Игорь ШЕРЕМЕТ: «Мы планируем кардинально исправить ситуацию с защитой информации в АСУ ТП на предприятиях ОПК»

Интервью с членом Военно-промышленной комиссии при Правительстве Российской Федерации

– В чем, на ваш взгляд, специфика рисков и угроз информационной безопасности АСУ ТП КВО применительно к оборонно-промышленному комплексу (ОПК)?

– Специфика состоит в том, что указанные системы являются приоритетными целями для кибератак со стороны потенциального противника. Ряд последних инцидентов показывает, что ведется целенаправленная разработка вирусных и специальных информационных технологий, предназначенных как для воздействия на технологические системы оборонных предприятий, так и для раскрытия используемых промышленных технологий, параметров изделий, объемов производств и т. д. К сожалению, использование в ОПК технологий иностранного производства существенно усложняет задачи парирования указанных атак.

– Какова, по вашим оценкам, реальность угроз кибератак на КВО и что можно сказать об их происхождении? Отличается ли ситуация от состояния дел в иных, гражданских, отраслях?

– Реальность угроз кибератак на КВО не вызывает никакого сомнения. Источниками таких атак могут быть спецслужбы иностранных государств и международные террористические организации, не исключаются промышленный шпионаж и другие проявления киберпреступности.

В случае коммерческих организаций нападению зачастую подвергаются цели, наиболее доступные и привлекательные для злоумышленников в плане финансовой выгоды. Что касается ОПК, то у противника заведомо больше технологических и людских ресурсов для организации атак. Такие атаки нацелены на конкретные производства и, как правило, больше связаны со скрытым сбором информации на постоянной долговременной основе.

– Как вы оцениваете состояние вопроса с защитой информации в АСУ ТП КВО на предприятиях ОПК? Насколько «равномерна» ситуация по отрасли? Можно ли говорить о примерах отдельных структур и холдингов, где данному вопросу уделяется достаточно внимания?

– В нормативном плане нам известны наработки ФСТЭК России по вопросам защиты информации в ключевых информационных инфраструктурах, а также отраслевые стандарты ТЭК. Однако на практике, если говорить в целом о предприятиях ОПК, состояние данного вопроса мы оцениваем пока как неудовлетворительное. Это связано с дефицитом специалистов в области информационной безопасности именно АСУ ТП, сведением вопросов информационной безопасности просто к физическим и административным мерам, наличием недоверенных программно-аппаратных изделий зарубежного производства, отсутствием средств и процедур анализа защищенности и т. д. Наш опыт говорит о том, что ситуация с защитой информации в АСУ ТП крайне неравномерна, причем не только в разных структурах, а даже внутри организаций на уровне отделов. Мы планируем кардинально исправить ситуацию, о чем свидетельствует обсуждение нового федерального закона и последние совещания в Совете Безопасности РФ и Военно-промышленной комиссии, в частности путем инициирования разработки комплекса нормативно-правовых актов в данной области.

– Каковы планы ВПК в данном вопросе? Какие меры и шаги планируется предпринять для исправления ситуации? Какова должна быть роль Совета по АСУ при ВПК?

– Роль Совета по АСУ при ВПК состоит в том числе и в формировании принципов построения эффективной системы защиты информации критически важных объектов на национальном уровне.

Приоритетными мерами, на наш взгляд, могут стать:

- совершенствование нормативно-методической базы в области тематических исследований и сертификации элементов инфраструктуры АСУ ТП КВО;
- внедрение систем централизованного мониторинга событий информационной безопасности;
- создание центров по тестированию защищенности, осуществляющих периодическое тестирование на возможность взлома АСУ ТП КВО;
- создание облачных технологий аудита безопасности программного кода;
- специальная подготовка специалистов ВПК в области методов, используемых противником для проведения атак;
- стимулирование научных изысканий в области разработки

эффективных механизмов защиты АСУ ТП КВО;
- развитие отечественной электронной промышленности и др.

– В свете подготовки федерального закона о защите критической информационной инфраструктуры России, будет ли ВПК формировать дополнительные требования для оборонной отрасли? Какие принципы регулирования должны/могут быть заложены в эти документы?

– Успешная деятельность оборонной отрасли может осуществляться только в условиях контроля и поддержки со стороны компетентных структур. Основными принципами регулирования должны стать:
- соответствие нормативно-методической базы современному уровню развития информационных технологий;
- приоритетность реальной защиты над формальным выполнением требований, внедрение систем и технологий анализа защищенности;
- приоритетность систем защиты информации отечественного производства, контроль за применением ИТ-решений иностранного производства.

– Как может/должен вписаться процесс наведения порядка в этом вопросе в общий вопрос модернизации предприятий ОПК? Учитывая мнение многих экспертов, о необходимости обеспечения защиты АСУ ТП на этапе внедрения и невозможности защиты уже работающей АСУ, как могут быть скоординированы эти процессы?

– Совершенно верно, информационную безопасность системы проще обеспечить в случае, если о требованиях безопасности вспоминают на этапе проектирования и внедрения, а не после ввода в эксплуатацию. Поэтому мы должны выработать четкие требования и набор методических документов, которые бы позволяли выстраивать комплексную систему защиты на всех этапах жизненного цикла АСУ ТП. Важным моментом является внедрение систем менеджмента информационной безопасности АСУ ТП, например.

– Насколько критично, на ваш взгляд, «засилье» западных продуктов на предприятиях ОПК? Насколько реально сегодня «закрыть» все вопросы отечественными разработками? Возможен ли компромиссный вариант?

– Последние новости показывают, что «засилье» западных (да и восточных) продуктов весьма критично на предприятиях ОПК. В случае недостатка контроля подобные решения зачастую содержат различные недекларируемые производителем возможности, которые, например, могут позволить получить удаленный доступ к системе, вывести оборудование из строя при определенных условиях и т. п.

Компромиссный вариант возможен только в случае строгого государственного контроля. В качестве мер по снижению указанных рисков можно назвать: приоритетное внедрение отечественных передовых наработок, использование программных компонентов с открытыми исходными кодами, аудит безопасности и сертификация иностранной продукции, а также постоянный анализ защищенности, контроль и мониторинг безопасности. Безусловно, следует обеспечить максимальное стимулирование создания и развития отечественных ИТ-корпораций, способных конкурировать на международном рынке. ■

Тенденции на рынке DLP

В ходе состоявшейся в Москве конференции DLP-Russia 2013 вниманию аудитории были представлены два свежих аналитических отчета. Согласно «Глобальному исследованию конфиденциальной информации в I полугодии 2013 г.», выполненному Аналитическим центром InfoWatch, за полгода в мире было зафиксировано 496 случаев утечки конфиденциальной информации, скомпрометированы более 258 млн записей, в том числе финансовые и персональные данные. Число «российских утечек» выросло почти на треть по сравнению с аналогичным периодом прошлого года – зарегистрировано 42 случая утечки конфиденциальной информации из компаний на территории РФ.

Больше всего утечек информации (93,8%) связано с персональными данными. Основными источниками таких утечек являются госорганы наряду с медицинскими учреждениями. Доля утечек из государственных и муниципальных учреждений остается стабильно высокой по всему миру. Аналитики делают вывод, что уровень защищенности конфиденциальной информации во всем мире по-прежнему очень низкий.

Информационно-аналитический центр Anti-Malware.ru провел анализ рынка средств защиты от утечек конфиденциальных данных в России. По темпам роста 2012 г. оказался рекордным для российского DLP-рынка – суммарно 64%, превзойдя сделанные годом ранее прогнозы. По мнению аналитиков, это связано с принципиальным выходом DLP на широкий рынок клиентов, т. е. за рамки нишевого решения для узкого круга крупных и богатых компаний-инноваторов. Другим драйвером рынка стало принятие DLP-решений в качестве неотъемлемого элемента практически любой системы безопасности крупнейших российских компаний.

Доли основных игроков отечественного рынка DLP в 2012 г. распределились следующим образом: InfoWatch – 38,9%; «Инфосистемы Джет» – 22,5; Zecurion – 18,1; Websense – 9,9; Symantec – 5,0; McAfee – 1,1; GTB Technologies – 0,6%. По объемам продаж лидируют InfoWatch (20,4 млн долл.), «Инфосистемы Джет» (11,8 млн долл.) и Zecurion (9,5 млн долл.). При этом объемы продаж InfoWatch и «Инфосистемы Джет» оценивались с учетом не только разрабатываемого ими ПО, но и сопутствующих услуг, а также лицензий на необходимые сторонние продукты. Наибольший рост продаж по сравнению с 2011 г. показали компании InfoWatch (94,3%); Websense (52,9%); McAfee (50%).

Ожидается, что в 2013 г. рынок продемонстрирует рост на уровне 45–50%, достигнув объема в 76–78 млн долл.