Л. А. Коваленко

ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ДЛЯ РАЗРАБОТКИ ПОЛИТИК БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Современная жизнь человечества невозможна без компьютерных систем. Однако компьютер, который работает один, приносит мало пользы, возникает необходимость в объединении компьютеров организаций, предприятий, учреждений (далее — организаций) в сети (локальные и глобальные) и предоставлении таким образом доступа к ресурсам своего компьютера другим пользователям. Но мы, сами того не подозревая, делаем наши системы уязвимыми для злоумышленников. В настоящее время с помощью новейших ИТ-технологий можно лишить население воды и электричества, вывести из строя банковскую систему и отключить оборонительную систему любой страны.

Компьютерные правонарушения наблюдаются во всех сферах деятельности человеческого общества [1].

Убыток, нанесенный России компьютерным пиратством в 2011 г., составил более 3,227 млрд. долларов. Именно такова коммерческая стоимость нелицензионного программного обеспечения, установленного на ПК по всей стране в прошлом году. Об этом свидетельствует проведенное международной ассоциацией компьютерных производителей Business Software Alliance (BSA) исследование.

Как отмечает The Bunker, британские компании, например, не прислушиваются к предупреждениям экспертов по безопасности. Более трети участников исследования заявили, что события прошлого года ощутимо повлияли на их компании — уровень осведомленности в вопросах безопасности, а также осознание необходимости обеспечивать надлежащий уровень защиты заметно выросли. Однако, несмотря на повышение уровня информированности, почти половина респондентов призналась, что они абсолютно ничего не сделали для того, чтобы улучшить свое положение.

При этом, эксперты говорят о нехватке специалистов в области защиты информации на предприятиях или в государственных учреждениях. И эта неприятная тенденция имеет место быть в тот период, когда киберпреступность процветает, пишет «Рейтер». «Это большая проблема для национальной безопасности», — говорит генеральный директор Symantec Энрике Салем (Enrique Salem), принявший участие в конференции Reuters Media and Technology Summit в Нью-Йорке [1].

Сегодня неотъемлемым элементом хозяйствующей деятельности многих организаций становится осуществление электронных транзакций по Интернету и другим публичным сетям. Электронная коммерция, продажа информации, оказание консультационных услуг в режиме on-line и многие другие услуги становятся для предприятий в новых условиях основными видами деятельности. Это уже норма жизни, поэтому разрушение информационного ресурса, его временная недоступность, нарушение конфиденциальности или несанкционированное использование могут нанести предприятию значительный материальный ущерб, а применительно к государственным информационным ресурсам — подорвать экономическую безопасность государства. В связи с этим информационные ресурсы и средства осуществления электронных сетевых транзакций необходимо защищать.

Стратегия национальной безопасности Российской Федерации отмечает, что нашей стране надлежит преодолеть технологическое отставание в важнейших областях информатизации, телекоммуникаций и связи [2]. Серьезную опасность при этом представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка, разработка рядом государств концепции информационных войн, получение несанкционированного доступа к информационным ресурсам [3, 4].

Задачи по обеспечению противодействия этим угрозам и реализации национальных интересов Российской Федерации в информационной сфере сформулированы в Доктрине информационной безопасности Российской Федерации [3].

Во избежание очевидных негативных последствий в информационной сфере требуется создать системы для обеспечения безопасности эксплуатации автоматизированных систем организаций.

Для всестороннего обеспечения безопасности эксплуатации автоматизированных систем организаций должны быть разработаны организационно-распорядительные документы. К таким документам в первую очередь относятся технические регламенты и стандарты.

Законодательством Российской Федерации установлено, что технические регламенты с учетом степени риска причинения вреда определяют минимально необходимые требования, обеспечивающие различные виды безопасности:

безопасность излучений,

биологическую безопасность,

взрывобезопасность,

механическую безопасность,

пожарную безопасность,

промышленную безопасность,

термическую безопасность,

химическую безопасность,

электрическую безопасность,

ядерную и радиационную безопасность,

электромагнитную совместимость в части обеспечения безопасности работы приборов и оборудования,

единство измерений [5].

При этом все виды технических регламентов в Российской Федерации разделяются на общие технические регламенты и специальные технические регламенты.

Общие технические регламенты принимаются по следующим вопросам:

безопасной эксплуатации и утилизации машин и оборудования;

безопасной эксплуатации зданий, строений, сооружений и безопасного использования прилегающих к ним территорий;

пожарной безопасности;

биологической безопасности;

электромагнитной совместимости;

экологической безопасности;

ядерной и радиационной безопасности. [5]:

Специальные технические регламенты Российской Федерации устанавливают требования только к тем отдельным видам продукции, процессам производства, эксплуатации, хранения, перевозки реализации и утилизации, в отношении которых цели, определенные Федеральным законом для принятия технических регламентов, не обеспечиваются требованиями общих технических регламентов [5].

Кроме того, специальные технические регламенты устанавливают требования только к тем отдельным видам продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, степень риска причинения вреда которыми выше степени риска причинения вреда, учтенной общим техническим регламентом.

Таким образом, можно констатировать, что в настоящее время в перечне регламентов, обязательных для применения и соблюдения в России, отсутствуют такие технические регламенты,

которые с учетом степени риска причинения вреда устанавливали бы минимально необходимые требования, определяющие состояние защищенности информационной среды граждан, организаций, государства.

Кроме того, проблема обеспечения безопасности в информационной сфере занимает все более значительное место при реализации автоматизированных систем и сетей по мере того, как возрастает их роль в информатизации общества.

Поэтому обеспечение безопасности ИТ представляет собой комплексную проблему, которая решается в направлениях совершенствования правового регулирования применения ИТ, совершенствования методов и средств их разработки, развития системы сертификации, обеспечения соответствующих организационно-технических условий эксплуатации.

Цель и задачи системы стандартов по защите информации, объекты стандартизации, структура, состав и классификация входящих в нее стандартов, а также правила их обозначения установлены Государственным стандартом Российской Федерации ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения» [6].

Положения настоящего стандарта являются рекомендуемыми при разработке нормативных документов по стандартизации в области защиты информации, независимо от организационно-правовой формы и формы собственности предприятия, учреждения, организации — разработчика стандарта, а также при организации работ по стандартизации в области защиты информации органами управления Российской Федерации.

Данный стандарт является основополагающим государственным стандартом Российской Федерации в области защиты информации.

Согласно статье 46 Федерального закона «О техническом регулировании», с 01 июля 2003 г. впредь до вступления в силу соответствующих технических регламентов требования, установленные действующими национальными стандартами, подлежат обязательному исполнению только в части, обеспечивающей достижение целей законодательства Российской Федерации о техническом регулировании [5].

Важным принципом процесса стандартизации в Российской Федерации является применение международных стандартов как основы разработки национальных стандартов. Процесс приведения национальных стандартов в соответствие с международными называется гармонизацией.

Стандарт организации предусмотрен Федеральным законом «О техническом регулировании» как единственный документ, в котором юридически закрепляются локальные правовые требования, нормы и правила, необходимые для обеспечения деятельности любой организации в области технического регулирования.

Деятельность организации в других областях регулируется иными правовыми актами в зависимости от характера и организационно-правовой формы организации.

Одним из таких актов утверждаются стандарты организации.

В качестве примера разработанного в Российской Федерации стандарта организации можно назвать Стандарт ЦБР «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», который был принят и введен в действие распоряжением ЦБР от 21июня 2010 г. № Р-705 [7].

В общем случае для защиты интересов субъектов информационных отношений в организациях необходимо сочетать меры следующих уровней:

- законодательного (законы, нормативные акты, стандарты и т. п.);
- административного (действия общего характера, предпринимаемые руководством организации);
- процедурного (конкретные меры безопасности, имеющие дело с людьми);
- программно-технического (конкретные технические меры).

Для соответствующих областей информационной безопасности (организационных, административных, технических и т. д.) защитные меры могут быть выбраны на основе рекомендаций, изложенных в стандартах ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 15408 и др.

Используемый сегодня в России национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» введен в действие с 1 января 2007 г. [8].

Кроме того, в настоящее время также применяются нормативные документы Гостехкомиссии России (ФСТЭК России) и ФАПСИ (ФСБ России). Однако документы ФСТЭК России на практике применяются обычно только к программным продуктам. Документы ФСБ России регламентируют, в основном, применение криптографических средств. Употребление этих регламентирующих документов в системе управления информационной безопасности организации практически невозможно, так как сами документы предназначались в первую очередь для программного обеспечения. Поэтому сертифицировать всю информационную систему организации на соответствие нормативным документам ФСТЭК России представляется достаточно сложным и не совсем эффективным действием.

В сфере информационной безопасности в настоящее время в Российской Федерации определяющим по отношению к компьютерным системам является Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-1-2008. Этим стандартом введен термин «политика безопасности организации» [9].

Политика безопасности — одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

Следовательно, политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которые руководство считает целесообразным выделить.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации.

Когда риски проанализированы и стратегия защиты определена, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п.

В настоящее время в отечественной практике административный уровень информационной безопасности реализуется фрагментарно. Это объясняется следующими причинами:

- отсутствуют законодательные акты, обязывающие организацию иметь политику безопасности;
- ни один из федеральных органов исполнительной власти, курирующих информационную безопасность, не предлагает типовых разработок в данной области;
- ни одно образовательное учреждение не готовит специалистов по составлению политик безопасности автоматизированных систем;
- мало кто из руководителей организаций знает, что такое политика безопасности (поскольку они получали высшее профессиональное образование в то время, когда термин «политика информационной безопасности» не был закреплен ни нормативными правовыми актами, ни нормативными правовыми документами);
- еще меньшее число организаций такую политику имеют.

В то же время без подобной основы прочие меры информационной безопасности повисают в воздухе, они не могут быть всеобъемлющими, систематическими и эффективными.

Разработка политики безопасности требует учета специфики конкретных организаций.

Можно потребовать от руководителей наличия политики безопасности (и в перспективе это правильно), но сначала нужно разъяснить, научить, показать, для чего она нужна и как ее разрабатывать.

Исходя из вышеизложенного в интересах обеспечения требуемого уровня информационной безопасности организации, адекватного современным угрозам в информационной сфере, рационально предусмотреть реализацию образовательной программы повышения квалификации «Основы разработки политики безопасности автоматизированных систем организаций».

В рамках такой программы представляется целесообразным рассмотреть следующие разделы:

1. Законодательство Российской Федерации о техническом регулировании;
2. Характеристика и структура технических регламентов;
3. Стандартизация в Российской Федерации;
4. Основные национальные стандарты Российской Федерации в области защиты информации и обеспечения безопасности;
5. Организация процедур подтверждения соответствия техническим регламентам и стандартам;
6. Аккредитация органов по сертификации и испытательных лабораторий (центров);
7. Ответственность за соблюдение требований технических регламентов;
8. Политика информационной безопасности;
9. Нормативно-правовое обеспечение политики информационной безопасности организации;
10. Последствия нарушения политики безопасности.

Объем такой программы может составить от 72 до 100 часов.

Учитывая дефицит в специалистах с высшим профессиональным образованием (потребности субъектов информационных отношений удовлетворяются не в полной мере — при запросе около 5000 специалистов в год выпуск составляет около 2000), после апробации в рамках образовательной деятельности государственных образовательных учреждений переподготовки и повышения квалификации такая программа могла бы стать программой вариативной части профессионального цикла федерального государственного образовательного стандарта по направлению подготовки 090900 «Информационная безопасность» (квалификация (степень) «бакалавр»).

При этом представляется целесообразным создание в отобранных образовательных учреждениях, входящих в состав Учебно-методического объединения высших учебных заведений Российской Федерации по образованию в области информационной безопасности, современной методической и материально-технической базы подготовки, переподготовки и повышения квалификации специалистов для разработки политики безопасности компьютерных систем организаций.

В результате можно ожидать, что в области подготовки специалистов будут обеспечены следующие результаты.

Во-первых, повышение квалификации специалистов в области информационных технологий, что позволит им уверенно действовать в современном информационном пространстве и своевременно обнаруживать угрозы в информационно-коммуникационной сфере.

Во-вторых, подготовка, переподготовка и повышение квалификации обслуживающего персонала объектов информатизации и автоматизированных систем, что позволит им в результате активно противодействовать угрозам инфокоммуникационного терроризма, а также минимизировать последствия внештатных ситуаций в работе автоматизированных систем, вызванных непреднамеренными действиями пользователей и обслуживающего персонала.

В-третьих, разработка необходимого учебно-методического обеспечения всех уровней и направлений для подготовки специалистов по разработке стандартов и политик безопасности, что позволит оказать в конечном итоге положительное влияние на укрепление информационной безопасности Российской Федерации.

Эти очевидные и взаимосвязанные задачи лежат в плоскости реализуемых в настоящее время программ социально-экономического развития России и модернизации системы государственного управления [2, 4].

СПИСОК ЛИТЕРАТУРЫ:

1. http://www.dailycomm.ru (дата обращения: 12.10.2012).
2. Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895).
4. Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 г. (одобрена распоряжением Правительства Российской Федерации от 27 сентября 2004 г. № 1244-р) (с изменениями от 29 июля 2005 г., 21 ноября 2006 г., 24 декабря 2008 г., 10 марта 2009 г.).
5. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (с изменениями от 9 мая 2005 г., 1 мая, 1 декабря 2007 г., 23 июля 2008 г., 18 июля, 23 ноября, 30 декабря 2009 г., 28 сентября 2010 г., 21 июля, 30 ноября, 6 декабря 2011 г., 28 июля 2012 г.).
6. Государственный стандарт Российской Федерации ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения» (принят постановлением Госстандарта Российской Федерации от 5 июня 2003 г. № 181-ст). М.: ИПК Издательство стандартов, 2003.
7. Стандарт Банка России СТО БР ИББС-1.2-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (принят и введен в действие распоряжением ЦБР от 21 июня 2010 г. № Р-705) // Вестник Банка России. 29.06.2010. № 36–37.
8. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 447-ст). М.: Стандартинформ, 2006.
9. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 519-ст). М.: Стандартинформ, 2009.