ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Вторник, 24 апреля 2007 №69
(№3645 с момента возобновления издания)
Цветные тематические страницы №25–40
являются составной частью газеты «Коммерсантъ»
Рег. №01243 22 декабря 1997 года.
Распространяются только в составе газеты.

Коммерсантъ

BUSINESS GUIDE

4601865000226
07117

SONY

VAIO рекомендует лицензионную
ОС Windows Vista™ Home Premium

VAIO серии LA

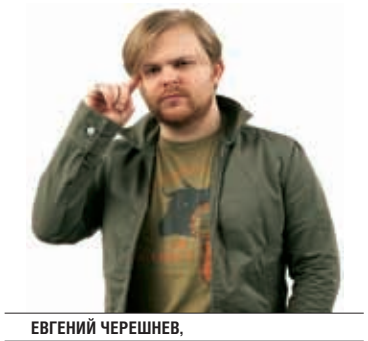
быть как никто другой

РЕКЛАМА. ТОВАР СЕРТИФИЦИРОВАН

like.no.other™

*Как никто другой

VAIO



ЕВГЕНИЙ ЧЕРЕШНЕВ,
РЕДАКТОР BUSINESS GUIDE
«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

УГОВОРЫ НЕ ПОМОГУТ

Наш интерес к информационной безопасности напоминает отношение к ВИЧ: все знают, что он есть, но далеко не всем известны меры предосторожности, кроме использования презерватива. Отсюда и плачевная статистика непобедимости вредоносных кодов.

Между тем истинное положение дел мало кто представляет — массовые атаки ушли в прошлое, а на их место пришли организованные и хорошо финансируемые команды хакеров, чьи подвиги довольно регулярно всплывают в прессе (похищенная недавно база МТС далеко не предел их возможностей). Рядовые пользователи, представители среднего и даже крупного бизнеса порой уверены в том, что причины всех проблем с защитой информации в несовершенстве средств этой самой защиты — криптографического оборудования, межсетевых экранов, антивирусов, операционных систем. Но это не так.

Борьбой с хакерами занимаются лучшие умы планеты — математики, программисты, системные архитекторы, и их усилия, поверьте, отнюдь не тщетны. Сегодня ничто не мешает создать эшелонированную надежную защиту персональных или глубоко конфиденциальных корпоративных данных. Вопрос только в желании, средствах и силе воли.

Но тут мы имеем дело с другой чертой человеческого характера — тягой к самообману. Не секрет, что подавляющее большинство пользователей, установив на компьютер FireWall, моментально чувствуют себя в безопасности, словно бронежилет надели. И, разумеется, сильно удивляются, когда пароль доступа к корпоративной почте оказывается украденным. То же самое касается корпоративного сектора — с поправкой на масштаб защитных периметров. Мы никак не поймем, что безопасность — это не состояние, а процесс. Длительный, сложный, подчас весьма недешевый, но, к сожалению, неизбежный.

Поэтому я не буду говорить о таких тривиальных вещах, как сертификация информационных процессов компании для приведения их в соответствие с международными стандартами безопасности ISO27001. Как показывает практика, обычные уговоры редко приводят к положительному результату. Но если для того, чтобы всерьез задуматься о методах защиты своей информационной собственности, вам требуется пережить взлом бесценной корпоративной базы данных, я вам искренне сочувствую.

КОЛОНКА РЕДАКТОРА

ВИРУСОЛОГИЯ

ЭКСПЕРТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ ЗАЩИТЫ И РАЗРАБОТЧИКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЕДИНОДУШНО ОТМЕЧАЮТ НЕУТЕШИТЕЛЬНУЮ ТЕНДЕНЦИЮ: ИЗ БАЛОВСТВА И ЛЮБОПЫТСТВА ХАКЕРСТВО ПРЕВРАТИЛОСЬ В ВЕСЬМА ДОХОДНЫЙ БИЗНЕС. 40 МЛН НОМЕРОВ КРЕДИТНЫХ КАРТ, ПОХИЩЕННЫХ В ПОЗАПРОШЛОМ ГОДУ ИЗ ПРОЦЕССИНГОВОГО ЦЕНТРА CARD SOLUTIONS В АТЛАНТЕ (США), СТАЛИ САМОЙ НАГЛОЙ ДЕМОНСТРАЦИЕЙ ВОЗМОЖНОСТЕЙ ХАКЕРОВ, ИСПОЛЬЗУЮЩИХ ПРОРЕХИ В ЗАЩИТЕ КОРПОРАТИВНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ. И ОКОНЧАТЕЛЬНЫМ ПОДТВЕРЖДЕНИЕМ НЕОБХОДИМОСТИ СЕРЬЕЗНОГО, А ГЛАВНОЕ, СИСТЕМНОГО ОТНОШЕНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ЕВГЕНИЙ ЧЕРЕШНЕВ

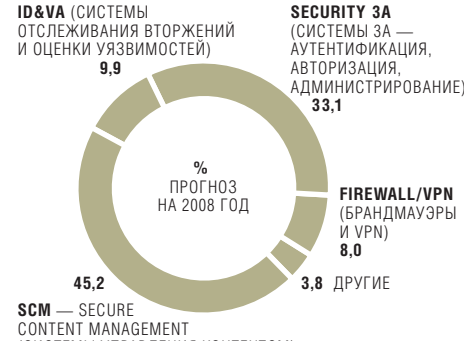
ЗАРАЖЕНИЕ ВЫМЫСЛОМ Экспериментальным путем доказано, что любая система, не защищенная антивирусом и межсетевым экраном (в английском варианте — FireWall), становится инфицированной спустя всего 40 минут после выхода в интернет. Соответственно, уже через несколько дней использования такой компьютер, кишащий сотнями, если не тысячами единиц вредоносного ПО, начинает массово рассылать по всей сети вирусы и спам.

Пользователь же спокойно работает с базами данных, электронной почтой, платными аккаунтами многочисленных сетевых сервисов и не подозревает, что все его пароли уже являются достоянием общественности, а скапливающиеся e-mail с предложениями купить виагру рассылаются с его же компьютера.

А ведь еще несколько лет назад большинство опасных вирусов носило концептуальный характер: программисты-энтузиасты, стремясь прославиться среди себе подобных, пытались максимизировать ущерб, наносимый создаваемыми программами. В результате факт заражения компьютера довольно быстро становился очевидным, и подавляющее большинство пользователей, заметив существенное замедление системы, появление сбоев в работе программ и других подозрительных симптомов, стремилось спешно установить на компьютер антивирус и провести тщательное сканирование.

Сегодня ситуация усложнилась: хакеры и вирус-мейкеры больше не стремятся к публичности, поэтому вредоносные программы зачастую работают по принципу крота — тихо, незаметно, но максимально эффективно.

«Поскольку современные компьютеры стали очень скоростными, пользователь попросту не замечает побочных процессов: рассылка спама, вирусов, украденных паролей и номеров кредитных карт с зараженного компьютера протекает без ущерба для основной деятельности, а следовательно, не побуждает пользователя беспокоиться о собственной безопасности. Этот тренд стал особенно актуальным в последние два года»,— говорит Александр Гостев, ведущий вирусный аналитик «Лаборатории Касперского».



ОБОРОТ МИРОВОГО РЫНКА ПРОГРАММНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИТ-БЕЗОПАСНОСТИ (IT-SECURITY SW)
ПО ДАННЫМ IDC.

Любопытно, что, несмотря крайне высокую активность злоумышленников, о масштабах проблемы осведомлена лишь малая часть пользователей сети — на интернет-форумах, посвященных вопросам компьютерной безопасности, довольно часто можно встретить обвинения разработчиков антивирусного ПО в нагнетании обстановки: мол, компьютер работает без единого сбоя уже пять лет и антивирус мне ни к чему, то есть вирусные эпидемии — вымысел разработчиков, которые борются за расширение рынка.

То есть рост числа зараженных компьютеров связан не только со скептическим отношением пользователей к собственной безопасности, но и с широким распространением пиринговых (P2P) сетей — e-Donkey, KaZaa, Bittorent, а также их аналогов. Работая в этих сетях, пользователи имеют возможность свободного обмена любыми файлами друг с другом. Разумеется, грамотные хакеры практически с момента зарождения P2P-движения стали использовать подобные сети для успешного внедрения троянских вирусов.

Причем, несмотря на то что сегодня многие из P2P-сетей закрыты как противозаконные, на темпах распространения вирусов и спама это не сказалось: охочие до бесплатного ПО пользователи культивируют свободный обмен на сайтах типа www.rapidshare.com и, разумеется, продолжают заражать друг друга и свои корпоративные сети.

AP

ЗАЧЕМ КРАСТЬ КАРТОЧКУ, ЕСЛИ МОЖНО УКРАСТЬ ВСЕ ОСТАЛЬНОЕ

ВИРТУАЛЬНЫЙ МУСОР Многие из нас задаются резонным вопросом: почему нельзя победить тот же спам раз и навсегда? Причин две, и обе они лежат на поверхности.

Во-первых, нельзя уничтожить то, что приносит прибыль, а во-вторых, невозможно сражаться с тварью, которая постоянно регенерирует: вирусы и спам связаны друг с другом, взаимозависимы и, соответственно, нереально живучи. К сожалению, спрос на услуги массовой рассылки существует и он весьма высок.

В феврале 2007 года в Корее арестовали двух спамеров, которые в 2006 году за два месяца разослали в общей сложности 1,6 млрд писем с привлекательными предложениями кредитов под залог недвижимости. Им пришло всего 12 тыс. ответов. Если считать в процентах — невероятно мало, а если в деньгах — довольно прилично: полученную клиентскую базу данных преступники продали заинтересованной компании, оказывающей подобные услуги, за $10–12 тыс. Неплохой доход, не так ли?

Проблема спама сейчас как никогда актуальна. По подсчетам аналитиков «Лаборатории Касперского», порядка 80% всего интернет-трафика нашей страны составляет спам. Огромные вычислительные и сетевые мощности заняты обработкой и передачей огромных куч мусора! В мировом масштабе ущерб в корпоративном и частном секторах исчисляется миллиардами долларов.

Что же касается регенерации, ситуация как нельзя удачно играет на руку злоумышленникам: число пользователей интернета постоянно растет. Только количество Wi-Fi хотспотов в Москве к концу прошлого года перевалило отметку в 1000 единиц, не говоря уже про DSL, EDGE, Ethernet и другие способы подключения к сети. Новые пользователи, как правило, являются дилетантами, поэтому о

СЕГОДНЯ СИТУАЦИЯ УСЛОЖНИЛАСЬ: ХАКЕРЫ И ВИРУС-МЕЙКЕРЫ БОЛЬШЕ НЕ СТРЕМЯТСЯ К ПУБЛИЧНОСТИ, ПОЭТОМУ ВРЕДОНОСНЫЕ ПРОГРАММЫ ЗАЧАСТУЮ РАБОТАЮТ ПО ПРИНЦИПУ КРОТА — ТИХО, НЕЗАМЕТНО, НО МАКСИМАЛЬНО ЭФФЕКТИВНО

РИСУНОК НА ОБЛОЖКЕ: МАРИЯ ЗАЙКИНА

средствах защиты имеют поверхностное представление — как следствие, имеем весьма высокий риск заражения.

Не стоит забывать и про некоторые аспекты проблемы пиратства. Дело в том, что антивирусные базы компаний «большой российской четверки» — «Лаборатории Касперского», Symantec, McAfee и Trend Micro — обновляются несколько раз в день (в особо критических ситуациях — раз в час). Пользователи, на компьютерах которых работает контрафактное ПО, зачастую лишены самой основы систем защиты — возможности загрузки обновленных антивирусных баз. А поскольку, по данным IDC, на текущий момент уровень пиратского программного обеспечения в общем обороте составляет порядка 80%, рассчитывать на очищение российской части интернета от вирусов и спама пока не приходится.

БАНАЛЬНАЯ БДИТЕЛЬНОСТЬ Да, вирусов не становится меньше. Да, количество спама постоянно растет. Но это не означает, что на рынке нет достойной защиты от этого зла. Напротив, современные отечественные антивирусы от Symantec, «Лаборатории Касперского», Trend Micro, MacAfee — вполне способны обеспечить пользователя достойной защитой. Не стопроцентной, но все-таки довольно высокой.

От пользователя и представителей бизнеса требуется не так много — серьезное и комплексное отношение к проблеме. Отказ от пиратского ПО позволит обновлять антивирусные базы и блок-листы спама по мере их обновления. Разъяснительная работа, проводимая службами IT и информационной безопасности, снизит риск заражения и кражи данных по неосторожности.

И наконец, банальная бдительность, воспетая социалистическим плакатным искусством, отнюдь не является бутафорией. Любопытный факт — для того чтобы смартфон пользователя заразился вирусом Kabir, распространяющимся по BlueTooth, от человека требуется как минимум несколько нажатий «Ok» на предложения соединиться с незнакомым телефоном. Статистика печальна: большая часть граждан, не задумываясь о последствиях, соглашается. То есть, по сути, никто не защитит нас, кроме нас самих.

Разработчики антивирусного ПО стараются сделать процесс общения пользователя и системы защиты максимально простым. В частности, на рынке ощущается довольно явная тенденция перехода от разработки нескольких разносторонних продуктов к одному боксу, сочетающему в себе и антивирус, и сканер, и межсетевой экран (FireWall), и анти-спам. Их задача — обеспечение максимально простой интеграции защитных продуктов в экосистему локальной корпоративной сети и совместимость с другим программным обеспечением.

Поскольку корпоративные клиенты в большинстве своем предпочитают не доверять вопросы безопасности одной компании, что совершенно оправданно, разработчикам приходится довольно усердно работать над программным кодом. Потому что когда хранилище файлов компании защищено антивирусом одного производителя, почтовый сервер — другого, а FireWall, фильтрующий трафик,— третьего, очень важно обеспечить бесконфликтность их работы. Ведь эти программы зачастую борются за одни и те же ресурсы системы, пытаются перетянуть одеяло на себя и иногда считают конкурентное защитное ПО тем самым подозрительным вредоносным кодом. В этом, собственно, и заключается главное отличие пользовательского ПО от корпоративного — в высокой степени корреляции с другими системами для получения максимального эффекта.

AP

40 МЛН НОМЕРОВ КРЕДИТНЫХ КАРТ УКРАЛИ В ПОЗАПРОШЛОМ ГОДУ ИЗ ЭТОГО ПРОЦЕССИНГОВОГО ЦЕНТРА CARD SOLUTIONS В АТЛАНТЕ (США)

МОБИЛЬНАЯ ЧАСТЬ В свое время в печати и электронных СМИ довольно активно обсуждалась проблема грядущего апокалипсиса среди пользователей смартфонов и коммуникаторов. Действительно, не стоит забывать о том, что любой смартфон, по сути, является тем же компьютером — со своей памятью, процессором и даже операционной системой, поэтому в теории ничто не мешает спаму, вирусам, троянам и шпионскому ПО плавно переместиться на мобильные платформы со всеми вытекающими отсюда последствиями. Однако слухи о мобильных эпидемиях довольно сильно преувеличены.

Если бы «умные» телефоны впервые появились в массовой продаже лет десять назад, вероятно, мы бы уже вовсю разбирались с последствиями краж информации и мобильным спамом. Однако последние тенденции в сфере киберпреступлений позволяют говорить о том, что никаких массовых эпидемий не произойдет. Поскольку рынок является самоорганизованным — злоумышленники работают по заказу, четко и узконаправленно, массовые эпидемии им не выгодны в принципе. Их появление повышает шансы обнаружения вирус-мейкеров. Вторая причина — отсутствие достаточного количества самих смартфонов по сравнению с теми же компьютерами — хакерам попросту негде масштабно развернуться. Впрочем, нельзя сказать, что они бездействуют. По данным экспертов «Лаборатории Касперского», сейчас существует порядка 35–40 мобильных вирусов, далеко не все их которых безвредны. Но эта цифра пока не способна состязаться с 200-тысячной вирусной базой для обычных компьютеров.

Однако в недалеком будущем, через три-четыре года, можно ожидать такие же выборочные организованные атаки на конкретные компании и персоналии. Поэтому пользователям мобильных устройств также придется заботиться о своей безопасности.

В ТЕОРИИ Доходы криминального кибербизнеса выходят на уровень, сопоставимый с торговлей наркотиками. И остановить их рост в настоящее время невозможно как минимум по двум причинам. Во-первых, большинство крупных компаний, подвергнувшихся атакам, в целях сохранения собственной репутации зачастую умалчивают о фактах вторжения. Такой подход не может не стимулировать злоумышленников. Вторая проблема фундаментальная: интернет изначально не разрабатывался под столь массовые нужды. Это была сугубо закрытая система, в которой военные и ученые могли свободно обмениваться информацией — никто попросту не предполагал такого массового развития.

В итоге мы получили сотни миллионов, по сути, анонимных пользователей — любой желающий может прийти в питерское интернет-кафе и устроить вирусную эпидемию в Германии. Каждый более или менее подкованный хакер может прикрыться чужим IP-адресом, чтобы взломать банк или базу данных. В сети не предусмотрено никаких процедур персонализации.

В идеале каждый, кто подходит к компьютеру и намеревается выполнить одну из операций в сети, должен представиться — скажем, по рисунку сетчатки глаза или отпечатку пальца. Это нужно для того, чтобы любая операция привязывалась к конкретной персоналии.

В теории эта глобальная и сложная задача вполне реализуема. Но, к сожалению, не на данном этапе развития сети. Однако если противоборство брони и снаряда будет продолжаться теми же темпами, мировое сообщество в течение ближайших пяти лет придет к необходимости весьма существенного пересмотра вопроса присутствия в сети и подхода к информационной безопасности в целом. ■

> НОВАЯ АНТИВИРУСНАЯ КОМПАНИЯ

По оценкам исследовательской компании IDC, рынок антивирусного ПО, чей объем в 2006 году составил около 2,09 млрд. долларов, стабилен и растет не более чем на 10% в год. 80% продаж обеспечивают три крупнейших производителя — Symantec, McAfee и Trend Micro.

Важнейшим событием конца 2006-начала 2007 года для всех производителей антивирусного ПО стал выход новой версии операционной системы от Microsoft - Windows Vista. К моменту начала поставок корпоративных выпусков Windows Vista (30 ноября прошлого года) большинство вендоров не успели обеспечить совместимость своих продуктов с новой ОС. Первой проблемой неожиданно стало наличие в Vista значительно усовершенствованных и переработанных функций безопасности, в частности, технологии защиты ядра операционной системы PatchGuard. Технология PatchGuard, реализованная в 64-битной версии Windows Vista, предназначена для блокирования доступа к ядру операционной системы вредоносных программ. Это вызвало резко негативную реакцию производителей антивирусного ПО, т.к. большинство антивирусов, включая продукты компаний McAfee, Symantec и Лаборатории Касперского, активно используют доступ к ядру для реализации части важных функций. В то же время, в технологии PatchGuard практически сразу после появления предварительных релизов были найдены уязвимости, позволяющие вредному коду отключать или обходить эту функцию. К выпуску окончательной версии корпорация Microsoft устранила обнаруженные «дыры», но вопрос о наличии других потенциального уязвимых мест новой защиты ядра остался открытым. То есть производители антивирусного ПО оказались в проигрыше относительно вирусописателей — вполне возможно, что зловредный код сможет отключать защиту ядра, а борющиеся с ним программы — нет.

Следует отметить, что у некоторых производителей антивирусов, таких как ESET NOD32 и малоизвестный в России Sophos, не возникло проблем с выпуском совместимых с Vista версий, так как в их продуктах не используется прямой доступ к ядру ОС.

Не исключено, что такая политика софтверного гиганта связана с планами отвоевать часть рынка для собственного антивирусного решения, интегрированного с операционной системой — Microsoft OneCare. Антивирус OneCare не встроен в операционную систему, а предлагается по подписке вместе с другими сервисами Windows Live. Выпуск Microsoft собственного антивирусного решения заставил задуматься всех производителей антивирусного ПО — всем памятны примеры постепенного завоевания корпорацией доминирующего положения в различных сегментах рынка даже в тех случаях, когда качество продукта уступало конкурентам. Microsoft воспринимает угрозы безопасности, как главный фактор, заставляющий пользователей задумываться об альтернативных операционных системах, поэтому взять защиту от вредоносного ПО в свои руки выглядит логичным шагом. Пока опасения вендоров оказались преждевременными.

Начало 2007 года ознаменовалось целой серией плохих новостей, связанных с качеством работы нового антивируса. Сначала OneCare провалил два независимых тестирования качества обнаружения вирусов. В тестировании известного специалиста по безопасности Андреаса Клементи, регулярно размещающего результаты тестирования ПО для защиты от вредоносного кода на веб-сайте AV Comparatives, продукт Microsoft оказался худшим из 17- и протестированных. Кроме того, Microsoft OneCare не получил сертификата VB-100, выдаваемого по результатам исследования независимой организацией Virus Bulletin. Затем специалисты сообщили о некорректной работе при сканировании хранилища приложения для работы с электронной почтой самой корпорации Microsoft — обнаружение вируса в письме приводило к удалению или порче всего PST, в котором хранится вся переписка пользователей. Техническая поддержка Microsoft рекомендовала пользователям регулярно создавать резервную копию файла .PST. После такого старта корпорация Microsoft признала, что ее антивирус OneCare требует доработки.

Тем не менее, в будущем, OneCare сможет занять определенную долю рынка. Как и в случае со встроенным в Windows файрволлом, антивирус от Microsoft может оказаться оптимальным выбором для нетребовательных пользователей, не уделяющих безопасности первостепенного внимания. При более основательном подходе к безопасности, например на корпоративном рынке, Microsoft придется конкурировать с традиционными производителями антивирусного ПО на равных.

АНДРЕЙ ВИНОКУРОВ

ЗАЩИТА ОТ ИНСАЙДЕРА

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ПОЯВИЛИСЬ ПРАКТИЧЕСКИ ОДНОВРЕМЕННО С ШИРОКИМ РАСПРОСТРАНЕНИЕМ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. ОДНАКО О СЕРЬЕЗНОСТИ УГРОЗЫ УТЕЧЕК ИЛИ УТРАТЫ ИНФОРМАЦИИ В РЕЗУЛЬТАТЕ ДЕЙСТВИЙ ИНСАЙДЕРОВ СПЕЦИАЛИСТЫ СТАЛИ ВСЕРЬЕЗ ЗАДУМЫВАТЬСЯ ТОЛЬКО НЕСКОЛЬКО ЛЕТ НАЗАД. А В ПОСЛЕДНЕЕ ВРЕМЯ ЧУТЬ ЛИ НЕ ЕЖЕМЕСЯЧНО СТАНОВИТСЯ ИЗВЕСТНО О ПОЯВЛЕНИИ В ПИРАТСКОЙ ПРОДАЖЕ БАЗ ДАННЫХ С КОНФИДЕНЦИАЛЬНЫМИ ДАННЫМИ О ГРАЖДАНАХ И КОМПАНИЯХ, «УТЕКШИХ» ИЗ ГОСУЧРЕЖДЕНИЙ И БАНКОВ. АНДРЕЙ ВИНОКУРОВ

НЕОБХОДИМОЕ ВО ЗЛО Традиционным подходом к борьбе с утечками являются организационные меры и запретительные политики: отключение на компьютерах сотрудников коммуникационных портов, доступа к определенным сайтам; запрет на пользование открытыми почтовыми службами и программами мгновенного обмена сообщениями. Нередки ситуации, когда с компьютеров служащих банка вообще нет доступа во «внешний мир», за исключением корпоративной электронной почты.

Как показывает практика, такие меры не всегда работают. Во-первых, глобальные запреты могут серьезно влиять на производительность: сотрудники из-за ограничений просто не могут получить доступ к нужной им информации или он затруднен. Во-вторых, принцип «все запретить» обычно не может защитить от действий злонамеренных инсайдеров, допускающих утечку данных не по ошибке, а сознательно. Компания, полагаясь на политику общего запрета, не контролирует действия с информацией внутри охраняемого периметра, а в политике запретов всегда есть послабления, вызванные производственной необходимостью.

«Если запретить все опасное и разрешить только самое необходимое (почта, интернет), но не обеспечивать контроль и аудит, например архивирование всего почтового и веб-трафика для ретроспективного анализа инцидентов, подготовки доказательства вины и соответствия требованиям нормативных актов, то данные все равно будут утекать»,— говорит Денис Зенкин, директор по маркетингу компании InfoWatch.

Полностью предотвратить утечки невозможно никакими техническими и организационными мерами — благодаря распространению персональных цифровых устройств любые документы, к которым имеет доступ широкий круг лиц, могут покинуть пределы компании, вопреки желанию ее руководителей. Сейчас трудно встретить мобильный телефон без встроенной цифровой камеры, и, в конце концов, нелояльный сотрудник может просто сфотографировать открытый на экране ПК или лежащий на столе документ.

Однако наибольший финансовый и репутационный урон наносят компаниям утечки больших объемов данных, например баз данных клиентов с информацией о банковских картах (которые затем могут быть использованы для кражи денег с банковских счетов) или сведений о заемщиках банка, включая их персональные данные.

Совсем недавно для специалистов по ИТ-безопасности стала очевидной потребность в специализированных решениях проблемы защиты критически важных данных от инсайдеров.

Защита от непреднамеренного или умышленного распространения конфиденциальных данных за пределы организации требует комплексного подхода: определения защищаемых данных, разработки политики ИТ-безопасности, обучения сотрудников, учета всех возможных каналов утечек. При создании полномасштабной системы информационной безопасности следует учитывать не только все возможные способы совершения внутренних атак и пути утечки информации.

НИКАКАЯ ЗАЩИТА НЕ СПАСЕТ ОТ ПРЕСЛОВУТОГО ЧЕЛОВЕЧЕСКОГО ФАКТОРА

AFP/GURTERIMAGES

Технически утечка может произойти по множеству каналов: через корпоративный почтовый сервер с помощью электронной почты, через интернет-канал при использовании бесплатных почтовых систем или веб-служб для размещения файлов, посредством беспроводных подключений (Wi-Fi, Bluetooth) через принтер — при физической печати документов, а также через мобильные носители: дискеты, оптические диски или мобильные накопители.

КОРНЕВЫЕ СИСТЕМЫ Программные и аппаратные средства, предназначенные для борьбы с этими утечками, аналитики IDC нарекли ILD&P-системами (Information Leakage Detection and Prevention).

ILD&P-решения — молодой рынок. Его развитие началось несколько лет назад с небольших компаний-стартапов, получивших венчурные инвестиции. Поэтому стандарты архитектуры специализированных решений защиты от утечек и злонамеренных действий инсайдеров пока не сформировались, и каждый производитель доказывает оптимальность именно своего подхода. Многие системы, представленные на рынке, развивались из специализированного ПО — например, софта для управления коммуникационными портами ПК или систем контроля доступного в корпоративной сети веб-содержимого.

За последние несколько лет крупнейшие производители антивирусов дополнили список своих продуктов не только файрволлами и решениями для борьбы со спамом, но и продуктами ILD&P. Например, компания McAfee в конце 2006 года приобрела израильский стартап Onigma и включила разработанную им систему предотвращения утечек данных в состав своих корпоративных решений.

Другой крупнейший производитель ПО в области информационной безопасности, Symantec, самостоятельно разрабатывает Symantec Database Security, контролирующий доступ пользователей к базам данных, содержащих критически важную информацию. А компания Websense, специализирующаяся на продуктах для контроля доступа к веб-содержимому, приобрела разработчика ПО PortAuthority, получив возможность предлагать клиентам комплексное решение по защите доступа к данным. Российский производитель InfoWatch, являясь дочерней компанией производителя антивирусов «Лаборатория Касперского», интегрирует свои продукты с корпоративными решениями AVK.

Целый ряд компаний предлагает ILD&P-системы, основой которых являются специальные программные агенты, устанавливаемые на компьютеры пользователей корпоративной сети. Например, продукт Sanctuary Device Control компании SecureWave позволяет системно контролировать доступ пользователей к интерфейсам USB, LPT, FireWire, Bluetooth, Wi-Fi, IrDA, PCMCIA, COM, IDE, SATA, поддерживая централизованное управление разрешениями и ведение журналов.

Программные агенты PC Activity Monitor (Acme) компании Raytown Corp. устанавливаются на все компьютеры корпоративной сети и внедряются в операционную систему на уровне ядра, что не позволяет пользователю отключить или обойти их (следует отметить, то Microsoft заблокировала возможность модификации ядра в ОС Windows Vista). Все действия пользователя по печати, копиро-

СОВСЕМ НЕДАВНО СПЕЦИАЛИСТАМ ПО ИТ-БЕЗОПАСНОСТИ СТАЛА ОЧЕВИДНА ПОТРЕБНОСТЬ В СПЕЦИАЛИЗИРОВАННЫХ РЕШЕНИЯХ ПРОБЛЕМЫ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ДАННЫХ ОТ ИНСАЙДЕРОВ

ванию, изменению защищаемых данных сохраняются в журнале, с которым можно работать централизованно. Однако передача информации по сети не контролируется.

Американская компания Verdasys реализовала с помощью агентов для ПК комплексное решение по защите: устанавливаемые на ПК и ноутбуки агенты контроля Digital Guardian предотвращают все каналы утечек непосредственно на компьютерах пользователей. При этом сервер управления используется для централизованного развертывания, настройки политик контроля и сбора журнала событий.

Еще один класс решений — системы, контролирующие информацию при передаче по сети. Обычно эти приложения используются для мониторинга почтового или сетевого трафика.

Продукты «Дозор-Джет», разработанные российской компанией «Инфосистемы Джет», предназначены прежде всего для контроля веб-трафика, фильтрации и архивирования электронной почты. Предотвращение потенциальных утечек обеспечивается за счет блокирования подозрительных соединений и писем (помещение в карантин). Кроме того, реализована важная функция накопления архива почтовых сообщений.

Некоторые системы, такие, как Onigma Platform (приобретенная в прошлом году McAfee), совмещают в себе функции пользовательских агентов и контроля трафика. При этом системы обеспечивают, как минимум, функции централизованного управления и развертывания, а также ведения журналов.

У систем, использующих фрагментарный подход, есть несколько существенных минусов. Например, ПО, контролирующее десктопы пользователей, обычно не обеспечивает архивирование электронной почты, тогда как наличие архива переписки обычно очень важно для расследования инцидентов безопасности и сбора доказательств. Кроме того, большинство из них не имеют возможности предотвратить (блокировать) утечку данных, инцидент безопасности может быть выявлен только постфактум, при анализе журналов.

Эволюцией решений, защищающих локальные участки, стали комплексные системы, контролирующие все возможные направления утечки данных.

Комплексные решения стремятся контролировать операции с данными на всех стадиях их хранения (серверы, базы данных), использования (рабочие станции пользователей, операции копирования изменения, печати и т. п.) и передачи по внутренним и внешним каналам (в сети, по электронной почте, на веб-узлы и т. п.). Непременным условием является хранение архива переданной информации (например, электронной почты) и действий по использованию защищаемых данных. Например, в решении российского производителя InfoWatch архивируются все сообщения электронной почты за семь лет и ведутся журналы отчетов от модулей контроля в универсальном архиве. Все это сопровождается функциями выявления инцидентов и создания отчетов по использованию данных.

Важной особенностью корпоративного решения InfoWatch является разделение прав операторов («офицеров информационной безопасности») для разделения ответственности. Это позволяет контролировать важную угрозу — похищение данных ИТ-персоналом или сотрудниками службы безопасности, имеющими доступ к данным (по мнению экспертов, ряд последних утечек из госорганов и банковских структур произошел при посредничестве обиженных работодателями ИТ-специалистов).

Для определения конфиденциальной информации, требующей защиты, в системах ILD&P в основном применяются вероятностные методы распознавания защищаемых данных — морфологический и сигнатурный анализ, а также технология «водяных знаков» (digital fingerprints). При применении сигнатур (наборов ключевых слов) (используется, например, в MIMEsweeper и Symantec Gateway Security) в базе фильтрации необходимо хранить все синтаксические формы ключевого слова (падежи, роды, спряжения, число и их сочетания). Для русского языка задача осложняется тем, что все словоформы должны храниться во всех кодировках.

КАКИЕ ПРОГРАММЫ ДОЛЖНЫ БЫТЬ НА НЕМ УСТАНОВЛЕНЫ, РЕШАЕТ РУКОВОДСТВО КОМПАНИИ. СОТРУДНИК, ВЫПОЛНЯЯ СВОИ СЛУЖЕБНЫЕ ОБЯЗАННОСТИ, ДОЛЖЕН ПОЛУЧАТЬ ДОСТУП ТОЛЬКО К ТОЙ ИНФОРМАЦИИ, НА КОТОРУЮ ИМЕЕТ ПРАВО

В решении InfoWatch используется комбинированный подход: пересылаемые данные сканируются на предмет наличия предопределенных ключевых слов и фраз. Лингвистический анализ позволяет учесть контекст, в котором используются ключевые слова и фразы. Кроме того, передаваемые данные сравниваются с постоянно обновляемыми «шаблонами» конфиденциальных сообщений, специфичных для каждого конкретного заказчика. При любом из этих методов требуется существенная настройка на информационную среду заказчика.

ОХРАНЯЕМЫЙ ПЕРИМЕТР Но пока продукты ILD&P нацелены на крупных корпоративных заказчиков. В мелких и средних фирмах такой уровень защиты данных от утечек зачастую не нужен, а ИТ-бюджет не предусматривает серьезных трат на этот аспект информационной безопасности.

Например, 55% всех внедрений программных продуктов «Дозор-Джет» осуществлены в крупных организациях (от 1 тыс. до 15 тыс. сотрудников), 28% — в средних (от 300 до 1 тыс. сотрудников) и лишь 17% — в организациях малого бизнеса (до 300 сотрудников). По данным компании InfoWatch, стоимость системы, включая затраты на внедрение, может составить $300–400 на одно рабочее место.

То есть пока ILD&P-системы не являются «коробочным» продуктом и требуют комплексного внедрения, подразумевающего стадии консалтинга (оценка существующей ИТ-инфраструктуры, коррекция или разработка политики защиты данных, установка и настройка ПО, обучение специалистов, отвечающих в компании за ИТ-безопасность).

Вендоры ПО защиты от внутренних утечек разрабатывают методологии внедрения, помогающие системным интеграторам и заказчикам интегрировать систему защиты от утечек в существующую ИТ-инфраструктуру и перекрыть все возможные каналы утечки данных. Кроме того, обычно решение требует значительной кастомизации в соответствии с требованиями заказчика и настройки под конкретные типы защищаемых данных.

Интенсивное развитие продуктов этого класса в ближайшие несколько лет приведет к стандартизации подходов, используемых для защиты данных внутри «охраняемого периметра». По мнению Дениса Зенкина из InfoWatch, продукты станут более «коробочными» и вендоры, окончательно поделившие рынок крупных клиентов, ринутся в сегмент небольших компаний.

Впрочем, уже сейчас очевидно, что обнаружение утечки после того, как она произошла, не может устраивать пользователей подобных систем. Функции интеллектуального предотвращения инцидентов являются основным полем для конкуренции и развития продуктов. Разработка ведется в направлении проактивных методов защиты, когда утечка распознается и блокируется на ранней стадии благодаря сопоставлениям действий пользователя с шаблонами подозрительной активности, а также выявлениям нетипичных операций.

Часть функций систем защиты от утечек может быть возложена на выделенные аппаратные компоненты. Модули системы, которым необходимо обслуживать большой объем операций (например, средства фильтрации данных, передаваемых по интернет-протоколам, или обращения к серверу баз данных), могут предлагаться заказчику в виде специализированного устройства (заменяющего выделенный сервер, на который устанавливается аналогичный программный компонент). В некоторых ситуациях это позволяет сократить затраты на оборудование и упростить развертывание решения в филиалах компании.

Тем не менее даже при использовании самых совершенных систем защиты от утечек требуется комплекс организационных мер — таких, как лишение пользователей прав администратора на ПК и стандартизация ПО. Такие меры способны затруднить использование средств, например шифрования и стеганографии, затрудняющих работу механизмов контентной фильтрации.

Будущее ПО обеспечения информационной безопасности — интеграция функций защиты от различных типов угроз, внутренних и внешних, в единые системы комплексной защиты. ■

«ДЕФИЦИТ КВАЛИФИЦИРОВАННЫХ УПРАВЛЕНЦЕВ»

Информационная безопасность — это необходимая часть корпоративной культуры, за которую несут ответственность все сотрудники компании, уверен РОБЕРТ ЭЙДЖИ, вице-президент, глава представительства компании Cisco Systems в странах СНГ. Об особенностях информационной безопасности с представителем крупнейшей мировой компании, определяющей принципы и подходы развития рынка ИТ-безопасности, беседовал ЕВГЕНИЙ ЧЕРЕШНЕВ.

BUSINESS GUIDE: Как вы оцениваете уровень развития рынка информационной безопасности в России?

РОБЕРТ ЭЙДЖИ: Скажем так, до совершенства еще далеко. Россия перестала изобретать велосипед, начала интегрировать, лицензировать и адаптировать международный опыт в области информационной безопасности в свою практику.

BG: Российский бизнес, на ваш взгляд, готов перенимать западный опыт в области информационной безопасности?

Р. Э.: Информационная безопасность и в США тема открытая, ею занимаются многие, но даже там впервые задумались о том, как просчитать окупаемость вложений в IT только два-три года назад. А до того, чтобы оценить возврат инвестиций в информационную безопасность, дело еще даже там не дошло.

BG: В ближайшие годы ситуация изменится?

Р. Э.: Как сегодня решаются проблемы безопасности? Наверняка где-то на периметре установлен FireWall и антивирус, как максимум — VPN. Редко дело доходит до более сложных систем. Поэтому в данных условиях, я думаю, в России все будет протекать весьма медленно и спокойно. Думаю, ничего революционного не произойдет. Все, что так или иначе востребовано рынком, уже изобретено, запатентовано, и в настоящее время компании пытаются все это изобилие превратить в нечто удобное, простое в управлении и для интеграции. В свое время по рынку долго ходил анекдот: «Чем отличается Windows 95 от Windows 98? Тем, что в первой не используется 95% ее возможностей, а во второй — 98%». Это утрированная ситуация, но не лишенная смысла.

BG: А в чем тогда проблема — в недостаточной квалификации ИТ-специалистов?

Р. Э.: В России действительно наблюдается острый дефицит квалифицированных управленцев. Отделы безопасности, как правило, возглавляют выросшие системные администраторы, программисты и математики, прекрасно владеющие технической стороной вопроса, но далекие от бизнеса — они попросту не умеют объясниться с руководителем на языке бизнеса, а не специфической терминологии. Второй вариант — директора по информационной безопасности старой закалки, которым, как правило, существенно за 50, а следовательно, и безопасность для них ассоциируется с противодействием на электромагнитных импульсах и наводках, шифровании и режимном документообороте. Что старомодно.

Но главная причина в другом. Российский топ-менеджмент еще не осознал, что информационная безопасность не технологическая проблема, а такой же бизнес-процесс, как, например, биллинг. Это часть корпоративной ответственности, за что отвечает и IT-директор, и CEO компании, и HR-отдел. Каждый сотрудник компании, все должны быть вовлечены в обеспечение безопасности.

BG: Зачем при этом вовлекать всех сотрудников?

Р. Э.: Человеческий фактор в информационной безопасности играет огромную роль. Утечки информации часто имеют место не потому, что FireWall пропустил атаку, а антивирус упустил свежего интернет-червя. Сотрудники теряют информацию, потому что не знают, как ее уберечь, или, что страшнее, делают это сознательно.

BG: Бывает и обратная ситуация. Системный администратор урезает права сотрудника так, что не открывается даже календарь! И к этому в итоге сводится обеспечение безопасности компании…

Р. Э.: Компьютер, за которым работает сотрудник, ему не принадлежит, поэтому то, какие программы должны быть на нем установлены, решает сама компания. Сотрудник, выполняя свои служебные обязанности, должен получать доступ только к той информации, на которую имеет право. Однако все это совершенно не означает, что надо впадать в крайность. Проблема России в известном максимализме: зачастую сотрудники привязаны к офису, а их рабочие места настроены так, что для качественного выполнения своих обязанностей им попросту не хватает инструментов. Такое положение вещей к информационной безопасности не имеет никакого отношения.

КРУПНЕЙШИЕ УТЕЧКИ ИНФОРМАЦИИ В РОССИИ

В 1992 году в Москве впервые появились компакт-диски с информацией о физических лицах—абонентах МГТС. Источник утечки не найден.

В 1996 году в продаже появилась информация об абонентах сотового оператора «Вымпелком». Компания позднее заявила, что нашла и наказала виновных.

В ноябре 2002 года в Москве появились диски с данными об абонентах сети МТС, в январе 2003 года вышел второй — с информацией о 5,5 млн абонентов. Источник утечки не найден.

20 мая 2003 года в Санкт-Петербурге появились диски с данными о 4,5 млн клиентов сотовых компаний «МегаФон», «Телеком XXI», «Северо-Западный телеком» и «Петерстар». По одной из версий, утечка была через правоохранителей.

В июле 2004 года «Вымпелком» сообщил о сайте sherlok.ru, предлагавшем информацию об абонентах «Билайна», «МегаФона» и МТС в Москве и Санкт-Петербурге. 26 ноября задержаны семеро подозреваемых, в числе которых трое сотрудников «Вымпелкома». В марте 2005 года суд приговорил их к штрафам.

В феврале 2005 года в Москве появилась база данных о банковских операциях Центробанка в 2003–2004 годах, 20 мая вышло дополненное издание. 25 октября заместитель главы управления безопасности и защиты информации МУ ЦБ Владимир Бабкин заявил, что канал утечки перекрыт.

В ноябре 2005 года появились в продаже данные о доходах за 2004 год 9,9 млн жителей Москвы и области. 16 ноября 2005 года ФСБ объявила о задержании лиц, причастных к хищению баз данных Центробанка РФ и ФНС. Их имена и судьба неизвестны.

15 августа 2006 года ряд бюро кредитных историй и банков получили предложение купить базу данных заемщиков, бравших потребительские кредиты. База содержала 700 тыс. записей. 7 сентября гендиректор Национального бюро кредитных историй Александр Викулин заявил, что утечка была из нескольких банков.

В октябре 2006 года Генпрокуратура РФ возбудила уголовное дело в отношении чиновников из аппарата правительства РФ, передавших представителю компании ТНК-ВР «копии документов с конфиденциальной информацией». В сообщении Генпрокуратуры подчеркивалось, что материалы могли быть использованы в целях, противоречащих «интересам государства в области энергетики».

За месяц до выхода нового романа Виктора Пелевина «Empire V», назначенного на начало ноября 2006 года, его текст появился в сети. Роман был украден из компьютерной системы издательства. По словам главы издательства «Эксмо», где готовили к печати рукопись, Леонида Шкуровича, удалось вычислить личность похитителя, но не удалось собрать против него конкретных улик. Подозреваемый не был штатным сотрудником «Эксмо».

АНДРЕЙ ВИНОКУРОВ

«А В ФСБ ДРУГАЯ СИСТЕМА СЕРТИФИКАЦИИ»

СЕГОДНЯ НИ ОДИН СЕРТИФИКАТ НЕ ГАРАНТИРУЕТ СТОПРОЦЕНТНОЙ ЗАЩИТЫ ДАННЫХ, УТВЕРЖДАЕТ ДИРЕКТОР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ MICROSOFT В РОССИИ ВЛАДИМИР МАМЫКИН В БЕСЕДЕ С КОРРЕСПОНДЕНТОМ BG ЕВГЕНИЕМ ЧЕРЕШНЕВЫМ. ПАНАЦЕЕЙ НЕ БУДЕТ И ПРОДУКТ, СЕРТИФИЦИРОВАННЫЙ ОРГАНАМИ ФСБ, СТРОГО СЛЕДЯЩИМИ ЗА СОВМЕСТИМОСТЬЮ ШИФРОВАЛЬНЫХ ПРОЦЕССОВ С АЛГОРИТМАМИ ГОСТ. ДАЖЕ ГОСУДАРСТВЕННЫЕ СЕКРЕТЫ УЯЗВИМЫ ДЛЯ АТАК ЗЛОУМЫШЛЕННИКОВ, ПОКА ИМЕЕТ СИЛУ ЧЕЛОВЕЧЕСКИЙ ФАКТОР.

ВЛАДИМИР МАМЫКИН, ДИРЕКТОР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ MICROSOFT В РОССИИ

BUSINESS GUIDE: Почти во всем цивилизованном мире сертификация программного обеспечения имеет международный статус. То есть сертификат на операционную систему, полученный, например, в США, будет действителен и в Европе, и в Азии, и в Латинской Америке. Везде, но не в России. С чем это связано?

ВЛАДИМИР МАМЫКИН: Я считаю, что в России очень правильная практика. Россия в свое время научилась хорошо защищать свои секреты от внешних угроз, поэтому у нас есть чему поучиться. Любая сертифицированная версия Windows, продающаяся в России, в обязательном порядке имеет свой персональный идентификационный номер, голографическую наклейку и набор необходимой документации.

Делается это для того, чтобы версия программного обеспечения, устанавливаемая в том числе на компьютеры государственного сектора, целиком, бит к биту совпадала с оригиналом, прошедшим сертификацию. Иначе где гарантия того, что, установив в своей компании Microsoft Windows XP, вы получите именно ее?

Встает вопрос доверенной загрузки — является ли то, что вы видите на экране, действительно Windows? Быть может, злоумышленник, решив получить доступ к секретам компании, создал и продал вам оболочку, эмулирующую работу системы — установку, загрузку, работу корпоративными ресурсами, и с набором программ по перехвату секретов. И пока вы, как вам кажется, работаете, внедренные программы пересылают ему ваши секреты, пароли, базы данных и так далее. Поэтому сертификация, проводимая ФСТЭК (бывшей Гостехкомиссией),— процедура хоть и сложная, но оправданная.

BG: Такая сертификация дает стопроцентную гарантию защиты от «закладок» и других прочих причин утечек секретов?

B. M.: Нет, конечно, не дает. Важно, в каком окружении находятся ваши системы. Известен надежный способ защиты данных, который сохраняет ваши секреты даже с самыми «дырявыми» программами. Его, кстати, иногда используют.

Для этого достаточно выкопать глубоко под землей бункер со стальными стенами толщиной не менее десяти сантиметров, запереть в нем компьютер с «дырявыми» программами, поставить на входе настоящего вооруженного часового, который будет пускать для работы на компьютере только вас, не давая вам ничего внести и ничего вынести (для этого просто переодевая вас целиком!). И при этом, конечно, никаких сетей и интернета.

Метод дает почти стопроцентную гарантию сохранности секретов. Работать только неудобно. И наоборот, если вы поедете в метро с самым суперзащищенным компьютером, в котором стоят сертифицированные по высшему классу программы, и будете там работать со своими секретами, они тут же станут доступны окружающим пассажирам: они их просто увидят. Поэтому, к сожалению, в современном мире всегда приходится искать некий баланс между защищенностью и комфортом.

BG: Но так или иначе, роль системы весьма значительна. А Microsoft, например, до сих пор очень обвиняют в том, что Windows полна уязвимостей, особенно в сравнении с Linux и Apple MacOS X…

B. M.: Количество найденных уязвимостей системы зависит не только от ошибок разработчиков, но и от степени интереса взломщиков. На сегодняшний день под Windows работает подавляющее количество компьютеров на планете. Разумеется, для получения максимальной выгоды взломщикам намного интереснее ломать Windows, чем Linux.

Но в настоящий момент, согласно независимым экспертам, Linux и MacOS значительно опережают Windows по количеству уязвимостей. Например, по результатам отчета CERT за 2005 год, только в ядре Linux было найдено более 350 уязвимостей, в то время как во всех продуктах Microsoft их было 219 — около 4% от общего числа уязвимостей, найденных в 2005 году. А для MacOS только за три месяца 2007 года руководству Apple пришлось выпускать патчи для латания целых 62 уязвимостей.

Кроме того, как я уже говорил, безопасность складывается из нескольких факторов: ничто не убережет информацию от кражи, если на компьютере помимо операционной системы не установлен антивирус, а пользователь, не задумываясь, открывает вложенные файлы от незнакомых адресатов.

Надо соблюдать, как я люблю говорить, базовые правила «компьютерной гигиены». А в случае работы с действительно конфиденциальной информацией еще и консультироваться со специалистами, той же ФСТЭК.

Ведь на безопасность влияет все: и система, и «железо», и даже место компьютера в комнате. Многие не знают, но во времена, когда компьютеры комплектовались ЭЛТ-мониторами, при наличии специальной аппаратуры можно было считать их сигнал с расстояния в 200 метров, настолько сильно они излучали. Сейчас дисплеи стали существенно более безопасны, однако это совершенно не означает, что с помощью спецсредств наблюдения злоумышленник, находящийся в соседнем здании, не сможет в деталях изучать и даже записывать все, что происходит на дисплее компьютера, стоящего «лицом» к окну.

BG: Помимо ФСТЭК, Windows прошли сертификацию в ФСБ. Чем отличаются эти процедуры?

B. M.: Требования к сертификации в ФСБ, в отличие от требований ФСТЭК, не являются открытыми. В ФСТЭК система сертификации является точным аналогом международной сертификации по «Общим критериям». А в ФСБ другая система сертификации.

Она отвечает за те процессы системы, которые связаны с шифрованием. Ведь именно шифрование обеспечивает гарантированность защиты государственных секретов. В частности, ФСБ проверяет, что алгоритмы шифрования ГОСТ, с помощью которых и можно шифровать государственные секреты, корректно работают с Windows.

Версией Windows, получившей сертификат ФСБ, может воспользоваться любой желающий, однако она в целом предназначена для тех, кому действительно необходим сертификат ФСБ. Для его получения российскими спецслужбами был разработан дополнительный модуль к Windows — Secure Pack Rus, который выполняет контролирующие функции.

BG: А чем занимается Secure Pack Rus?

B. M.: Так как это не наша разработка, то мы не старались особо вникать ее суть. Просто без нее получить сертификат ФСБ было нельзя — что-то там в нашей системе не удовлетворяло их требованиям. А с этим модулем все требования ФСБ выполняются. Вообще говоря, во многих странах есть свои требования к системам, используемым в госструктурах. И не всегда эти требования доступны. Это есть и в Европе, и в Японии, и в США. Это нормально.

BG: Бывали ли случаи, когда в результате проверки Windows специалисты ФСТЭК или ФСБ РФ обнаруживали дефекты системы?

B. M.: Мне о таких случаях неизвестно.

BG: В операционную систему встроены определенные криптографические возможности, позволяющие владельцу компьютера довольно надежно хранить свои данные. В этой связи невольно приходит в голову вопрос о существовании мастер-ключа, с помощью которого теоретически можно открыть любой файл.

B. M.: Подобная аналогия появилась потому, что среди нас много людей путешествующих, часто останавливающихся в отелях. Что происходит, когда вы теряете ключ от своего номера? Приходит портье с мастер-ключом и спокойно открывает дверь. Однако сравнивать электронный ключ с металлическим неправильно. Для обычного замка в принципе можно изготовить универсальную отмычку. А вот сделать универсальный электронный ключ для расшифровывания нельзя в принципе.

Это я вам как профессионал говорю. Как человек, который более 20 лет занимался теорией и практикой шифрования в КГБ. На этом и держится наука криптография, которую используют для защиты своих секретов все без исключения страны мира. Помню такой случай, когда я работал до Microsoft в другой компании, которая также производила средства шифрования жестких дисков.

Приходят как-то к нам военные, показывают захваченный во время какой-то из операций с преступниками жесткий диск, зашифрованный нашей программой, просят расшифровать мастер-ключом. А мы не можем, не можем в принципе! Так как только пользователь, знающий свой ключ шифрования, может расшифровать диск.

Эта ситуация общая. Ни Microsoft, ни другая компания, использующая шифрование в продуктах, не имеют возможности им помочь. В современных условиях, когда длина ключа достигает 512 бит и больше, утерянный ключ означает безвозвратную потерю данных. Время, необходимое на расшифровку, может исчисляться миллионами лет. К этому вопросу автоматически напрашивается еще один — о так называемых недокументированных возможностях, о способности управлять информационными системами вопреки владельцу системы.

BG: Да, есть такой вопрос! Были ли просьбы вставить «закладки» в какой-то из ваших продуктов?

B. M.: Что ж, я могу на него ответить просто, с точки зрения бизнеса. Это будет понятнее и доказательнее. Для крупной транснациональной корпорации вроде нашей совершенно невыгодно встраивать такие функции в продукты. Просто невыгодно! Если договоренность о встройке таких функций с каким-то государством произойдет и о ней узнают другие страны, то такая компания потеряет все рынки сбыта, кроме страны, с которой она договорилась о таком темном деле.

А это убытки такого уровня, в том числе и финансовые, и репутационные, которые никакая транснациональная корпорация не может себе позволить. Да и любому государству намного выгоднее иметь в своих рядах масштабного налогоплательщика. А страну местопребывания сейчас так легко сменить. Кстати, не так давно в Великобритании депутат парламента возмущался, что в Windows Vista не предусмотрено подобных функций, и предлагал их встроить с тем, чтобы спецслужбы могли получать информацию с компьютеров. Мы, разумеется, отказались.

BG: Насколько Windows Vista более защищена по сравнению с той же XP? Совершенно понятно, что речь идет о разных архитектурах, но бизнес лучше понимает язык цифр.

B. M.: Хороший вопрос, но, к сожалению, я не знаю, как на него проще ответить. Появление Vista не означает, что Windows XP SP2 отныне продукт второго сорта или небезопасна. Даже с предыдущей версией операционной системы вы можете получить потрясающую защищенность, если ваши специалисты правильно ее настроят и будут вовремя скачивать необходимые апдейты.

Но у Vista совершенно другая архитектура: в ней заложено гораздо больше средств обеспечения безопасности. Вопрос в том, что все это надо уметь настраивать. Для того чтобы сделать систему максимально неприступной, требуются определенные знания и навыки. Конечно, Windows, в отличие от Linux, устанавливается в автоматическом режиме и начинает работать без дополнительных настроек. Но это не означает, что система Microsoft Windows Server проста — у опытного системного администратора она будет непробиваема, а вот у плохого администратора — весьма средненькой. Полностью защищенных систем не бывает. Поскольку это процесс и в нем всегда есть слабое звено — люди. ■

ИЗВЕСТЕН НАДЕЖНЫЙ СПОСОБ ЗАЩИТЫ ДАННЫХ: ВЫКОПАТЬ ГЛУБОКО ПОД ЗЕМЛЕЙ БУНКЕР СО СТАЛЬНЫМИ СТЕНАМИ, ЗАПЕРЕТЬ В НЕМ КОМПЬЮТЕР И ПЕРЕОДЕВАТЬСЯ (ЦЕЛИКОМ!) В СПЕЦИАЛЬНУЮ ОДЕЖДУ. И, КОНЕЧНО, НИКАКИХ СЕТЕЙ И ИНТЕРНЕТА… РАБОТАТЬ ТОЛЬКО НЕУДОБНО

БЕЗЗАЩИТНЫЕ ДАННЫЕ

В КОНЦЕ ПРОШЛОГО ГОДА ПОЯВИЛАСЬ И СРАЗУ СТАЛА ХИТОМ НЕЛЕГАЛЬНЫХ ПРОДАЖ БАЗА С НАЛОГОВЫМИ ДЕКЛАРАЦИЯМИ ПОЧТИ 10 МЛН МОСКВИЧЕЙ, С УКАЗАНИЕМ ИХ МЕСТА РАБОТЫ И АДРЕСОВ. ЭТО ПЕРЕПОЛНИЛО ЧАШУ ТЕРПЕНИЯ ЗАКОНОДАТЕЛЕЙ, И В ГОСДУМУ БЫЛ ВНЕСЕН ПЕРВЫЙ ВАРИАНТ ЗАКОНОПРОЕКТА «О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ». В ЯНВАРЕ 2007 ГОДА ЗАКОН ВСТУПИЛ В СИЛУ, НО ЗАМЕТНЫХ ИЗМЕНЕНИЙ НА РЫНКЕ ЭТО ПОКА НЕ ПРОИЗВЕЛО. ПО КРАЙНЕЙ МЕРЕ, В ПРОДАЖЕ, КАК И РАНЬШЕ, ЕСТЬ КРАДЕНЫЕ БАЗЫ ДАННЫХ БАНКОВ, МОБИЛЬНЫХ ОПЕРАТОРОВ И ТАМОЖНИ. ВИКТОРИЯ ЗАВЬЯЛОВА

КРАДУТ ПО-ПРЕЖНЕМУ Впрочем, нельзя сказать, что закон предъявил рынку какие-то новые требования, скорее унифицировал существовавшие ранее. Главное, что сделал закон,— зафиксировал ответственность компаний, допустивших утечку информации о клиентах, а также регламентировал порядок работы с персональными данными клиентов. Информация о гражданах и их персональных данных должна храниться таким образом, чтобы утечки не произошло. А если это все-таки случилось, компания может быть наказана штрафом или лишением лицензии. И наконец, отвечать за утечку данных будет не только компания, откуда они были украдены, но и продавец информации.

Серьезных изменений на рынке технологий обеспечения информационной безопасности после выхода закона еще не произошло, но в будущем, полагают специалисты, этот рынок окажется в большом выигрыше. «Мы считаем, что в перспективе закон обязательно отразится на нашем бизнесе,— говорит технический специалист департамента программных решений „HP Россия“ Сергей Знаменский.— В частности, на продажах наших программных продуктов для управления доступом к ИТ-ресурсам — HP Select Access Software. Сегодня это ПО применяется на российских предприятиях и обладает возможностями по защите идентификационной информации и персональных данных».

Представители ИТ-компаний и эксперты в целом оценивают закон позитивно и говорят о его положительном влиянии на рынок. По мнению старшего менеджера, руководителя направления информационной безопасности в России и странах СНГ компании Deloitte & Touche Нины Парфеновой, принятие закона активизировало внедрение средств шифрования и создание соответствующей инфраструктуры хранения данных.

А директор по информационной безопасности Владимир Мамыкин, вице-президент Microsoft в России и СНГ, считает, что уже сейчас заметно влияние закона на коммерческие и государственные структуры, работающие с информацией о гражданах. «Возрос не только спрос на защиту соответствующих приложений, работающих с такими данными, но и внимание контролирующих органов к выполнению положений этого документа, что отрадно,— отмечает Владимир Мамыкин.— Что касается технологий Microsoft, которые потребители могут использовать для выполнения требований этого закона, то их спектр очень широк, он охватывает большинство наших продуктов. Хотя, вне всякого сомнения, повышенным спросом для этих целей у потребителей пользуются сертифицированные в ФСТЭК и ФСБ по требованиям российского законодательства продукты — от операционных систем до офисных приложений и баз данных».

СЕРГЕЙ МИХЕЕВ

УЖЕ ПОСЛЕ ПРИНЯТИЯ ЗАКОНА «О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ» ПИРАТСКИЕ ДИСКИ ПРИ ЖЕЛАНИИ МОЖНО НАЙТИ В ПОДЗЕМНЫХ ПЕРЕХОДАХ, НА РАЗВАЛАХ И НЕКОТОРЫХ САЙТАХ

ТРЕБОВАНИЯ БУДУТ ЗАВТРА Что касается ужесточения требований к работе самих компаний, то здесь, как всегда, строгость российских законов сводится на нет необязательностью их исполнения. Участники рынка, может, и рады бы выполнить, но пока не могут. Закон не содержит конкретных требований. В нем, например, говорится, что для защиты информации организация должна принимать необходимые технические меры. В том числе использовать шифровальные (криптографические) средства, «чтобы защитить персональные данные от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения». А какими именно должны быть эти средства, не сказано. Эти требования должна сформулировать Федеральная служба по техническому и экспортному контролю (ФСТЭК) Министерства обороны РФ, но когда это будет сделано, неизвестно: в Минобороны от комментариев на эту тему отказались. Пока же основным документом, регламентирующим работу компаний, остаются «Специальные требования и рекомендации по технической защите конфиденциальной информации». Они были разработаны ФСТЭК еще в 2002 году, в них описываются и меры по технической защите персональных данных, но многие из этих мер уже утратили актуальность.

Так что большинство компаний в ожидании указаний сверху используют прежние системы защиты данных. «С технической точки зрения мы готовы к тем требованиям, которые накладывает на нас закон,— говорит пресс-секретарь МТС Ирина Осадчая.— У нас гибкая инфраструктура, и мы давно работаем с системами защиты данных. Вместе с тем, пока уполномоченным контрольным органом не разработаны необходимые критерии, мы не можем провести оценку того, насколько наши системы защиты соответствуют требованиям закона».

АБОНЕНТ В ЗАКОНЕ Статья 9 закона («Согласие субъекта персональных данных на обработку персональных данных») предусматривает необходимость получения письменного согласия клиента на передачу сведений о нем третьему лицу. В ней же приведено шесть необходимых ус-

КАК ВСЕГДА, СТРОГОСТЬ РОССИЙСКИХ ЗАКОНОВ КОМПЕНСИРУЕТСЯ НЕОБЯЗАТЕЛЬНОСТЬЮ ИХ ВЫПОЛНЕНИЯ. УЧАСТНИКИ РЫНКА, МОЖЕТ, И РАДЫ БЫ «ВЫПОЛНИТЬ», НО НЕ МОГУТ — ПО НЕ ЗАВИСЯЩИМ ОТ НИХ ПРИЧИНАМ

КАК УТЕКАЕТ У НИХ

Ужесточение и развитие законодательства в сфере информационной безопасности — мировая тенденция. К примеру, новый законопроект по защите персональных данных, который обещает ввести жесткую ответственность компаний за утечки сведений, готовят сейчас в США. Инициаторами выступают независимый сенатор Бернард Сандерс и Патрик Лихи от демократической партии. Согласно проекту закона, наказание должны нести не только преступники, но и компании, допустившие утечку. Новые правила для компаний об обязательном уведомлении граждан в случае любой утечки или кражи информации с начала этого года разрабатывает и Европейская комиссия. Правило, согласно которому компании будут обязаны сообщать об утечке персональных данных, вводит и главный надзорный орган над финансовым рынком Великобритании FSA (Financial Service Authority). Причиной такого решения стало то, что британские компании часто скрывают факты утечки персональных данных, при этом халатно относясь к хранению информации. Например, как выяснилось этой осенью, некоторые банки выбрасывают носители информации, содержащие приватные сведения о клиентах, в обычные мусорные баки. В конце 2006 года расследование офиса комиссара по информации (Information Commissioner's Office) выявило 11 крупных организаций, которые нарушают закон о защите информации. Среди них оказались United National Bank, Barclays Bank, HFC Bank и даже почта Соединенного Королевства — UK Post Office. То есть в цивилизованном мире информацию крадут не реже, чем в России.

Одна из самых скандальных историй последних лет — утечка 40 млн записей о владельцах кредитных карт MasterCard, Visa, American Express и Discover (см. статью на стр. 27). В России информацию обычно сливает источник в компании, здесь же действовали внешние враги — хакеры. Как выяснилось, крупный обработчик информации для банков и фирм CardSystems Solutions не уделял должного внимания обеспечению безопасности. Компания продолжала хранить записи, подлежащие удалению, а данные о транзакциях не шифровались. Хакеры смогли установить в сети CardSystems Solutions трояна, перехватывающего данные о кредитных картах в процессе проведения финансовых транзакций. Так они получили информацию об именах владельцев карт, номерах их счетов и кодах подтверждения. Вскоре сообщения о мошенничествах стали поступать из банков. То, что перехват происходит через CardSystems, выяснили специалисты Cybertrust. Через некоторое время Visa, на которую приходилось больше половины операций CardSystems, отказалась работать с этой компанией.

Печальная история произошла в Bank of America. Его сотрудники потеряли носители с информацией о более чем 1 млн клиентов, среди которых были и американские сенаторы. Пропадали и персональные данные Калифорнийского и Стэндфордского университетов, информационных брокеров ChoicePoint и LexisNexis. В прошлом году отметились банк Sovereign, министерство образования и министерство транспорта США. Перечислять можно до бесконечности. И во всем мире одним из наиболее значительных факторов риска в системе защиты данных остается не несовершенство технологий или законодательства, а внутренняя угроза, исходящая от сотрудников компаний и банков.

ВИКТОРИЯ ЗАВЬЯЛОВА

ловий для оформления такого согласия. Компании-операторы мобильной связи вышли из положения просто. К примеру, как сообщили BG в пресс-службе МТС, с Нового года компания внесла изменения в договор. Теперь при его заключении абонент дает согласие на использование сведений о нем (в том числе третьими лицами) «в случаях, необходимых для исполнения договора».

Более сложная проблема стояла перед МГТС. Как отмечает заместитель генерального директора компании по коммерческой деятельности Денис Лобанов, на бизнесе по большому счету закон никак не отразился. Однако он косвенно сказался на обслуживании абонентов-граждан, так как теперь данные об абоненте-физлице могут включаться в систему информационно-справочного обслуживания только с его согласия. В МГТС сейчас идет реконструкция сети, часть абонентов переводится с кода 495 на код 499. «Иногда меняется не только код, но и часть номера,— отмечает Денис Лобанов.— Абоненты оповещаются о предстоящей замене и сообщают об этом близким. Но иногда кто-то из знакомых абонента не знает о смене номера, набирает старый и не может дозвониться. Тогда он обращается в справочную МГТС и просит дать новый номер телефона. Но по закону МГТС не имеет права дать такую информацию, ведь это персональные данные абонента, который добровольного согласия на их предоставление не давал».

Для выхода из этой ситуации в МГТС была введена платная услуга «Барышня, соедините» по 009. Оператор может позвонить тому, у кого сменился номер, и спросить, согласен ли абонент на соединение с человеком, который его разыскивает. В случае согласия оператор соединяет абонентов. «Однако я не уверен, что это решение, подходящее всем без исключения абонентам,— говорит Денис Лобанов.— Вместе с тем МГТС может предоставлять другим операторам связи без согласия абонентов данные, для которых установлено исключение из режима конфиденциальности. Это Ф.И.О., абонентский номер, адрес установки конечного оборудования — стационарного телефона. Эти данные необходимы в рамках межоператорских взаимоотношений, мы имеем право предоставить их на условиях конфиденциальности тому оператору, который оказал услугу абоненту МГТС».

КАК ОНИ УТЕКАЛИ Именно база данных МГТС появилась на рынке одной из первых — в 1992 году. В дальнейшем она постоянно обновлялась, и приобрести диски можно до сих пор. Регулярно крадут данные и из различных государственных ведомств. В 2002 году, к примеру, отличился Госкомстат — в продаже появилась его база, содержавшая результаты Всероссийской переписи населения. Ведомство нашло простой выход из неприятной ситуации — не признало факта утечки. А вот Центробанку не удалось так легко замять проблему с базами данных о платежах через расчетно-кассовые центры за второй и третий кварталы 2004 года. Диски появились в продаже в феврале 2005 года по цене 3 тыс. рублей. Депутаты Госдумы потребовали от Генпрокуратуры расследовать инцидент.

Однако серьезных результатов это обращение не принесло. Через несколько месяцев воры усовершенствовали продукт — в продаже появилась новая, более полная версия диска ЦБ, включавшая данные за четвертый квартал 2004 года. После этого Банк России провел наконец собственное расследование. В конце октября 2005 года в управлении безопасности ЦБ заявили, что «источник утечки перекрыт». Кто именно был ее виновником, так и осталось неизвестно. А в феврале 2006 года появились спам-сообщения с предложениями о продаже базы ЦБ за первый квартал 2005 года. Впрочем, диск не содержал информации ни об одной реальной проводке, продавцы всего лишь попытались заработать на продолжительной истории с утечками из Центробанка.

В ноябре прошлого года хитом нелегальных продаж стала база с налоговыми декларациями за 2004 год. Информацию о почти 10 млн москвичей с указанием их мест работы и адресов продавцы оценили вдвое дешевле, чем базу ЦБ,— всего в 1,5 тыс. рублей.

Пожалуй, именно после этого происшествия терпение законодателей переполнилось, и в Думу был внесен первый вариант законопроекта «О защите персональных данных». Документ вполне мог бы не дойти до последнего чтения, если бы за этой историей не последовала еще более шокирующая.

Внимание соответствующих органов привлек Московский центр экономической безопасности (МЦЭБ), который уже около года принимал на своем сайте заказы на базу паспортных данных 16 млн москвичей. Кстати, стоила эта информация недешево — $1,2 тыс. Однако никаких юридических оснований для привлечения представителей МЦЭБ к ответственности не было — продажа чужих персональных данных в России, по сути, на тот момент еще являлась легальным бизнесом. А вот сотрудники московской паспортно-визовой службы, укравшие эту информацию, могли бы ответить по закону — если бы их нашли. Аналогичная история произошла с данными на московских и петербургских клиентов «большой тройки» — «Вымпелкома», МТС и «МегаФона». Информация предлагалась на сайте sherlok.ru. Провели расследование, задержали семерых подозреваемых, в том числе сотрудников «Вымпелкома». А сайт благополучно существует по сей день — ответственность за продажу личной информации ввел лишь закон о персональных данных.

ВНУТРЕННЯЯ УГРОЗА Впрочем, утечки информации из МГТС и компаний-операторов мобильной связи были цветочками по сравнению с тем, что произошло в августе 2006 года. На черный рынок поступили сразу две базы данных (700 тыс. и 3 тыс. записей), содержащие кредитные истории людей, бравших потребительские кредиты в нескольких российских банках, в частности в Хоум Кредит энд Финанс Банке, банке «Русский стандарт» и Финансбанке. Они включали фамилию, имя, отчество и адрес заемщика, название торговой сети, где приобретались товары, размер и срок кредита, ежемесячный платеж и размер просрочки.

В начале апреля нынешнего года депутат Госдумы Анатолий Аксаков заявил, что это фальшивка. Когда СМИ сообщили о появлении в продаже баз заемщиков банков, он обратился с запросом в правоохранительные органы. «В ответ мне было сказано, что было проведено специальное расследование МВД и соответствие тех данных, которые продавались, реальным не выявлено»,— сообщил Анатолий Аксаков. Не подтвердили факт утечки и сами банки, проводившие внутреннее расследование. Однако тогда, в августе 2006-го, обзвон журналистами Ъ заемщиков, указанных в базе, подтвердил, что данные настоящие.

В середине марта этого года Банк России отреагировал на прошлогодние скандалы — разослал письма с предупреждениями о грядущих проверках уровня информационной безопасности, то есть мер защиты от утечки конфиденциальной информации, в первую очередь о клиентах. В стандарте ЦБ «Обеспечение информационной безопасности организаций банковской системы РФ», утвержденном распоряжением ЦБ №Р-27 от 26 января 2006 года, указывается, что наибольшими возможностями для того, чтобы устроить утечку информации, обладает персонал банка. Кстати, как показало исследование «Внутренние ИТ-угрозы в банковском секторе 2005», проведенное компанией Infowatch, банкиры с мнением ЦБ согласны: 54% опрошенных считают, что основная причина утечки — халатность сотрудников. В стандарте ЦБ приводятся конкретные рекомендации по защите от инсайда, в том числе регламентируются методики моделирования угроз утечки данных, политика и система управления информационной безопасностью, а также требования к программным средствам внутреннего контроля. Впрочем, эти требования носят рекомендательный характер, исполнять их необязательно. ■

В МГТС ВВЕДЕНА ПЛАТНАЯ УСЛУГА «БАРЫШНЯ, СОЕДИНИТЕ» ПО 009. ОПЕРАТОР МОЖЕТ ПОЗВОНИТЬ ТОМУ, У КОГО СМЕНИЛСЯ НОМЕР, И СПРОСИТЬ, СОГЛАСЕН ЛИ ТОТ НА СОЕДИНЕНИЕ С ЧЕЛОВЕКОМ. В СЛУЧАЕ СОГЛАСИЯ ОПЕРАТОР СОЕДИНЯЕТ АБОНЕНТОВ

НЕКОТОРЫЕ ТРЕБОВАНИЯ ЗАКОНОВ ЗАПАДНЫХ СТРАН К ИТ-БЕЗОПАСНОСТИ

Закон SB 1386 (Калифорния, США)
Секция 2 (a): «Любая организация, которая владеет персональными компьютерными данными или лицензирует их, обязана оповестить всех резидентов штата Калифорния об утечке или потенциальной утечке их приватных данных в незашифрованном виде. Сделать это следует немедленно — сразу же после того, как утечка будет выявлена».

Data Protection Directive (Евросоюз)
Статья 17 секция VIII глава 2: «Персональные данные должны быть защищены разумными средствами безопасности от таких угроз, как утрата или неавторизованный доступ, разрушение, использование, модификация или утечка».

Data Protection Act (Великобритания)
Приложение 1 часть 2 пункт 9: «Каждая организация должна реализовать разумные технические меры, чтобы предотвратить ущерб своих клиентов в результате неавторизованной или незаконной обработки персональных данных, а также их потери, уничтожения или повреждения. Вдобавок каждая организация должна сделать разумные шаги, чтобы обеспечить надежность любого служащего, имеющего доступ к персональным данным».

Personal Information Protection Act 2003, PIPA (Япония)
Статья 21: «Когда организация, на попечении которой находится персональная информация, использует служащих для обработки этих данных, она должна внедрить необходимые и адекватные меры наблюдения и контроля, чтобы обеспечить безопасность персональной информации».

The Federal Privacy Act или Privacy Act 1988 (Австралия)
Принцип 4: «Каждая организация, на попечении которой находятся личные сведения граждан, должна убедиться, что эта информация защищена от утечки, потери, неавторизованного доступа, использования, модификации и другого злоупотребления. Кроме того, организация обязана предусмотреть средства контроля над тем, чтобы доступ к информации и полномочия по ее использованию имели только те работники, которым это необходимо в силу служебных обязанностей».

Personal Information Protection and Electronic Document Act, PIPEDA (Канада)
Приложение 1 принцип 4: «Каждой организации, на попечении которой находятся персональные данные граждан, рекомендуется назначить ответственное лицо, которое будет следить за безопасностью этой информации и соблюдением положений приватности». Пункт 4.7: «Каждой организации рекомендуется принимать меры безопасности для защиты приватной информации в соответствии с характером ее чувствительности».
Пункт 4.7.1: «Эти меры безопасности должны защитить персональные данные от утечки, потери или кражи, неавторизованного доступа, копирования, использования или модификации».

АЛЕКСЕЙ ДОЛЯ

ПОДЗАКОННЫЕ СТРАНЫ

За последние годы законодательная база многих государств эволюционировала в сторону улучшения защиты персональных данных граждан. Практически каждая страна имеет нормативные акты, регулирующие оборот приватных сведений граждан и защищающие личную информацию от утечки, разглашения, неавторизованного использования и т. д. Область действия таких законов включает в себя абсолютно все организации, действующие на территории страны. При этом основная цель — предотвратить утечку и злонамеренное использование личной информации граждан. Бизнесу самому по себе невыгодно допускать утечку персональных данных. Например, согласно последнему исследованию Forrester Research, в ходе которого было опрошено 28 компаний, допустивших утечки в последнее время, каждая украденная запись о клиентах фирмы обходится ей в $90–305. Наибольшая часть этого ущерба приходится на потерю репутации, отток лояльных клиентов и трудности в привлечении новых клиентов. Казалось бы, зачем нужны законы, если компаниям невыгодно допускать утечки? Оказывается, существуют государственные организации, а также целый ряд коммерческих компаний, успех которых практически не зависит от имиджа и привлечения новых клиентов. Такие организации представлены в основном в секторах со слабой конкуренцией. Например, даже если госструктура допустит утечку информации, покинуть ее, перейдя к конкуренту, граждане не смогут. Таким образом, чтобы исключить безалаберное отношение к персональным данным даже в таких предприятиях со слабой конкуренцией, государства возводят защиту приватных сведений в ранг закона.

Наибольшие трудности в этом отношении испытывают крупные организации, ведущие операции на рынках нескольких стран. В этом случае бизнесу приходится иметь дело с требованиями сразу целого ряда законов. Отметим, что помимо этих законов практически в каждой стране существуют специализированные нормативные акты, действие которых распространяется на компании, работающие в определенных секторах экономики. Например, в США закон HIPAA требует от организаций защищать приватные медицинские сведения граждан, а закон GLBA предписывает обеспечить безопасность приватных финансовых записей.

На первый взгляд сам факт существования закона о приватности должен устрашающе действовать на представителей бизнеса и заставлять их очень бережно обращаться с персональными данными клиентов. Однако на практике законы часто дают сбои.

Японский закон PIPA (Personal Information Protection Act 2003) был принят в 2003 году, а в начале 2007 года прокуратура не смогла его применить в реальном судебном разбирательстве. Дело обстояло следующим образом. Хирофуми Йокояма, инсайдер из полиграфического и электронного гиганта Dai Nippon Printing, украл винчестер с приватными данными (именами, адресами, телефонами и номерами кредитных карт) почти 9 млн граждан летом 2006 года. Прежде чем полиция задержала инсайдера, он успел продать часть добытых сведений. Пострадали клиенты 43 компаний, в том числе Toyota Motor Corp., American Home Assurance, Aeon Co. и NTT Finance. Когда дело дошло до суда, обвинение не смогло инкриминировать инсайдеру нарушение закона PIPA. И его обвиняют лишь в краже винчестера стоимостью $200. По мнению экспертов InfoWatch, это показательный случай. Так что ожидать скорой отдачи от российского закона «О персональных данных» не приходится.

Между тем не все так плохо. Примером в области защиты приватности может служить Великобритания. Национальный закон о приватности уже много раз доказывал свою состоятельность. Например, в начале 2006 года служащие Гранд Отеля в Брайтоне выбросили в мусорный бак тысячи бумажных документов с именами, адресами, номерами кредитных карт, телефонными номерами и подписями постояльцев гостиницы. Когда об этом стало известно, вопросы к руководству Гранд Отеля возникли даже у членов британского парламента. Компанию обвинили в нарушении закона DPA (Data Protection Act), она долго извинялась и компенсировала ущерб пострадавшим.

Крупные утечки персональных данных практически всегда приводят к многомиллионным убыткам для организации. Даже если у властей нет действенного инструмента в виде закона о приватности, они всегда могут найти повод придраться к фирме и оштрафовать ее. Скажем, в США все еще нет единого федерального закона, но власти могут обвинить фирму в недобросовестной конкуренции, нарушении отраслевых нормативных актов, а также закона о защите прав потребителей. По мнению аналитического центра InfoWatch, закон о защите прав потребителей действительно очень часто спасает обвинение в зале суда, так как утечка персональных данных может привести к нарушению некоторых его положений.

АЛЕКСЕЙ ДОЛЯ

«ПРИ ПОПЫТКЕ ПОДОБРАТЬ КЛЮЧ ПАСПОРТ БЛОКИРУЕТСЯ»

К 2009 ГОДУ КАЖДЫЙ ЖИТЕЛЬ РОССИИ СТАНЕТ ОБЛАДАТЕЛЕМ ЭЛЕКТРОННОГО ПАСПОРТА. ОДНАКО ГАРАНТИРОВАТЬ, ЧТО ЛИЧНЫЕ ДАННЫЕ ВЛАДЕЛЬЦА НЕ БУДУТ ВЗЛОМАНЫ, ТРУДНО — РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ СИСТЕМЫ ИЗВЕСТНЫ ЛИШЬ КОМПЕТЕНТНЫМ ОРГАНАМ. ПРИ ЭТОМ ОБЩАЯ СТОИМОСТЬ ВНЕДРЕНИЯ ПРОЕКТА ВЕСЬМА ВНУШИТЕЛЬНА — 14 МЛРД РУБ. ДИРЕКТОР КОМПАНИИ—ГЕНЕРАЛЬНОГО ПОДРЯДЧИКА ПО РАЗРАБОТКЕ ПРОЕКТА ФГУП НИИ «ВОСХОД» ЛЕОНИД ЮХНЕВИЧ ПОПЫТАЛСЯ ПРОЛИТЬ СВЕТ НА ТО, КАК БУДЕТ ОБЕСПЕЧЕНА ЗАЩИТА ИНФОРМАЦИИ О ВЛАДЕЛЬЦЕ НОВОГО ПАСПОРТА.

ЛЕОНИД ЮХНЕВИЧ,
ДИРЕКТОР
ФГУП НИИ «ВОСХОД»

BUSINESS GUIDE: Чем подтверждается высокий уровень технологий, которые использовались при разработке системы защиты?

ЛЕОНИД ЮХНЕВИЧ: Все технические средства подлежат обязательной сертификации в соответствии с законодательством РФ. А импортные помимо обязательной сертификации должны еще пройти целый ряд специальных исследований и проверок. Что касается российских технологий, используемых в автоматизированной системе оформления, изготовления и контроля электронных паспортов, то все программное обеспечение, автоматизирующее документооборот, использование ЭЦП, считывание данных из паспорта, обработку фотографий, а в перспективе дактилоскопию и создание 3D-фотографий, разработано специалистами наших компаний. В основном, конечно, это продукты самого НИИ «Восход».

В проекте принимали участие более 30 соисполнителей. Это российские ИТ-предприятия, имеющие большой опыт работы в области биометрических технологий и защиты информации, который позволяет им предлагать наиболее оптимальные решения для разработки и внедрения системы. Кроме того, учитывая большую географическую протяженность проекта, выгодно и целесообразно привлекать ведущие региональные компании для инсталляции, обслуживания и мониторинга системы.

BG: Использовались ли западные разработки?

Л. Ю.: Безусловно. Проект паспортов нового поколения возник не сам по себе, это результат работы многих стран по стандартизации, созданию, формализации процедур и правил работы с этими документами в составе Международной организации гражданской авиации (ICAO). Россия не может быть в стороне от этого процесса, страна является ее полноправным участником. Естественно, все рекомендации ICAO в этом проекте мы учитываем.

Мы четко следуем международным стандартам в плане защиты документа, но процедуры его изготовления, оформления, выдачи и пограничного контроля осуществляются государственной информационной системой, к которой предъявляются дополнительные требования. Когда паспорт формируется, важно знать, что процесс идет правильно и никакие хакеры или другие вредные воздействия извне не смогут повлиять на работу этой системы, например, на этапе передачи информации от паспортно-визового управления, где гражданин оформил свою анкету, в Гознак. С этой целью в системе создан специальный орган, обеспечивающий мониторинг безопасности информации.

Понятно, что все передается по защищенным каналам с использованием систем, сертифицированных соответствующими органами. Так что на международные стандарты накладываются еще и наши российские требования, которые, поверьте мне, сегодня очень жесткие. И если говорить о паспортной системе, то требования по безопасности к ней не имеют равных среди аналогичных систем, кроме систем специального применения.

BG: Какие гарантии у российских потребителей, что их данные не будут взломаны, ведь в Европе уже были подобные прецеденты?

НИКИТА ИНФАНТЬЕВ

ПРОЕКТ ВНЕДРЕНИЯ ЭЛЕКТРОННЫХ ПАСПОРТОВ ОБОЙДЕТСЯ РОССИЙСКИМ НАЛОГОПЛАТЕЛЬЩИКАМ В 14 МЛРД РУБЛЕЙ

Л. Ю.: Первое, что хотелось бы отметить: у нас нет достоверных данных, что кому-то удалось подделать паспорт, содержащий RFID-чип (см. статью на стр. 34), который является основой биометрических паспортов. Есть газетные сообщения и статьи в интернете, но это неподтвержденная информация. Если говорить о защите, используемой в нашей системе, то отечественный паспорт соответствует международным стандартам защиты информации в электронных удостоверениях личности. Предъявляемые ими требования к криптографическим средствам одинаковы для всех стран. Рекомендации по безопасности предлагает ICAO. Их вполне достаточно для надежной защиты. Если предположить, что какая-то структура или частные лица, ознакомившись со стандартами (они, кстати, находятся в открытом доступе), создали оборудование для изменения содержимого чипа паспорта, это немедленно обнаружится при предъявлении документа на паспортном контроле. Это особенность построения самой системы контроля паспортно-визовых документов.

Что касается считывания данных на расстоянии — считать данные закрытого паспорта, находясь в нескольких метрах от его обладателя, невозможно. Для этого нужно завладеть чужим паспортом и считать машиночитаемую строку, выделить из нее ключ, и только после этого становится возможным считать информацию из чипа. Что касается ключа для расшифровки данных, то по стандарту ICAO BAC (базовый контроль доступа) он действительно формируется из информации, записанной в машиночитаемую строку на пластиковой странице паспорта, и считать его можно только на специальном считывателе на пограничном контроле. А при попытке подобрать ключ российский паспорт заблокируется.

BG: Проводилось ли тестирование разработанной системы защиты и если да, то каковы результаты этих тестов?

Л. Ю.: Безусловно, проводилось. Что касается результатов… Могу сказать лишь, что они полностью удовлетворяют стандартным требованиям компетентных органов власти.

Записала ВИКТОРИЯ ЗАВЬЯЛОВА

КАК ВЗЛАМЫВАЮТ ПАСПОРТА

Летучий голландец

В 2006 году специалисты голландской тестовой лаборатории Riscure bv, занимающейся вопросами информационной безопасности, показали, как на расстоянии десяти метров можно считать всю информацию с RFID-чипа паспорта. Согласно стандарту Международной организации гражданской авиации (ICAO), которая курирует переход на документы с RFID-чипами единого образца по всему миру, каждая страна имеет право самостоятельного выбора — хранить данные в чипе с шифрованием или без. Но тот же стандарт жестко описывает форму секретного ключа. Он должен формироваться на основе номера паспорта, даты окончания срока его действия и даты рождения владельца. Это не секретная информация, иначе на постах контроля невозможно было бы расшифровать данные с чипа. Таким образом, для взлома паспорта остается перебрать незначительное количество комбинаций — порядка 35.

Электронная неопределенность

В Великобритании биометрические паспорта начали выдавать еще в 2006 году. А в конце прошлого года группа NO2ID, выступающая против введения электронных документов, заявила, что ей удалось скопировать из RFID-чипов личные данные владельцев паспортов. Взломать документы, по сообщению некоторых британских СМИ, удалось всего за 48 часов. Справедливости ради надо отметить, что группа NO2ID — организация довольно специфическая. Начиная с названия — «Нет ID», то есть удостоверениям личности, и заканчивая проводимой ею акцией «Покажи им, что ты не число». Для участия в ней противникам удостоверений надо всего лишь прислать свое фото NO2ID. Тем не менее сейчас парламентарии Великобритании высказывают серьезные опасения по поводу микрочипов электронных паспортов. В последнем докладе Национальной аудиторской службы говорится, что гарантировать безопасность чипа в документе можно только в течение двух лет. Аудиторы прямо говорят: неизвестно, что может произойти с чипами в будущем. К примеру, совершенно непонятно, как отразится на них постоянное считывание сканерами, если обладатель документа много путешествует. При том что срок годности паспорта в Великобритании десять лет, ситуация становится еще более неопределенной.

Британский совет

Независимый консультант по вопросам безопасности Адам Лори опубликовал в интернете исходные тексты своего комплекса программ по исследованию RFID с говорящим названием RFIDIOt. По его словам, благодаря собственным разработкам он успешно провел атаку на паспорт с RFID-чипом. Для этого ему понадобились обычное считывающее устройство и специально подготовленный код. Узнать последний не составило труда. Адам Лори выяснил, что вся информация, которую пассажиры передают авиаперевозчикам, накапливается в авиакомпаниях, хранится без должной защиты и может быть получена широким кругом лиц, включая злоумышленников. «Мне удалось считать данные с RFID-микросхемы паспорта, находившегося в запечатанном конверте,— говорит Адам,— что доказывает: важную информацию можно украсть незаметно для жертвы». Сама атака была направлена все на те же слабые места стандарта ICAO.

Американская история

После трагедии 11 сентября госдепартамент США предложил ввести гражданские паспорта с RFID-метками для пересечения границ с соседними странами, где раньше не требовалась даже виза. Неожиданно с острой критикой этого предложения выступила организация Smart Card Alliance, которая объединяет практически всех разработчиков и изготовителей смарт-карт и RFID-чипов и которая как никто другой заинтересована в развитии данной технологии. Главные замечания Smart Card Alliance касаются того, что технология, первоначально разработанная для контроля над перемещением товаров и грузов, не соответствует общепринятым нормам защиты персональных данных. Участники организации также обратили особое внимание на недостаточную степень защиты данных и возможность считывания информации с большого расстояния. Неэффективность системы признают даже в отдельных структурах правительства США. Так, например, специалисты консультативного совета при департаменте государственной безопасности США подготовили отчет «Использование RFID для идентификации личности» (The Use of RFID for Hu-man Identification). Однако статус этого документа не поднялся выше черновика. По всей видимости, выводы специалистов, заявивших, что «RFID порождает уязвимости в безопасности, несвойственные другим процессам идентификации, которые не опираются на радиочастотную передачу данных», не совпадали с генеральной линией правительства.

Шахидский след

Но главное, никакая защита, никакой чип не может защитить от банальной коррупции при выдаче паспортов. Чтобы доказать это, корреспондент BBC Шахида Тулаганова провела собственное расследование. За пять месяцев она стала обладательницей 20 (!) паспортов стран Евросоюза — Чехии, Польши, Бельгии, Франции и т. д. С технической стороны все эти паспорта нельзя назвать фальшивками: они были оформлены уполномоченными организациями как подлинные документы. Сегодня на черном рынке стоимость подобного документа колеблется от $200 до $3000 в зависимости от страны нового «гражданства». Шахида также раскрыла некоторые способы получения фальшивого паспорта. К примеру, в Чехии достаточно было найти через посредника внешне похожую на Тулаганову женщину, готовую подать свои документы на паспорт и приложить к ним фотографию британской журналистки.

МИХАИЛ ШАРОВ

МЕЖДУНАРОДНЫЙ СТАНДАРТ БЛАГОНАДЕЖНОСТИ

В ФЕВРАЛЕ КОМПАНИЯ МТТ, ИЗВЕСТНЫЙ ОПЕРАТОР МЕЖДУГОРОДНОЙ И МЕЖДУНАРОДНОЙ СВЯЗИ РФ, ОБЪЯВИЛА ОБ УСПЕШНОМ ЗАВЕРШЕНИИ СЕРТИФИКАЦИОННОГО АУДИТА НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ МЕЖДУНАРОДНОГО СТАНДАРТА ISO/IEC 27001:2005. ПО ЕГО РЕЗУЛЬТАТАМ КОМПАНИЯ ПОЛУЧИЛА СЕРТИФИКАТ НА СИСТЕМУ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (СУИБ). ЭТО ПЕРВЫЙ СЛУЧАЙ НА РОССИЙСКОМ РЫНКЕ, КОГДА ОПЕРАТОР СВЯЗИ ПОДТВЕРЖДАЕТ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ОКАЗЫВАЕМЫХ УСЛУГ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ МЕЖДУНАРОДНОГО СТАНДАРТА. МИХАИЛ ШАРОВ

ОАО «Межрегиональный транзиттелеком» (МТТ) — национальный оператор междугородной и международной связи. Компания основана в 1994 году для обеспечения взаимодействия между региональными сетями операторов подвижной связи. МТТ предоставляет широкий спектр телекоммуникационных услуг и обеспечивает организацию эффективного взаимодействия более 300 сетей сотовых операторов и более 100 сетей операторов фиксированной связи в России между собой. В мае 2005 года компания получила лицензию Россвязьнадзора №32042 на оказание услуг междугородной и международной связи конечным потребителям на всей территории Российской Федерации и вышла на рынок международной связи.

В 2005 году доход компании составил около $220 млн, объем трафика в сети МТТ превысил 4,2 млрд минут. Система менеджмента качества ОАО МТТ в июле 2006 года сертифицирована на соответствие международному стандарту ИСО 9001–2001.

КОНКУРЕНТНОЕ ПРЕИМУЩЕСТВО Эта история начиналась в середине 2005 года. К тому моменту специалисты компании МТТ, занимающиеся информационной безопасностью, осознали, что множество технических средств безопасности, работающих на площадках провайдера, живут сами по себе. Не существовало понимания того, что это оборудование работает по общепризнанным мировым стандартам.

Более того, появились проблемы. Во-первых, не было прописано четкого разделения ответственности между пользователями СУИБ, что для комплексной задачи по защите информации вопрос первостепенный. Во-вторых, с ростом числа угроз, изменением сервисов, постоянным строительством сети передачи данных встал вопрос обеспечения непрерывности информационной безопасности как процесса. Из этого следовало, что необходимо построить систему, которая мобильно изменялась бы вместе со средой и адекватно ей.

Решение задачи специалисты ОАО МТТ начали с изучения существовавших на тот момент стандартов, которые делятся на два типа. Первые — сугубо технические — регламентируют конкретные и узкие задачи информационной безопасности. Фактически они декларируют, каким инструментарием и в какой ситуации необходимо пользоваться, чтобы защититься от тех или иных угроз.

Второй тип стандартов — процессные, основанные на цикле Деминга, или PDCA-цикле. Они содержат рекомендации по построению в организации эффективной системы управления информационной безопасностью, функционирующей в контексте общей системы управления. С помощью этого типа стандартов необходимо определить, какие активы для бизнеса критичны; выяснить, какие угрозы возможны для них; рассчитать предполагаемый ущерб для бизнеса; создать план по обработке этих рисков; согласовать план с высшим руководством; начать внедрение СУИБ; производить постоянный мониторинг и модификацию плана работ согласно изменениям, которые происходят в компании.

К моменту, когда в МТТ определились со своим типом, британский стандарт управления информационной безопасностью BS 7799 с некоторыми изменениями стал международным стандартом ISO 27001:2005. Появилось еще одно преимущество работы с ним: официальная, признанная во всем мире сертификация системы.

Это немаловажный вопрос для компании, работающей на международном рынке связи. Иностранные компании, тем более такие старожилы, как Vodafone или British Telecom, в первую очередь спрашивают: «Как у вас решены проблемы информационной безопасности?» Сертификаты и лицензии российских силовых органов впечатления, как правило, не производят, ибо вся информация о правилах получения подобных документов скрыта в недрах российских спецслужб.

В то же время документ от Международной организации по сертификации не требует дальнейших разъяснений, тем более когда аудит на соответствие стандарту проводит

ИНОСТРАННЫЕ КОМПАНИИ, ТЕМ БОЛЕЕ ТАКИЕ СТАРОЖИЛЫ, КАК VODAFONE ИЛИ BRITISH TELECOM, В ПЕРВУЮ ОЧЕРЕДЬ СПРАШИВАЮТ: «КАК У ВАС РЕШЕНЫ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?» РОССИЙСКИЕ СЕРТИФИКАТЫ И ЛИЦЕНЗИИ ВПЕЧАТЛЕНИЯ НЕ ПРОИЗВОДЯТ

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР МТТ КОНСТАНТИН СОЛОДУХИН (СПРАВА) ВМЕСТЕ С ПРЕДСТАВИТЕЛЕМ BSI РОБЕРТОМ ВИТЧЕРОМ КРЕПКО ДЕРЖИТ В РУКАХ СЕРТИФИКАТ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ МЕЖДУНАРОДНОГО СТАНДАРТА ISO/IEC 27001:2005

НЕИЗВЕСТНЫЙ ISO27001/IEC 27001:2005

Стандарт на систему управления информационной безопасностью ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» имеет британские корни. В его основу лежит английский стандарт BS 7799, разработанный Британским институтом стандартов (BSI, British Standards Institution) совместно с рядом коммерческих организаций, таких как Shell UK, British Telecommunications, Association of British Insurers, Unilever, Marks &Spencer и др.).

BSI удалось увязать воедино 126 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определенных на основе лучших практик мирового опыта в данной области. С 1995 года BS 7799 имеет статус государственного стандарта Великобритании. Стандарт состоит из двух частей: Часть 1: Практические правила управления информационной безопасностью и Часть 2: Спецификация системы управления информационной безопасностью.

В 1999 году первая часть BS 7799 после доработки была передана в Международную организацию по стандартизации. В 2000 году претерпев ряд незначительных правок документ был утвержден в качестве стандарта ISO/IEC 17799:2000. Вторая часть BS 7799 стала основой для принятого ИСО стандарта ISO/IEC 27001:2005.

Чуть позже, в сентябре 2002, после внесения нескольких дополнений и изменений, версия обновилась до BS7799-2:2002. 15 октября 2005 года Международная Организация по Стандартизации (ISO) приняла стандарт BSI BS 7799-2:2002 в качестве международного — ISO/IEC 27001:2005. Основная цель стандарта — создание общей методологии для разработки, внедрения и оценки эффективности СУИБ, применимой для коммерческих компаний и государственных некоммерческих структур. В 2007 году ожидается развитие стандарта: на смену ISO/IEC 17799:2005 должен прийти ISO/IEC 27002:2007.

ISO/IEC 27001:2005 не является техническим стандартом, он не предписывает использование определенных способов шифрования данных или устройств защиты от сбоев. Стандарт определяет общую организацию, классификацию данных, системы доступа, направления планирования, ответственность сотрудников, использование оценки риска и другие аспекты в контексте информационной безопасности. Внедрение Системы на основе этого стандарта и последующая сертификация в BSI даёт компании инструмент, позволяющий управлять конфиденциальностью, целостностью и доступностью важного актива компании — информации, и может с одинаковым успехом применяться в компаниях разного размера — от индивидуальных предпринимателей до предприятий с численностью сотрудников в десятки тысяч человек.

ISO/IEC 27001:2005 предполагает управление защитой любого вида информации: финансовой, кадровой, удаленных партнерских баз данных — словом всего, что уязвимо с точки зрения безопасности. Хакеры, промышленный шпионаж, внутренние утечки, пиратство, сбои в работе ПО, вирусы — все эти риски в результате подготовки к сертификации сводятся к минимуму.

СУИБ, разработанная в соответствии с ISO/IEC 27001:2005 обеспечивает наличие отлаженной структуры, которая инициирует, реализует, поддерживает в рабочем состоянии и управляет информационной безопасностью внутри предприятия. Процедура разработки и внедрения СУИБ занимает от полугода до нескольких лет в зависимости от количества охватываемых СУИБ активов, процессов, их сложности и количества персонала компании. Затраты на проекты внедрения и сертификации сильно варьируются в зависимости от перечисленных факторов.

ISO — Международная организация по стандартизации (ИСО) была создана в 1946 году двадцатью пятью национальными организациями по стандартизации. СССР был одним из учредителей организации. Дважды за всю историю глава Госстандарта избирался председателем ИСО. Россия является правоприемницей СССР в рядах ИСО, а с сентября 2005 года входит в Совет ИСО.

Вопреки распространенному заблуждению, название организации не является акронимом. При выборе названия главной целью ставилось одинаковое звучание на всех языках мира. Для этого было решено использовать греческое слово isos — равный, которое многими неверно истолковывается как сокращение от International Organization for Standardization.

ЕВГЕНИЙ ЧЕРЕШНЕВ, МИХАИЛ ШАРОВ

известная британская фирма BSI. Это большое конкурентное преимущество для работы с внешними партнерами-операторами, не скованными условностями российских сертифицирующих органов.

Еще одним голосующим фактором за начало сертификации на этот стандарт послужила репутация компании-аудитора.

Компания BSI Management Systems — это не просто автор-разработчик стандарта информационной безопасности. BSI в России развернула очень серьезную кампанию по пропаганде ISO 27000, обучению персонала заказчика. А главное, BSI — это мировой лидер: более 40% всех сертификатов на соответствие этому стандарту в мире выдано именно этой компанией.

КОРПОРАТИВНЫЙ ЭФФЕКТ В качестве подрядчика была выбрана компания «Инфосистемы Джет» — один из ведущих системных интеграторов, входящий в Топ–20 российского ИТ-рынка, и поставщик решений в области информационной безопасности. Системы, разработанные этой компанией, имеют государственные сертификаты на высокие уровни доверия и применяются в госучреждениях на территории РФ.

«Проект по внедрению СУИБ в соответствии с требованиями стандарта ИСО 27000 длился ровно год,— рассказывает Борис Симис, начальник центра информационной безопасности компании „Инфосистемы Джет“.— Это не считая времени, потраченного на тендер, когда компания обошла ряд крупных консалтинговых фирм, в том числе и из „большой четверки“ — Deloitte & Touche, Ernst & Young, PricewaterhouseCoopers и KPMG. Поставленные задачи были тяжелыми, но интересными. Заказчики очень быстро поняли, что проект выходит за рамки одного подразделения, занимающегося исключительно информационной безопасностью. Надо привлекать все отделы МТТ. Это, кстати, одно из требований стандарта, так как задача обеспечения информационной безопасности не может существовать вне контекста общих бизнес-задач компании».

Чтобы не пытаться объять необъятное, в качестве первого объекта для сертификации был выбран биллинг компании. И, кстати, стандарт ISO 27000, равно как и любой стандарт, основанный на процессном подходе, позволяет сертифицировать не только всю деятельность компании в целом, но и отдельные бизнес-процессы. В описательной части сертификата всегда указывается, в какой области, на каких задачах проводился аудит соответствия стандарту.

Борис Симис поясняет: «В случае с МТТ проверялась система управления информационной безопасностью биллинга компании. С точки зрения компании, биллинг — это почти всегда „черный ящик“. Люди внутри него знают, что они делают, люди из бизнес-подразделений, не связанных с биллингом, практически никогда не в курсе их деятельности. В рамках своих работ мы формализовали бизнес-процессы, связанные с биллингом, то есть конкретно описали, что делают сотрудники, вплоть до малейших инструкций. Проводилась просветительская работа — мы читали курсы, организовывали тренинги. Проводили ликбезы по информационной безопасности для специалистов финансового отдела, отдела продаж, секретариата, то есть людей, не связанных с ИТ напрямую. И такая работа с персоналом дала позитивные результаты. Все очень живо восприняли эту тему, задавали много интересных вопросов. И, мне кажется, это еще один из плюсов стандарта, что темой информационной безопасности прониклись люди, которые по долгу службы напрямую не занимаются этим».

Как показал результат, все было не зря. Пользователи из самых различных подразделений МТТ в процессе внедрения и освоения требований системы очень активно и со знанием дела стали принимать участие в процессе обеспечения ИБ — сообщали об инцидентах, которые могут повлиять на защиту системы; стали интересоваться, как повлияют их действия на общую защищенность компании, и т. д.

Вполне закономерный эффект дала работа по анализу рисков и описанию активов заказчика в области информационной безопасности и возможных финансовых ущербов. Сегодня руководство ОАО МТТ по стандартной отчетности ИТ-отдела, заложенной в механизм СУИБ, может точно подсчитать, сколько денег было сэкономлено благодаря тем или иным средствам по защите информации. Это очень важный момент для понимания самого механизма защиты информации. Раньше средства на это выделялись, но не было четкого понимания, сколько необходимо и сколько денег тратится впустую.

«То есть прежде в МТТ высший менеджмент и сотрудники ИТ-службы,— по мнению Бориса Симиса,— разговаривали на разных языках. И в ответ на вопрос об эффективности средств, затраченных на покупку оборудования, получали лишь число отраженных за отчетный период атак и предотвращенных утечек информации. Понятно, что подобные цифры невозможно понять неспециалисту. Теперь же с внедрением международного стандарта ISO/IEC 27001:2005 для руководства компании будет очевиден и экономический эффект от действия подразделения».

Одним из косвенных подтверждений успешности реализованного решения стал договор МТТ о межсетевом сотрудничестве с английским провайдером British Telecom, подписанный в марте этого года на выставке CeBIT'2007. Одним из оснований сделки послужила сертификация МТТ на стандарт ISO 27001:2005. ■

ИТАР-ТАСС

КОМПАНИЯ МТТ ТЕПЕРЬ ДАЖЕ НА СТОЛЕТНЕМ ДЕЙСТВУЮЩЕМ КОММУТАТОРЕ КОМПАНИИ ERICSSON МОЖЕТ ПРЕДОСТАВЛЯТЬ СВЯЗЬ ПО МЕЖДУНАРОДНЫМ СТАНДАРТАМ

ДОКУМЕНТ ОТ МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИИ ПО СЕРТИФИКАЦИИ НЕ ТРЕБУЕТ РАЗЪЯСНЕНИЙ, ТЕМ БОЛЕЕ, КОГДА АУДИТ ПРОВОДИТ ИЗВЕСТНАЯ БРИТАНСКАЯ ФИРМА BSI. ЭТО БОЛЬШОЕ КОНКУРЕНТНОЕ ПРЕИМУЩЕСТВО ДЛЯ РАБОТЫ С ВНЕШНИМИ ПАРТНЕРАМИ-ОПЕРАТОРАМИ

ОСВЕДОМЛЕННОСТЬ РОССИЙСКОГО БИЗНЕСА О СТАНДАРТЕ ISO27001 ОСТАЕТСЯ НЕДОСТАТОЧНОЙ

В декабре 2006 года компания «МТТ» обратилась в крупнейший международный орган по сертификации BSI (Британский Институт Стандартов) для проведения сертификационного аудита СУИБ. Аудит был проведен специалистами российского офиса BSI и подтвердил соответствие СУИБ МТТ требованиям международного стандарта ISO/IEC 27001:2005». ЕВГЕНИЙ ШИПИЛОВ, директор по продажам BSI Management Systems CIS, LLC ответил на вопросы ЕВГЕНИЯ ЧЕРЕШНЕВА.

Компания BSI (Британский институт стандартов) является признанным мировым лидером в области обучения и сертификации Систем менеджмента, одним из основателей Международной организации по стандартизации (ISO), автором британских стандартов, ставших впоследствии самыми известными международными стандартами ISO серий 9000, 14000, 18000, 22000, TS 16949, 17799, 27001. На долю BSI приходится 40% мирового рынка услуг по сертификации Систем управления информационной безопасностью.

BUSINESSGUIDE: Я понимаю, что вы хорошо оцениваете инициативу компании «МТТ». И все же, какие у компании были реальные основания и мотивация получения сертификата ISO27001?

ЕВГЕНИЙ ШИПИЛОВ: Когда весной 2005 года компания «МТТ» получила лицензию на оказание международной связи на всей территории Российской Федерации, у руководства появился дополнительный стимул минимизации рисков нарушения целостности абонентской базы и построении эффективной системы взаимодействия с зарубежными партнерами. Внедрение Системы Управления Информационной Безопасностью (СУИБ) было определено как одно из ключевых составляющих новой ветви развития бизнеса.

BG: Насколько я понимаю, процесс подготовки к сертификационному аудиту — процесс не быстрый? Сколько времени занял проект «МТТ»?

Е. Ш.: Процесс разработки и внедрения СУИБ по избранному компанией международному стандарту ISO/IEC 27001:2005 «Системы управления информационной безопасностью. Требования» занял почти полтора года и потребовал от компании определенных финансовых и временных вложений на пересмотр существующей системы управления информационной безопасностью, оптимизацию бизнес процессов и разработку и внедрение авторской методологии управления рисками, внедрение нового оборудования и переподготовку кадров.

BG: Во всем мире приведение информационных потоков компании в соответствие с международными стандартами безопасности — процедура закономерная и логичная. Чего нельзя сказать о России. С чем это связано? Приведет ли опыт МТТ изменению ситуации, формированию некоего положительного тренда?

Е. Ш.: Компания МТТ, став первой российской телекоммуникационной компанией, получившей международный сертификат по данному стандарту, смогла привлечь внимание Российского рынка к проблеме и показать эффективность применения лучших мировых практик для защиты ключевых активов компании и критичной для бизнеса информации. Несмотря на то, что Стандарт существует уже 11 лет, только за последние полтора года в России появился положительный тренд. В сравнении 2005 годом, который можно было охарактеризовать как этап становления и продвижения стандарта, начиная с первой в России и на постсоветском пространстве сертификации на соответствие требованиям BS 7799, разработки детальных и многоплановых курсов по СУИБ, 2006 год ознаменовался рядом успешно завершенных сертификационных проектов.

BG: А ваши планы?

Е. Ш.: С целью повышения качества внедряемых Систем BSI разработал Партнерскую Программу, которая позволила объединить в своих рядах около 20 ведущих системных интеграторов России, Украины и Молдавии. В рамках партнерской программы проводятся совместные мероприятия, направленные на продвижение Стандарта на рынках России и стран СНГ.

На данный момент осведомленность Российского бизнеса о международных подходах обеспечения информационной безопасности и, в частности, о международном стандарте ISO27001 остается недостаточной. С момента опубликования международного стандарта ISO27001 в октябре 2005 года в России сертифицировано 5 компаний. Однако, к концу текущего года партнеры BSI закончат проекты внедрения СУИБ в более чем 15 крупных компаниях. По нашим прогнозам эта цифра будет ежегодно расти высокими темпами.

Особенно актуальным внедрение и сертификация Систем Менеджмента в соответствии с международными стандартами видится на фоне предстоящего вступления России во Всемирную Торговую Организацию и постоянно растущего количества Российских компаний, выходящих на IPO.

ИГРА НА ВЫЛЕТ

КОГДА ПОЯВЛЯЕТСЯ НОВЫЙ КРУПНЫЙ СЕГМЕНТ РЫНКА ИЛИ ВЫРАСТАЕТ ДО ОПРЕДЕЛЕННЫХ РАЗМЕРОВ УЖЕ СУЩЕСТВУЮЩИЙ, ТУДА УСТРЕМЛЯЮТСЯ ГИГАНТЫ ОТРАСЛИ. ОНИ НЕ СМОТРЯТ ПОД НОГИ И НЕ ОБРАЩАЮТ ВНИМАНИЯ НА МЕЛКИХ ИГРОКОВ. В РЕЗУЛЬТАТЕ БЫВШИЕ ПАРТНЕРЫ СТАНОВЯТСЯ ВРАГАМИ, А СЕМЕЙНЫЕ ФИРМЫ ЛИБО ВЛИВАЮТСЯ В СТРУКТУРУ КРУПНЕЙШИХ КОРПОРАЦИЙ, ЛИБО УХОДЯТ В ОЧЕНЬ УЗКИЕ НИШИ, ЧТОБЫ ВЫЖИТЬ. ИМЕННО ЭТО ПРОИСХОДИТ СЕЙЧАС НА РЫНКЕ ИТ-БЕЗОПАСНОСТИ, А ТОЧНЕЕ, В САМОМ ПЕРСПЕКТИВНОМ ЕГО СЕГМЕНТЕ — ЗАЩИТЫ ОТ ВНУТРЕННИХ УГРОЗ, ИЛИ ИНСАЙДЕРОВ. АЛЕКСЕЙ ДОЛЯ

РУКА MICROSOFT В июне 2003 года корпорация Microsoft поглотила небольшую румынскую компанию RAV, производителя антивирусов. Это был неожиданный ход — по крайней мере, для остальных антивирусных поставщиков. В этом поглощении была интересная деталь. Компания RAV — по сути, середнячок в своей отрасли — разрабатывала антивирусы как для Windows, так и для Linux/UNIX. Ясно, что Microsoft не нужны продукты, предназначенные для других операционных систем, поэтому команду UNIX-разработчиков выставили за дверь. Правда, вскоре ее пригласила к себе «Лаборатория Касперского». В результате сегодня этот российский игрок имеет очень сильные мировые позиции в защите UNIX-систем.

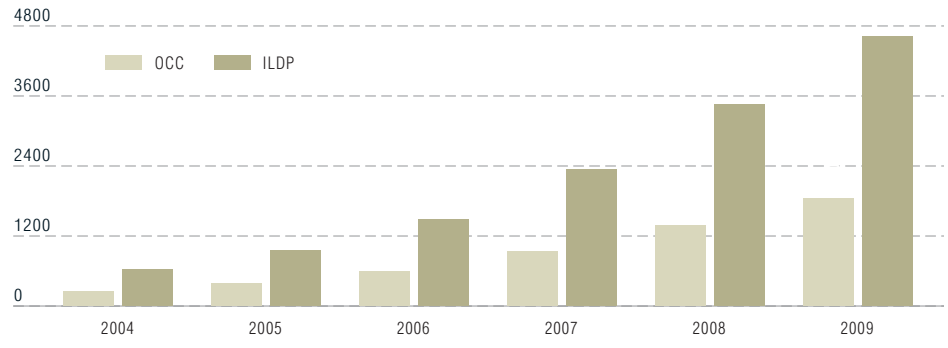
Беспокойство поставщиков антивирусов было недолгим. Скоро им стало ясно: на то, чтобы Microsoft стал полноценным производителем антивирусных продуктов, потребуется три-четыре года. И за это время надо успеть диверсифицировать свой бизнес и постараться уйти в технологический отрыв.

Реакция на агрессию Microsoft не заставила себя долго ждать. В декабре 2004 года корпорация Symantec объявила о поглощении компании Veritas. Это были примерно равные по размеру компании — правда, Symantec была чуть крупнее. По завершении оформления сделки акционерам Symantec досталось приблизительно 60% объединенной компании, а акционерам Veritas — около 40%.

В конце 2004 года Symantec была крупнейшим поставщиком решений ИТ-безопасности, а Veritas — крупнейшим разработчиком систем хранения данных. После завершения сделки все это перешло по наследству к Symantec. В результате в мире информационных технологий появился очередной гигант. Если раньше бизнес Symantec был связан с антивирусами и другими продуктами ИТ-безопасности, до которых мог легко дотянуться Microsoft, то теперь Symantec диверсифицировала свой бизнес, получила новые технологии и существенную точку опоры в виде рынка систем хранения данных.

Далее мы увидим, что существенного облегчения это не принесло. Хотя задумано было здорово.

17 ПОГЛОЩЕНИЙ ЗА ТРИ ГОДА Время шло. Компания Microsoft все ближе подбиралась к рынку ИТ-безопасности, причем в первую очередь занялась своим имиджем. Если раньше практически каждый пользователь знал, что Windows — небезопасная система, а Internet Explorer — опасный браузер, то теперь ситуация изменилась в корне. Хотя за два-три года степень защищенности продуктов Microsoft вряд ли существенно увеличилась, сегодня у софтверного гиганта совсем другой имидж. Windows Vista позиционируется чуть ли не как самая защищенная операционная система. Несколько маркетинговых кампаний Microsoft (таких как Trustworthy Computing) действительно заставили сомневаться в том, что Linux безопаснее и что в Internet Explorer «дыр» больше, чем в браузерах с открытым исходным кодом.



МИРОВОЙ РЫНОК ВНУТРЕННЕЙ ИТ-БЕЗОПАСНОСТИ: АНАЛИЗ И ПРОГНОЗ ($МЛН)
ПРИМЕЧАНИЕ: ILDP – ВЕСЬ РЫНОК ВНУТРЕННЕЙ ИТ-БЕЗОПАСНОСТИ. ОСС – ОДИН ИЗ СЕГМЕНТОВ ILDP.
ИСТОЧНИК ОСС: WORLDWIDE OUTBOUND CONTENT COMPLIANCE 2005–2009, IDS. ИСТОЧНИК ILDP: ILDP MARKET FORECAST 2005–2009, INFOWATCH.

Профессиональные пользователи интернета, посещающие те или иные сайты, посвященные безопасности, просто не могли не заметить огромных баннеров Microsoft. Все они несут только одно подспудное сообщение: «Microsoft равно безопасность». Видимо, это как раз тот случай, когда размер имеет значение. Колоссальные инвестиции в собственный брэнд сделали свое дело. Сегодня Microsoft разрабатывает безопасные продукты, не говоря уже о том, что поставляет продукты для безопасности.

В начале 2005-го, спустя два года после первого поглощения на рынке ИТ-безопасности, софтверный гигант сделал следующий шаг — приобрел еще одну компанию, Sybari. Это довольно солидный поставщик решений для борьбы с вредоносными кодами и спамом в корпоративном секторе. Однако в отличие от RAV компания Sybari вряд ли обладает современными технологиями. Весь ее продукт построен на использовании нескольких движков от других производителей, в том числе «Лаборатории Касперского». Так что сегодня Microsoft продает антивирус Касперского.

Отметим, что с точки зрения технологий благодаря своему приобретению Microsoft получил весь необходимый арсенал средств для того, чтобы защитить от вирусов и спама свой почтовый сервер Exchange. Это, во-первых, позволяет поднять ценность самого почтового продукта Microsoft, а во-вторых, помогает выйти на самый привлекательный корпоративный сегмент антивирусной защиты — рынок фильтрации почты на предмет вирусов и спама.

Крайне агрессивную политику в сфере поглощений продемонстрировала и компания Symantec. В 2003 году она поглотила трех маленьких игроков, в 2004 году — девять, а в 2005 году — еще пять. Не надо быть профессиональным аналитиком для того, чтобы понять: темпы расширения корпорация набрала просто огромные. Между тем специалисты прекрасно знают, что волна слияний и поглощений накрывает рынок тогда, когда игроки не уверены в будущем и не могут точно прогнозировать сценарии развития.

Конечно, несколько слияний и поглощений вполне могут быть направлены на добычу новых технологий, покупку определенных клиентов и выход на трудные рынки. Однако 17 стратегических сделок за три года свидетельствуют о том, что рынок ждут серьезные перемены.

В ЭТО ВРЕМЯ В РОССИИ Когда мы говорим о ИТ-безопасности в России, то имеем в виду прежде всего «Лабораторию Касперского».

Как уже отмечалось, эта компания в конце 2003 года перекупила у Microsoft румынскую команду UNIX-разработчиков RAV.

AP

КУПИВ ЗА $800 МЛН КОМПАНИЮ IRONPORT, ЗАНИМАЮЩУЮСЯ ФИЛЬТРАЦИЕЙ ВХОДЯЩЕГО И ИСХОДЯЩЕГО ТРАФИКА, КОМПАНИЯ CISCO СОВЕРШИЛА В ТЕКУЩЕМ ГОДУ САМУЮ КРУПНУЮ СДЕЛКУ ПОГЛОЩЕНИЯ

Начиная с 2002 года «Лаборатория» активно наращивала и расширяла свою продуктовую линейку. Это нельзя считать полноценной диверсификацией, но конкурентное преимущество компания получила. Во-первых, она одной из первых выпустила персональный межсетевой экран. В 2002 году это был довольно оригинальный ход для антивирусной компании. Однако уже через год его скопировали практически все: одни путем покупки соответствующих компаний, другие с помощью собственных разработок. Далее «Лаборатория Касперского» выпустила средство для фильтрации спама. Конечно, первой ее на этом рынке назвать нельзя, но среди антивирусных компаний это снова был довольно оригинальный ход. Правда, двигало ею не столько намерение диверсифицироваться, сколько желание получить прибыль и обойти конкурентов. Этот маневр также повторили другие участники рынка.

Тем не менее «Лаборатория Касперского» сделала очень важный шаг. В 2002 году она начала разработку собственной системы защиты от внутренних угроз ИТ-безопасности. Сейчас об этом принято говорить как о защите от инсайдеров, которые либо по неосторожности, либо по злому умыслу наносят вред работодателю. Результатом работы над этим проектом стало появление компании InfoWatch.

Судя по всему, «Лаборатория» с самого начала ориентировалась главным образом на западные рынки. Дело в том, что в США и Европе действуют нормативные акты, обязывающие топ-менеджмент защищать компанию от внутренних угроз. Взять хотя бы американский закон SOX (Sarbanes-Oxley Act of 2002), согласно которому все, что служащие делают с конфиденциальной информацией (например, финансовой отчетностью), должно контролироваться. Кстати, после того, как SOX был принят, в США и Европе появились десятки мелких фирм, разрабатывающих продукты для совместимости с этим нормативным актом и защиты от некоторых внутренних угроз. Сейчас все эти фирмы рискуют либо остаться не у дел, либо быть поглощенными более крупными игроками. Дело в том, что за последние годы рынок внутренней ИТ-безопасности вырос настолько, что теперь является самым лакомым куском для гигантов ИТ-рынка.

Итак, в 2004 году «Лаборатория» основала дочернюю компанию InfoWatch, специализирующуюся на защите от инсайдеров и утечек конфиденциальной информации. Это была уже настоящая диверсификация бизнеса. Крупные игроки, включая Microsoft, обычно воздерживаются от проникновения в какой-то сегмент рынка, пока он не вырастет примерно до $1 млрд. Сейчас это произошло.

НЕМАТЕРИАЛЬНЫЕ АКТИВЫ Первой после «Лаборатории Касперского» на рынок внутренней ИТ-безопасности обратила внимание корпорация Symantec. Этот гигант пополнил свой портфель еще одной поглощенной компанией — IMlogic. Она производит продукты для конт-

ОСНОВНОЕ ПРЕИМУЩЕСТВО НЕБОЛЬШОЙ ФИРМЫ — ВЫДАВАТЬ БЛЕСТЯЩИЕ РЕШЕНИЯ, ЧТО ОТРАЖАЕТСЯ НА КАЧЕСТВЕ ПРОДУКТА, НО ОНО РЕШАЕТ НЕ ВСЕ. А ЗА СПИНОЙ ГИГАНТОВ ОГРОМНЫЕ ВОЗМОЖНОСТИ, СЕТЬ ПАРТНЕРОВ И НЕОГРАНИЧЕННЫЙ ПОТЕНЦИАЛ ИНВЕСТИЦИЙ

роля над исходящим трафиком сетевых пейджеров (IM — Instant Messenger), что позволяет не только обеспечить соответствие нормативным актам, но и обезопасить этот канал связи от ряда внутренних и внешних угроз.

Правда, Symantec нельзя считать полноценным игроком этой отрасли. Сейчас ходят слухи о том, что она приобретет компанию Vontu, одного из конкурентов InfoWatch. Правда, эксперты сомневаются, что это произойдет. Дело в том, что руководство корпорации сейчас озабочено совсем другим. По результатам деятельности за 2006 финансовый год чистая прибыль Symantec резко упала, составив $157 млн против $536 млн в 2005 финансовом году. Если говорить о прибыли на акцию, то за год она составила $0,15 против $0,74 в прошлом году. То есть чистая прибыль компании упала на 71%. Так что топ-менеджмент сейчас думает скорее о том, как удержаться в своих креслах, нежели о выходе на новый перспективный рынок. Вдобавок все указывает на то, что акционеры Symantec устали от постоянных поглощений, а без них выйти в новый сегмент вряд ли удастся. Разрабатывать свои технологии с нуля слишком поздно.

А недавно к рынку внутренней безопасности проявила интерес корпорация IBM. Причем не просто проявила — IBM купила одного из нишевых игроков компанию Consul. Решения этой фирмы теперь органично дополнят функциональность IBM Tivoli, которой не хватало как раз внимания к внутренним угрозам. Сравнивания решения Consul с InfoWatch, нельзя не отметить коренного различия в подходах. Продукты Consul концентрируются на аудите действий служащих и выполнении требований нормативных актов. Другими словами, они не предотвращают утечку, но минимизируют риски юридического преследования и позволяют выявить внутреннее нарушение постфактум. Решения InfoWatch, напротив, работают в активном режиме — выявляют и пресекают утечку сразу, хватая инсайдера за руку. Здесь снова проявляется то преимущество во времени, которое «Лаборатория Касперского» успела использовать, выйдя на рынок внутренней ИБ раньше конкурентов.

Нельзя обойти стороной и довольно интересную и странную сделку компании WebSense. Прежде всего заметим, что эта фирма является довольно диверсифицированным поставщиком решений в сфере ИТ-безопасности. Она защищает от вредоносных кодов, нецелевого использования ИТ-ресурсов, фишинга и т. д. Несмотря на это, корпорация WebSense поглотила компанию PortAuthority Technologies, которая, как и InfoWatch, занимается только защитой от инсайдеров и утечек. Почему сделка названа странной? Из-за финансовых условий. Дело в том, что WebSense согласилась заплатить $90 млн наличными. Между тем оборотный капитал PortAuthority составляет всего $5 млн, а долги — целых $4 млн. Что же купила корпорация WebSense? Получается, что нематериальные активы. Например, технологии и раскрученную марку. Однако с технической точки зрения продукты PortAuthority выглядят далеко не так блестяще, чтобы за них можно было выложить почти $100 млн. Так что коэффициент x15 в данном случае указывает на то, что руководство PortAuthority просто смогло на волне интереса к рынку внутренней ИТ-безопасности продать свою компанию по значительно более высокой цене, чем она на самом деле стоит.

На рынке ИБ есть еще одна крупная компания, решившая диверсифицировать свой бизнес и отправиться в новый сегмент. Это корпорация McAfee, которая довольно неожиданно купила небольшую израильскую фирму Onigma, специализирующуюся на предотвращении утечек и защите от инсайдеров. За нее McAfee заплатила $20 млн наличными, что можно считать вполне справедливой ценой. Дело в том, что о компании Onigma и ее технологиях известно очень мало. Сайт фирмы появился в 2005 году, причем на нем не сообщалось ни об одном клиенте компании, а также об используемых технологиях. Вполне возможно, что за вывеской Onigma скрывалась небольшая команда израильских инженеров и разработчиков. И McAfee обеспечила себе быстрый выход на рынок, сразу интегрировав продукты Onigma в свою линейку.

IBM ВСЕГДА НАЙДЕТ КОГО КУПИТЬ
AP

Подводя итоги, можно сказать, что волна слияний и поглощений на рынке внутренней ИБ не закончилась. На рынке еще есть крупные и средние игроки, которые могут захотеть интегрировать функциональность по защите от утечек и инсайдеров в свои продукты или просто включить дополнительные продукты в свою линейку. Не исключено, что следующей стратегической покупкой станет одна из российских компаний.

ПИГМЕИ ПРОТИВ ГИГАНТОВ $1,5 млрд — это та сумма, в которую сегодня принято оценивать рынок внутренней ИТ-безопасности. Причем по итогам 2007 года он достигнет $2,5 млрд. Так что здесь определенно есть предмет для разговора (см. рис. 1).

Откуда взялись такие цифры? Прежде всего компания IDC в 2006 году оценила лишь один из сегментов рынка внутренней ИТ-безопасности в $600 млн. Это так называемый сегмент OCC (Outbound Content Compliance), куда входят продукты и услуги для защиты от утечек по сетевым каналам (например, по электронной почте и интернету). Однако если оценивать весь рынок, то в него входит еще целый ряд каналов: принтеры, порты рабочей станции, сменные носители и т. д. Причем, по оценке аналитического центра InfoWatch, в 2006 году общий размер рынка составил почти $1,5 млрд. Правда, на Россию приходится лишь небольшая часть этого — $50 млн.

Такие объемы, безусловно, привлекают внимание многих игроков, но наибольший энтузиазм инвесторов и менеджеров вызывают темы роста рынка. В среднем в мире рынок растет на 60–65% ежегодно.

Если на Россию приходится всего 3% рынка, то где же его львиная доля? Известно где — в США. Именно там сегодня находится основное количество поставщиков, каждый из которых уже привлек несколько десятков миллионов долларов на раскрутку. Анализ фандрайзинг-активности пяти крупнейших конкурентов показывает, что в период 2002–2005 годов средний объем венчурных инвестиций составил около $35 млн. К примеру, Proofpoint — $36 млн, Reconnex — $37 млн, Vontu — $30 млн, Tablus — $24 млн, PortAuthority — $31 млн, Orchestria — $49 млн, Oakley Networks — $20 млн, Vericept — $37,5 млн.

Постоянно растет интерес к рынку внутренней безопасности со стороны крупных игроков. Например, IBM и Symantec, McAfee и WebSense, а также «Лаборатория Касперского» уже обеспечили свое присутствие в этом сегменте. Причем если гиганты ИТ-индустрии просто купили действовавших на этом рынке поставщиков, то «Лаборатория Касперского», как уже говорилось, разработала собственную технологию InfoWatch, которая сегодня развивается в виде самостоятельной компании InfoWatch.

В интернете бытует шутка, что Билл Гейтс даже не остановится, чтобы поднять с пола $100, так как его время стоит значительно дороже. Однако в каждой шутке есть доля правды. Корпорация Microsoft может по праву считаться гигантом ИТ-индустрии, и отрасль размером менее $1 млрд ее в принципе не должна интересовать. Но если какой-то сегмент ИТ-рынка перейдет этот порог, софтверный гигант приложит все усилия к тому, чтобы начать доминировать в новом для него сегменте. То же справедливо и для других крупнейших игроков, за спиной которых огромные маркетинговые возможности, сеть партнеров по всему миру и практически неограниченный потенциал инвестиций. Все это позволяет захватить новый рынок довольно быстро, лишь бы игра стоила свеч.

А уже сейчас ясно, что рынок внутренней ИТ-безопасности — это интересный сегмент и что по своим размерам он уже превосходит либо перерастет в ближайшем будущем рынки антивирусов, межсетевых экранов, фильтров спама и многие другие сегменты. Прямо сейчас на рынке наблюдается бум слияний и поглощений, причем комбинации могут быть самые разные.

Не исключено, например, что в недалеком будущем InfoWatch выкупит активы материнской компании и «удочерит» «Лабораторию Касперского».

Но что будет с рынком дальше? Тут возможно несколько сценариев.

Весь рынок как самостоятельный сегмент может просто исчезнуть. Например, крупные игроки используют приобретенные технологии, чтобы встроить в свои продукты. Другими словами, эти компании ищут синергию между своими продуктами и купленными средствами по защите от инсайдеров и утечек. Создав комплексное решение, поставщики хотят повысить ценность своего предложения именно за счет этой антиинсайдерской составляющей. Эта функциональность не случайно названа антиинсайдерской, так как пример того, как вполне определенный сегмент рынка ИТ-безопасности был по кусочкам растащен всеми игроками, лежит на поверхности. Это антишпионские программы.

Еще три года назад было много небольших компаний, разрабатывавших средства защиты от шпионов. Но где они все сейчас? Куда подевался вообще весь этот сегмент рынка? Его разобрали по частям крупные антивирусные компании. Теперь антишпионских программ в чистом виде нет, есть комплексные антивирусы, которые защищают в том числе и от шпионов.

То же самое может произойти и с системами защиты от утечек. Действительно, что может сделать маленькая фирма, если на нее покусилась транснациональная корпорация? Основное конкурентное преимущество небольшой семейной фирмы чаще всего состоит в 10–15 технарях, которые разбираются в какой-то области настолько глубоко, что могут время от времени выдавать блестящие технические решения. Однако это отражается только на функциональных характеристиках продукта, а они решают далеко не все.

И все же рынок решений для защиты от инсайдеров вполне может сохранить самостоятельность. Это произойдет в том случае, если крупным игрокам индустрии не удастся нащупать синергию или она будет настолько мала, что покупать комплексное решение будет невыгодно. Кроме того, даже если большие рыбы съедят почти всех маленьких, почти всегда оставшиеся в живых компании смогут занять очень удачную позицию, заявив о том, что сфокусированы на внутренней ИТ-безопасности. Действительно, поставщик, который позиционируется как разработчик средств защиты от какой-то одной определенной группы угроз, будет иметь неоспоримое преимущество по сравнению с поставщиком универсальных продуктов. Так что позитивные перспективы рынка очевидны в любом случае. ■

ВОЛНА СЛИЯНИЙ И ПОГЛОЩЕНИЙ НА РЫНКЕ ИБ НЕ ЗАКОНЧИЛАСЬ. ЕЩЕ ЕСТЬ КРУПНЫЕ ИГРОКИ, КОТОРЫЕ МОГУТ ЗАХОТЕТЬ ВКЛЮЧИТЬ ДОПОЛНИТЕЛЬНЫЕ ПРОДУКТЫ В СВОЮ ЛИНЕЙКУ. НЕ ИСКЛЮЧЕНО, ЧТО СЛЕДУЮЩЕЙ ПОКУПКОЙ СТАНЕТ ОДНА ИЗ РОССИЙСКИХ КОМПАНИЙ

САМЫЕ КРУПНЫЕ ПОГЛОЩЕНИЯ НА РЫНКЕ ИТ-БЕЗОПАСНОСТИ

КОМПАНИЯ	ПОГЛОЩЕНИЕ
SYMANTEC	В ФЕВРАЛЕ 2006 ГОДА КОРПОРАЦИЯ SYMANTEC ПОГЛОТИЛА IMLOGICS, РАЗРАБОТЧИКА СРЕДСТВ ЗАЩИТЫ IM-ТРАФИКА, В ТОМ ЧИСЛЕ, И ОТ ИНСАЙДЕРОВ. ЭКСПЕРТНАЯ ОЦЕНКА СУММЫ СДЕЛКИ $15 МЛН.
MCAFEE	В ОКТЯБРЕ 2006 ГОДА КОМПАНИЯ MCAFEE ПРИОБРЕЛА НЕБОЛЬШУЮ ИЗРАИЛЬСКУЮ ФИРМУ ONIGMA ЗА $20 МЛН. ONIGMA СПЕЦИАЛИЗИРОВАЛАСЬ ТОЛЬКО НА ЗАЩИТЕ ОТ ИНСАЙДЕРОВ И УТЕЧЕК.
WEBSENSE	В ДЕКАБРЕ 2006 ГОДА КОМПАНИЯ WEBSENSE ПОГЛОТИЛА PORTAUTHORITY, ВЫЛОЖИВ $90 МЛН. ПРОДУКТЫ PORTAUTHORITY ПРЕДНАЗНАЧЕНЫ КАК РАЗ ДЛЯ ЗАЩИТЫ ОТ ИНСАЙДЕРОВ.
IBM	В ДЕКАБРЕ 2006 ГОДА КОРПОРАЦИЯ IBM ОБЪЯВИЛА О ПОГЛОЩЕНИИ CONSUL, ПОСТАВЛЯЮЩЕЙ ПРОДУКТЫ ДЛЯ ОБЕСПЕЧЕНИЯ СОВМЕСТИМОСТИ С НОРМАТИВНЫМИ АКТАМИ И ВНУТРЕННЕГО АУДИТА. ЭКСПЕРТНАЯ ОЦЕНКА СУММЫ СДЕЛКИ $40 МЛН.
CISCO	В ЯНВАРЕ 2007 ГОДА CISCO КУПИЛА ЗА $800 МЛН. КОМПАНИЮ IRONPORT, ЗАНИМАЮЩУЮСЯ ФИЛЬТРАЦИЕЙ ВХОДЯЩЕГО И ИСХОДЯЩЕГО ТРАФИКА.

www.kommersant.ru

Я загружать подарки

Дополнительные бизнес-приложения
для вашего мобильного офиса.

Между нашими телефонами есть много отличий, но в качестве мобильного офиса они все необыкновенно удобны.
Купите один из телефонов Sony Ericsson P990i, M600i или W950i в период с 1 апреля по 20 мая
и получите в подарок пакет из шести бизнес-приложений Paragon. Подробности об условиях акции
вы можете найти на сайте www.sonyericsson.com и в салонах-участниках акции.

Sony Ericsson