CIO
Chief Information Officer
РУКОВОДИТЕЛЬ ИНФОРМАЦИОННОЙ СЛУЖБЫ • МАЙ 2002 • №4 (4)

Помните о безопасности.

Илья Трифаленков

СМИ периодически сообщают о новых фактах взломов и атак и возрастающих масштабах причиняемого злоумышленниками ущерба. Компьютерная пресса периодически помещает статьи-"страшилки" на тему информационной безопасности. Большинство руководителей компаний осознают наличие угроз как для информационной инфраструктуры, так и для среды взаимодействия с клиентами и партнерами.

В то же время руководители компаний и технические специалисты зачастую имеют недостаточно полное представление о проблеме: какие именно сведения и почему необходимо защищать, откуда следует ждать целенаправленных атак или непреднамеренных вредоносных воздействий, какие действия нужно предпринять, чтобы уменьшить вероятность взлома корпоративной информационной системы и иной несанкционированной деятельности, и чем может обернуться для компании недостаточно серьезное отношение к проблеме.

Текущая ситуация в области безопасности ИТ

На протяжении последних лет наблюдается рост числа нарушений информационной безопасности в области ИТ, в том числе влекущих тяжелые последствия. Общее количество нарушений ИБ в мире растет более чем на 100% в год.

В России ранее наблюдалось некоторое отставание по количеству нарушений от мирового уровня, однако этот разрыв сокращается быстрыми темпами. Согласно статистике правоохранительных органов, число выявленных преступлений в сфере компьютерной информации растет каждый год в среднем в 3-4 раза. В такой же пропорции ежегодно растет и общая сумма ущерба от компьютерных преступлений. Среди наиболее громких преступлений - попытки незаконного доступа к ряду банков данных, включая закрытые базы данных государственных организаций и правоохранительных органов; распространение закрытых баз данных (ГИБДД, таможня, прописка, собственники Москвы); распространение конфиденциальной информации крупных компаний. Распространенными нарушениями являются попытки взлома электронных платежных систем, использование чужих кредитных карт, нарушения авторских прав и другие.

Российские компании, по данным Ernst & Young, наиболее часто сталкиваются с вирусными атаками, попытками проникновения в информационную систему извне и несанкционированным доступом изнутри, атаками типа "отказ в обслуживании" (DoS), в том числе на критически важные для бизнеса системы.

Отношение компаний к проблеме ИБ

Компании достаточно инертно меняют свою политику в области обеспечения безопасности, а степень защищенности информационной инфраструктуры оставляет желать лучшего. Такая ситуация зачастую наблюдается даже в тех компаниях, в которых в силу специфики деятельности уровень риска весьма высок. Например, у многих предприятий электронного бизнеса отсутствует продуманная стратегия по вопросам обеспечения безопасности и конфиденциальности, что регулярно приводит как к финансовым, так и к репутационным потерям.

В большинстве компаний в настоящее время только разрабатывается политика обеспечения информационной безопасности и проводится работа по повышению уровня осведомленности персонала.

Многие компании неадекватно соотносят свою деятельность с существующими рисками, плохо понимают, откуда могут исходить угрозы. Руководители зачастую имеют ошибочное убеждение, что единственной функцией системы безопасности должна быть защита корпоративных систем от несанкционированного вмешательства извне, и недооценивают внутренние угрозы, хотя по статистике большинство взломов информационных систем происходит именно "изнутри".

И даже в тех организациях, где существует политика информационной безопасности, зачастую встречается халатное отношение к мерам ее обеспечения, например, к парольной защите - не производится плановая смена паролей, не удаляются эккаунты после увольнения сотрудника.

Меры и средства обеспечения безопасности

Подавляющее большинство компаний используют один или два вида технических средств защиты. Согласно исследованию Ernst & Young, самыми распространенными средствами обеспечения безопасности являются антивирусные программы и межсетевые экраны, менее широко используются средства шифрования, виртуальные сети (VPN) и системы обнаружения несанкционированного проникновения.

Большинство компаний не имеет официально оформленных процедур мониторинга и регулярного тестирования используемых средств информационной безопасности для подтверждения их адекватности.

Таким образом, во многих компаниях проблема обеспечения информационной безопасности требует скорого и квалифицированного решения.

Законодательные основы защиты информации

Для предприятий и организаций, деятельность которых связана с обработкой информации ограниченного доступа, содержащей государственные или военные секреты, ситуация с нормативным обеспечением защиты наиболее ясная: здесь действуют давно разработанные и утвержденные законы, стандарты, положения, инструкции, методики и нормы. О защите других видов конфиденциальной информации должны заботиться сами руководители предприятий.

При обработке конфиденциальной информации компаниям необходимо руководствоваться следующими нормативными документами:

- Конституция Российской Федерации;
- Закон "Об информации, информатизации и защите информации" № 24-ФЗ от

20.02.95г.;

- Закон "О государственной тайне" № 5485-1 от 21.07.93г.;
- Закон "О правовой охране программ для электронных вычислительных машин и баз данных" № 3523-1 от 23.09.92г.;
- Указ Президента "Об утверждении Перечня сведений, отнесенных к государственной тайне" № 1203 от 30.11.95г.;
- Указ Президента "Об утверждении Перечня сведений конфиденциального характера" № 188 от 06.03.97 г.;
- Постановление Правительства "О Перечне сведений, которые не могут составлять коммерческую тайну" № 35 от 05.12.91г.

Виды сведений, подлежащих защите

Помимо государственной тайны, законодательством определено еще несколько видов тайн и иных конфиденциальных сведений.

Под служебной или коммерческой тайной понимаются сведения, не являющиеся государственными секретами, но связанные, прежде всего, с производственной, управленческой, финансовой или другой экономической деятельностью организации, разглашение (передача, утечка, хищение) которых может нанести ущерб ее интересам или интересам их владельцев.

Законодательной основой защиты служебной и коммерческой тайны является часть вторая Гражданского кодекса РФ, введенного в действие с 01.01.1995 г. В статье 139 ГК РФ определены понятия этих видов тайн:

"Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры по охране ее конфиденциальности.

Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами".

Указом Президента РФ № 188 от 6 марта 1997 г. утвержден Перечень сведений конфиденциального характера, в который включены:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, составляющие тайну следствия и судопроизводства;
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телефонных или иных сообщений и т. д.);
- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна);
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации о информации о них.

На сегодняшний день отсутствуют некоторые нормативно-правовые документы (прежде всего, закон "О коммерческой тайне"), а также единая методология выделения сведений, которые могут и должны составлять служебную или коммерческую тайну. Это затрудняет организацию и проведение работ по защите сведений, являющихся собственностью компаний. Набор сведений, которые должны быть отнесены к категории конфиденциальных, во многом зависит от особенностей деятельности компании,

характера ущерба, который может быть нанесен интересам деятельности компании в случае их несанкционированного распространения, экономических и иных преимуществ и недостатков открытого и закрытого (внутреннего) использования таких сведений.

Федеральным законом "О банках и банковской деятельности" определено понятие банковской тайны (ее составляют сведения об операциях, о счетах и вкладах клиентов и корреспондентов), а также ответственность банков и иных кредитных организаций, их должностных лиц и сотрудников за разглашение банковской тайны, включая возмещение нанесенного ущерба.

В соответствии с законом "Об информации, информатизации и защите информации" должна быть обеспечена защита персональных данных граждан. Законом определены основные требования к правовому режиму, а также установлена ответственность за его нарушение. Персональные данные не могут быть открыты другим лицам без достаточных оснований, следовательно, в компании должны быть приняты меры для защиты от несанкционированного доступа и предотвращения злоумышленной модификации персональных данных лицами, не имеющими на то полномочий.

Также необходимо обеспечить защиту интеллектуальной собственности и авторских прав в соответствии с законом "Об авторском праве и смежных правах" № 5351-1 от 09.07.1995 г. Ответственность за нарушение предусмотрена статьей 146 УК РФ "Нарушение авторских и смежных прав".

Приведенные нормативно-правовые акты определяют законодательную основу ответственности за несанкционированное распространение сведений, составляющих служебную, коммерческую, профессиональную и иные виды тайн, а также устанавливают правовые нормы в борьбе с недобросовестными конкурентами.

Угрозы информационной безопасности и виды возможного ущерба

Чтобы выполнять требования действующих нормативных актов и обеспечивать надежную защиту конфиденциальных сведений, нужно понимать, от кого и от чего их необходимо защищать.

В общем случае, в современной информационной системе можно выделить следующие основные классы угроз безопасности:

- угрозы, реализуемые преднамеренным воздействием на программное обеспечение и конфигурацию системы;
- угрозы, возникающие в результате непреднамеренных действий пользователей, операторов и обслуживающего персонала, в том числе обусловленные ошибками проектирования и разработки компонентов информационной системы;
- угрозы, связанные с выходом из строя используемых технических средств обработки информации, связи и т. д.;
- угрозы, связанные с перехватом побочных электромагнитных излучений и наводок, возникающих с использованием специализированных средств технической разведки.

Какие именно угрозы являются наиболее значимыми в конкретном случае - зависит от специфики деятельности компании и особенностей используемой системы обработки информации. Результатом реализации угроз информационной безопасности могут быть:

- несанкционированное ознакомление, хищение, копирование конфиденциальной или важной информации (новейших разработок, персональных данных сотрудников и клиентов, паролей пользователей и т. д.);
- искажение информации (подделка передаваемых платежных документов) или ее уничтожение;
- сбои в работе или вывод из строя информационной системы, приводящие к нарушению нормального режима работы компании.

Обеспечение защиты информационных систем

Для того чтобы свести к минимуму возможность нарушения информационной безопасности, необходимо, в первую очередь, проанализировать возможные источники угроз, факторы, способствующие их проявлению, определить актуальные угрозы и возможные негативные последствия.

Современные средства обеспечения безопасности весьма разнообразны. Только их видов по типу решаемых задач насчитывается более десяти - межсетевые экраны, системы аутентификации/авторизации и защиты от несанкционированного доступа, средства антивирусной защиты, анализа защищенности и обнаружения атак, средства криптографии и создания виртуальных сетей (VPN), а также относительно новые классы средств - системы мониторинга и фильтрации содержимого электронной почты и веб-ресурсов, средства создания инфраструктуры открытых ключей и управления безопасностью.

Чтобы яснее представить пути и возможности обеспечения информационной безопасности, рассмотрим ситуацию на рынках соответствующих продуктов и услуг.

Мировой рынок ИБ

Основными потребителями продуктов и услуг ИБ на мировом рынке являются страховые, инвестиционные и телекоммуникационные компании, банки, предприятия электронной коммерции - компании, бизнес процессы которых зависят от бесперебойной работы информационных систем.

Объем продаж по всем направлениям рынка продуктов информационной безопасности (средства идентификации, авторизации, криптографии, управления безопасностью и антивирусные средства) вырос более чем на 25% по сравнению с 2000 годом, при этом сегмент рынка межсетевых экранов вырос на 42%. Ожидается дальнейший рост мирового рынка средств обеспечения безопасности в среднем на 23% в год, его общий объем к 2005 году достигнет $14 млрд.

Рынок ИБ в России

Отечественный рынок продуктов и услуг в области информационной безопасности также находится на подъеме. В 2000 году объем рынка составил около 20 млн. долларов, в 2001 году этот показатель удвоился и превысил 40 млн. долларов.

Потребителей продуктов и услуг информационной безопасности на российском рынке можно разделить на две категории. К первой относятся государственные учреждения и те организации, которым предписано следовать требованиям руководящих документов Гостехкомиссии России и ФАПСИ. Во вторую категорию входят банки и другие финансовые организации, предприятия нефте- и газодобывающей отрасли и топливно-энергетического комплекса, промышленные и телекоммуникационные компании и др.

Большую долю в структуре реализуемых продуктов составляют антивирусные средства и межсетевые экраны, далее следуют средства защиты от несанкционированного доступа, средства создания VPN и системы обнаружения атак. Менее широко используются средства управления безопасностью и средства криптографической защиты.

Доля услуг на рынке информационной безопасности пока невелика. Это во многом объясняется распространенным ошибочным подходом компаний к обеспечению безопасности, при котором единственным видом применяемых защитных мер является закупка и установка одного или двух видов технических средств без каких-либо исследований защищаемой системы и проведения организационных мероприятий.

Большинство аналитиков прогнозируют значительный рост спроса на продукты и услуги в области информационной безопасности. Ожидается ужесточение конкуренции, появление на рынке новых игроков и продуктов.