихся на совершении преступлений в сфере незаконного оборота платежных карт на территории страны.

Среди особенностей оперативной обстановки за истекший период можно считать уменьшение числа выявленных преступлений, совершаемых с использованием поддельных банковских платежных карт («белого пластика»).

Работа по дальнейшему регулированию сегмента продолжается. Есть еще такие перспективные направления, как регламентация рекомендаций по противодействию банкоматным вирусам, вирусам на электронных устройствах, используемых для оплаты через каналы дистанционного банковского обслуживания, фишингу, смишингу. План совместных действий государственных органов и участников финансового рынка по развитию в Республике Беларусь системы безналичных расчетов по розничным платежам с использованием современных электронных платежных инструментов и средств платежа на 2013–2015 годы, утвержденный Постановлением Совета Министров Республики Беларусь и Национального банка Республики Беларусь от 01.04.2013 г. №246/4, предполагает увеличение показателей доли безналичного денежного оборота в розничном товарообороте организаций розничной торговли и доли безналичного денежного оборота в объеме платных услуг населению к 1 января 2016 года до 50%, что подчеркивает актуальность проведения дальнейших активных мероприятий. Также следует учитывать опыт Российской Федерации, где, к примеру, разработаны Методические рекомендации о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиентов. В Российской Федерации принят Федеральный закон от 27.06.2011 г. №161-ФЗ «О национальной платежной системе». Согласно статье 9 этого закона, вступающего в силу с 2014 года, также устанавливается порядок возможности отмены транзакций с признаками мошенничества. К слову, там держателю карты банк будет обязан вернуть денежные средства на карту в течение 24 часов в случае хищения, когда нет явной вины держателя. А уже затем сам банк собирает материалы и передает в правоохранительные органы для возмещения ущерба, нанесенного уже банку, а не держателю карты.

Актуальность проведения специализированных мероприятий (профессиональных семинаров, форумов) обусловлена недостаточными знаниями и пониманием всего процесса при расследовании таких инцидентов. Зачастую банки неэффективно взаимодействуют с правоохранительными органами, многие банки не знают либо не

Продолжение на стр. 24 →

Эволюция мошенничества в системах интернет-банкинга

Суханов Максим Андреевич, специалист отдела расследований инцидентов информационной безопасности компании Group-IB

Справка ТБ

Суханов Максим Андреевич, образование – высшее техническое, квалификация – инженер по специальности «Стрелково-пушечное, артиллерийское и ракетное оружие». Обладает обширным опытом в области реагирования на инциденты в системах ДБО и проведения соответствующих криминалистических исследований компьютерной информации. Участник международных и российских проектов, посвященных судебным компьютерным экспертизам. В компании Group-IB с августа 2010 года.

По статистике, большинство хищений денежных средств с использованием систем интернет-банкинга происходит за счет действий злоумышленников, не связанных с пострадавшей стороной трудовыми договорами или иным непосредственным способом.

Методы и средства похищения денежных средств.

Схема хищения денежных средств проста: злоумышленник создает платежное поручение, подписывает его электронной подписью, а затем передает в банк; банк, в свою очередь, проверяет платежное поручение и исполняет его; после исполнения платежного поручения, зачисленные на счет подставного физического или юридического лица денежные средства обналичиваются, иногда похищенные денежные средства перед обналичиванием передаются через цепочку юридических лиц в другой регион.

Основным элементом этой схемы является подпись платежного поручения, которая осуществляется одним из следующих способов:

1. Злоумышленник копирует ключи электронной подписи с компьютера пострадавшего лица на свой компьютер. Дальнейшее формирование мошеннического платежного поручения осуществляется злоумышленником на своем компьютере.

2. Злоумышленник, имея полный доступ к управлению компьютером пострадавшего лица, ожидает подключения носителя ключей и формирует платежное поручение при его подключении непосредственно на компьютере пострадавшего.

3. Злоумышленник использует вредоносную программу для автоматической подмены реквизитов легитимного платежного получения (реквизитов получателя и его банка, суммы платежа, назначения платежа), которое формирует пострадавшее лицо, непосредственно перед его подписью и передачей в банк.

Копирование файлов ключей электронной подписи на свой компьютер злоумышленник может выполнить с использованием стандартных средств операционной системы Windows либо с использованием каких-либо программ, не обязательно относящихся к категории вредоносных, в том числе и программ для удаленного управления компьютером.

Формирование платежного поручения непосредственно на компьютере пострадавшего может быть произведено вручную с помощью различных программ для удаленного управления компьютером (Radmin, TeamViewer, RDP-сервер Windows и т.д.). Такие программы предварительно конфигурируются для скрытой от пользователя работы в операционной системе: отключается отображение значка программы в области уведомлений, отключаются любые уведомления пользователя о входящих соединениях и т.п. Иногда удаленное управление компьютером обеспечивается вредоносной программой или ее модулем. В зависимости от функциональности используемой программы, злоумышленник может работать в сессии легитимного пользователя (в момент, когда пользователь отошел от компьютера) либо в параллельной сессии (в этом случае окна запускаемых злоумышленником программ, его работа с курсором и ввод с клавиатуры легитимному пользователю не видны).

Программные средства.

Особое внимание заслуживают вредоносные программы. Злоумышленникам доступно большое количество вредоносных программ различных классов, в т. ч. ZeuS, SpyEye, Carberp, RDPdoor и Shiz.

Все эти классы вредоносных программ предназначены для хищения денежных средств из систем интернет-банкинга, а некоторые из них ориентированы на незаконную деятельность в отношении физических и юридических лиц в России и в странах бывшего СССР. В последнее время, в связи с распространением носителей с неизвлекаемыми ключами электронной подписи и необходимостью автоматизировать процесс хищения денежных средств, злоумышленники применяют вредоносные программы, подменяющие реквизиты легитимных платежных поручений непосредственно перед их подписанием: такая подмена производится модификацией данных, обрабатываемых клиентской частью системы дистанционного банковского обслуживания. К примеру, если система интернет-банкинга реализована в виде веб-сервиса, для доступа к которому клиент использует браузер, то для подмены реквизитов платежного поручения в содержимое веб-страницы, предназначенной для ввода данных платежа, вредоносной программой может добавляться небольшая программа на языке программирования JavaScipt. Эта программа внедряется в содержимое веб-страницы локально, т.е. на компьютере клиента системы интернет-банкинга, а в результате ее запуска (при нажатии на кнопку подписи платежного поручения) происходит подмена содержимого полей ввода текстовой или числовой информации, что в итоге приводит к подписи и передаче в банк мошеннического платежного поручения. Такой способ

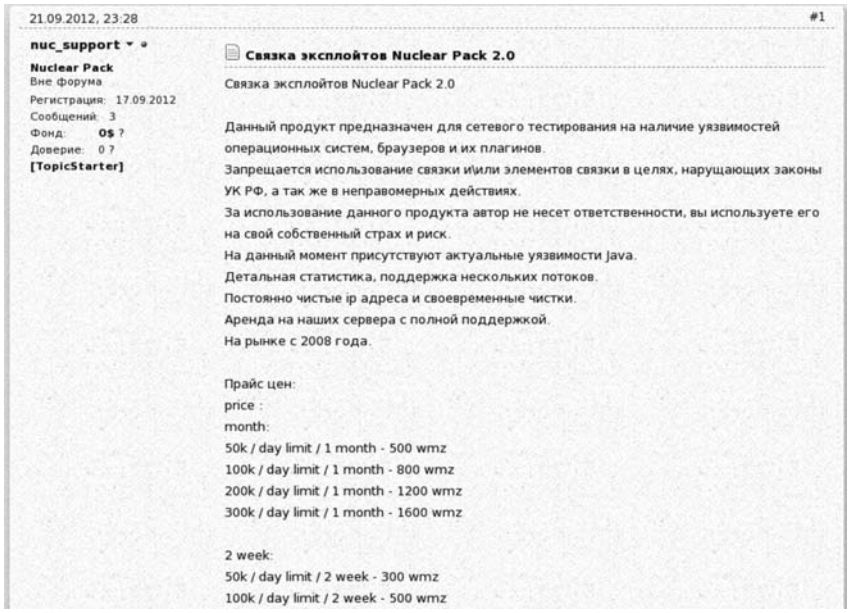
формирования мошеннических платежных поручений называется «автозаливом» («авто» – автоматически, а слово «залив» на жаргоне интернет-мошенников обозначает процесс хищения денежных средств). Следует отметить, что «автозалив» используется не только для подмены реквизитов легитимного платежного поручения, но и для автоматического создания мошеннических платежных поручений по определенным правилам, их немедленного подписания с последующей передачей в банк.

Для распространения вредоносных программ злоумышленники используют связки эксплоитов (эксплоитом, в общем случае, является совокупность данных и команд, предназначенных для эксплуатации какой-либо уязвимости в программном обеспечении с определенной целью; иногда эксплоитом является набор данных, не содержащий команд, эксплуатирующий какую-либо уязвимость). Среди связок эксплоитов можно выделить некоторые наиболее разрекламированные: Blackhole и Nuclear Pack.

Эти связки эксплоитов предназначены для эксплуатации уязвимостей в популярных браузерах (Internet Explorer, Mozilla Firefox и др.) и используемых ими программных модулях (Flash, Java, модули для просмотра PDF-файлов) с целью загрузки и запуска произвольных (задаваемых злоумышленником) программ, в т.ч. вредоносных. Ссылки на такие эксплоиты могут размещаться на взломанных веб-сайтах (наибольшую ценность для мошенничества в системах интернет-банкинга представляют взломанные веб-сайты, ориентированные на бухгалтеров) или на специально созданных для этого веб-сайтах, на которые различными способами приглашаются посетители. На различных хакерских форумах можно встретить множество объявлений о продаже доступов к взломанным веб-сайтам различной тематики.

Одним из способов привлечения посетителей на вредоносную страницу веб-сайта является покупка трафика (под трафиком в данном случае понимаются посетители веб-сайта). Такая покупка может быть произведена на специализированных биржах, где за деньги продают определенное количество переходов посетителей заданной тематической категории на какую-либо страницу (одним из легальных способов использования бирж трафика является раскрутка веб-сайтов, когда владелец веб-сайта покупает посетителей из тематической категории, которым его веб-сайт будет интересен;

Объявление о продаже вредоносной программы Carberp



Объявление о сдаче в аренду связки эксплоитов Nuclear Pack

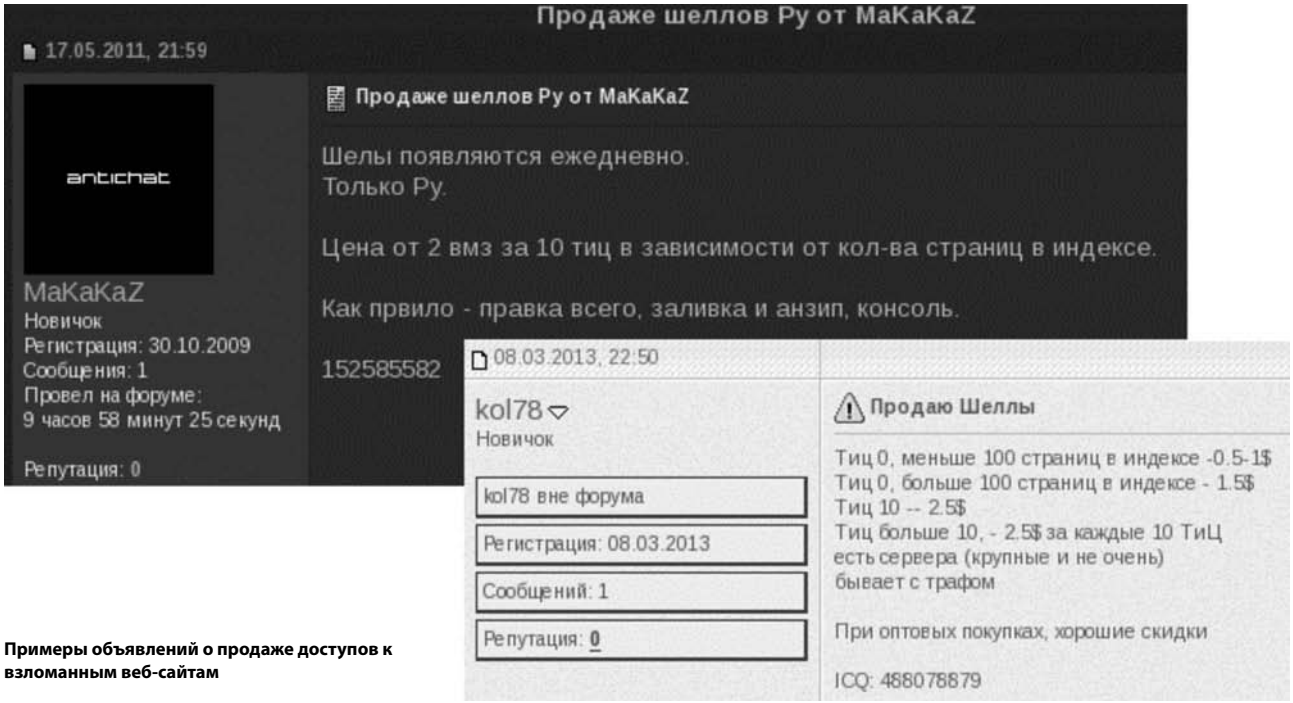
биржи трафика во многом похожи на баннерные сети, только в них вместо показов баннеров продаются переходы на сайт). Следует отметить, что биржи трафика обычно противодействуют перенаправлению посетителей на мошеннические сайты или на сайты, распространяющие вредоносные программы: для этого производится регулярная проверка (модерация) ссылок на интернет-ресурсы, предоставляемые клиентами биржи трафика. В то же время злоумышленники находят способы обмануть администраторов и модераторов бирж трафика и перенаправлять их переходы на интернет-страницы, не содержащие мошеннического или вредоносного содержимого, хотя остальные посетители перенаправляются на интернет-страницы с именно таким содержимым.

Способы обналичивания денежных средств.

Наиболее популярным и наиболее простым способом обналичивания является перевод денежных средств на банковскую карту с последующим их снятием через банкомат.

Еще одним способом обналичивания является пополнение лицевых счетов абонентов оператора сотовой связи с последующим расторжением договоров на оказание услуг связи, что влечет выплату остатков на лицевых счетах наличными. Для реализации такого способа обналичивания злоумышленнику необходимо приобрести большое количество SIM-карт, оформленных на подставных лиц.

Другой способ обналичивания заключается в переводе денежных средств на счет индивидуального предпринимателя с последующим их снятием через кассу банка. Аналогичная схема возможна и с переводом денежных средств на счет юридического лица, однако такой способ обналичивания похищенного является редким.



Примеры объявлений о продаже доступов к взломанным веб-сайтам

Основные этапы эволюции мошенничества в системах интернет-банкинга в контексте защитных мер и контрмер.

Мера: первичной мерой по противодействию мошенничеству является криптографическая подпись платежных поручений.

Контрмера: основным противодействием этой мере является копирование злоумышленником ключей электронной подписи.

Мера: для защиты от копирования ключей электронной подписи злоумышленником банки начали применять носители с неизвлекаемыми ключами (токены).

Контрмера: подпись платежного поручения при установленном носителе ключей («автозалив» с помощью вредоносной программы, ручное формирование платежного поручения злоумышленником с помощью программы для удаленного управления компьютером).

Мера: подтверждение переводов по телефону.

Контрмера: злоумышленник инициирует подтверждающий звонок в банк от имени клиента (для этого привлекаются call-центры, специализирующиеся на мошенничествах, в которых всегда можно выбрать мужской или женский голос, язык общения и акцент).

Мера: внедрение СМС-подтверждений.

Контрмера №1: злоумышленник заказывает восстановление SIM-карты по поддельной доверенности (номер телефона, привязанный к учетной записи в системе интернет-банкинга, может запрашиваться у пользователя вредоносной программой под каким-либо предлогом).

Контрмера №2: злоумышленник использует вредоносную программу для мобильных телефонов с целью полу-

«Одна из популярных бирж трафика»

чения кода подтверждения перевода (для установки вредоносной программы на мобильный телефон пользователя может использоваться уже функционирующая на его компьютере вредоносная программа, которая блокирует доступ к интернет-банкингу и отображает пользователю уведомление о необходимости установки на мобильный телефон дополнительной программы).

Мера: внедрение «антифрод»-систем, детектирующих мошеннические платежные поручения по определенным критериям.

Контрмера: приведение текста назначения мошеннического платежа в соответствие с характером деятельности организации; отправка мошеннического платежного поручения с компьютера организации (IP- и MAC-адреса, связанные с процессом передачи платежного поручения, в этом случае соответствуют обычно используемым); учет ограничений по сумме платежа и т.п.

Мера: ускорение реакции на мошенничество, попытки немедленной остановки движения похищенных денежных средств по заявлению представителя пострадавшей организации.

Контрмера №1: вывод операционной системы компьютера пострадавшей организации из строя (удаление файлов операционной системы, перезапись первых секторов накопителя или перезапись всех секторов накопителя), что позволяет отсрочить момент обнаружения факта мошенничества пострадавшим.

Контрмера №2: подмена отображаемого пользователю остатка на счете, а также сокрытие мошеннических платежных поручений из списка (осуществляются вредоносной программой).

Реакция на случаи мошенничества в системах интернет-банкинга.

Процесс реагирования для правоохранительных органов разделяется на три составляющих: запрос относящихся к инциденту сведений у банков (а равно – выемка этих сведений), запрос относящихся к инциденту сведений у интернет-провайдера потерпевшего (а равно – выемка этих сведений), получение (копирование) данных у пострадавшего (а равно – выемка соответствующих носителей информации).

У банка пострадавшего целесообразно запросить следующие сведения:

1. IP-адреса, с которых входили в систему интернет-банкинга.

2. MAC-адреса, с которых входили в систему интернет-банкинга (MAC-адреса сохраняются у большинства систем дистанционного банковского обслуживания юридических лиц за счет запуска на компьютере клиента соответствующей программы).

У банка, в котором обслуживается подставное лицо, участвующее в получении похищенных денежных средств и их дальнейшей пересылке, целесообразно запросить те же самые сведения, а также копии сообщений электронной почты (с техническими заголовками), которые были получены от этого лица службой технической поддержки банка (запросы на перевыпуск ключей, запросы техническим специалистам банка и т.п.). Такие сообщения электронной почты могут содержать дополнительные сведения об IP-адресах, использованных мошенниками.

У интернет-провайдера пострадавшего целесообразно запросить любые доступные сведения, касающиеся работы клиента (статистика его сетевых подключений, журналы прокси-сервера и т.п.).

У самого потерпевшего целесообразно осуществить выемку следующих предметов и документов:

1. Машинные носители информации из бухгалтерского компьютера (накопители на жестких магнитных дисках, накопители на основе флэш-памяти). Если на момент выемки компьютер включен, то целесообразно скопировать содержимое его оперативной памяти.

2. Носители ключевой информации (дискеты, токены, носители типа «USB Flash»).

3. Журнальные файлы всех сетевых устройств (прокси-серверы, ретрансляторы сетевых адресов и т.д.). Также целесообразно скопировать сетевой трафик, передаваемый в локальной вычислительной сети пострадавшего, за небольшой промежуток времени.

4. Описание инцидента со слов работников.

При реагировании настоятельно рекомендуется следовать положениям разработанной компанией Group-IB инструкции, доступной по следующему интернет-адресу: http://www.group-ib.ru/images/files/Group-IB_dbo_instruction.pdf . ■

← *Начало на стр. 20*

Актуальность проведения мероприятий на тематику расследования инцидентов информационной безопасности в системах электронных платежей

используют Свод рекомендаций. Вместе с тем внутренние расследования банков зачастую либо не проводятся, либо проводятся формально и инциденты «спускаются на тормозах». Также немаловажным фактором является принятие решения банками о неразглашении инцидентов, так как это может негативно сказаться на репутации банка. Пока такие факторы будут являться доминирующими в банках, подобные эпизоды инцидентов останутся безнаказанными и это уже, в свою очередь, будет подстегивать криминальные круги использовать свои схемы и в дальнейшем. Необходимо только совместными усилиями добиваться искоренения преступности в нашем сегменте, для чего каждый представитель службы безопасности банков должен понимать, как в дальнейшем собранная информация об инциденте будет использована при расследовании государственными органами. Банк должен понимать, каковы успехи в расследовании преступлений государственными органами, эффективность взаимодействия банков, Министерства внутренних дел Республики Беларусь, как органа, собирающего материалы преступления, Следственного комитета Республики Беларусь, как органа уголовного преследования, и органов прокуратуры на финише, при принятии судебных решений.

Не все инциденты связаны с прямым финансовым ущербом, и банки также должны знать, какие эффективные методы внутренних расследований могут применяться. На семинарах данной тематики выступают эксперты по расследованию инцидентов информационной безопасности из соседних стран. Семинар «Расследование инцидентов информационной безопасности в системах электронных платежей», проведенный 27 марта 2013 года, является знаковым в данном направлении для Республики Беларусь, так как на этом мероприятии эксперты из Российской Федерации и Республики Беларусь впервые подняли пласт такой проблематики для белорусских банков и иных организаций. ■

National Hi-Tech Crime Unit.RU
Национальный центр по борьбе с преступлениями в сфере высоких технологий

Особенности производства экспертиз по делам о несанкционированном доступе к реквизитам банковских карт и систем ДБО

Юрин Игорь Юрьевич,
генеральный директор
ООО «Национальный
центр по борьбе
с преступлениями в сфере
высоких технологий»
(Россия)

Справка ТБ

Юрин Игорь Юрьевич, образование высшее, математик, в 2002 году окончил Саратовский государственный университет имени Н.Г. Чернышевского. С 2002 года – сотрудник кафедры теоретических основ компьютерной безопасности и криптографии СГУ имени Н.Г. Чернышевского, заведующий лабораторией компьютерной безопасности. Опыт производства компьютерных и компьютерно-технических экспертиз с 2003 года по настоящее время. Автор методических рекомендаций и специализированного программного обеспечения для производства компьютерных экспертиз.

В современном мире компьютерные преступники проявляют самый минимальный интерес к взлому банковских серверов. Они уже давно убедились, что взламывать аккаунты юридических лиц в системах дистанционного банковского обслуживания (ДБО) или использовать реквизиты банковских карт физических лиц гораздо проще и эффективнее, ввиду их меньшей защищенности и большей распространенности.

Преступления, связанные с несанкционированным доступом (НСД) к системам ДБО имеют некоторые особенности, влияющие на методы и средства производства компьютерных и компьютерно-технических экспертиз и исследований.

Этапы НСД:

- первичное проникновение;
- закрепление своих позиций на ПК;
- сбор информации о системе ДБО;
- подготовка «путей отхода»;
- ожидание поступления денежных средств на счет;
- перевод денежных средств;
- «заметание следов».

Первичное проникновение – внедрение любой из вредоносных программ на компьютер, например, через эксплоиты.

Закрепление позиций – установка копировщиков ключей ЭЦП со сменного носителя информации (USB-диска или дискеты), клавиатурных шпионов для копирования пароля на доступ к этим ключам (с целью дальнейшего осуществления денежного перевода с компьютера злоумышленника). Для того, чтобы не потерять контроль над зараженным компьютером, на него дополнительно может быть установлен нестандартный пакет утилит для удаленного администрирования (R-Admin, TeamViewer, WinVNC и т.п.), а также ежедневно осуществляется обновление версий установленных вредоносных программ, чтобы избежать их детектирования антивирусными программами. Поэтому при производстве экспертиз антивирусные программы практически не помогают установить использовавшиеся для НСД вредоносные программы, и эксперту нужно самостоятельно осуществлять поиск, ориентируясь на нестандартные файлы, зарегистрированные в системе. В Екатеринбурге братья-хакеры изготавливали банковских троянцев под каждую конкретную взламываемую организацию.

Сбор информации. Как правило, перевод денежных средств не осуществляется в первый же день после заражения компьютера с установленным клиентом ДБО. Злоумышленники тренируются работать в конкретной используемой системе Интернет-банкинга, проверяют выписки по счетам, изучают особенности проводимых платежей (последние номера платежных поручений, стандартные тексты о назначении платежа, размер используемого НДС и т.п.).

Ожидание поступления денежных средств – злоумышленники ожидают поступления большой суммы на банковский счет организации. Пример – в Белгороде со дня первичного внедрения до дня снятия 6 млн. руб. прошло 5,5 месяцев.

Перевод денежных средств может осуществляться непосредственно с зараженного компьютера с использованием подключенного к нему USB-токена или с компьютера злоумышленника, с использованием скопированных реквизитов доступа.

Заметание следов – после совершения несанкционированного платежа злоумышленники должны оперативно или обналичить деньги, или осуществить их перевод на другие счета по цепочке, возможно раздробив украденные деньги на более мелкие суммы. Для того, чтобы владелец счета не обнаружил пропажу и не мог обратиться в банк с просьбой заблокировать деньги на счете, злоумышленники стараются прервать или затруднить работу пользователя со своим счетом. Для этого на зараженный компьютер устанавливаются специальные вредоносные программы, мешающие работе пользователя (блокирующие работу пользователя), удаляющие некоторые файлы операционной системы или полностью уничтожающие всю файловую систему на дисках компьютера. В последнем случае исследование компьютера средствами, имеющимися в распоряжении экспертов МВД или частными экспертами, не представляется возможным. В случае удаления только файлов операционной системы, возможно проведение исследования путем подключения НЖМД зараженного компьютера в качестве вторичного диска с использованием блокиратора к стендовой ЭВМ эксперта.

Каждая из используемых злоумышленниками программ оставляет свои следы и на НЖМД зараженного компьютера эксперту предстоит обнаружить:

1) дату и время первичного заражения компьютера, источник заражения;

2) тип, характеристики, настройки вредоносных программ, использованных для НСД, отчеты и журналы их работы;

3) информацию, персонализирующую автора вредоносных программ;

4) действия, осуществлявшиеся злоумышленником в системе, и адреса, с которых злоумышленник проводил удаленное администрирование компьютера;

5) сведения о подготовке платежных поручений (черновики).

Достаточно большое количество областей персонального компьютера может хранить сведения о совершенном НСД. Поэтому при производстве экспертиз необходимо исследовать:

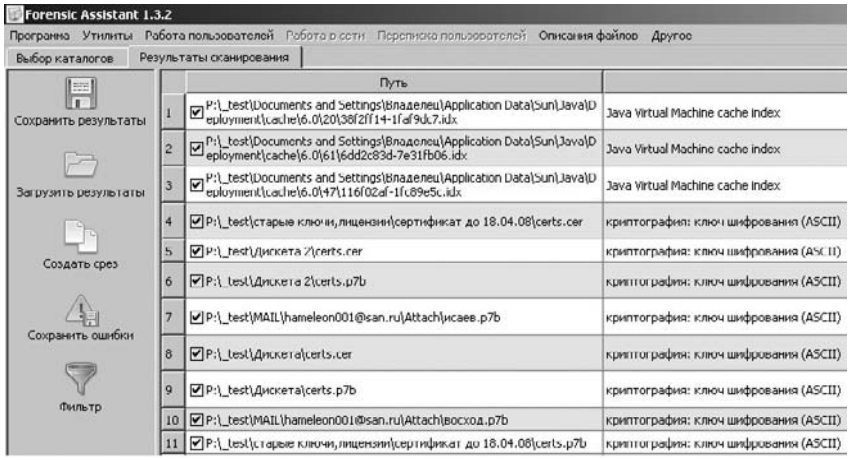
- индексные файлы ОС Windows (index.dat) – все блоки, включая LEAK;
- журналы событий ОС Windows (Event Logs), включая Windows Vista/7 (*.evt, *.evtx);
- иные служебные файлы ОС Windows (Prefetch – *.pf, Link – *.lnk, setupapi.log, *.xml DataColl);
- служебные файлы программ-браузеров (Internet Explorer, Opera, Firefox, Chromium (Google Chrome, Xpom, Yandex.Browser, Chrome OS и тд.));
- кэш виртуальной машины Java;
- файлы троянских программ.

Поскольку для первичного заражения, как правило, используются эксплоиты на сетевых страницах, то имеет смысл осуществлять осмотр кэша Java-приложений, загружаемых на компьютер, с целью установления IP-адреса источника заражения и получения экземпляра вредоносной программы. Для определения конкретной сетевой страницы, ставшей источником заражения (возможно – по цепочке редиректов), необходимо исследовать кэш браузера. В автоматизированном режиме все необходимые исследования позволяет проводить специализированная экспертная программа «Forensic Assistant».

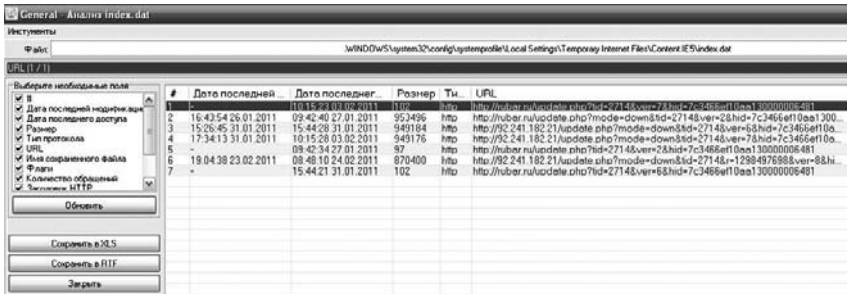
Установление типа обнаруженных на компьютере вредоносных программ является немаловажным этапом экспертного исследования, поскольку эксперт должен определить – можно ли было (с использованием обнаруженных вредоносных программ) осуществить НСД к системе ДБО, или они не имеют отношения к данному компьютерному преступлению. Исследование недетектируемых вредоносных программ возможно с использованием отладчиков или в среде виртуальных машин. Необходимо учесть, что современные вредоносные программы имеют в своем арсенале алгоритмы выявления и противодействия отладчикам и виртуальным машинам.

Адреса, с которых осуществлялся дистанционный доступ к зараженному компьютеру, могут быть обнаружены в журналах работы утилит удаленного администрирования.

В том случае, если перевод осуществлялся с другого компьютера, сведения



Выявление файлов с сертификатами ЭЦП. Снимок экрана специализированной программы «Forensic Assistant»



Выявление адресов, на которые отправлялась информация с компьютера и получались обновления троянцев. Снимок экрана специализированной программы «Forensic Assistant»

об искомом платежном поручении будут отсутствовать на пользовательском компьютере.

Совершению преступлений способствуют существующие проблемы в системах ДБО:

- отсутствие дополнительных программных защит (кроме антивирусов и файерволов) на стороне пользователя;
- отсутствие выраженного внимания банка

к проблемам клиентов (не предлагают фильтрацию по IP, не предлагают современные средства защиты, не проводят своевременное оповещение об угрозах и т.п.);

- нарушения в документообороте банка (утрата документов);
- несовершенство систем ДБО – отсутствие качественной фильтрации поступающих платежных документов на стороне банка (двойная подпись, фильтрация по IP, ошибки с НДС, нет фильтрации контрагентов по «черным» и «белым» спискам и т.д.).

В случае с физическими лицами, реквизиты магнитных банковских карт могут быть получены злоумышленниками как при помощи специализированного оборудования (скиммеров), так и методами социальной инженерии. Хищение денежных средств со счетов граждан осуществляется либо путем снятия денег через банкомат при помощи поддельных пластиковых карт (как правило, «белый пластик», не имеющий нанесенных на него реквизитов банковской карты), либо путем приобретения дорогостоящих товаров в магазинах (в этом случае пластиковая карта подделывается на более высоком уровне). Оборудование и расходные материалы для этих операций приобретаются злоумышленниками через сеть Интернет. В случае выявления поддельных или вызывающих подозрение пластиковых карт в ходе экспертизы требуется установить:

1) соответствие нанесенных на карту реквизитов с информацией на магнитной полосе;

2) корректность информации на магнитной полосе (в том числе – соответствие записанных треков между собой);

3) банк, выпустивший карту, и иные характеристики, указанные на магнитной полосе (актуально для «белого пластика»);

4) информацию на магнитной полосе (для поврежденных пластиковых карт);

5) технические характеристики устройств, использовавшихся для работы с картой (трасология).

Информационное исследование данных магнитной полосы банковских карт позволяет осуществлять программа «Forensic Assistant», начиная с версии 1.3.3. ■

Расследование вирусозависимых компьютерных инцидентов: типичные ошибки пользователей до и после

Борис Шаров, генеральный директор компании «Доктор Веб»

Справка ТБ

Родился 1 августа 1964 года. В 1986 году окончил Институт стран Азии и Африки Московского государственного университета, социально-экономический факультет по специальности «Международные экономические отношения». После службы в Вооруженных силах в 1992–1999 гг. работал в качестве телевизионного журналиста в японской телекомпании. В 1999–2002 гг. принимал участие в российско-японских информационных и образовательных проектах. В 2002–2003 гг. – директор по развитию бизнеса, а позже – коммерческий директор компании «ДиалогНаука», Россия. Бессменный директор компании «Доктор Веб» со дня ее основания. Свободно говорит на английском, французском и японском языках.

Актуальность тематики.

Интерес к данной теме присутствует очень большой, что понятно. И мы были очень рады предоставленной нам возможности выступить на прошедшем семинаре.

При этом надо понимать, что мы, в основном, говорим о ситуации в России, так как о том, что происходит в Беларуси в сегменте расследований инцидентов в электронных системах, мы не осведомлены.

Итак, прежде всего, несколько фактов. МВД и Следственный комитет нашли причины не явиться на данный семинар. Это нормально. Фактически, от банковского сообщества зависит, будет ли это продолжаться. В России ситуация схожая. У нас есть банковский форум, организуемый ежегодно в Магнитогорске. В последний раз организаторам пришлось особо настойчиво и через самых высоких государственных руководителей убеждать управление «К» МВД России присутствовать на мероприятии. Присутствовало, в итоге, не только управление «К», но и ФСБ России. Был даже доклад от них – больше в области рекомендаций. А вот выступление управления «К», которое занимается, в частности, и банковскими хищениями, вызвало фурор. Был поднят вопрос о поголовной зараженности в России людей компьютерными вирусами, большинство из которых являются банковскими троянцами. Много было уделено внимания и такому явлению, как кардинг.

Полицейская статистика говорит об уменьшении числа преступлений в области информационной безопасности. Наше глубокое убеждение – там, где люди говорят о снижении количества преступлений, что-то методологически хромает. Или пытаются что-то скрыть.

В Китае, по некоторым данным, также идет резкое сокращение числа зараженных машин. Почему? На сцену выходят бесплатные антивирусы. Когда они становятся стандартом всей страны, естественно и «сокращается» число зараженных машин. Вредоносные программы просто не детектируются.

В принципе, и Национальный банк, и органы, которые должны этим заниматься, налаживают взаимодействие по решению этой проблемы. Очень хочется призвать банковское сообщество двигаться в сторону обмена информацией, как с Россией, так и с Украиной. Мы попрежнему остаемся единым пространством. Однако наша разъединенность мешает тому огромному потенциалу, который есть у банков в области ИБ, у правоохранительных органов, бороться с киберпреступностью, нацеленной на банковский сектор и его клиентов.

Приведем следующий пример. Не так давно, в конце 2012 года в Казани был арестован один злоумышленник. За ним охотились 3 года. Весьма осторожный и хитрый. На связь он ни с кем и никогда не выходил. По иронии судьбы, в момент обыска у него в квартире была найдена пачка «белого пластика», тех самых поддельных карт. Нашли их с трудом, хотя милиция знала, что они там есть. Не обошлось без казуса, на этой пачке сидел понятой. Ирония в том, что именно в момент обыска ему пришел платеж из Белоруссии в полтора миллиона рублей. Это лишний раз показывает, как динамичны и гибки взаимосвязи тех же злоумышленников. За ними нельзя угнаться только в одной стране, а тем более в рамках одной территории. Очевидно, что эту разобщенность следует искоренять, сводить на нет.

Типичные ошибки и методы их решения.

Теперь перейдем к вопросу о зараженности и огромном количестве мошеннических операций. Специально для противодействия этим процессам мы создали подразделение в нашей компании, которое занимается расследованием вирусозависимых инцидентов. Мы также занимаемся исследованием бот-сетей и ботами, стараемся их не просто детектировать – стараемся детектировать их создателей.

Есть очень важная вещь, которую пора всем понять – если мы не будем бороться за то, чтобы любое компьютерное преступление не оставалось безнаказанными, мы никогда не поборем это зло. Люди на той стороне прекрасно чувствуют и знают законодательные нюансы, желания банков и правоохранительных органов с ними бороться. Они четко представляют, какой условный срок они получат, когда их арестуют, сколько денег надо будет выложить на услуги адвокатов.

Когда мы занимаемся именно расследованиями, снимаем образ диска, начинаем разбираться и пр., мы обсуждаем каждое слово, которое потом передадим экспертам. Оно должно быть выверено «до миллиметра». Как ни странно, самые подготовленные в этой области – адвокаты. Мы боремся за каждое слово в постановлении следователя о проведении экспертизы. Это крайне важно – адвокаты подсудимого в любой момент могут опротестовать неправильно вы-

Продолжение на стр. 31 →

Андэк

Предотвращение мошенничества при проведении банковских транзакций

Павел Ложкин, заместитель генерального директора компании «Андэк»

Справка ТБ

Ложкин Павел Эдуардович, образование – высшее техническое. Закончил Балаковский филиал Саратовского Государственного технического университета, специализация – автоматика в технических системах. Диплом «Передача сигналов аналоговых устройств по оптоволоконному кабелю на большое расстояние с целью минимизации воздействия сильных электромагнитных помех», проект действующий, система внедрена на Саратовской гидроэлектростанции. Опыт работы: компания «РенетКОМ» телеком-провайдер в Саратовской области, руководил группой системного администрирования; «ДельтаБанк» (в настоящее время GE Moneybank), ИТ-аудит и риски, техническое обеспечение ИБ, криптография и защита информации, ведение ИТ-проектов; «Фаберлик», CIO/Директор по ИТ; «СитиБанк», руководство внедрением процессов и управлением рисками в телекоме и ИТ по СНГ и Восточной Европе; «АбсолютБанк», директор по ИБ; в настоящее время в компании «Андэк» руководит направлением по бизнес-рискам и практикам.

Распределение ответственности за потери, произошедшие в результате мошенничества – как основная проблема.

Про мошенничество в различных системах электронных платежей говорят много слов, предлагают различные варианты действий. Но, как показывает практика, в этом классическом противодействии брони и снаряда, побеждает, как водится, снаряд, то есть злоумышленник. Внедрение все новых и новых методов защиты позволяет получить только временную передышку, после чего попытки хищений начинаются по новой и еще в больших размерах, чем прежде. Проблема мошенничества гораздо глубже, чем кажется на первый взгляд, и весьма многогранна – традиционные методы борьбы с подобными преступлениями не работают и вот почему.

Законодательство многих стран не определяет, кто отвечает за потери, произошедшие в результате мошенничества – банк или его клиент. Если ответственность законодательно закрепить за банком (РФ 161ФЗ 9 статья, вступающая в действие с 1.01.2014 г.), то совершенно очевидно, что клиент палец о палец не ударит, чтобы обеспечить свою безопасность: при инциденте, издержки покроет банк. Не то, чтобы клиент совсем не предпринимает никаких шагов по защите своих денег, разумные меры предосторожности, конечно же, будут приняты клиентом, поскольку, несмотря на закрепленную законом ответственность банка, возмещения потерь придётся ждать долгое время, это потребует определенной бумажной волокиты и временных затрат, что попросту неудобно. Однако в этом случае не стоит ждать от клиента высокой заинтересованности и очень активной позиции, он будет делать только необходимый минимум по самозащите от мошенников. Причем, минимум действий, который не потребует от него весомых денежных и временных затрат.

Если же ответственность законодательно возложить на клиента или не оговорить, кто несет ответственность, то банк всегда найдет лазейку, как сделать клиента виноватым и нарушившим какой-либо пункт договора обслуживания, зачастую написанным мелким шрифтом на тридцать третьем листе договора. Возникает обратная ситуация: банк помогает клиенту по остаточному принципу, ведь банк – сугубо коммерческая и весьма прагматичная организация, нацеленная на получение прибыли, а помощь клиенту в подобной затруднительной ситуации только отчасти позволяет эту самую прибыль получить за счет сохранения его лояльности, если удастся этого добиться после подобного инцидента. Поэтому клиент зачастую остается один на один с мошенниками. Обращение же в правоохранительные органы – это довольно сложная процедура в наших реалиях, поскольку необходимо юридическим языком изложить суть обращения и предоставить необходимые доказательства. В противном случае имеется почти стопроцентный шанс получить отказ в возбуждении уголовного дела по формальным признакам: ушлый следователь, которому не хочется возиться, найдет, к чему прицепиться, чтобы отказать в возбуждении уголовного дела. Подготовка необходимых документов и сбор доказательств по факту мошенничества – это весьма сложная и неочевидная процедура, которой занимаются, как правило, специализированные компании, привлеченные для проведения расследования. Сами же правоохранительные органы, как не прискорбно это констатировать, как правило, никакой помощи не оказывают.

Ситуация еще более усложняется ввиду трансграничности современных сетей Интернет: международное законодательство не гармонизировано, границы очень мешают во взаимодействии правоохранительных органов разных стран и, если мошенники находятся за границей, либо украденные деньги снимаются в банкомате за рубежом, многократно снижаются шансы поймать мошенников.

Очень часто клиент в самом начале возникновения инцидента, когда хищение еще можно предотвратить, может заметить аномальную работу системы банк-клиент и позвонить в банк. Но, поскольку клиент зачастую формулирует свои страхи слишком неконкретно: «система как-то странно себя ведет», а техподдержка на стороне банка не очень-то интересуется проблемами клиента, то и совет клиенту выдается минимально простой: «перезагрузите свой компьютер, и все пройдет». Либо, если на стороне клиента уже произвели несанкционированное перечисление денежных средств и уничтожили программу банк-клиента вместе с операционной системой, то просто посоветуют переустановить операционную систему и заново войти в систему банк-клиент. При этом специалист на стороне банка не производит проверки платежей клиента или каких-либо иных аномалий, хотя мог бы, и деньги вполне благополучно отправляются прямиком к мошенникам. Самое обидное, что в этот момент все можно еще было бы

исправить и свести потери к минимуму. Все перечисленные варианты – это реальные каждодневные ситуации из практики. Когда банк не несет значительных рисков и имеет юридические основания все потери перенести на клиента, то и отношение со стороны его персонала будет соответствующим.

Попытки распределения ответственности, когда часть рисков лежит на банках, а часть – на клиентах, также практикуется, но пока и они далеки от идеала, поскольку достаточно сложно провести эту границу, при этом все равно больший вес ответственности переносится на банки. Об этом говорилось на крупнейшей в мире ежегодной конференции по информационной безопасности RSAC 2013, но приемлемых для обеих сторон практических предложений так и не было выдвинуто, кроме предложения полностью переложить риски мошенничества на крупный и средний бизнес.

Распределение полномочий в банковских структурах

Второй большой проблемой, ввиду отсутствия внимания к мошенничествам со стороны банков, является проблема отсутствия ответственного за противодействие мошенничеству внутри банка. Ответственность распределяется между несколькими подразделениями и все происходит ровно, в соответствии с известной поговоркой «у семи нянек дитя без глазу», когда каждое подразделение решает только кусок проблемы, а не всю проблему целиком. Чуть лучше ситуация с пластиковыми картами. Как средство платежа пластиковые карты существуют на рынке уже более сорока лет и методы борьбы с мошенничеством с их использованием уже хорошо изучены, есть выделенные ответственные (fraudofficers) за противодействие мошенничеству. Но пластик традиционно живет в банках несколько обособленно, зачастую имея официально или де-факто свое собственное ИТ-подразделение, свой набор систем и, зачастую, антифрод-систему, встроенную в процессинг, которая решает массу проблем. Поэтому, в общем-то не очень сложная, с точки зрения технических средств по ее автоматизации, проблема противодействия мошенничеству в системах ДБО становится такой болезненной и долго играющей.

В связи с этим следует отметить тот факт, что инженерно-технические подразделения безопасности рассматривают проблему с технической точки зрения, в разрезе имеющихся у инженеров компетенций, пытаясь оперировать техническими терминами при общении с бизнес-подразделениями. Для технических специалистов природа техногенных угроз очевидна, как очевидно и то, что вал таких проблем будет нарастать. Но сформулировать свои выводы на языке рисков и возможных потерь способен далеко не каждый инженер. И поскольку прямых потерь от совершенных мошеннических действий банки не несут (пока это – потери клиентов), то прагматичный бизнес не может и не хочет вникать в технические детали. Поэтому эффективного диалога не получается, что также не способствует повышению скорости в решении проблемы мошенничества. С другой стороны, некорректно утверждать, что этой проблемой борьбы с мошенничествами со стороны банков не занимаются вовсе. Банки все же несут, как минимум, репутационные риски, остается также риск потерять клиента, недовольного тем, что банк не защитил его от мошенников и отказал в выплате потерянных им средств. Но пока проблема не решается эффективно, внимания ей уделяется недостаточно.

Угрозы – методы и средства.

Тем не менее, на сегодняшний день с технической точки зрения для защиты от мошенников сделано уже довольно много: достаточно защищенной от воздействия внешнего злоумышленника является «принимающая» сторона – банк. Каналы связи также имеют серьёзную криптозащиту, и злоумышленники редко охотятся на них, поскольку гораздо проще направить вектор атаки туда, где защита слабее всего: в место инициации транзакции на стороне клиента. При этом наиболее проблемной зоной является компьютер бухгалтера, в особенности в небольших компаниях, где он используется для работы, доступа в интернет и осуществления работы с ДБО. Несмотря на многочисленные предупреждения, носитель (токен) с ключом ЭЦП зачастую подключен все время, поскольку клиенту неудобно и лень переподключать его каждый раз, когда ведется работа с клиент-банком. И это при условии, если используется внешний носитель – токен с ключом ЭЦП. Увы, но еще не все банки перешли к использованию токенов с неизвлекаемым ключом ЭЦП. Впрочем, и это мало помогает при современном развитии технологий проникновения, но все же является определенной защитой. Часто ключи лежат просто на жестком диске компьютера, да еще в папке «C:\Ключи для ДБО», что делает работу для мошенника легкой и приятной.

Существует ряд известных троянских программ, которые используются для заражения распространенных систем ДБО. Это и делает проблему такой острой: поскольку рынок систем ДБО сильно монополизирован и существует всего несколько ключевых игроков, именно под их программы и адаптированы эти трояны.

Среди всех видов мошенничества с электронными средствами платежа наиболее распространено мошенничество с пластиковыми картами, что связано с тем, что данный платежный инструмент известен давно; применяемые технологии устарели, и замена пластиковых карт с магнитной полосой на EMV-карты пока не приводит к улучшению ситуации, поскольку карты выпускаются комбинировано, с EMV-чипом и магнитной полосой, а все операции с чиповой картой обязательно происходят с PIN-кодом. Соответственно, PIN-код перехватить становится легче из-за необходимости его постоянного использования в различных точках. При считывании же магнитной полосы данную карту (уже без чипа) злоумышленники выпускают на «белом» пластике и снимают в ближайшем банкомате все деньги.

Также уязвимым местом в процессе являются банкоматы, скимминг, нашумевший банкоматный вирус, просто поддельные банкоматы, устанавливаемые с целью собрать данные магнитной полосы и получить пин-коды. Эти данные являются товаром сами по себе. Мошенники давным-давно ввели «специализацию»: кто-то занимается технической частью – кражей и продажей данных пластиковых карт, а кто-то покупает эту информацию и осуществляет хищение денежных средств. Однако все это – звенья одной и той же преступной цепи, но, с точки зрения ответственности за преступление, разницы между ними нет.

На стороне банка, как правило, защита достаточно устойчива к взлому, и работают квалифицированные ИТ и ИБ-специалисты, однако, это только одна сторона медали. В этом случае уязвимость носит скорее нетехнический характер, с которой эффективно могут справиться инженеры. Об инсайдерах и внутреннем мошенничестве говорилось много, повторять особого смысла нет. Отметить стоит только то, что инсайдер гораздо опаснее, поскольку возможностей у него куда больше, поэтому необходим комплекс мер, в большинстве своем нетехнических: мониторинг поведения персонала, работа с мотивацией и многое другое. Технические системы плохо защищают от инсайдеров просто потому, что зачастую срабаты-

вают уже после того, как мошенничество совершилось, либо пропускают активность, которую считают легитимной. Именно поэтому инсайдер так и опасен, поскольку действуя в рамках тех доступов к системам, которые выданы ему в соответствии с исполняемыми им служебными обязанностями, он получает совершенно легальный доступ к массе важной информации. И технические системы контроля тут, зачастую, бессильны, поскольку действия инсайдера при совершении мошеннических действий в системах, с точки зрения системы контроля, не изменяются и остаются обычными и легальными. Тут необходимы нетехнические методы: выстраивание процессов, кадровая работа. С технической стороны очень важно обеспечить необходимые защитные средства и выстроить процессы. В частности, если для передачи данных внутри банка используется файловый обмен, то это – постоянная головная боль в плане безопасности: очень сложно и ресурсозатратно контролировать права доступа на файловый ресурс, через который производится этот самый обмен.

Зачастую в разработанных системах изначально кроется процессная уязвимость, например, оператор системы ДБО, который производит привязку сгенерированных клиентом ключей к его ID в системе, делает это единолично и никто не мешает ему привязать не тот ключ, как по ошибке, так и с умыслом. При этом данное событие отследить практически невозможно: в лог-файле системы, о которой идет речь, это событие не отображается. Это – реальный случай. При этом вводить компенсирующие меры и процессно решать этот вопрос достаточно сложно, поскольку потребует создания сложных контролей вокруг системы и высоких затрат на обеспечение безопасности на этом участке, что на практике привело бы к фактическому удвоению штата работающих с системой.

Противодействие – методы и средства.

Во-первых, лекарство должно соответствовать болезни, т.е. универсального технического средства с рубильником «отключить мошенничество», к сожалению, не будет придумано никогда. Бизнес, даже банковский, всегда достаточно индивидуален – в разрезе предлагаемых продуктов/услуг, категорий и моделей обслуживания клиентов, клиентской базы и так далее. Соответственно, риски и меры по их снижению также разнятся.

Во-вторых, для каждого типа систем возможны разные варианты защиты.

Например, можно различными способами обеспечивать защиту на стороне клиента, либо вводить второй фактор аутентификации, использовать независимые средства визуализации подписываемого документа (smarttoken), причем, применять все эти методы, как по отдельности, так и все вместе.

Простым, но при этом весьма эффективным методом защиты, является создание списков контрагентов для каждого плательщика с возможностью его пополнения с дополнительной аутентификацией, в этом случае так называемый белый и серый список. Данный метод основывается на том, что, как правило, компании имеют достаточно фиксированный список получателей платежей, которые можно считать доверенными. При появлении нового получателя тоже можно добавить его в этот список, но только после дополнительной аутентификации, например, путем ввода SMS-ключа или подтверждающего звонка в банк. Иначе платеж не будет проведен. Возможны также черные списки – то есть списки получателей, которые «засветились» в мошеннических схемах и являются априори «не доверенными». В этом случае требуется явное волеизъявление клиента для проведения подобного платежа. Этот метод также применим и для платежей физических лиц, если система позволяет производить перевод средств не по фиксированному списку получателей. Например, только коммунальные платежи, что автоматически является «белым» списком без возможности его модификации клиентом.

Более сложным методом является установка систем анализа транзакций, или, как их еще называют, antifraud системы. Сейчас существует тенденция называть системами противодействия мошенничеству – antifraud вообще все, вплоть до антивирусов и систем «продвинутой» аутентификации. Но стоит всё же ограничиться классом систем, которые способны по заданному алгоритму, с использованием или без использования методов статистического анализа, оперативно принимать решения по отклонению или одобрению финансовой транзакции. По сути, автоматизация белых и серых списков – это и есть антифрод-система первоначального уровня, основанная на статической фильтрации. Системы с использованием методов статистического анализа применяются, как правило, когда в системе обрабатывается множество транзакций для множества клиентов, то есть большое количество клиентов – физических лиц. Система способна создать так называемые «поведенческие» модели, как индивидуальных клиентов, так и групп клиентов с приблизительно одинаковым поведением. Идея в том, что клиенты совершают платежи и покупки все время примерно одинаково, и, если возникают серьезные отклонения в поведении клиента, то подобные операции являются более рискованными и, в зависимости от процесса, могут быть либо заблокированы, либо потребовать дополнительной авторизации (callback, одноразовый пароль по SMS, иные варианты).

Еще одной мерой минимизации потерь, но не противодействия мошенничеству, является введение лимитов. Если ограничить максимальную сумму целиком, либо по операциям в день, либо отдельных типов операции, то можно рассчитывать на то, что в случае реализации сценария fraud, размер потерь будет меньше и позволит минимизировать ущерб. Но от мошенничества это не спасет.

Можно также воспользоваться услугами страхования, но это выгодно не всегда: страховая компания, являясь

коммерческой организацией, играет просто на законах больших чисел, распределяя риски и потери более равномерно по большему удельному числу клиентов, так что при росте клиентской базы уровень расходов на страхование превысит уровень вероятных потерь.

Огромную роль по снижению рисков играет информирование клиентов обо всех движениях по счету, ведение постоянной программы по информированию клиентов о правилах работы с электронными средствами платежей. Это длительный и сложный процесс, тем не менее, очень важный. Основная сложность заключается в том, что большой объем информации необходимо втиснуть в очень маленький объем коммуникации – никто из клиентов не будет читать многостраничный труд формата «Война и Мир», посвященный совершенно прозаическим правилам, которые, тем не менее, надо соблюдать. Если их не соблюдать, то рано или поздно, причем скорее рано, чем поздно, произойдет кража. Из практики, более чем лист-два информации никто читать не станет, поэтому необходимо тщательно разрабатывать систему информирования клиентов. Т.е. по факту проведения экспресс-обучения информационной безопасности, хотя бы в минимальном, необходимом для работы, объеме. Причем это делается для защиты и с целью предотвратить мошенничество, позаботиться о клиенте. К сожалению, активно знакомиться с правилами начинают уже тогда, когда потеряли деньги. Тут работает известная поговорка «пока гром не грянет – мужик не перекрестится».

Варианты рисков разнообразны, также разнообразны методы, средства и способы снижения этих рисков, но совершенно очевидно, в том числе и из вышесказанного, что универсального рецепта на все случаи жизни нет в принципе. Есть большое количество средств защиты, которые различаются по способу применения, ценовому диапазону и многому другому, однако подбирать эти средства надо каждый раз в соответствие с теми рисками, которые максимальны. При этом решение должно быть адекватным по стоимости и эффективным (costeffective). Если прогнозируемые потери невелики, нет смысла ставить дорогую и сложную antifraud систему, вполне возможно обойтись другими методами по снижению рисков и другими защитными средствами. При этом сама по себе защитная система не будет эффективна без выстроенных вокруг нее процессов, подготовленного и обученного персонала.

Нет универсального рецепта, работа по снижению рисков – долгая и сложная, должна вестись на регулярной основе, поскольку риски постоянно видоизменяются. Но вести ее необходимо, в противном случае уровень потерь будет расти очень быстро. ■

← *Начало на стр. 27*

Расследование вирусозависимых компьютерных инцидентов: типичные ошибки пользователей до и после

несенное постановление о проведении экспертизы.

Нюансы в экспертной работе есть и в белорусском законодательстве. Не дело банковского сообщества Беларуси их изучать. Но тем, кого здесь нет, очень бы хотелось пожелать, чтобы они этим буквам закона следовали. Тема очень деликатная. Ведь речь идет о виртуальных вещах, которые не положишь на стол.

Наше выступление также посвящено и типичным ошибкам, которые случаются до действий злоумышленников. Тут идет речь не об информационных структурах банков, не об их системах безопасности. Речь о пользователях. Банки действительно прилагают много усилий, чтобы обезопасить транзакции. Вводятся различные преграды для злоумышленников, и мы это видим. Чувствуется кропотливая работа специалистов-безопасников. С другой стороны, их работа идет в разрез с интересами банковских бизнес-подразделений, которые стремятся проще и быстрее доставить деньги до клиентов. Это противоречие обуславливает некоторую неосведомленность среди пользователей. Пользователи не всегда знают, что антивирус должен стоять на компьютере, что любой банковский троянец перед выпуском в свет проходит тестирование на антивирусах, как платных, так и бесплатных. Если вредоносную программу уже детектируют антивирусы, ее просто не выпустят. Злоумышленники также стремятся определить, как каждый антивирус реагирует на действия их вредоносных программ в живой природе, а это не показывает ни один антивирусный тест. От этого, по сути, зависит успешность работы тех самых злоумышленников. Любые проблемы с антивирусами, с обслуживанием, с обналичиванием тут же оставляют этих людей без куска хлеба.

Многие из тех пользователей, кто пользуется интернет-банкингом, применяют бесплатные антивирусы. Или же не обновляют коммерческие продукты. Много и тех, кто не использует антивирус вовсе.

Как происходит заражение? В основном все начинается с инфицирования сайтов. Не фишинговые, не порнографические, а самые обычные сайты, которыми мы с вами пользуемся: информационные, для бухгалтеров, даже сайты правоохранительных органов. Все это заражается. После того, как на компьютере жертвы оказывается троянец, он может снимать с него все, что угодно. Записывать все, что он вбивает на клавиатуре, снимать видео, делать аудиозапись и пр.

Есть банки, которые, не понимая этого, устраивают многоступенчатую систему защиты на своих ресурсах. Пользователи в процессе этого вводят массивы конфиденциальной, персональной информации о себе. Некоторые требуют ввести и данные кредитной карты пользователя. Это просит банк, не мошенники или фишеры. Так вот, вся эта информация может попасть к злоумышленникам. Не думая о том, как могут быть атакованы пользователи, банк выстраивает условную систему защиты, показывая свою заботу, а в результате все это уходит на сторону. О том, что компьютер заражен, пользователь, естественно, не подозревает.

Что происходит после того, когда деньги жертвы утекли к злоумышленникам? Осознав, что деньги со счета исчезли, люди звонят в банк. Естественно, они тут же устанавливают или обновляют свой антивирус, запускают сканирование. Антивирус свое дело сделает. И все, потом уже никаких экспертиз, ни расследований не будет. В ряде антивирусных продуктов есть функция анонимизации пользователя: история браузера, cookies – все удаляется. В принципе, все это можно и через браузер сделать. Однако когда это делается антивирусом, все приобретает особый смысл. Раз советует антивирус, пользователь, доверяя ему, уж конечно так и сделает. Т.е., антивирус не оставит никаких шансов экспертам что-то потом сделать. Тут речь не только о самой угрозе, но и о пути заражения, что тоже важно понять при расследовании. Мы призываем обращать на это пристальное внимание. Нам бы хотелось, чтобы банки информировали пользователей об этом, держа в голове, что такая экспертиза может понадобиться. ■

ВирусБлокАда

Применение антивирусных программных средств в расследовании инцидентов информационной безопасности

Резников Юрий, руководитель группы по работе с клиентами ОДО «ВирусБлокАда»

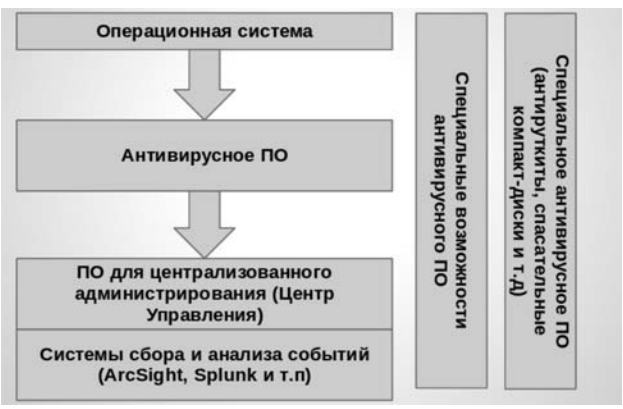
Справка ТБ

Резников Юрий Геннадьевич, руководитель группы по работе с клиентами ОДО «ВирусБлокАда». Образование высшее, специалист по защите информации, радиофизик. В 2010 году окончил факультет радиофизики (сейчас радиофизики и компьютерных технологий) Белорусского Государственного Университета. Защитой информации занимается с 2007 года. Имеет опыт преподавания предметов, связанных с информационной безопасностью.

Расследование инцидентов информационной безопасности большинство специалистов воспринимают как работу с большим количеством дорогостоящих специальных средств, однако мало кто задумывается, что мощный инструмент для расследования инцидентов в большинстве случаев уже установлен на компьютер-жертву. Эта статья посвящена тому, как обходиться малым при расследовании инцидентов информационной безопасности без потери в качестве получаемой информации.

Минималистичное расследование инцидентов.

Ни для кого не секрет, что установка антивируса на компьютеры организации повышает среднестатистическую защищенность, однако при целевых атаках или злонамеренных действиях сотрудников-инсайдеров возможен обход антивирусных программных средств и заражение целевой системы. К сожалению, такие ситуации возможны, и, зачастую, при их возникновении специалисты игнорируют те возможности, которые предоставляет сама операционная система и установленный антивирусный продукт для расследования инцидентов.



Обобщенная схема процесса получения информации об инциденте ИБ

Можно выделить следующие задачи антивирусных программных средств при расследовании:

- предоставить информацию об инциденте, достаточную для начала расследования;
- позволить провести анализ ситуации в ходе расследования;
- принять меры для предотвращения подобных ситуаций в будущем (позволить проанализировать информацию + отправить информацию компании-разработчику средств защиты).

Действительно, большинство присутствующих на рынке антивирусных решений позволяют получить информацию достаточную, по крайней мере для того, чтобы продолжить исследование с применением специальных средств, либо чтобы получить полную картину инцидента информационной безопасности. Если к этой информации добавить данные из операционной системы, то можно получить достаточно полную картину произошедшего инцидента. Схематически процесс получения информации об инциденте можно изобразить так:

Получение информации об инциденте.

Информация, предоставляемая ОС. Основной информацией, предоставляемой операционной системой для расследования инцидента являются журналы событий ОС. **Журнал событий** или *EventLog* – стандартный способ для приложений и операционной системы записи и централизованного хранения информации о важных программных и аппаратных событиях. При исследовании журналов безопасности можно обнаружить:

- вероятное использование уязвимостей. Например, Worm.Win32.Kido вызывает переполнение буфера в процессе svchost, что отражается в системном журнале событий;
- аудит попыток входа в систему;
- обнаружение конфликтов ПО.

Эти данные позволяют сделать первые шаги в расследовании инцидента и, при необходимости, принять соответствующие меры.

Информация из журналов антивируса – современные антивирусные программы сохраняют достаточно информации о своей работе, что позволяет в полной мере использовать их при расследовании инцидентов информационной безопасности. Запись информации может проводиться в нескольких форматах:

- проприетарный формат разработчика антивирусного средства;
- формат системных журналов MS Windows;
- текстовый файл или файл разметки.

Чаще всего информация из этих файлов дублируется в систему сбора статистики и управления антивирусом

в корпоративной сети, однако есть случаи (например, обход вредоносной программой самозащиты антивируса), когда анализ таких журналов может принести больше информации, чем анализ системы статистики и управления.

Возможности продуктов компании «ВирусБлокАда» для расследования инцидентов.

Компания «ВирусБлокАда» имеет достаточный опыт в расследовании инцидентов информационной безопасности, что повлияло на некоторые возможности разрабатываемых компанией продуктов. В аспекте расследования инцидентов информационной безопасности можно отметить следующие продукты:

- Vba32 USB;
- Vba32 ControlCenter;
- Vba32 Antirootkit;
- Vba32 CS.W (Remote Console Scaner).

Модуль Vba32 USB – предназначен для контроля подключаемых к компьютеру USB-флеш накопителей как на отдельно стоящем компьютере, так и компьютерах в корпоративной сети.

Данный модуль предоставляет следующие возможности:

- ограничение работы пользователя только авторизированными USB-флеш накопителями;
- ведение отчета о выполненных операциях с файлами на USB-накопителе;
- интеграция с Vba32 Центром Управления.

Эти возможности позволяют, в том числе, предотвратить инциденты, связанные с использованием личных флеш-накопителей в сети организации.

В файле отчета модуля Vba32 USB можно найти:

- название рабочей станции;
- имя учетной записи;
- время и дата события;
- уникальные номер носителя или имя файла, действия над которым проводились;
- действие, проведенное с носителем информации или файлом (путь к файлу также указывается в отчете).

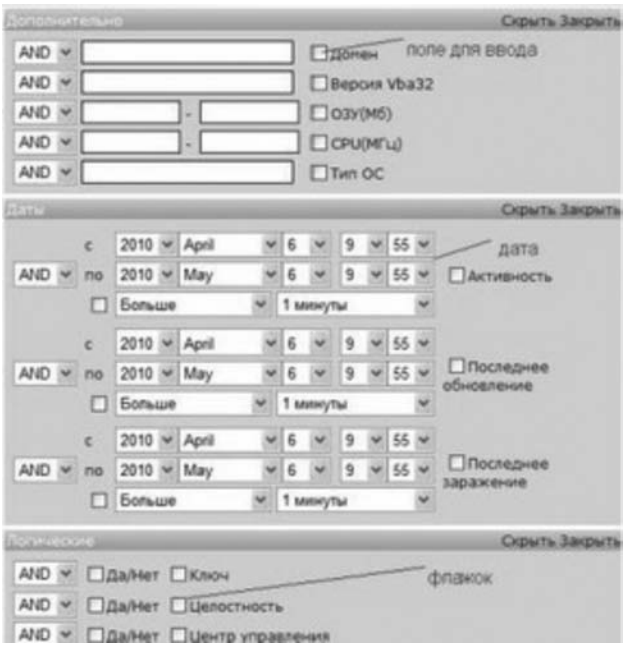
Как видно, предоставляется начальная информация, в том числе для начала расследования инцидентов, связанных с утечкой данных.

***Vba32* Центр Управления** – представляет собой инструмент для сбора статистики и управления средствами антивирусной защиты в корпоративной сети. Для расследования инцидентов важны следующие функции данного продукта:

- Возможность удаленного запуска приложений на компьютере пользователя с правами пользователя SYSTEM.
- Гибкая система фильтрации данных.

Система фильтров предоставляет следующие возможности:

- Фильтрация по характеристикам ПК и комплекса.
- Фильтрация по дате происшествия.
- Логические фильтры для параметров (наличие ключа, целостность комплекса и т.д.).



Приведем простейший пример расследования инцидента с помощью Vba32 Центра Управления.

Исходные данные: активное заражение на одном компьютере в сети, остальные компьютеры заражению не подверглись, Центр Управления содержит множество событий virus.found и virus.cured.

Ход расследования: анализ событий ЦУ показал, что очагом заражения является компьютер, который отправил событие loader.unloaded перед началом заражения.

Результат расследования: приняты административные меры.

Как видно из этого простейшего примера, в некоторых случаях расследование инцидента может быть проведено только с помощью Центра Управления.

***Vba32* Antirootkit** – утилита, предназначенная для глубокого анализа операционной системы и обнаружения и нейтрализации руткитов – программ, обеспечивающих постоянное, устойчивое и неопределяемое присутствие на компьютере. При этом осуществляется поиск как уже известных (добавленных в базу), так и неизвестных типов руткитов.

Для расследования инцидентов полезны следующие функции продукта:

- поиск аномалий в ядре ОС (модули ядра, перехваты системных вызовов, нотификаторы и т.д.);
- анализ запущенных процессов (загруженные и выгруженные модули);
- поиск аномалий в реестре;
- доступ к файловой системе на уровне контроллера жесткого диска. И в этом случае может проводиться проверка с помощью антивирусного ядра;
- продвинутая система самозащиты (технология Vba32 Defender);
- поддержка запуска программы на выделенном рабочем столе.

Vba32 Antirootkit позволяет специалисту увидеть результат полного анализа системы и принять решение, необходимое для продвижения расследования инцидента.

Компания «ВирусБлокАда» всегда готова прийти на помощь пользователям в трудную минуту. ■

Ежегодный отчет Symantec об угрозах интернет-безопасности показал рост объемов кибершпионажа

В апреле 2013 года корпорация Symantec опубликовала ежегодный отчет об угрозах интернет-безопасности (Internet Security Threat Report, ISTR, том 18). Данные отчета демонстрируют резкое увеличение количества направленных атак, объем которых за последний год возрос на 42%. Подобные атаки направлены на кражу интеллектуальной собственности и все чаще оказываются нацеленными на малый бизнес (31% всех подобных атак). Малые компании, представляя ценность сами по себе, могут являться ключом доступа к более крупным предприятиям – их компьютерные сети и системы могут иметь дополнительные привилегии доступа к старшему партнёру по бизнесу. Помимо этого, рядовые пользователи все также остаются уязвимыми перед вирусами-вымогателями и мобильными угрозами, в особенности на платформе Android.

«Из отчета ISTR 2013 ясно, что киберперступники не намерены снижать темпы наращивания кибер-угроз и изобретают все новые способы кражи информации у частных лиц и организаций любого масштаба. Изощренность атак умноженная на сложность современных ИТ, использующих технологии виртуализации, мобильные и облачные вычисления, заставляют компании занимать всё более активную позицию в совершенствовании защиты своей информации и применять технологии «глубокой защиты» от современных угроз», – сказал Стивен Триллинг (Stephen Trilling), технический директор компании Symantec.

Малый бизнес – «путь наименьшего сопротивления» для злоумышленников.

Количество атак на компании со штатом менее 250 сотрудников растет и уже составляет 31% всех атак, что в 3 раза превышает показатели прошлого года. И хотя малые компании обычно не считают себя потенциальными объектами направленных атак, их клиентская и банковская информация, а также их интеллектуальная собственность, вызывают интерес злоумышленников. Также, за счёт отсутствия в малых компаниях инфраструктуры безопасности, злоумышленники зачастую используют их как способ проникновения к своей конечной цели – крупной корпорации.

Количество веб-атак в 2012 году также выросло на 30%. Их основой чаще всего становились взломанные веб-сайты, через которые затем осуществлялись атаки типа watering hole. Суть приема заключается в том, что злоумышленники взламывают веб-сайт, часто посещаемый выбранной жертвой, и размещают на нём источник заражения. После того, как жертва заходит на подготовленный к атаке взломанный сайт, на ее компьютер незаметно устанавливается вредоносная программа. Группа хакеров Elderwood Gang стала первопроходцем в применении такого рода атак – в 2012 году всего за одни сутки им удалось поразить системы 500 организаций.

Промышленные предприятия и информированные сотрудники как главные цели.

В 2012 году интерес злоумышленников переместился с государственных учреждений на промышленные предприятия. Эксперты Symantec считают, что это связано с ростом количества атак на цепочки поставок – злоумышленники находят эти компании наиболее уязвимыми и при этом обладающими ценной интеллектуальной собственностью. Часто через производственные предприятия в цепочке поставок злоумышленники получают доступ к конфиденциальной информации более крупных компаний. При этом руководство предприятий перестало быть самой распространенной целью злоумышленников – чаще всего жертвами таких атак теперь становятся сотрудники, работающие с информацией и имеющие доступ к интеллектуальной собственности (27%), а также менеджеры по продажам (24%).

Вредоносные сайты и атаки на мобильные устройства ставят бизнес и частных пользователей под угрозу.

В прошлом году рост количества вариаций вредоносных программ для мобильных устройств составил 58%, а мобильных угроз, связанных с кражей информации в целом, – 31%. Не следует думать, что это связано с 30% ростом количества уязвимостей в мобильной среде. В операционной системе iOS от Apple было найдено наибольшее количество уязвимостей – 387, но существует всего лишь одна угроза. При этом на платформе Android обнаружено лишь 13 уязвимостей, а угроз – 103, больше, чем на любой другой мобильной операционной системе. Доля рынка, занимаемая Android, открытость платформы, а также множество путей распространения приложений, в которые может быть встроен вредоносный код, делают Android идеальной платформой для вирусописателей.

Кроме того, 61% всех вредоносных веб-сайтов – это легитимные сайты, которые были подвергнуты атаке и заражены вредоносным кодом. В пятерку заражаемых сайтов вошли страницы, посвященные бизнесу и технологиям, а также интернет-магазины. Эксперты Symantec связывают успешность таких атак с наличием у взломанных сайтов незакрытых уязвимостей. Сначала злоумышленники использовали такие сайты для продажи ничего не подозревающим пользователям фальшивых антивирусов, затем эти методы уступили место программам-вымогателям. Через взломанные веб-сайты злоумышленники заражают компьютеры пользователей и блокируют работу с ними, требуя выкуп за восстановление работоспособности. Ещё одним ресурсом, через который активно распространяются вредоносные программы, стала вредоносная реклама – злоумышленники законным образом покупают рекламные места в интернете и используют их для распространения вредоносного кода.

О Symantec

Корпорация Symantec защищает информацию и является мировым лидером в области решений для обеспечения безопасности, резервного копирования и высокой доступности данных. Инновационные продукты и услуги компании защищают людей и информацию в любых средах – от самых маленьких мобильных устройств до центров обработки данных предприятий и облачных систем. Всемирно известная экспертиза Symantec в области защиты данных, аутентификации и обмена данными дает клиентам уверенность в мире информационных технологий. Больше информации доступно по адресу **www.symantec.ru .** ■

Платформа информационной безопасности Symantec: protection, prevention, control

Symantec is Protection.

С недавнего времени среди производителей средств защиты от информационных угроз стала популярной тема о неэффективности использования антивирусных продуктов при создании корпоративных систем безопасности. С каждым годом растет количество таргетированных (направленных) атак, в которых злоумышленники используют технологии и инструменты, разработанные под конкретный атакуемый объект. Наиболее часто используемыми «мостиками» являются уязвимости в системном и прикладном программном обеспечении, некорректные настройки телекоммуникационного оборудования и несоблюдение регламентов прав доступа. Все это, на фоне низкого уровня культуры информационной безопасности пользователей, не оставляет антивирусам никаких шансов. Наличие антивирусной защиты снижает и порог психологической готовности пользователей (и, что наиболее опасно, администраторов систем) к возможным угрозам. Негативным моментом является также временной лаг между появлением зловредного кода, его обнаружением и разработкой противоядия. Согласно исследованиям Symantec, средний срок жизни zero-day уязвимости составляет более полугода. В случае необходимости обеспечения сохранности и высокой доступности корпоративных данных, такой подход является недопустимым и значительно повышает риски и стоимость исправления инцидентов.

Альтернативный вариант защиты критических бизнес-ресурсов заключается в концепции «сохранения целостности». Специальные технологии, реализованные в продукте **Symantec Critical System Protection**, обеспечивают выполнение в вычислительной инфраструктуре ограниченного и заранее определенного перечня приложений (процессов), отслеживают и блокируют нежелательное поведение программ, пользователей и администраторов. Система позволяет создать особую среду обработки данных,

Кочнев Алексей Михайлович, менеджер по развитию бизнеса корпорации Symantec в Республике Беларусь

не подверженную любым внешним воздействиям: разрешаются только санкционированная активность и допустимые изменения, а неизвестные и непредусмотренные процессы считаются ненужными/опасными и запрещаются.

Symantec Critical System Protection позволяет предотвращать: все виды известных и неизвестных информационных угроз, направленные многоуровневые атаки, злонамеренные и непредумышленные опасные действия администраторов, некорректные действия пользователей и приложений, разрушительные конфликты аппаратных и программных компонентов. При этом продукт не требует обновлений сигнатур или других баз и является универсальным щитом против современных угроз.

Решение находит активное применение при защите специализированных систем, выполняющих критически важные задачи (банкоматы и платежные киоски, системы биллинга, веб-серверы, контроллеры домена, операторские места и т.п.), и обеспечивает непревзойденную устойчивость инфраструктур заказчика, сохраняя активы в эталонном состоянии.

Symantec is Prevention.

Наиболее обсуждаемой технологией отечественного рынка информационной безопасности последних 2-3 лет является DLP – комплекс противодействия утечкам конфиденциальной информации. Подогреваемые производителями споры о сравнительных преимуществах той или иной системы, мнимых различиях в скорости и сложности внедрения и прочие манипуляции достаточно умело отвлекают взгляд потенциальных заказчиков от принципиально важных вещей. Во-первых, напомним, что в аббревиатуре DLP ключевой является третья буква – «P» (от Prevention – предотвращение). Система DLP изначально задумывалась как профессиональный инструмент недопущения инцидентов, связанных с несанкционированным распространением корпоративной/ конфи-

Технологии **Symantec Critical System Protection:**

– белые списки (whitelisting) – разрешение на активность приложениям из доверенного списка и по определенному сценарию;
– контроль приложений (sandbox) – создание для каждого приложения/процесса системы индивидуальной политики поведения и доступа к ресурсам системы;
– мониторинг целостности (integrity control) – отслеживание изменений программного кода (операционная система, приложения, файлы) и запрет на непредусмотренное изменение;
– защита сетевых соединений (network protection) – определение и соблюдение правил сетевых соединений.

Symantec Data Loss Prevention позволяет:
– предотвратить несанкционированное распространение и ограничить доступ к конфиденциальной информации неуполномоченных лиц;
– осуществлять мониторинг за широким спектром каналов, по которым возможна утечка информации (рабочие станции, мобильные устройства, серверы, системы хранения, сеть, почтовые системы, буфер обмена, съемные накопители, системы мгновенных сообщений, социальные медиа);
– не допустить возникновения финансовых и репутационных потерь предприятия;
– контролировать исполнение регламента использования корпоративных документов и формировать культуру информационной безопасности сотрудников;
– обеспечить соответствие принятым законодательным нормам и исполнение требований регуляторов.

денциальной информации. А подход, основанный на сборе статистики о перемещении данных и принятии мер по факту совершения нарушений, выглядит более чем странным. Зачем ограничиваться анализом событий постфактум, если можно их предотвращать? Во-вторых, достаточно опасной ловушкой является позиционирование продукта, как средства для решения нескольких (часто противоположных) задач. Полнофункциональная DLP, спроектированная для работы с конфиденциальной информацией, не может всерьез использоваться и для мониторинга рабочего времени сотрудников. Желание клиента получить «решение-для-контроля-всего-в-одном» объяснимо с экономической точки зрения, но неразумно с технической и идеологической сторон. Лучшие мировые практики управления защитой информации и многолетнее лидерство **Symantec Data Loss Prevention** лишь подтверждают эти правила.

Полноценная классическая система DLP позволяет заказчикам ответить на три основополагающих вопроса обеспечения сохранности коммерческих данных: где находится моя конфиденциальная информация? что происходит с этой информацией? как обеспечить ее надежную защиту? **Symantec Data Loss Prevention** – комплексное решение для поиска, отслеживания и защиты конфиденциальных данных с учетом их содержания, работающее вне зависимости от расположения данных: в сети, на устройствах хранения или на конечных точках. Система позволяет обнаружить критически важную для бизнес-процессов информацию и организовать ряд процедур по обеспечению ее сохранности. **Symantec Data Loss Prevention** осуществляет активный мониторинг различных способов использования конфиденциальных данных и сигнализирует о таких операциях. Встроенные механизмы реагирования и расследования инцидентов позволяют принимать корректирующие меры в режиме реального времени.

Symantec is Control.

Центральной проблемой функционирования любой информационной системы являются вопросы управления и управляемости. Современные инфраструктуры характеризуются большим количеством составляющих элементов, многообразием программных и аппаратных платформ, отсутствием унифицированного инструментария мониторинга и управления. Негативными факторами выступают также быстрый (часто непропорциональный) рост систем и недостаточный уровень квалификации персонала. Подобные объекты являются легкой мишенью для злоумышленников, которые могут использовать все доступные уязвимости. В такой ситуации крайне важно владеть актуальной информацией об уровне готовности инфраструктуры к внешним негативным воздействиям. Наиболее доступным и эффективным решением проблемы является платформа сбора и управления событиями (SIEM). Система воспринимает любое событие информационной среды (действия пользователей, поведение приложений, активность оборудования и т.п.) как источник информации и на основе таких событий выстраивает целостную картину происходящего.

Symantec Security Information Manager помогает организациям выявлять угрозы безопасности, направленные на наиболее важные бизнес-ресурсы, определять их приоритеты, анализировать и устранять эти угрозы. Решение выполняет роль центра мониторинга информационной безопасности предприятия, оперативно предоставляя актуальные данные о состоянии защищенности вычислительных ресурсов и формируя рекомендации по обработке инцидентов и минимизации возможных рисков.

Механизм работы **Symantec Security Information Manager** основан на сборе и обработке логов/журналов, генерируемых вычислительными и сетевыми устройствами, программными платформами, средствами обеспечения информационной безопасности (брандмауэры, антивирусы, DLP) и т.д. Активность компонентов инфраструктуры предприятия сопоставляется с поведением пользователей/администраторов и коррелируется с глобальной базой знаний об информационных угрозах Symantec Global Intelligence Network. На основе такого анализа система выявляет уязвимые места в контуре безопасности и помогает обрабатывать возникшие инциденты, уменьшая негативные последствия для бизнеса.

Symantec Security Information Manager позволяет выявить:
– ошибки конфигураций и уязвимости в средствах защиты и информационных системах;
– направленные атаки во внутреннем и внешнем периметре;
– вирусные эпидемии или отдельные вирусные заражения, бэкдоры и трояны;
– попытки несанкционированного доступа к ресурсам;
– мошенничество и технический фрод.

Symantec Security Information Manager отличается простотой внедрения в информационную систему предприятия и широким перечнем поддерживаемых источников данных. Это позволят использовать решение как универсальный центр мониторинга всей доступной инфраструктуры и основной инструмент для оценки эффективности и защищенности ресурсов. ■

Синтез современных технологий в системах комплексной информационной безопасности организации

Никифоров Сергей Никанорович, главный инженер ООО «Нейрон-М»

Информационная безопасность организации (ИБ) – это целенаправленная деятельность с использованием разрешённых сил и средств по достижению состояния защищённости информационной среды организации и обеспечивающее её нормальное функционирование и динамичное развитие – примерно так трактует понятие информационной безопасности Википедия. Попробуем же разложить это определение на ряд составляющих и синтезировать общие схемы и средства для обеспечения максимальной защиты информационных ресурсов от утечек. Говоря об информационной безопасности, необходимо остановить свое внимание на различных аспектах ИБ, так как эту проблему необходимо рассматривать в комплексе – в комплексе различных технологий, средств как программных, так и аппаратно-программных. В данной статье мы будем касаться только технических средств, организационные же методы, имеющие не меньшее значение, отдадим на откуп руководителям предприятий и организаций.

Итак, для обеспечения ИБ необходимо обеспечить ряд мер по организации предотвращения утечек информации по каналам связи (мобильная и проводная связь), утечек конфиденциальной информации через технические средства обеспечения производственной деятельности (компьютерные сети, интернет), защиты от несанкционированного доступа к охраняемым сведениям. Классифицировать различные средства ИБ будем следующим образом:

1. Речевые технологии в системах защиты от несанкционированного доступа (НСД) и удаленного доступа к информационным ресурсам:

средства авторизации и избирательного управления доступом;

системы удаленного голосового доступа к информационным ресурсам.

2. Системы мониторинга сетей:

системы предотвращения и выявления утечек конфиденциальной информации (DLP-системы) и анализаторы протоколов.

3. Средства контроля каналов связи (мобильных и проводных) с применением средств голосовой биометрии.

4. Средства раннего предупреждения (для банковских и других финансовых организаций):

Оповещение и предупреждение по каналам связи недобросовестных клиентов о сроках внесения платежей.

Остановимся подробнее на каждом из указанных пунктов.

1. Речевые технологии в системах защиты от несанкционированного доступа (НСД или СКУД) и удаленного доступа к информационным ресурсам.

Системы управления контролем доступа – это целый спектр хорошо зарекомендовавших себя решений от различных отечественных и зарубежных производителей, поэтому останавливаться на них не будем. Затронем одно из этих направлений, сравнительно новое, но уже набирающее в мировой практике темп – системы голосового управления доступом или, как его часто называют, голосовой ключ. Рост разработок и производства подобных систем в мире за последние несколько лет буквально удвоился. Это связано с последними достижениями в технологиях распознавания голоса. Голосовой ключ – это компьютерная программа, которая идентифицирует, т.е. сравнивает ключевую фразу, произнесенную человеком, и распознает принадлежность голоса данного диктора определенному сотруднику, произнесшему эту фразу, и хранящуюся в базе эталонов. Эта технология может успешно использоваться для удаленного доступа к информационным ресурсам предприятия и прекрасно дополняет биометрические системы доступа по отпечаткам пальцев и парольный доступ. В настоящее время точность идентификации данных систем достигает 95-98%, что делает эту технологию наряду с отпечатками пальцев весьма перспективной.

2. Системы мониторинга сетей и DLP системы.

Основная задача DLP-систем, как известно, минимизация рисков утечек конфиденциальной информации. Большинство современных DLP-систем, несмотря на их многообразие, имеют один общий недостаток – отсутствие контроля ВСЕХ каналов связи. Объективно, конечно, это достаточно сложная задача, особенно в связи с бурным развитием компьютерной техники и беспроводных средств коммуникаций, таких как Wi-Fi, Lan, и других, тем не менее, только максимальный охват контролем всех возможных коммуникационных средств компьютера (беспроводных, USB, принтеров, Skype, ICQ, интернет-пейджеров,

различных зашифрованных вариантов передачи данных) позволит говорить о какой-то надежности использования DLP–систем. В настоящее время, кроме обеспечения контроля максимально возможного числа каналов, все большее значение приобретает оснащение DLP-систем аналитическими функциями, такими как поиск по ключевым словам и фразам, по регулярным выражениям для типизированных данных, учету грамматических словоформ и многое другое. Таким образом выстроим образ идеальной DLP-системы: она должна уметь перехватывать все типы каналов, запрещать или ограничивать выход на заданные каналы, быть достаточно интеллектуальной, т.е. уметь искать нужную информацию по самым различным критериям, «предсказывать» возможное наличие конфиденциальной информации в переданных сообщениях, идентифицировать сотрудника, передавшего конфиденциальную информацию по характерным для него словосочетаниям, голосу (Skype), иметь развитую наглядную систему составления отчетов (графическое отображение, диаграммы, схемы, статистические данные). К сожалению, систем, полностью удовлетворяющих всем описанным требованиям – единицы. Таким образом, для разработчиков DLP-систем поле деятельности, и, следовательно, рынок еще очень большой.

3. Средства контроля каналов связи.

К средствам контроля каналов связи мы относим многоканальные системы мониторинга или записи телефонных переговоров. Не будем подробно останавливаться на этом разделе в силу широкой распространенности различных систем записи речевой информации. Отметим только, что требования к данным системам очень схожи с требованиями, предъявляемыми к DLP-системам, а именно: максимальный охват всех типов линий связи – аналоговые, цифровые потоки ISDN PRI, ISDN BRI, IP-телефония, развитая система отчетности, различные варианты поиска нужных фонограмм по ключевым словам, по голосу (кроме традиционных – по номеру), дате, времени и пр. Многообразие на рынке различных систем записи вовсе не означает, что этот рынок заполнен. Мало кто может предложить сегодня системы, имеющие простой удобный интерфейс, хорошую статистику, удобную подсистему поиска нужной информации по любым критериям, возможность доступа к архиву из любой точки через Интернет, при этом достаточно защищенную от перехвата при передаче по каналам.

4. Средства раннего предупреждения.

К такого рода системам, использование которых характерно для банков, финансовых организаций, можно отнести системы массового автоматического оповещения и предупреждения по каналам связи клиентов о задолженностях, кредитах, необходимости различного рода оплат и т.д. При этом сообщения могут передаваться как голосом при дозвоне до нужного абонента, так и с помощью SMS-сообщений. Требования к этим системам опять же перекликаются с перечисленными выше – работа по любым каналам связи – аналоговым, цифровым, GSM. Здесь так же необходим повышенный интеллект, т.е. возможность записи ответа абонента для последующего анализа, любое заданное число звонков, организация сессии звонков по расписанию, ведение несложного диалога, распознавание голоса абонента для начала вывода ему голосового сообщения. Хотя это направление косвенно относится к безопасности информации, но, тем не менее, оно позволяет сократить расходы и сократить возможные финансовые потери от недобросовестных кредитополучателей. Так по данным, полученным в результате анализа внедренных систем, платежи после проведения сессии предупреждений увеличиваются на 25-30%.

В заключение небольшого обзора остановимся на технологии распознавания голоса, как одного из перспективных для систем защиты информации.

На сегодня известен целый ряд фирм и предприятий, ведущих разработки в области голосовой биометрии. Это известные за рубежом «Neuance», Российские «Центр речевых технологий», «Вокорд» и другие.

В Беларуси работы по созданию системы идентификации, мониторинга каналов связи ведутся группой специалистов ООО «НЕЙРОН-М» под научным руководством заведующего лабораторией распознавания и синтеза речи Объединенного института проблем информатики НАН Беларуси (ОИПИ) доктора технических наук Б.М. Лобанова. Эти разработки, выполненные специалистами ООО «Нейрон-М», уже заслужили одобрение ГЭКЦ (Государственного экспертно-криминалистического центра РБ), апробированы в ряде организаций Беларуси и позволяют сделать смелое предположение о том, что данные технологии будут развиваться и использоваться в системах информационной безопасности предприятий. Система идентификации представляет собой программный комплекс, адаптируемый под базу Заказчика и позволяющий в удобном режиме анализировать голоса абонентов, при этом в режимах «только один» выделяется один абонент, голос которого наиболее подходит под голос испытуемого абонента. Эксперту может быть выдан перечень наиболее подходящих для данного абонента записей, а решение принимает эксперт.

Модули поиска по ключевым словам и фразам сегодня используются в системах записи телефонных переговоров и позволяют оперативно найти нужную информацию, какой бы давней она не была. Также указанные разработки сегодня находятся в приложениях DLP–систем, и в ближайшее время мы увидим их в разработках ведущих производителей систем DLP.

В заключение необходимо еще раз подчеркнуть, что эффективная защита информационных ресурсов, финансовых средств, своевременное раскрытие и предотвращение каналов утечки конфиденциальной информации возможно только при комплексном подходе к организации системы ИБ предприятия или организации.

Полный комплекс оборудования и программного обеспечения по всем вышеописанным вопросам Вам может предоставить ООО «НЕЙРОН-М», Республика Беларусь. ■

Впервые на рынке Беларуси

ГАРАНТИЯ НАДЕЖНОСТИ И КАЧЕСТВА!

СервисСбытАвтоматика

Мы продаем безопасность

СТРЕЛЕЦ

220024, г. Минск,
ул. Стебенева, 12, офис 6

Отдел продаж:
(017) 380 20 21,
(044) 598 09 83,
(044) 598 19 80
Факс (017) 275 61 12

www.ssa101.by

Стрелец – Надежно. Просто. Удобно. Гарантировано!

Каждый Гражданин обязан думать и заботиться о своей личной безопасности, безопасности своей семьи, своего имущества (квартиры, загородного дома, дачи).

Каждый Руководитель обязан думать и заботиться о безопасности предприятия.

Беспроводная пожарно-охранная сигнализация СТРЕЛЕЦ – это надежная защита от несанкционированных проникновений (непрошенных гостей) и возгораний.

СТРЕЛЕЦ позволяет:

- избежать укладки ненужных проводов в квартире, доме, промышленном объекте;
- контролировать систему на любом удалении от места размещения (Вы получаете информацию о состоянии системы по GSM каналу);
- контролировать утечку воды и газа;
- подключать до 400 датчиков к одной системе;
- размещать датчики на удалении до 600 метров от блока управления;
- легко работать с системой, поскольку это не требует специальных навыков и знаний, в том числе при снятии системы для транспортировки (находка для арендаторов зданий и сооружений, а также граждан – Вы переезжаете, СТРЕЛЕЦ переезжает вместо с Вами);
- интегрироваться с любой проводной системой;
- управлять системой как при помощи пульта, так и при помощи компьютера.

220024, г. Минск,
ул. Стебенева, 12, офис 6

Отдел продаж:
(017) 380 20 21,
(044) 598 09 83,
(044) 598 19 80
Факс (017) 275 61 12

www.ssa101.by

Радиосистема СТРЕЛЕЦ

Карачун Петр Владимирович.,
директор ОАО «Завод Спецавтоматика»

Радиосистема СТРЕЛЕЦ была разработана российским предприятием ЗАО «Аргус-Спектр». Группа разработчиков системы была удостоена премии правительства РФ в области науки и техники. На сегодняшний день «Аргус-Спектр» оснастила радиосистемой СТРЕЛЕЦ более 25 000 объектов на всей территории РФ. Кроме того, СТРЕЛЕЦ получил признание и широкое распространение в Европе.

В 2008 году между белорусским предприятием ОАО «Завод Спецавтоматика» и российским ЗАО «Аргус-Спектр» было достигнуто соглашение о внедрении уникальной системы СТРЕЛЕЦ на белорусский рынок и ее производстве на территории Республики Беларусь. В рамках соглашения было создано совместное белорусско-российское предприятие СЗАО «Аргус-Спецавтоматика», которое совместно с российским и белорусским заводами освоило выпуск системы СТРЕЛЕЦ в Республике Беларусь.

После появления СТРЕЛЬЦа в Беларуси, в 2012 году на базе ОАО «Завод Спецавтоматика» было учреждено частное торговое унитарное предприятие «СервисСбытАвтоматика», основной целью деятельности которого стало проведение исследований и работы по внедрению системы на белорусский рынок.

Благодаря слаженной работе команды предприятий на объектах республики стала появляться радиоканальная (беспроводная) адресно-аналоговая система пожарной и охранной сигнализации СТРЕЛЕЦ, которая быстрыми темпами стала набирать популярность по всей территории.

НАЗНАЧЕНИЕ СИСТЕМЫ СТРЕЛЕЦ:

- беспроводная и проводная адресно-аналоговая пожарная и охранная сигнализация;
- беспроводная и проводная система управления оповещением и эвакуацией;
- беспроводная и проводная система автоматического управления пожаротушением;
- система контроля и управления доступом;
- система видеорегистрации;
- автоматический мониторинг по всем каналам связи.

ОСНОВНЫЕ ОСОБЕННОСТИ:

- гибридность системы: «радио» + «провод»;
- интеграция с промышленной автоматикой (LonWorks);
- автоматический мониторинг по всем каналам (Радио, IP-сеть, GSM, Contact ID).

Ключевыми техническими элементами системы являются:

- высокая помехоустойчивость;
- двухсторонний протокол обмена между всеми радиоустройствами;
- 10 радиочастотных каналов передачи (с автоматическим и ручным выбором);
- динамическая маршрутизация;
- до 400 радиоустройств, находящихся в зоне взаимной радиовидимости на одном радиочастотном канале передачи;
- возможность построения адресной пожарной радиосистемы;
- программируемый период передачи контрольных радиосигналов от 12 секунд до 2 минут;
- криптографическая защита сигналов с механизмом динамической аутентификации;
- микросотовая топология системы;
- функционирование в диапазоне рабочих температур от -30 до +55°.

Емкость системы:

- до 16 радиорасширителей;
- до 512 радиоизвещателей и технологических детекторов (до 32 на каждый радиорасширитель);
- до 256 радиоканальных исполнительных устройств и устройств управления (до 16 на каждый радиорасширитель + до 16 глобальных на систему).

Дальность:

- до 600 метров в пределах микросоты;
- до 1000 метров между микросотами;
- до 15 000 метров – 15 участков ретрансляции (при использовании динамической маршрутизации).

Продолжительность работы радиоизвещателей:

- от 3 до 7.5 лет от основной батареи;
- не менее 2 месяцев от резервной батареи.

В отличие от проводных систем пожарной сигнализации, радиосистема СТРЕЛЕЦ способна работать до тех пор, пока функционирует хотя бы один извещатель. Благодаря радиоканальной, «неперегораемой» связи между всеми устройствами система способна контролировать динамику развития пожара в здании, сообщать о ней дежурным центра «101» и мобильного штаба пожаротушения, а также оперативно управлять эвакуацией людей даже после начала пожара.

СТРЕЛЕЦ не использует дорогостоящий термокабель, ему вообще не нужны провода, благодаря чему достигается экономическая эффективность системы, в том числе и за счет сокращения вдвое времени работ по ее монтажу. В ряде случаев, когда необходимо сохранить объект в первозданном виде (церковные фрески, памятники архитектуры, историко-культурные здания и сооружения), а также сохранить эргономику объекта, когда вид кабеля, заложенного в кабель-канал, на стенах и потолках неприемлем, СТРЕЛЕЦ – это единственное возможное решение. ■

Стрелец в Беларуси и России

Клиническая больница им. Петра Великого Санкт-Петербург

Здание Третьяковской галереи

Курский вокзал

Аэропорт Ростова-на-Дону

Костел Святых Сымона и Алены в Минске

Червенский рынок в Лошице (Минск)

Радиосистемой СТРЕЛЕЦ оснащены более 25 000 объектов на всей территории Российской Федерации. Количество беспроводных устройств на объектах колеблется от нескольких десятков до нескольких тысяч. Среди оборудованных в России и Беларуси зданий:

- клиническая больница им. Петра Великого при академии им. И.И. Мечникова (Санкт-Петербург);
- Государственная Третьяковская галерея (Москва);
- ОАО «Уралмашзавод» (Екатеринбург);
- ФГУ «Уральский научно-исследовательский институт охраны материнства и младенчества» (Екатеринбург);
- Курский вокзал (Москва);
- аэропорт Ростова-на-Дону;
- ФГБУ Всероссийский центр экстренной и радиационной медицины им. А.М. Никифорова МЧС России (Санкт-Петербург);
- московская психиатрическая больница №1 им. П.П. Кащенко (Москва);
- городская клиническая больница №1 им. Н.И. Пирогова (Москва);
- госпиталь для ветеранов войн №3 (Москва);
- городская клиническая больница им. О.М. Филатова (Москва);
- городская больница №36 (Москва);
- Архикафедральный костел Святых Сымона и Алены на Красной площади (площади Независимости) (Минск);
- новый Червенский рынок в Лошице (Минск);
- складские помещения УП «Элос» (Минск).

СервисСбытАвтоматика
Мы продаем безопасность

http://ssa101.by/
Республика Беларусь
220024 г. Минск, ул. Стебенева, 12 офис 6-7
+375 (17) 380 20 21

Стрелец в Европе

Королевы в Шотландии (Belmoral Castle)

Canary Wharf Tower в Лондоне

Кембриджский университет

Венгерская Академия Наук

Школа Раттенберг. Австрия

В Объединенном Королевстве под защитой СТРЕЛЬЦА находятся более 70 объектов. В большинстве этих зданий установлена полностью радиоканальная система, в остальных функционируют гибридные системы. Количество беспроводных устройств на одном объекте колеблется от 50 до 3000, в некоторых помещениях использовались извещатели, декорированные под основной цвет интерьера. Среди оборудованных в Англии и других городах Европы радиосистемой зданий:

- резиденция Королевы в Шотландии;
- небоскреб Canary Wharf Tower в Лондоне;
- Кембриджский университет;
- Итонский университет;
- Лондонская библиотека;
- библиотека Лондонского университета;
- Уимблдонский теннисный клуб;
- головной офис Евробанка в Афинах (Греция);
- филиалы банка HSBC в различных городах Великобритании;
- Эдинбургский дворец;
- офис Олимпийского комитета в Лондоне;
- собор Святого Мориса в городе Киларни;
- отели Hilton в Ливерпуле и Royal Beach в Портсмуте;
- офис налоговой службы HMRC в г. Кардифф;
- бизнес-центры Thomas Moore Square, Halam Street, Whitehall Court и др. в Лондоне;
- театры Adam Smith в Шотландии и Old Vic в Лондоне;
- здание муниципалитета Nuneaton and Bedworth;
- здание старой мэрии в Оксфорде;
- медицинский реабилитационный центр Headley Court;
- аэропорт г. Корк;
- Дом Сената в Лондоне;
- Венгерская Академия Наук (Будапешт);
- школа Раттенберг (Австрия);
- здание Королевской оперы Валлонии в г. Льеж (Бельгия);
- резиденция Королевской семьи (Голландия).

Информация о компаниях

Symantec Corporation

www.symantec.ru
Год основания: 1982
Контактные лица:
Кочнев Алексей Михайлович, менеджер по развитию бизнеса в Республике Беларусь
Производство: программные средства защиты информации и обеспечения высокой доступности данных

Альфа Портал, ООО

224014, г. Брест, ул. Писателя Сергея Смирнова, 165/1
Тел.: (0162) 20-86-13, (029) 725-45-30 , (029) 326-46-76
E-mail: info@microdigital.by
Сайт: www.microdigital.by
Год основания: 2007 г.
УНП: 290479641
Контактные лица:
- Громик Ирина, специалист по сбыту;
- Войтухович Ирена Васильевна, директор.

Производство: полный комплекс продукции для CCTV и IP-видеонаблюдения.
Услуги: прямые поставки в Республику Беларусь продукции для CCTV и IP-видеонаблюдения.
Поставка: прямые поставки в Республику Беларусь полного комплекса продукции для CCTV и IP-видеонаблюдения.
Дистрибьютор компаний: MICRODIGITAL Inc.

АльфаСистемы, ООО

220090, г. Минск, Логойский тракт, д. 22а, оф. 206, 207
Тел.: (017) 262-84-64, 268-05-36
Факс: (017) 265-12-59
E-mail: info@cctv.by
Сайт: www.cctv.by
Год основания: 2005 г.
УНП: 190598104
Контактное лицо: Гаврютиков Александр Анатольевич, директор.
Услуги: технические консультации, поставка оборудования, гарантийное и послегарантийное обслуживание систем видеонаблюдения, систем контроля и управления доступом.
Дистрибьютор компаний:
- Samsung Techwin (Корея);
- AXIS Communications (Швеция);
- CBC (Ganz/Computar) (Япония);
- Arecont Vision (США);
- IFS (США);
- ComNet (США);
- LevelOne (Германия);
- Videotec (Италия);
- TOPCAM (Китай);
- SC&T (Тайвань);
- Widearea Times Technology Co. (Китай);
- ITV (РФ).

ВирусБлокАда, ОДО

220088, г. Минск, ул. Смоленская, 15 – 803б
Тел./факс: (017) 294-84-29
E-mail: info@anti-virus.by
Год основания: 1997
УНП: 101294617
Контактное лицо: коммерческий директор Резников Геннадий Константинович
Лицензии:
№01019/50 на право осуществления деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи, выдана ОАЦ при Президенте РБ, действительна до 14.12.2014.
Сертификаты:
21 декабря 2006 г. компании получила сертификат соответствия системы менеджмента качества проектирования, производства и технической поддержки программного продукта требованиям белорусского стандарта СТБ ИСО 9001-2001 и немецкого DIN EN ISO 9001: 2000 (ежегодно компания проходит подтверждение соответствия).
Услуги:
Разработка, внедрение и эксплуатация программного обеспечения, предназначенного для защиты от воздействия вредоносных программ в промышленных и иных организациях республики для замещения аналогичных импортных продуктов;
Экспорт разработанного ОДО «ВирусБлокАда» национального программного обеспечения, предназначенного для защиты от воздействия вредоносных программ, способного конкурировать с лучшими мировыми аналогами.
Проекты и разработки:
- комплекс антивирусных программ Vba32;
- автоматизированное рабочее место администратора «Комплекса VBA32»;
- система фильтрации нежелательной электронной почтовой корреспонденции в Национальном банке Республики Беларусь, функционирующей совместно с компонентами комплекса Vba32 программных средств защиты от воздействия вредоносных программ и др.

Нейрон-М, ООО

220119, г. Минск, ул. Тикоцкого, 16, оф 75в
Тел./факс: (017) 261-49-63, (029) 661-49-63, (029) 142-45-18
E-mail: info@neuron-m.by, kv_home@mail.ru
Год основания: 2010
УНП: 191338429
Поставка:
DLP-системы, системы записи телефонных переговоров, системы оповещения по каналам связи, система идентификации по голосу
Проекты и разработки:
системы идентификации по голосу, системы поиска по ключевым словам, распознавание речи, многоканальная запись аудиоинформации
Дистрибьютор компаний:
Атом Парк (РФ), Нетворк Профи (РФ), Вентор (РФ)

НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (НИИ ТЗИ), НП РУП

220088, г. Минск, ул. Первомайская, 26/2
Тел./факс: (017) 294-01-71, 285-31-86
E-mail: info@niitzi.by
Сайт: www.niitzi.by
Год основания: 1986
УНП: 100036784
Контактное лицо: директор Картель Владимир Федорович.
Лицензии:
- № 01019/0531779 на право осуществления деятельности по технической защите информации, в том числе криптографическими, включая применение электронной цифровой подписи методами выдана ОАЦ при Президенте РБ, действительна до 20.03.2012;
- № 02010/9833 на право осуществления охранной деятельности выдана МВД РБ, действительна до 12.06.2013;
- № 03070/0336515 на право осуществления деятельности, связанной с криптографической защитой информации и средствами негласного получения информации выдана КГБ РБ, действительна до 13.04.2013;
- № 02240/0069106 на право оказания деятельности по оказанию юридических услуг; выдана Министерством юстиции РБ, действительна до 29.07.2014; – № 03130/0256499 на право осуществления деятельности, связанной с продукцией военного назначения выдана Государственным военно-промышленным комитетом РБ, действительна до 24.04.2014.

Сертификаты:
- сертификат соответствия Государственного комитета по стандартизации Республики Беларусь, что система менеджмента качества оказания услуг по проведению научно-исследовательских и опытно-конструкторских работ в области технической защиты информации; аттестации объектов информатизации и систем защиты информации, проведению испытаний средств защиты информации; проектированию и монтажу систем защиты информации, охранной и пожарной сигнализации, систем видеонаблюдения, контроля доступа, локальных вычислительных сетей; разработке и производству программных и программно-аппаратных средств защиты информации соответствует требованиям СТБ ISO 9001-2009;
- аттестат аккредитации Государственного комитета по стандартизации Республики Беларусь, что испытательная лаборатория по требованиям безопасности информации соответствует критериям Системы аккредитации Республики Беларусь и аккредитована на соответствие требованиям СТБ ИСО/МЭК 17025.

Услуги: аудит систем защиты информации, информационных ресурсов и систем на информационную безопасность; разработка политик безопасности, заданий по безопасности, сопутствующих нормативно-методических документов; подбор, сертификация, поставка и установка средств защиты информации; сертификационные испытания программных и аппаратно-программных продуктов информационных технологий (ИТ), технических средств защиты информации на соответствие требованиям безопасности информации, оценка заданий по безопасности; создание систем защиты информации информационных систем и автоматизированных систем в защищенном исполнении, их аттестация. специальная проверка защищаемых помещений и технических средств на наличие возможно внедренных специальных технических средств негласного съема информации; подготовка, аттестация объектов информатизации на соответствие требованиям руководящих и нормативных документов по безопасности информации, сопровождение и периодический инструментальный контроль аттестованных объектов информатизации; проектирование и монтаж вычислительных сетей, защищенных от утечки информации по техническим каналам.

Разработки:

1. **Устройство системы технических средств для обеспечения оперативно-розыскных мероприятий.** Предназначено для съема и обработки информации, передаваемой конкретными пользователями услуг электросвязи по сети передачи IP– трафика.
2. **Аппаратно-программный комплекс «Авангард».** Предназначен для криптографической защиты конфиденциальной информации, передаваемой по первичным цифровым каналам E12.
3. **Носитель специализированный «Носитель».** Предназначен для разделения/сборки секретов при организации хранения криптографических ключей, контроля доступа к конфиденциальной информации, шифрования данных и сохранения зашифрованных данных на стандартном USB флэш-накопителе.
4. **Устройство защиты линий электропитания и заземления от утечки информации «Рокот».** Предназначено для активной защиты объектов СВТ от утечки информации за счет наводок по линиям электропитания и заземления.
5. **Комплекс защиты информационных сетей «IP-барьер».** Предназначен для защиты от несанкционированного доступа ресурсов сети организации (ведомства) при ее подключении к внешним сетям (например, Интернет) и при объединении отдельных локальных сетей организации в единую защищенную сеть.
6. **Программно-аппаратный комплекс средств для гарантированного уничтожения информации на магнитных носителях «Информация».** Предназначен для уничтожения конфиденциальной информации, хранящейся на жестких магнитных дисках.
7. **Программно-аппаратный комплекс «Филин».** Предназначен для проведения специальных исследований средств вычислительной техники в диапазоне частот от 9 кГц до 1800 МГц, контроля защищенности помещений от утечки информации по акустическим и виброакустическим каналам в диапазоне частот от 100 Гц до 10 кГц.
8. **Программный комплекс эталонных тестовых средств «Эталон».** Предназначен для формирования периодических последовательностей информативных электрических комбинаций для проведения специальных исследований.
9. **Программно-аппаратный комплекс для выполнения ремонта средств вычислительной техники «Ограничение»**, содержащих информацию ограниченного распространения, и восстановления хранящейся на них информации.
10. **Аппаратный комплекс для транспортировки магнитных носителей «Транспорт».** Предназначен для предотвращения несанкционированного доступа к транспортируемым магнитным носителям.
11. **Распределенная система радиомониторинга «Беседь»**, размещаемая на подвижном объекте, выполняет функции радиомониторинга и пространственной локализации (пеленга) источников излучений.
12. **Средство защиты информации от утечки по цепям электропитания ИБП «Стриж».** Предназначено для подавления индустриальных радиопомех и защиты информации от утечки по цепям электропитания в однофазной сети в широком диапазоне частот.
13. **Автоматизированный мобильный комплекс «Сож».** Предназначен для специальных исследований средств вычислительной техники и контроля посторонних сигналов в местах применения средств вычислительной техники и средств связи с повышенными требованиями к защите информации.
14. **Комплекс автоматизированный мобильный «Шум-3М».** Предназначен для проведения измерений параметров акустических и виброакустических сигналов при проведении инструментального контроля защищенности объектов информатизации.
15. **Детектор поля.** Предназначен для оперативного обнаружения радиопередающих прослушивающих систем промышленного шпионажа.
16. **Фильтр-ограничитель «Гомий».** Предназначен для обеспечения защиты от утечки речевой информации через двухпроводные линии телефонных сетей, цепи систем директорской и диспетчерской связи за счет ограничения сигналов акустоэлектрических преобразований и подавления сигналов ВЧ-навязывания.
17. **Автоматизированный испытательный комплекс для измерения побочных электромагнитных излучений**, состоящий из GTEM камеры, рабочего места оператора с комплектом автоматизированной измерительно-регистрирующей аппаратуры, средств видеонаблюдения за объектом испытаний и специального программного обеспечения.
18. **Программный комплекс «Криптотестер».** Предназначен для автоматизации процессов тестирования реализаций криптографических алгоритмов.
19. **Аппаратура считывания «Мираж».** Обеспечивает считывание, отображение, криптографическую обработку считанной с радиочастотных идентификаторов информации и информационный обмен по проводному и беспроводному каналам связи с центром обработки информации.
20. **Сканер «Контролер»** – программно-аппаратное средство контроля эффективности защиты распределенных информационных ресурсов от воздействия компьютерных атак.

Дистрибьютор ЗАО «Конструкторское бюро «ПРИБОР».
Дилер ЗАО «Научно-производственный центр Фирма «НЕЛК».

Частное торговое унитарное предприятие «СервисСбытАвтоматика»

СервисСбытАвтоматика
Мы продаем безопасность

220024 г. Минск, ул. Стебенева, 12 офис 6-7
Юр. адрес: 223062 Минская обл., Минский р-н, Луговослободской с/с (р-н д. Прилесье), М4, 17-й км, здание ООО «Спелпайс-Плюс», 2, каб.23
Телефон/факс: (17) 275 61 12, (17) 380 20 21, (44) 5980 983, (44) 5981 980
E-mail: info@ssa101.by
Сайт: www.ssa101.by
Год основания: 2012
УНП: 691430930
Контактные лица:
Жихарев Александр Станиславович, руководитель отдела продаж, (17) 380 20 21, (44) 5980 983
Лицензии:
№02300/2709, решение МЧС РБ от 02.04.2012 г. №15км, срок действия – 5 лет.
Сертификаты:
№0128571 от 05.10.2012г. срок действия – 5 лет (ОАО «Завод Спецавтоматика»)
№0210454 от 10.08.2010г. срок действия – 5 лет (СЗАО «Аргус-Спецавтоматика»)
Производство:
«СервисСбытАвтоматика» – только продажа оборудования.
Пожарная и охранная сигнализация, оборудование и материалы охранной и пожарной сигнализации (СЗАО «Аргус-Спецавтоматика», ОАО «Завод Спецавтоматика»).
Услуги:
Проектирование, монтаж, пуск-наладка, сервисные и гарантийные услуги, обслуживание систем (ОАО «Завод Спецавтоматика»).
Поставка:
Охранные и пожарные материалы и оборудование любого производителя.
Объекты, на которых установлена радиосистема СТРЕЛЕЦ:
Червенский рынок в Лошице (г. Минск), Архикафедральный собор Святого Имени Пресвятой Девы Марии (Минск), складские помещения УП «Элос» (Минск).
Дистрибьютор компаний:
СЗАО «Аргус-Спецавтоматика», ОАО «Завод Спецавтоматика».

Сталвиском, ООО

ЭНЕРГИЯ ЛИДЕРА SKYROS CORPORATION

220007, г. Минск, ул. Володько, 12-102
Тел./факс: (017) 205-48-24
E-mail: sale@stalviscom.by
Сайт: www.stalviscom.by
УНП: 191194104
Контактные лица: Стабровский Александр Леонидович, заместитель директора по общим вопросам.
Поставка:
- цифровые системы безопасности;
- системы видеонаблюдения;
- системы контроля и управления доступом;
- домофоны;
- переговорные устройства;
- замки, доводчики;
- шлагбаумы, приводы для ворот;
- турникеты, ограждения, металлодетекторы;
- системы оповещения.

Дистрибьютор компаний: официальный представитель «Skyros», VideoNet, PandaCCTV, Microdigital Inc., NSGate.

Сфератрэйд, ОДО

СФЕРАТРЭЙД
сфера вашей безопасности

220118, г. Минск, ул. Машиностроителей, 29-117
Тел: (017) 341-50-50, (029) 641-50-50 Velcom, (029) 541-50-50 МТС
E-mail: info@secur.by
Сайт: www.secur.by
Год основания: 1995 г.
УНП: 100972915
Контактное лицо: Малаховский Денис Святославович, директор.
Лицензия:
- № 02300/50 на право осуществления деятельности по обеспечению пожарной безопасности, выдана МЧС РБ, действительна до 10.02.2016 г.

Услуги:
- технические консультации по вопросам обеспечения безопасности любого уровня сложности;
- обследование и экспертная оценка состояния технических средств безопасности на объектах административного, производственного и других назначений;
- составление технического задания и проекта;
- поставка оборудования;
- гарантийное и послегарантийное обслуживание поставляемого оборудования.

Поставка:
- IP и CCTV-системы видеонаблюдения;
- системы контроля и управления доступом;
- системы охранно-пожарной сигнализации;
- системы защиты товаров от краж;
- системы аварийного оповещения и звуковой трансляции;
- сопутствующие материалы для монтажа и др.

Дистрибьютор компаний: AXIOM, MOBOTIX AG (Германия), SALTO (Испания), Truen (Корея), ZAVIO (Тайвань), NUUO (Тайвань), Roger (Польша), KT&C (Южная Корея), Fujinon (Япония), Pinetron (Южная Корея), GSN Electronic (Израиль), Rielta (РФ), LOB (Польша), Elmes (Польша), QUIKO (Италия), JIS (Испания), Kenwei (Китай), Seoul Commtech Co. (Южная Корея), PERCo (РФ), ITV (РФ), JSB Systems (РФ), AccordTec (РФ), Elesta (РФ), Bolid (РФ) и др.

Унибелус, СП ООО

UNIBELUS

220033, г. Минск, ул. Нахимова, 10
Тел./факс: (017) 291-15-05, 230-72-40
E-mail: info@unibelus.com
Сайт: www.unibelus.by
Год основания: 1994 г.
УНП: 100834637
Контактное лицо: Забабуха Юлия Аркадьевна, генеральный директор.
Производство: система трансляции и оповещения о пожаре «АРИЯ».
Услуги: от консультации и проектирования до пусконаладочных работ и последующего сервисного обслуживания всех слаботочных сетей.
Поставка: систем пожарной сигнализации, трансляции и оповещения, конференц-связи и синхроперевода, видеонаблюдения, контроля доступа, пожаротушения, мультимедийной, локально-вычислительные сети, охранной сигнализации, периметральной системы охраны, противокражной диспетчеризации; телефония; часофикация; радиофикация; система автоматизации.
Дистрибьютор: Arecont Vision (США), Aiphone (Япония), Amtel Security (США), Autec (Германия), AVerMedia Information (Тайвань), Avalon s.r.o (Чехия), Cisa (Италия), CEM Systems, TYCO Group (Северная Ирландия), CBC (Ganz, Computar), CISCO (США), Cominfo A.S. (Чехия), Daiwon optical (Корея), DNH (Норвегия), FEIG Electronic (Германия), Green (Чехия), JVC Professional Europe (Германия), JTS Professional Co., JTS (Тайвань), IKME (Германия), Kocom (Корея), LG Iris (США), LTD (Тайвань), Matting Schauer (Австрия), Openers&Closers (Испания), OT Systems (Гон-Конг), Panasonic (Япония), PERCO (РФ), Samsung Techwin (Корея), STA-Grupa (Латвия), Suprema Inc. (Ю.Корея), TOA (Япония), Tasker (Италия), TAIDEN Industrial Co., Ltd. (Китай), Win4net (Корея), Артон, ЧП (Украина), ТПД Паритет (РФ), Тахион (РФ), Технос-М (РФ) и др.

FOR A GOOD **REASON**

GRUNDIG

Инновационные системы видеонаблюдения от немецкого производителя

Официальный дистрибьютор в Республике Беларусь - компания «АльфаСистемы»
г. Минск, Логойский тракт 22а, офис 207
Тел./факс: (+375 17) 262 84 64, 268 05 36 / 265 12 59
info@cctv.by www.cctv.by

УНП 190598104

UNEX
системы видеонаблюдения

www.unexpro.ru

3 МЕГАПИКСЕЛЯ
WDR
Преодолевая контрастность освещения

Исключительная четкость и яркость изображения даже в условиях высокой контрастности

Мегапиксельные камеры UIP-E D-серии сочетают в одном изображении светлые зоны, снятые с высокой скоростью затвора, и темные зоны, снятые с низкой скоростью затвора. Встроенный режим sens-up обеспечивает четкое изображение даже при низкой освещенности

До 3 мегапикселей
Работа при низкой освещенности
Двойная скорость затвора при WDR
WDR до 120 дБ

УНП 100834637

ONVIF

UNEX
системы видеонаблюдения

СП «Унибелус» ООО, г. Минск, ул. Нахимова, 17, Тел.: +375 (17) 291 15 05
info@unibelus.com www.unibelus.by