Проблемы обеспечения безопасности критически важных инфраструктур

Картель Владимир Федорович, директор Государственного предприятия «НИИ ТЗИ»

Информационные системы и их сети являются неотъемлемыми компонентами таких критически важных инфраструктур, как управление государством, энергетика, транспорт, банковская сфера, жизнеобеспечение населения и др. Критически важные объекты информатизации (КВОИ) этих инфраструктур во многих странах уже стали объектами кибернетических атак отдельных нарушителей, криминальных групп, государственных структур. Воздействие на КВОИ сектора экономики в настоящее время является одним из основных направлений враждебных действий в отношении любого государства.

КВОИ представляют собой широкое множество компьютерных систем и средств, управляющих критически важными процессами или уникальным оборудованием на объектах отраслевых инфраструктур, нарушение функционирования которых может иметь существенные отрицательные последствия по многим аспектам.

Успешная кибернетическая атака на КВОИ может привести к тяжелой техногенной катастрофе, большому экономическому ущербу, гибели людей, нарушению систем управления государством, обороной и, в конечном итоге, к нарушению национальной безопасности.

Понятия «кибернетическая атака», «информационная война» стали признаками главной проблемы сегодняшнего дня — обеспечения безопасности кибернетического пространства страны.

Анализ безопасности национальных инфраструктур показал, что большинство жизненно важных отраслей экономики уязвимы к возможным кибернетическим атакам.

Отсюда вытекают стратегические цели обеспечения национальной безопасности в рассматриваемой области:

– идентификация и обеспечение гарантий защиты тех инфраструктур, систем управления и их активов, которые считаются критически важными для национальной безопасности;

– государственный контроль за обеспечением защиты КВОИ критически важных инфраструктур;

– обеспечение безопасности критически важных инфраструктур и их активов путем последовательного выполнения специальных мероприятий по созданию совместной окружающей среды, в которой органы власти и управления на всех уровнях (государственном, региональном, локальном) и негосударственный сектор могут лучше организовать их защиту;

– своевременное предупреждение субъектов информационного пространства страны об опасности кибернетических атак и оказание помощи при защите или восстановлении тех критических инфраструктур и их КВОИ, которые сталкиваются с определенной неизбежной угрозой.

Защита критических инфраструктур и КВОИ от незаконного вмешательства в их функционирование является основной задачей поддержания внутренней экономической, политической стабильности и национальной безопасности в целом. Проблема обеспечения безопасности КВОИ таких инфраструктур должна рассматриваться по нескольким основным направлениям.

Основные направления обеспечения безопасности КВОИ

Создание системы правовых нормативных актов, обеспечивающих организацию действенной системы управления безопасностью критических инфраструктур.

Эта система должна устанавливать обязанности государства и владельцев инфраструктур по обеспечению нормального функционирования, защите критически важных объектов этих инфраструктур от кибернетических и иных атак, защите населения и окружающей среды от техногенных катастроф, связанных с авариями на объектах этих инфраструктур.

В Республике Беларусь решение этой задачи начато с принятия Концепции национальной безопасности, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. N 575. В ней впервые обеспечение надежности и устойчивости функционирования КВОИ отнесено к основным национальным интересам в информационной сфере, а нарушение функционирования КВОИ — к основным потенциальным либо реально существующим угрозам национальной безопасности. Несовершенство системы обеспечения безопасности КВОИ признается существенной внутренней угрозой национальной безопасности.

В развитие положений Концепции национальной безопасности приняты ряд нормативных правовых актов, одним из которых является Указ Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации». В соответствии с Указом создается Государственный реестр КВОИ, утверждено Положение об отнесении объектов информатизации к критически важным, обеспечении и контроле их безопасности.

Вместе с тем следует отметить, что законодательное поле Республики Беларусь еще не соответствует современным требованиям правовой охраны объектов критически важных инфраструктур, а документы, регламентирующие деятельность по обеспечению информационной безопасности критически важных инфраструктур и их объектов, в должном объеме еще не разработаны.

Создание системы правовых нормативных технических актов (ТНПА), устанавливающих современные требования к обеспечению безопасности КВОИ на всех этапах их жизненного цикла.

В развитие Указа Президента Республики Беларусь № 486 Институтом (НИИТЗИ) в 2011 году по поручению Оперативно-аналитического

центра при Президенте Республики Беларусь выполнена научно-исследовательская работа «Киберзащита», в рамках которой разработан ряд ТНПА, устанавливающих классификацию КВОИ по уровню безопасности, общие требования к их защите и профили защиты в соответствии с классами безопасности, учитывающие повышенные требования к надежности функционирования и готовности компьютерных систем при обращении к ним.

Особое внимание в республике уделяется проблеме информационной безопасности строящейся АЭС. Защита КВОИ АЭС, к которым относятся компьютерные системы контроля и управления реактором, обеспечивающими системами и коммуникациями, системы, относящиеся к защите реактора, системы охраны и др. является основой обеспечения безопасности станции в целом, защиты населения и окружающей ее среды от выбросов ядерных материалов, вызванных нарушением функционирования этих систем и управляемого ими оборудования.

Следует признать, что положения национальных стандартов, разработанных в Республике Беларусь, а также стандартов, реализованных путем прямого введения стандартов ИСО (серии 27000, 15408 и др.) ориентированы на достаточно простые в архитектурно-технологическом и организационно-административном плане объекты. Это обстоятельство — дополнительный источник уязвимостей КВОИ, которые в большинстве отраслевых инфраструктур являются специальными промышленными компьютерными системами.

Поэтому при разработке стандартов для АЭС использованы лучшие достижения мировой практики, представленные в стандартах и руководствах международных и национальных организаций (МЭК, МАГАТЭ, ISACA и др.), в большей степени ориентированных на промышленные системы управления.

АЭС относится к особо опасным и режимным предприятиям. Поэтому следует рассмотреть вопрос разработки и аттестации ее систем контроля и управления, важных для безопасности, и их компонентов с применением требований военной приемки.

Необходима также разработка нормативных документов, учитывающих мировой и национальный опыт обеспечения безопасности критически важных промышленных объектов и специфику инфраструктур национального экономического сектора (энергетика, промышленность, транспорт, жизнеобеспечение населения и т.п.), содержащих требования по реализации и контролю эффективных мер защиты автоматизированных систем управления такими инфраструктурами и их технологическими процессами.

Разработка новых методов и средств защиты КВОИ

Основное внимание должно быть уделено повышению надежности и расширению функциональных возможностей средств защиты КВОИ. Гарантия безопасного функционирования КВОИ в значительной степени обеспечивается качеством обслуживания и мониторингом безопасности КВОИ в процессе их эксплуатации. Это, в свою очередь, требует использования современных подходов к организации защиты, в частности, предупреждения несанкционированного доступа к его активам и быстрого восстановления функционирования КВОИ в случае реализации угрозы.

Потенциальным направлением исследований в этой области должны стать проекты по созданию автоматизированных систем мониторинга безопасности, позволяющие обнаруживать угрозы КВОИ, оценивать их корреляцию и реагировать на них в режиме реального времени.

Сертификация персонала

Персонал, работающий на КВОИ, должен быть сертифицирован на профессиональную компетентность в соответствии с ролью каждого в задаче обеспечения качества функционирования и безопасности КВОИ. Институтом разработаны два стандарта, касающиеся требований и порядка сертификации персонала для критически важных систем, которые могут применяться для организации и оценки качества подготовки персонала КВОИ.

Важную роль в процессе информационной безопасности КВОИ инфраструктур играет осведомленность административного персонала в вопросах безопасности.

Соблюдение правил информационной безопасности является сегодня важнейшим компонентом «культуры безопасности» любого предприятия.

Международное сотрудничество

Создание «виртуальной аналитической среды», которая соединит в одно целое тех, кто осуществляет сбор, распределение, анализ и использование информации об угрозах критически важных инфраструктур и способах противодействия им, сегодня может стать основой инвестиционной и технической политики в области использования компьютерных технологий во всех отраслях.

Ее создание особо важно для наших стран, поскольку наши критические инфраструктуры (электроэнергетика, передача нефти и газа и др.) взаимосвязаны, носят трансграничный характер и их надежное функционирование важно не только для Республики Беларусь и России, но и для других стран.

Вместе с тем следует учитывать, что международное сотрудничество в области кибернетической безопасности будет существенно сдерживаться отсутствием согласованных законов и соответствующего инструментария для преследования нарушителей и принудительного исполнения норм международного права.

Таким образом, при создании системы противодействия кибернетическим атакам на КВОИ критических инфраструктур необходимо:

– проведение системных научных исследований и прикладных работ в данном направлении при активном участии государственных и коммерческих структур, работающих в данной области;

– тесное взаимодействие государственных органов, организаций и бизнес структур на национальном и международном уровне при проведении мероприятий, направленных на поиск источников угроз, атак и защиту КВОИ;

– комплексный подход к обеспечению информационной безопасности подконтрольных объектов, предполагающий скоординированную систему мер и мероприятий, моделей, механизмов и инструментальных средств на всех уровнях его реализации (правовом, административном, программно-техническом и др.);

Эти задачи решаются в заданиях Союзной программы и соответствующих программ Республики Беларусь.

Государственное предприятие "НИИ ТЗИ"
220088, г.Минск,
ул.Первомайская, д.26, к.2
Тел.: (17) 294-01-71
Факс: (17) 285-31-86
E-mail: info@niitzi.by
www.niitzi.by