Лось А. Б., Кабанов А. С., Водолаженко А. А.

ПРОБЛЕМЫ СОЗДАНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ ЭФФЕКТИВНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ

Аннотация. *В статье рассматриваются проблемы создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы страны. Дан анализ мировой правовой практики в части защиты от информационных угроз и анализ решения данного вопроса в России. Приведены основные этапы реализации атак на информационные системы и структура системы их обнаружения и нейтрализации. Обоснована необходимость создания эффективной системы противодействия компьютерным атакам, отмечены сложности на пути ее создания, в частности, дан анализ состояния и перспектив развития отечественной электронной промышленности. На основе проведенного анализа предложены и обоснованы варианты решения данной задачи, сформулированы основные выводы и рекомендации для ее решения. Для решения поставленных в статье задач применяется метод теоретического анализа исходных данных в различных областях рассматриваемого вопроса, метод обобщения полученных результатов и выработки необходимых путей решения. Актуальность рассматриваемой проблематики связана с постоянно обостряющимся противостоянием мировых держав в информационном пространстве и открытым втягиванием ряда стран в информационные войны. Предлагаемая статья является реакцией на указ президента России о создании эффективной системы защиты страны от угроз в информационной сфере. Научная новизна работы состоит в проведении теоретического анализа всех сторон данной проблемы, включающего анализ мирового информационного права, состояние отечественной элементной базы, разработок в области программного обеспечения. На основании проведенного анализа авторами предложены пути создания государственной системы защиты от информационных угроз.*

Ключевые слова: *информационные войны, информационное оружие, компьютерные атаки, обнаружение компьютерных атак, конвенция, парадигма, уязвимость информационной системы, угрозы информационной системе, электронная промышленность, стандарт информационной безопасности.*

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com
DOI: 10.7256/2073–8560.2014.5.11942

Введение

Стремительно нарастающий интерес к проблематике киберпространства во многом связан с активностью развитых стран в вопросах кибервойн и кибербезопасности. Приставка «кибер» к известным терминам «война», «оружие», «безопасность» означает, как это принято в научной литературе, применение данных терминов к информационной сфере и сфере информационных технологий. Одной из причин возможных конфликтов в информационном пространстве и, в частности, возникновения кибервойн, является отсутствие международных документов, ограничивающих разработку и применение кибероружия.

С точки зрения международного права наибольший интерес представляют два документа, в которых, так или иначе, затрагиваются вопросы информационного противоборства:

1. Конвенция Совета Европы «О киберпреступности»[1] (далее — Конвенция Совета Европы) открытая для подписания 23 ноября 2001 года (вступила в силу в 2004 году).
2. Проект Конвенции Организации Объединённых Наций (ООН) «Об обеспечении международной информационной безопасности»[2] (далее — Проект Конвенции ООН) подготовленный в 2011 году Российской Федерацией в рамках Шанхайской организации сотрудничества (ШОС).

В результате появления указанных документов в мировом правовом пространстве сформировались две правовые парадигмы, ни одна из которых в настоящее время не принята ведущими странами. Следствием данного обстоятельства является тот факт, что в случае начала крупномасштабных конфликтов в киберпространстве, правовые инструменты остановки агрессии будут малоэффективны. Следует отметить, и это, в частности, отражено в военных доктринах многих стран, что серьезный конфликт в киберпространстве может повлечь за собой реальный военный конфликт. Кроме того, целью кибератак могут быть объекты повышенной опасности, в частности, атомные электростанции, гидроэлектростанции, сбой в работе которых может повлечь техногенные катастрофы. Таким образом, важность проблемы правового регулирования киберпространства, с точки зрения международного права, сложно переоценить. Рассмотрим основные правовые парадигмы, существующие на настоящий момент.

В проекте Конвенции ООН дается определение ключевым понятиям, таким как «информационная война», «информационная безопасность», «информационное оружие», «терроризм в информационном пространстве». Прописаны вопросы сохранения суверенитета государства над его информационным пространством, а также положения, направленные на защиту от «действий в информационном пространстве с целью подрыва политической, экономической и социальной систем другого государства, психологической обработки населения, дестабилизирующей общество».

Во многом проект Конвенции ООН является противовесом Конвенции Совета Европы, которую западные страны представляют как документ «глобального» характера в вопросах кибербезопасности. Противников Конвенции Совета Европы, в том числе и Россию, в частности, не устраивает статья 32 данного документа, в которой речь идет о «трансграничном доступе». Содержание статьи 32 упомянутой

[1] Конвенция об обеспечении международной информационной безопасности (концепция), Электронный ресу-рс: http://www.scrf.gov.ru/documents/6/.

[2] Проект Конвенции Организации Объединённых Наций (ООН) «Об обеспечении международной информацио-нной безопасности», Электронный ресурс: http://www.scrf.gov.ru/ documents /6/.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2014.5.11942

Конвенции позволяет спецслужбам одних стран проникать в компьютерные сети других стран и проводить там операции без уведомления национальных властей. Противники Конвенции Совета Европы считают, что следует говорить обо всём комплексе мер, связанных с возможным противоправным (враждебным) использованием информации или информационно-коммуникационных технологий. Сторонники Конвенции настаивают на том, что достаточно ограничиться вопросами киберугроз. Положения Конвенции Совета Европы исключают из сферы международно-правового регулирования информационно-психологические операции, которые в последние годы осуществляются всё чаще, в частности, через социальные сети. Любая попытка внести эти вопросы в круг проблем кибербезопасности или информационной безопасности рассматривается сторонниками Конвенции Совета Европы как желание оказать давление на гражданское общество, а также как угроза свободе слова и усиление авторитарных тенденций.

Сложившиеся международные правовые противоречия привели к тому, что Россия оказалась недостаточно защищена от различного вида угроз в информационной сфере.

В связи с этим, закономерным является решение руководства страны о создании собственной системы защиты от возможных угроз в информационной сфере, закрепленное в Указе Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»[1].

[1] О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютер-ных атак на информационные ресурсы Российской Федерации: Указ Президента РФ от 15.01.2013 № 31с, Режим доступа: cons/cgi/online.

Атаки на информационные системы и их обнаружение

Вопросы исследования информационных атак и методов их обнаружения достаточно широко представлены в научной и технической литературе[2 3 4].

Еще несколько десятилетий тому назад компьютерные системы были преимущественно однопользовательскими и обменивались информацией по низкоскоростным каналам. Построение сетей на основе коммутации пакетов позволило значительно повысить скорость обмена информацией. В настоящее время любая деятельность, связанная с обменом информацией не обходится без использования компьютерных сетей. Пропускная способность и охват самой крупной сети — сети Интернет постоянно возрастает. Это способствует развитию распределенных приложений для работы по всему миру. Такие системы широко используются в областях кредитования, страхования, здравоохранения, права, военных приложений, связи и многих других. Совместное использование информационных ресурсов позволяет в значительной мере повысить качество обслуживания потребителей, эффективность работы бизнеса и государственных организаций. Таким образом, для организаций и отдельных пользователей характерна высокая степень связанности через открытые сети и, следовательно, зависимость от бесперебойной работы и защищенности информационных потоков.

Вместе с тем, повсеместное внедрение сетей увеличило количество потенциальных злоумышленников, имеющих доступ

[2] Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети, М., Горячая линия, Телеком, 2013, 220 с.

[3] Лукацкий А. Обнаружение атак, СПб: БХВ, 2001, 625 с

[4] Корт С. С. Теоретические основы защиты информации, М: «Гелиос АРВ», 2004, 233 с

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com
DOI: 10.7256/2073–8560.2014.5.11942

к открытым системам. Одним из опасных видов преступной деятельности в сети Интернет являются так называемые сетевые кибератаки.

Предотвращение сетевых атак — одна из самых сложных задач в области защиты информационных систем. Большинство современных информационных систем имеют распределенную структуру, в основе их построения лежит использование сетевых технологий. Очевидно, что обеспечение эффективной работы таких систем зависит от способности противостоять злонамеренным действиям, которые направлены на нарушение работы, как самой сети, так и информационной системы, функционирующей в ее рамках.

Данные интернет — источников[1], в частности, ежегодные отчёты Института Компьютерной безопасности CSI[2], Координационного Центра Немедленного Реагирования США CERT[3] и Центра реагирования на компьютерные инциденты Российской Федерации RU-CERT[4], свидетельствуют о том, что количество сетевых атак продолжает расти, а методы, которые используют преступники, постоянно развиваются и совершенствуются. В то же время современные системы обнаружения вторжений еще не совершенны и недостаточно эффективны с точки зрения безопасности. Поэтому работы в этом направлении необходимы и актуальны.

Любые атаки нарушителей реализуются путём активизации той или иной уязвимости системы. Примерами уязвимостей могут являться некорректным образом составленная политика безопасности, отсутствие определённых средств защиты или ошибки в используемом программном обеспечении. На рисунке 1 показаны примеры уязвимостей, атак и их возможных последствий**.**

Информационная атака представляет собой совокупность действий нарушителя, приводящих к нарушению безопасности информационной системы. В результате успешно реализованной атаки нарушитель может, например, получить несанкционированный доступ к информации, нарушить работоспособность системы или исказить содержимое данных. В качестве потенциальных целей атаки могут выступать серверы, рабочие станции пользователей или коммуникационное оборудование. В общем случае любая атака может быть разделена на четыре стадии:

1. *Стадия рекогносцировки*. На этой стадии нарушитель старается получить как можно больше информации об объекте атаки, на основе которой планируются дальнейшие этапы атаки (например, тип и версия операционной системы, список пользователей, зарегистрированных в системе, сведения об используемом прикладном программном обеспечении и др.).
2. *Стадия вторжения*. На этом этапе нарушитель получает несанкционированный доступ к ресурсам тех систем, на которые совершается атака.
3. *Стадия атакующего воздействия*. Данная стадия атаки направлена на достижение нарушителем тех целей, для которых и предпринималась атака. Прим ерами таких действий могут являться нарушение работоспособности, кража конфиденциальной информации, хранимой в системе, удаление или модификация данных системы и др. При этом атакующий может также осуществлять действия, которые могут

[1] Сабадаш В. Деятельность центров реагирования на компьютерные инциденты: опыт зарубежных стран. Электронный ресурс: http://cybersafetyunit.com/deyatelnost-tsentrov-reagirovaniya-na-kompyuternyie-intsidentyi-kak-sredstvo-protivodeystviya-internet-oshennich-estva-opyit-zarubezhnyih-stran/?lang=en.

[2] Институт Компьютерной безопасности CSI, Электронный ресурс: http://www. gocsi.com.

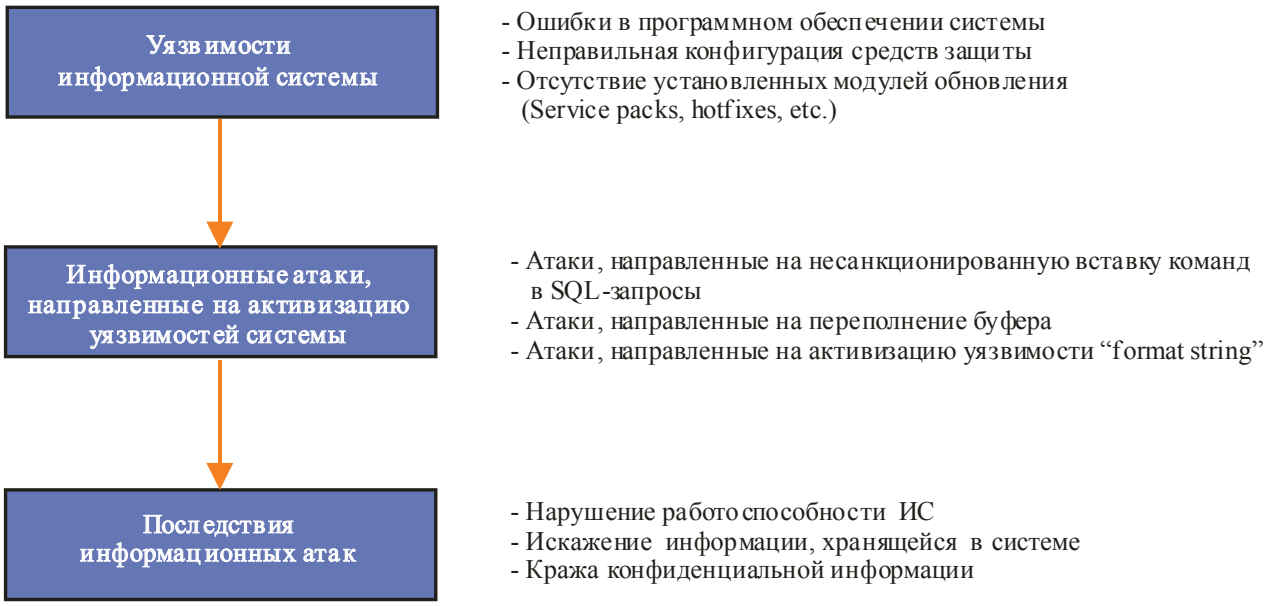
[3] Координационный Центр Немедленного Реагирования США CERT, Электронный ресурс: http://www.cert.org .

[4] Центр реагирования на компьютерные инциденты Российской Федерации RU-CERT, Электронный ресурс: http://www.cert.ru

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2014.5.11942

Рис. 1. Примеры уязвимостей, информационных атак и их последствий



быть направлены на удаление следов его присутствия.

4. *Стадия дальнейшего развития атаки.* На этом этапе выполняются действия, которые необходимы для продолжения атаки на другие объекты.

Процесс обнаружения информационных атак, представленный на рисунке 2, начинается со сбора исходных данных, необходимых для вывода о проведении атаки. Примерами таких данных являются:

- сведения о пакетах данных, передаваемых в системе;
- информация о производительности программно-аппаратного обеспечения (вычислительная нагрузка на процессор, загруженность оперативной памяти, скорость работы прикладного программного обеспечения и др.);
- сведения о доступе к файлам;
- информация о регистрации новых пользователей в системе и др.

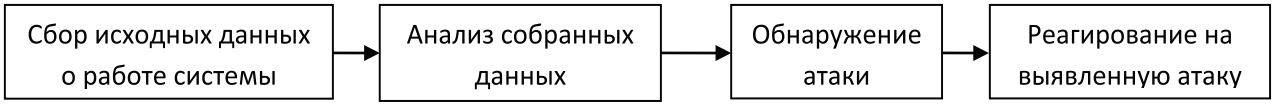
Сбор исходных данных осуществляется при помощи специализированных датчиков системы обнаружения атак, размещаемых в информационной системе. Система обнаружения может включать в себя два типа датчиков — сетевые и хостовые. Сетевые датчики предназначены для сбора информации о пакетах данных, передаваемых в том сегменте информационной системы, где установлен датчик. Хостовые датчики предназначены для сбора информации о событиях, возникающих на компьютерах где они установлены. Примерами такой информации являются сведения о сетевом трафике, поступающем на этот хост, а также системные события, регистрируемые в журналах аудита операционной системы хоста. При этом на одном узле может присутствовать одновременно несколько хостовых датчиков, предназначенных для сбора различной информации. Информация, собранная сетевыми и хостовыми датчиками, анализируется системой обнаружения с целью выявления возможных атак нарушителей.

Проблемы создания отечественной Системы защиты от компьютерных атак

Рассмотрим существующие проблемы на пути создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на инфор-

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com
DOI: 10.7256/2073–8560.2014.5.11942

Рис. 2. Схема процесса обнаружения информационной атаки



мационные ресурсы страны, необходимость создания которой очевидна[1 2].

Одной из главных проблем создания данной системы является отсутствие в стране единой политики в области обеспечения информационной безопасности. Несмотря на наличие в Совете Безопасности России межведомственной комиссии по информационной безопасности, многие вопросы защиты информации решаются в разных министерствах и ведомствах по-своему, ввиду отсутствия единой, проработанной идеологии, политики и нормативной базы.

Среди программно-технических проблем, в свою очередь, необходимо выделить следующие проблемы:

- отсутствие собственного программного обеспечения, операционных систем, в том числе и защищенных. Существующие сертифицированные операционные системы и программное обеспечение создаются, как правило, на основе свободно распространяемого программного обеспечения (freeware) и к отечественным разработкам их можно отнести весьма условно;
- отсутствие собственной элементной базы. Состояние отечественной электронной промышленности ведет к использованию «условно отечественного» аппаратного обеспечения (схемотехнические решения);
- телекоммуникационное оборудование на всей территории страны преимущественно иностранного производства. В связи с этим, например, критичной является проблема использования эталонных генераторов сетей иностранного производства. Использование не доверенного телекоммуникационного оборудования создает серьезные риски работоспособности сетей страны;
- топология транспортной сети страны требует пересмотра и перестройки, в частности, с точки зрения ее живучести. До недавнего времени при построении многих сетей, в том числе и государственных, вопросы обеспечения живучести и надежности были на втором плане, что привело к наличию многих уязвимостей в части обеспечения доступности.

Следствием программно-технических проблем, в свою очередь, являются следующие проблемы:

- отсутствие доверенного оборудования и программного обеспечения систем обнаружения компьютерных атак;
- отсутствие доверенного оборудования и программного обеспечения систем противодействия компьютерным атакам.

Следует отметить, что системы и продукты, имеющие соответствующие сертификаты ФСБ и ФСТЭК России не могут быть гарантированно отнесены к доверенным. Им можно оказать только определенную степень доверия — оправданный риск. По мнению авторов, использование сертифицированных систем базирующихся на иностранном аппаратном и программном обеспечении оправдано, с точки зрения возможного риска, только в системах, не относящихся к критически важным.

[1] ФСБ создаст единую систему защиты от компьютерных атак, Электронный ресурс: http://www.rg.ru/2013/01/18/komp-ataki-site-dok.html.

[2] Медведев В. Россия воздержалась от подарка хакерам, Электронный ресурс: http://polit. ru/author/vyacheslav medvedev/.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2014.5.11942

Анализ состояния и перспективы развития отечественной электронной промышленности

Рассмотрим состояние и перспективы развития в России электронной промышленности и собственной элементной базы.

Электронная промышленность — это промышленность, производящая различные компоненты для электронной техники, а также оборудование и изделия, которые содержат данные компоненты. Средний годовой прирост мировой электронной промышленности составляет более 15%, при товарообороте в 200 миллиардов долларов. Данный процесс идет уже более 30 лет и, по прогнозам экспертов, продлится еще в течение нескольких последующих десятилетий. Для сравнения отметим, что объем всей нефтедобычи стран ОПЕК в денежном выражении меньше, чем объем производства электроники[1].

В период СССР отечественная электронная промышленность в первую очередь работала на оборону. Та ее часть, которая обслуживала гражданские отрасли народного хозяйства, играла второстепенную роль и была как бы придатком военной. Поэтому, с переходом к рыночной экономике, отечественная бытовая техника не могла конкурировать с изделиями наиболее развитых стран не только на мировом, но и на российском рынке, а сокращение армии и военного заказа поставило предприятия отрасли на грань исчезновения. Только в конце 90-х годов наметились пути выхода из кризиса.

Как отмечалось выше, для обеспечения информационной безопасности России необходимы собственные изделия микроэлектроники.

Во всем мире электронная промышленность развивается как бизнес, в России она не нацелена на рыночные отношения. В нашей стране электронная промышленность может стабильно развиваться только при государственной поддержке. Кроме того, государству и бизнесу необходимо тесно взаимодействовать, поскольку бизнесу необходимы государственные заказы.

В отечественной электронной промышленности пока наблюдается недостаточная конкуренция ввиду незначительного количества собственной продукции. Слабое развитие объясняется также небольшим числом потребителей данной продукции. Основная часть потребителей ориентирована на импортную продукцию, практически полностью отсутствуют масштабные заказы отечественной продукции. По уровню производства и потребления электронной продукции наша страна очень сильно отстает от других стран, таких как Америка или Япония.

По заявлению заместителя председателя подкомитета по развитию радиоэлектронной индустрии Комитета ТПП по промышленному развитию А. Брыкина[2], в последнее время наметились шаги к улучшению, в частности, электронная промышленность была названа одним из основных, приоритетных национальных направлений государственной политики России. В 2007 году принята Стратегия развития электронной промышленности до 2025 года. Кроме того, в эту сферу поступают достаточно большие инвестиционные средства. Одним из главных преимуществ нашей страны перед остальными является то, что наш рынок еще недостаточно развит, и мы еще можем его заполнить. Сейчас

[1] Электронная промышленность, Электронный ресурс: http://biznestoday.ru/pr/102-elektronnaya promyshlennost.html.

[2] Брыкин А. Началась реализация долгосрочной госпрограммы «Развитие электронной и радиоэлектронной промышленности России на 2013–2025 годы», Электронный ресурс: http: //www.rg.ru/2013/03/05/elektron.html.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com
DOI: 10.7256/2073–8560.2014.5.11942

главное обеспечить не только частные инвестиционные средства, но и государственные. Государство и бизнес должны работать в тесном взаимодействии друг с другом. Существенно улучшить положение сможет общая модернизация наших ключевых производств в электронной промышленности, а также оптимизация отрасли на основе частно — государственного партнерства и создание рыночной инфраструктуры.

Подходы к созданию отечественной Системы защиты информации

Рассмотрим возможные подходы создания эффективной государственной Системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее — Системы).

Подход 1. В настоящее время в России имеется много IT-ресурсов, представляющих различную ценность для государства. Указ Президента от 15 января 2013 г. № 31с «Системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» не содержит требований деления активов по степени важности, что не вполне корректно с точки зрения последствий инцидентов. Для устранения данной проблемы, в дополнение к Указу Президента № 31с, разработан проект Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», который предположительно вступит в силу с 1 января 2015 года[1 2].

В соответствии с проектом данного закона, безопасность критической информационной инфраструктуры обеспечивается за счет организации взаимодействия этой системы с государственной Системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Кроме того, проект закона предписывает проведение дифференцируемой защиты различных объектов, поскольку обеспечение «максимальной защиты» всем ресурсам страны приведет к весьма значительным тратам бюджетных средств, кроме того, зачастую это просто невозможно. По мнению авторов, слабым местом проекта закона является отсутствие указания компаниям и организациям по порядку проведения классификации критических информационных структур, а также положение, в соответствии с которым оценку ценности активов организации и уровня защищенности объектов должны проводить аккредитованные ФСТЭК России организации.

Целесообразно рассмотреть подход к построению государственной Системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, закрепляющий классификацию возможной ценности активов организации на законодательном уровне с разделением требований по защите, а не путем решения данного вопроса организациями, аккредитованными ФСТЭК России. Следовательно, необходимо на федеральном уровне провести работу по анализу ценности активов, например, государственных критических инфраструктур, ресурсов банков, частных ресурсов. Это позволит оценить защищаемые активы с точки зрения применения адекватных мер и средств защиты. Закрепление ценности активов на законодательном уровне устранит много неопределенностей, возникающих при решении проблем безопасности в федеральном масштабе. Весьма логично рассмотреть

[1] Лукацкий А. Новый законопроект о безопасности критически важных объектов, Электронный ресурс: http://regulation.gov.ru/project/ 5890.html?point= view_project&stage= 2&stage_id=2938.

[2] Позиция РАЭК по законопроектам ФСБ России о безопасности критической информационной инфраструктуры, Электронный ресурс: http://raec.ru/times/.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2014.5.11942

международный опыт построения защищенных систем, например, стандарты серии ISO 27000[1] и отечественных аналогов[2]. Сильной стороной международных стандартов по информационной безопасности является применение принципа «разумной достаточности» в вопросах установления ценности активов организаций и применимости адекватных средств защиты.

Важным этапом работы после проведения классификации активов является разграничение критически важных объектов и остальных информационных структур.

Ввиду отсутствия отечественной элементной базы электронных средств и ограниченности отечественного программного обеспечения, целесообразно изолировать особо важные информационные сети и системы. Как разумный компромисс, возможна односторонняя связь с внешними сетями, при условии выполнения требований гальванической развязки. Целесообразность изоляции особо важных систем обусловлена отсутствием, в силу указанных выше причин, гарантии их полной безопасности.

Некритические активы, а таких, очевидно, большинство, целесообразно защищать с помощью существующих сертифицированных средств. Данные активы представляют значительно меньший интерес для таких мощных атакующих структур, как, например, спецслужбы иностранных государств. Поскольку сертифицированные средства являются средствами «повышенного доверия», целесообразно использовать их для защиты большинства систем.

Отметим положительные стороны рассмотренного подхода.

Возможность создания Системы произвольной структуры (деление сегментов Системы по министерствам, ведомствам, организациям).

Относительно небольшая стоимость работ (не требуется создавать свои программно-технические средства).

Изоляция особо критичных инфраструктур дает заведомо большую гарантию их безопасности, чем подключение через доверенные средства.

Недостатком рассмотренного подхода является необходимость изоляции части системы, что приведет к неудобствам, снижению оперативности работы в системе и т. д.

Подход 2. В настоящее время наблюдается параллельное создание идентичных IT- систем, в том числе в области информационной безопасности, в различных министерствах и ведомствах страны. Это приводит к дублированию функций, наличию разнотипного программного и аппаратного обеспечения, неоправданным затратам на содержание аналогичных систем, большим тратам на сопряжение систем и тому подобным проблемам. Кроме того, создание собственных систем министерств и ведомств, не объединенных единым координационным центром, создает благоприятную почву для коррупции. Следует отметить, что наличие абсолютно идентичных по выполняемым задачам собственных систем и сетей в министерствах и ведомствах (наблюдается в России очень часто) непозволительная роскошь даже для самых благополучных и развитых стран мира. Сложившаяся в России ситуация приводит не только к огромным малоэффективным тратам, но и ухудшает управляемость системами и сетями в масштабах государства, поскольку управление изолированными системами всегда крайне затруднено.

Главная идея предлагаемого подхода к построению Системы, в отличие от первого, состоит в поиске критических мест и их защита полностью доверенными

[1] ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements.

[2] ГОСТ Р ИСО/МЭК 13335–2006. Информационная технология. Методы и средства обеспечения безопасности. М., 2007.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com
DOI: 10.7256/2073–8560.2014.5.11942

средствами. Представляется целесообразным не делить активы по их важности, а применить единую отечественную вновь созданную программно-техническую платформу. По-видимому, имеет смысл не создавать сегменты министерств и ведомств и не распылять и так ограниченные ресурсы, а использовать все средства для создания Системы на одной программно-аппаратной платформе с единой Идеологией безопасности и обеспечения надежности. При этом особое внимание следует уделить выявлению критичных точек размещения средств обнаружения угроз, например, на шлюзах подключения к информационным системам других государств и тому подобных. По мнению авторов статьи, в этом случае, при концентрации административного, людского и финансового ресурса на решении главной задачи, появляется возможность создания надежных отечественных образцов программно-технических средств и реальная возможность обеспечения полной безопасности не только государственных, но и других информационных структур.

С точки зрения организации процесса создания Системы, необходимо назначить ответственного исполнителя с чрезвычайными полномочиями. Разрешить только одну, в исключительных случаях две ступени субподряда. Предлагаемый подход при грамотном и взвешенном руководстве позволит создать эффективную Систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Отметим положительные стороны рассмотренного подхода.

Во-первых, отсутствует необходимость изоляции сегментов и создается единое защищенное информационное пространство с «прозрачным» администрированием. Как следствие, повышается оперативность, улучшается контроль всех процессов. Во-вторых, защита всей инфраструктуры страны обеспечивается отечественными программно-техническими средствами с максимально высоким уровнем защиты.

К недостаткам предлагаемого подхода следует отнести высокую стоимость проекта, поскольку, как минимум, необходимо разработать, реализовать и внедрить собственные программно-технические средства. Другая очевидная проблема на пути реализации проекта — временные затраты. Учитывая крайнюю степень бюрократии во всех сферах деятельности нашего государства, на создание эффективно работающей и надежной Системы может понадобиться не один год.

Заключение

1. В результате проведенного анализа рассматриваемой проблемы можно сделать следующие основные выводы:
2. С точки зрения международного права Российская Федерация не защищена от различного рода массированных компьютерных атак, в частности, от проведения операций психологического воздействия на население страны.
3. Создание эффективной гарантированной Системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации возможно только путем разработки полностью отечественных систем защиты информации.
4. До появления отечественных образцов защищенных систем, необходимо изолировать критически важные информационные системы и сети.
5. В области обеспечения информационной безопасности нужна адекватная государственная политика, включающая решение всех вопросов защиты информации.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2014.5.11942

Библиография

1. Конвенция об обеспечении международной информационной безопасности (концепция), Электронный ресурс: http://www.scrf.gov.ru/documents/6/.
2. Проект Конвенции Организации Объединённых Наций (ООН) «Об обеспечении международной информационной безопасности», Электронный ресурс: http://www.scrf. gov.ru / documents /6/.
3. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: Указ Президента РФ от 15.01.2013 № 31с., Электронный ресурс: http://base. consultant.ru/cons/cgi/online.
4. Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети, М., Горячая линия, Телеком, 2013, 220 с.
5. Лукацкий А. Обнаружение атак, СПб: БХВ, 2001, 625 с.
6. Корт С. С. Теоретические основы защиты информации, М: «Гелиос АРВ», 2004, 233 с.
7. Сабадаш В. Деятельность центров реагирования на компьютерные инциденты: опыт зарубежных стран. Электронный ресурс: http://cybersafetyunit.com/deyatelnost-tsentrov-reagirovaniya-na-kompyuternyie-intsidentyi-kak-sredstvo-protivodeystviya-internet-oshennichestva-opyit-zarubezhnyih-stran/?lang=en.
8. Институт Компьютерной безопасности CSI, Электронный ресурс: http://www. gocsi.com
9. Координационный Центр Немедленного Реагирования США CERT, Электронный ресурс: http://www.cert.org .
10. Центр реагирования на компьютерные инциденты Российской Федерации RU-CERT, Электронный ресурс: http://www.cert.ru.
11. ФСБ создаст единую систему защиты от компьютерных атак, Электронный ресурс: http://www.rg.ru/2013/01/18/komp-ataki-site-dok.html.
12. Медведев В. Россия воздержалась от подарка хакерам, Электронный ресурс: http://polit.ru/ author/vyacheslavmedvedev/.
13. Электронная промышленность, Электронный ресурс: http://biznestoday.ru/pr/102-elektronnaya promyshlennost.html.
14. Брыкин А. Началась реализация долгосрочной госпрограммы «Развитие электронной и радиоэлектронной промышленности России на 2013–2025 годы», Электрон-ный ресурс: http: //www.rg.ru/2013/03/05/elektron.html.
15. Лукацкий А. Новый законопроект о безопасности критически важных объектов, Электронный ресурс: http://regulation.gov.ru/project/ 5890.html?point= view_ project&stage= 2&stage_id=2938.
16. Позиция РАЭК по законопроектам ФСБ России о безопасности критической информационной инфраструктуры, Электронный ресурс: http://raec.ru/times/.
17. ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements.
18. ГОСТ Р ИСО/МЭК 13335–2006. Информационная технология. Методы и средства обеспечения безопасности. М., 2007.
19. Савинов А. Н., Меркушев О. Ю.. Защита биометрических подсистем управления доступом. // Программные системы и вычислительные методы.—2013.—№ 4.— С. 335–343. DOI: 10.7256/2305–6061.2013.4.11092

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com
DOI: 10.7256/2073–8560.2014.5.11942

20. Горохов В.Г., Сюнтюренко О.В.. Технологические риски: информационные аспекты безопасности общества. // Программные системы и вычислительные методы.—2013.—№ 4.— С. 344–353. DOI: 10.7256/2305–6061.2013.4.9708
21. Шелеметьева Я.В.. Исследование технологии удаленного прямого доступа к памяти в архитектурах высокопроизводительных систем. // Программные системы и вычислительные методы.—2013.—№ 3.— С. 250–256. DOI: 10.7256/2305–6061.2013.3.1077
22. Сидоркина И.Г., Шумков Д.С.. Кусочно-линейная аппроксимация при решении задач извлечения данных. // Программные системы и вычислительные методы.—2013.—№ 2.— С. 171–175. DOI: 10.7256/2305–6061.2013.2.7943
23. А.Н. Савинов. Анализ причин возникновения ошибок первого и второго рода в системах авторизации основанных на распознавании клавиатурного почерка. // Программные системы и вычислительные методы.—2012.—№ 1.— С. 53–59.
24. А.Г. Коробейников, И.Г. Сидоркина, С.Ю. Блинов, А.В. Лейман. Алгоритм классификации информации для решения задачи фильтрации нежелательных сообщений. // Программные системы и вычислительные методы.—2012.—№ 1.— С. 89–95.

References (transliterated)

1. Konventsiya ob obespechenii mezhdunarodnoi informatsionnoi bezopasnosti (kontseptsiya), Elektronnyi resurs: http://www.scrf.gov.ru/documents/6/.
2. Proekt Konventsii Organizatsii Ob'»edinennykh Natsii (OON) «Ob obespechenii mezhdunarodnoi informatsionnoi bezopasnosti», Elektronnyi resurs: http://www.scrf. gov.ru / documents /6/.
3. O sozdanii gosudarstvennoi sistemy obnaruzheniya, preduprezhdeniya i likvidatsii posledstvii komp'yuternykh atak na informatsionnye resursy Rossiiskoi Federatsii: Ukaz Prezidenta RF ot 15.01.2013 № 31s., Elektronnyi resurs: http://base. consultant.ru/ cons/cgi/online.
4. Shelukhin O.I., Sakalema D. Zh., Filinova A.S. Obnaruzhenie vtorzhenii v komp'yuternye seti, M., Goryachaya liniya, Telekom, 2013, 220 s.
5. Lukatskii A. Obnaruzhenie atak, SPb: BKhV, 2001, 625 s.
6. Kort S.S. Teoreticheskie osnovy zashchity informatsii, M: «Gelios ARV», 2004, 233 s.
7. Sabadash V. Deyatel'nost» tsentrov reagirovaniya na komp'yuternye intsidenty: opyt zarubezhnykh stran. Elektronnyi resurs: http://cybersafetyunit.com/deyatelnost-tsentrov-reagirovaniya-na-kompyuternyie-intsidentyi-kak-sredstvo-protivodeystviya-internet-oshennichestva-opyit-zarubezhnyih-stran/?lang=en.
8. Institut Komp'yuternoi bezopasnosti CSI, Elektronnyi resurs: http://www. gocsi.com
9. Koordinatsionnyi Tsentr Nemedlennogo Reagirovaniya SShA CERT, Elektronnyi resurs: http://www.cert.org .
10. Tsentr reagirovaniya na komp'yuternye intsidenty Rossiiskoi Federatsii RU-CERT, Elektronnyi resurs: http://www.cert.ru.
11. FSB sozdast edinuyu sistemu zashchity ot komp'yuternykh atak, Elektronnyi resurs: http://www.rg.ru/2013/01/18/komp-ataki-site-dok.html.
12. Medvedev V. Rossiya vozderzhalas› ot podarka khakeram, Elektronnyi resurs: http://polit. ru/author/vyacheslavmedvedev/.
13. Elektronnaya promyshlennost», Elektronnyi resurs: http://biznestoday.ru/pr/102-elektronnaya promyshlennost.html.
14. Brykin A. Nachalas› realizatsiya dolgosrochnoi gosprogrammy «Razvitie elektronnoi i

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073–8560.2014.5.11942

radioelektronnoi promyshlennosti Rossii na 2013–2025 gody», Elektron-nyi resurs: http: //www.rg.ru/2013/03/05/elektron.html.
15. Lukatskii A. Novyi zakonoproekt o bezopasnosti kriticheski vazhnykh ob''ektov, Elektronnyi resurs: http://regulation.gov.ru/project/ 5890.html?point= view_ project&stage= 2&stage_id=2938.
16. Pozitsiya RAEK po zakonoproektam FSB Rossii o bezopasnosti kriticheskoi informatsionnoi infrastruktury, Elektronnyi resurs: http://raec.ru/times/.
17. ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements.
18. GOST R ISO/MEK 13335–2006. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. M., 2007.
19. Savinov A. N., Merkushev O. Yu.. Zashchita biometricheskikh podsistem upravleniya dostupom. // Programmnye sistemy i vychislitel'nye metody.—2013.—№ 4.— C. 335–343. DOI: 10.7256/2305–6061.2013.4.11092
20. Gorokhov V. G., Syuntyurenko O. V.. Tekhnologicheskie riski: informatsionnye aspekty bezopasnosti obshchestva. // Programmnye sistemy i vychislitel'nye metody.—2013.—№ 4.— C. 344–353. DOI: 10.7256/2305–6061.2013.4.9708
21. Shelemet'eva Ya.V.. Issledovanie tekhnologii udalennogo pryamogo dostupa k pamyati v arkhitekturakh vysokoproizvoditel'nykh sistem. // Programmnye sistemy i vychislitel'nye metody.—2013.—№ 3.— C. 250–256. DOI: 10.7256/2305–6061.2013.3.1077
22. Sidorkina I. G., Shumkov D. S.. Kusochno-lineinaya approksimatsiya pri reshenii zadach izvlecheniya dannykh. // Programmnye sistemy i vychislitel'nye metody.—2013.—№ 2.— C. 171–175. DOI: 10.7256/2305–6061.2013.2.7943
23. A. N. Savinov. Analiz prichin vozniknoveniya oshibok pervogo i vtorogo roda v sistemakh avtorizatsii osnovannykh na raspoznavanii klaviaturnogo pocherka. // Programmnye sistemy i vychislitel'nye metody.—2012.—№ 1.— C. 53–59.
24. A. G. Korobeinikov, I. G. Sidorkina, S. Yu. Blinov, A. V. Leiman. Algoritm klassifikatsii informatsii dlya resheniya zadachi fil'tratsii nezhelatel'nykh soobshchenii. // Programmnye sistemy i vychislitel'nye metody.—2012.—№ 1.— C. 89–95.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com
DOI: 10.7256/2073–8560.2014.5.11942