Безопасность бизнеса сегодня

Слово «бизнес» в сознании большинства людей ассоциируется с понятиями «инициатива» и «ответственность». Ответственность бизнесмена подразумевает не только обдуманность каждого шага в процессе развития своего дела, но и своевременные действия по защите компании от экономических потрясений и посягательств со стороны конкурентов и недоброжелателей. Те, кто из разных побуждений стремятся вставить палки в колеса растущему бизнесу, были, есть и будут всегда.
Не нужно забывать и о том, что компании должны стремится к тому, чтобы их бизнес был легален, а государство должно обеспечить максимально безопасные условия работы.
Мы попытались рассмотреть лишь небольшую часть того, что называется безопасностью бизнеса. И затронули вопросы информационной безопасности, обеспечения безопасности поставок грузов, защиты интеллектуальной собственности, а также меры профилактики внутреннего воровства в магазинах и складах компаний.
Понятно, что эта тема очень обширна, и поэтому другие аспекты этой проблемы мы будем поднимать в наших следующих номерах.

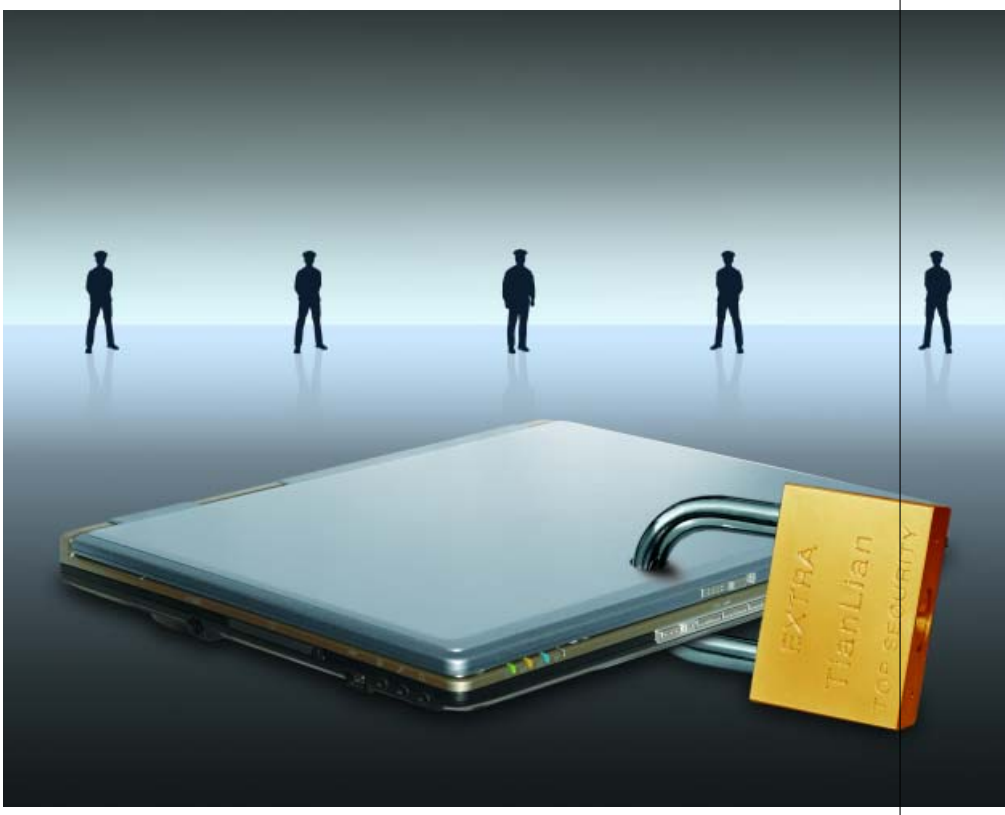
Руководитель бизнеса не обязан знать тонкости настройки антивирусов, межсетевых экранов, средств сканирования на уязвимость, сетевых средств обнаружения атак, особенности аутентификации и идентификации, криптографические методы шифрования, а также принципы работы камер слежения и правила поведения охранника.

— Достаточно понимать реальность проблемы, которая может принести реальные убытки, и получить общее представление о распространенных инструментах, техниках защиты и способах ее организации в масштабах компании, — разъясняет **начальник отдела защиты информации департамента информационно-технологического развития ОАО «Росбанк» Олег Чепиков**. — Этого достаточно для принятия решений о выделении средств на технические и организационные мероприятия, а также взаимодействия с привлеченными или собственными специалистами, ответственными за корпоративную безопасность.

Соотношение затрат и акценты

В результате быстрого повышения роли информационных технологий в бизнес-процессах многие потребители не успевают разобраться в нюансах происходящего, а значит, не могут принять меры, адекватные имеющимся угрозам. Решения о финансировании чаще всего основываются не на системном подходе и поддержании комплексной системы безопасности бизнеса, разработка которой базируется на основе рисков и угроз. В большинстве случаев деньги инвестируются в развитие тех элементов системы безопасности, о которых руководство имеет наилучшее представление. Или же решения о выделении средств принимаются, когда случился «пожар» и его надо тушить.

— Оглянитесь вокруг! Охранник



КОММЕНТАРИЙ

Обеспечение безопасности поставок грузов

Леонид Ухлинов, Главное управление информационных технологий ФТС России

Геополитическое положение России обуславливает прохождение через ее территорию кратчайших транспортных путей из Европы в Азию, что требует от государственных органов обеспечения контроля за перемещаемыми через государственную границу товарами и транспортными средствами.

Одним из основных способов контрабанды оружия, боеприпасов, наркотических и взрывчатых веществ является их перевозка в морских контейнерах, автофургонах, железнодорожных вагонах с маскировкой реальными грузами.

Однако для качественного досмотра крупногабаритных грузов требуется выполнение целого комплекса трудоемких и длительных разгрузочно-погрузочных работ (2-3 ч на одно транспортное средство), наличия специально выделенных для этого площадок, что практически делает возможным только единичный выборочный досмотр этих объектов. Кроме того, по этим же причинам также выборочно досматриваются и сами транспортные средства, их конструкционные узлы, которые потенциально могут использоваться в качестве тайников для сокрытия предметов контрабанды.

В связи с особой опасностью использования указанных видов объектов таможенного контроля для целей организованной контрабанды мировая таможенная практика, наряду с осуществлением оперативных мероприятий, в последнее время стремится максимально исключить возможность контрабанды за счет использования для ее поиска специальной техники. Наиболее эффективной техникой в настоящее время является инспекционно-досмотровые комплексы (ИДК).

ИДК позволяет за минимальное время (3-5 мин.) без вскрытия и разгрузки грузового транспортного средства получить его изображение и изображение перевозимых в нем товаров с характеристиками, позволяющими идентифицировать перевозимые товары, конструкционные узлы транспортного средства, обнаруживать в них предметы, запрещенные к перевозке, а также проводить ориентировочную оценку количества перевозимых товаров.

Анализ применения указанных комплексов в таможенных службах и службах безопасности ряда государств Европы и Азии показывает их высокую эффективность по противодействию контрабанде и незаконному перемещению грузов, надежному выявлению оружия и боеприпасов, наркотических и взрывчатых веществ.

В настоящее время ИДК оснащены таможенные службы Германии, Великобритании, Франции, Бельгии, Норвегии, Словакии, Голландии, США, Японии, Китая, Австралии, ОАЭ и ряда других стран.

Ведущими странами, производящими ИДК, являются Германия (SMITHS HEIMANN) и Китай (NUCTECH COMPANY LIMITED).

На сегодняшний день действует или находится в процессе построения 30 систем Heimann Cargo Vision (изготовитель — SMITHS HEIMANN) и 59 систем TH-SCAN (NUCTECH COMPANY LIMITED).

Рядом российских предприятий в рамках научно-исследовательских и опытно-конструкторских работ созданы отдельные составные части и узлы ИДК.

ФГУП НИИЭФА им. Д.В. Ефремова (С.-Петербург) создан экспериментальный стенд, на котором отрабатываются технические параметры, алгоритмы и программы. ЗАО «НПЦ «Аспект» (Дубна) по заказу министерства промышленности и науки Московской области ведется опытно-конструкторская работа по созданию мобильного ИДК.

ИДК выпускаются фирмами в стационарном, перебазируемом и мобильном варианте для досмотра морских контейнеров и большегрузных автомобилей.

Стационарные ИДК с энергетикой 9 МэВ (проникающая способность по эквиваленту стали — 380 мм) являются инспекционными системами, которые дают точное рентгеновское изображение полностью загруженных морских контейнеров и грузовых автомобилей и, как правило, используются в морских пунктах пропуска. Пропускная способность — до 25-ти контейнеров в час. Указанные комплексы требуют значительной радиационной защиты и размещаются в стационарных рентгенозащитных сооружениях.

Легковозводимые (перебазируемые) ИДК с энергетикой 6 МэВ (проникающая способность по эквиваленту стали — 300 мм) позволяют по полученному рентгеновскому изображению принимать решение о соответствии перевозимого груза заявленному в товаросопроводительных документах до 85% товаров относительно стационарных ИДК.

Данные комплексы используются на автомобильных пунктах пропуска и обеспечивают пропускную способность до 20-ти грузовых автомобилей в час.

Технологическое оборудование комплекса размещается в быстровозводимом сооружении либо сооружении из сборных бетонных модулей (перебазируемый вариант) с упрощенной радиационной защитой.

Мобильные ИДК с энергетикой до 3 МэВ (проникающая способность по эквиваленту стали — до 220 мм), смонтированы на шасси автомобиля и требуют при работе наличия санитарной зоны. Они позволяют по полученному рентгеновскому изображению принимать решение о наличии либо отсутствии грузов в контейнере и соответствии товаросопроводительным документам товаров с малыми объемными плотностями. Мобильные ИДК в основном используются в интересах оперативных подразделений таможенных и других правоохранительных органов. До настоящего времени на оснащении российских таможенных органов ИДК отсутствовали.

В текущем году Федеральной таможенной службой (ФТС) России начато строительство легковозводимого ИДК в пункте пропуска «Троебортное» Брянской таможни Центрального таможенного управления. Ввод в эксплуатацию намечен на I-й квартал 2005 года.

ФТС России планируется создание системы таможенного контроля крупногабаритных грузов и транспортных средств, состоящей из ИДК различных типов и модификаций, размещенных на пунктах пропуска через государственную границу.

По оценке ФТС России потребность таможенных органов составляет не менее 40 ИДК.

на входе на объект есть обязательно, потому что «у всех так», — делится наблюдениями исполнительный директор Ассоциации индустрии безопасности Михаил Мачнев. — Хотя, возможно, в конкретном случае эффективнее было бы установить сигнализацию. Обнаружились недостатки в торговом зале или на складе — бросаемся оснащать помещения камерами видеонаблюдения. При этом чуть внимательнее приглядеться к персоналу как-то в голову не приходит... О защите информации говорят сегодня много и правильно — повод для того, чтобы как можно быстрее пригласить специалистов для «зачистки» помещений, защитить информацию в компьютерах. А «в довесок» не помешает купить аппаратуру, подавляющую диктофоны, — ведь модно, да и не дорого!

Во всех подобных случаях плохо то, что принимаемые решения импульсивны, а порой и нелогичны. У руководителей организаций нет системного понимания того, какие риски и угрозы существуют сегодня, а какие с высокой вероятностью приобретут актуальность завтра и как все их предотвращать. Сегодня мы являемся свидетелями борьбы за увеличение или сохранение бюджетов на отдельные виды услуг и продуктов в области безопасности, например защиты и информации, и физической охраны. В отдельных случаях эта борьба приводит к увеличению финансирования, в других — к перераспределению средств.

— Но сопереживая тем, у кого

Исполнительный директор Ассоциации индустрии безопасности Михаил Мачнев

бюджеты сокращаются, либо радуясь вместе с теми, кто получает дополнительные денежные вливания, не стоит забывать о важнейшем моменте, — размышляет Михаил Мачнев. — Клиента (инвестора, собственника и т.п.) не очень волнует, какие именно услуги безопасности ему оказывают. Руководителю необходимо состояние безопасности

КОММЕНТАРИЙ

Государство — главный источник угроз

Президент Ассоциации РАТЭК Александр ПЛЯЦЕВОЙ

О минимизации угроз говорят сегодня много. И эта тема, безусловно, стоит того. Конечно же, очень важно правильно учесть все виды опасностей и уделить каждому из них пристальное внимание. С развитием информационных технологий и взятием на вооружение бизнесом новых механизмов ведения дела источников опасности только прибавилось. Однако, говоря о комплексном подходе к решению проблемы безопасности предприятия, действительно позволяющем минимизировать риски, поставщики и интеграторы средств технической охраны и информационной безопасности, предлагая своим клиентам анализ их рисков, умалчивают об угрозе, которая может в одночасье погубить даже компанию, вкладывающую в свою защиту максимум финансовых средств. (Яркий пример — дело компании «ЮКОС»). Главная угроза для предприятий отрасли электроники исходит со стороны государства.

Первопричиной возникновения и нарастания опасности со стороны государственных служб является непрозрачность бизнеса. Цепочка поставка — продажа, к сожалению, до сих пор остается разорванной. В механизме поставки электроники заведомо заложена системная ошибка. Одно только это может привести к закрытию компании налоговым, таможенным или другим государственным органом.

Единственным реальным средством защиты от такого рода угроз может выступать только принадлежность компании к объединению предприятий, способному донести коллективные интересы разных бизнесов до регулирующих и силовых структур, вести диалог с государством. Для решения такого рода стратегических проблем бизнеса и существует наша Ассоциация РАТЭК, которая выступает за легализацию рынка и год за годом кропотливо работает над достижением этой цели.

На мой взгляд, для любой фирмы лучше зарабатывать не очень много, но долго, чем остаться лишь на страницах истории компанией. когда-то умудрявшейся иметь сверхприбыли. Крупные предприятия отрасли приняли этот подход как единственно верный принцип ведения бизнеса и оперативно готовят письма о легализации в адрес В. Путина и Г. Грефа. Фирмы поменьше тешат себя надеждой на то, что «ими будут заниматься в последнюю очередь». И пока это вполне логично: излюбленным методом регулирования рынка со стороны государственных чиновников и поныне является взять игрока покрупнее и как следует «стукнуть его по голове», чтоб предприятия поменьше забегали, судорожно пытаясь «привести в порядок» свои дела. «Пока», потому что эта традиция изживает себя, и массированная атака на предприятия с относительно небольшими оборотами обязательно состоится.

Процесс федерализации идет полным ходом, через какое-то время дело дойдет и до торговли. Изменение «вкусов» государства сегодня напоминает сошествие сметающего все на своем пути ледника, движущегося сверху вниз не очень быстро, но неудержимо. В такой ситуации вряд ли имеет смысл давать определения (по признаку величины выплачиваемых налогов) «более легально работающая» или «менее легально работающая» компания. Все компании в стремлении сохранить конкурентоспособность пребывают вне правового поля и «дамоклов меч» висит над всеми. Поэтому единственным выходом из тупика я считаю активизацию диалога между государством и бизнесом.

Если говорить о внешнеэкономической деятельности, то достижению согласия может способствовать повышение продуманности работы и заинтересованности сотрудников таможенных органов: ведь от них зависит соотношение объемов легального и нелегального потоков ввозимой электроники. При организации стопроцентного легального ввоза вся последующие звенья бизнес-цепочки отстроятся сами собой.

Наша статистика показывает, что государство за счет незарегистрированных продаж только в сегменте электроники теряет около $3 млрд в год. То есть оно (а не только торговые компании, оборот самой крупной из которых сегодня достигает $2 млрд!) должно быть остро заинтересовано в легализации рынка. При всем при этом очень важно, чтобы «правила игры» между государством и бизнесом для всех компаний изменялись одновременно. Тогда и казна будет пополняться исправно, и бизнесмен не будет тревожиться за безопасность с превеликим трудом выпестованного детища.

(почувствуйте разницу! — безопасность как состояние и услуга как процесс) — за которое он и готов платить.

Составить общее представление о том, как правильно оценить масштаб и источники угроз, поможет руководителю следующий раздел нашей статьи.

Новые технологии — новые угрозы

На сегодняшний день информационные технологии — уже не дань моде и не что-то непонятное, дорогостоящее. Они стали повседневностью российского бизнеса. ИТ ощутимо снижают издержки, повышают производительность труда и позволяют больше зарабатывать. На Западе использование информационных технологий позволяет компании легче выходить на фондовый рынок, повышать свою капитализацию и стоимость торговой марки, ее акции начинают котироваться на бирже. Привлечение передовых ИТ дает большие шансы на получение дополнительных инвестиций в развитие компании, делает клиентов более лояльными при принятии решений о передаче критичных для них данных в ее распоряжение. Однако появление новых инструментов в руках предпринимателя привело и к появлению принципиально новых угроз для его дела.

За примерами далеко ходить не надо: сегодня в Интернете можно скачать вредоносные программы. В них достаточно только ввести адрес сайта, который вы хотите взло-

Системный подход — основа безопасности компании

Кандидат технических наук, председатель совета директоров группы компаний «Атлант» Шафигулин Олег Мансурович

Важнейшей и очевидной проблемой существования бизнеса является проблема обеспечения его безопасности. Разумный лидер или группа лидеров заблаговременно готовятся к предполагаемым опасностям, выстраивая отношения с сотрудником, ответственным за корпоративную безопасность. Полученный результат особенно зависит от правильности поставленной задачи.

Систему руководящих принципов построения безопасности бизнеса можно назвать Доктриной корпоративной безопасности. Сформулировать ее может только лидер в зависимости от целей бизнеса, возникающих угроз и финансовых возможностей. Предлагаемая система проверена временем и практикой. При кажущейся простоте она позволяет организовать оптимальную работу над комплексным обеспечением безопасности фирмы.

Первое, с чего следует начать, — это сформулировать свои корпоративные долгосрочные интересы с учетом того, что интересы первых лиц компании могут быть различны, противоречить и друг другу, и интересам самой компании. Цели могут быть как наступательными, например, захват новых рынков, поглощение, так и оборонительными — сохранение стабильности достигнутого положения.

Наиболее простая и часто встречающаяся ситуация в компании такова: есть выраженный лидер — единоличный либо неконфликтная группа руководителей, — корпоративная цель сформирована и носит оборонительный характер.

В этом случае Доктрина должна отвечать на основные вопросы: *что следует защищать, от кого защищать, кому и как защищать, как контролировать адекватность защищенности, сколько это стоит?*

Итогом работы над документом должен стать заблаговременно определенный комплекс инженерных и оперативно-технических мероприятий, назначены ответственные, выработан план рациональных действий в период возможного возникновения и при реализации угроз.

Объекты защиты

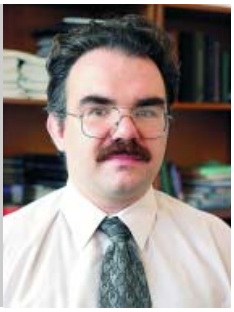
Защите подлежат корпоративные и личные объекты, жизненно важные для бизнеса.

Таблица 1. Типовые жизненно важные помещения стандартного офиса

Наименование жизненно важных помещений	Модель неприемлемого ущерба
Кабинет руководителя	Выемка конфиденциальной информации Закладка технических средств шпионажа
Бухгалтерия	Выемка конфиденциальной информации
Серверная	Несанкционированный доступ
Место хранения ценностей	Выемка ценностей
Компьютерные сети	Несанкционированный доступ
Архив	Выемка конфиденциальной информации

Анализируем угрозы

Бороться есть смысл с тем, кого есть шанс победить, с остальными следует договариваться. Отличить одних от других — важнейшая задача лидера, решаемая заблаговременно в рамках Доктрины корпоративной безопасности. Правильный ответ зависит от стоимости стоящих перед бизнесом задач, публичности объектов защиты, наличием недоброжелателей и степени их агрессивности. Как



Менеджер по развитию бизнеса компании Cisco Systems Алексей Лукацкий

мать, и... Причем это еще «цветочки». С помощь отдельных хакерских «произведений» возможны и более серьезные варианты воздействия: нарушение работоспособности сети, кража и модификация информации, циркулирующей в информационной системе, и т.д.

— Опасность этого в том, что такого рода воздействию подвержена на сегодняшний день любая компания без исключения, — предостерегает менеджер по развитию бизнеса компании Cisco Systems и авторитетный эксперт Алексей Лукацкий. — Даже Microsoft, которая тратит на информационные технологии огромные средства и может себе позволить широчайшие каналы выхода в Интернет, страдает, например, от атак массового обслуживания. Около полутора-двух лет назад атака, направленная на ресурсы этой компании, привела к отказу в ее системах, и ущерб от временной неработоспособности ресурсов Microsoft составил около $500 млн. Что же говорить о более мелких компаниях, которые не имеют выходов в Интернет с гигабитными скоростями, и, соответственно, против них проводить атаки гораздо проще?..

Кому это надо?

Традиционно сетевые атаки связывают с нападением хакеров. Как ни странно, но по статистике, собранной компанией IBM, до последнего времени 90% хакеров оставались любителями, и только 0,1% — это люди, которые зарабатывают своими знаниями деньги. Но многие специалисты отмечают постепенную криминализацию IT-преступности, т.е. сколачивается все больше преступных группировок, работающих именно в виртуальном пространстве. Сегодня в Интернете при желании можно найти прайслисты на услуги подобных сообществ. В России особой пользуется популярностью преступная услуга, стоящая всего несколько десятков долларов. Заплатив эту сумму, можно, например, «заказать» сайт работодателя, который вас уволил, и его выведут из строя направленной DDOS-атакой, суть которой заключается в единовременной загрузке ресурса миллионами бессмысленных запросов.

То же самое касается и спама. При желании любой человек за $100-$200 может виртуально арендовать сеть из сотен инфицированных компьютеров, которые генерируют огромный поток писем, и за час отослать лавину из нескольких миллионов сообщений. То есть любой человек, даже с небольшим доходом, может нарушить бизнес крупной компании.

— Результаты специальных исследований показывают, что на

Таблица 2. Типовые угрозы

Виды угроз	Мотив	Объекты нападения	Модель воздействия
Хулиганство	Случайная агрессия, месть	п. 1-6 табл. 1	Уничтожение имущества
Неорганизованная преступная группа	Краткосрочный, имущественный	п. 1,2 табл. 1	Скрытое проникновение, выемка имущества, отход
Конкуренты	Корпоративная разведка, компрометация	п. 1,5 табл. 1	Несанкционированный удаленный доступ к компьютерным сетям
Ведомства	Заказ как инструмент в конкурентной борьбе	п. 1-3 табл. 1	Внезапное появление, выемка документов, опечатывание закрытых помещений
Организованная преступная группа	Долгосрочный контроль над бизнесом	п. 1-3 табл. 1	Скрытая выемка информации, оперативное давление на руководителя

правило, ответ получается волевым решением, в то же время существуют типовые предположения. Задача анализа — определить область возможных решений. Оперативное же решение всегда принимает руководитель.

Начальный этап работ

Лидер, в режиме консультации с сотрудником, ответственным за корпоративную безопасность составляет список жизненно-важных помещений, приведенный в таблице 1. Ему же отдается приоритет определения угроз, от которых следует защищаться (табл.2). После этого ответственный за безопасность формирует гипотезы поражения, то есть определяет несколько расчетных сценариев нанесения неприемлемого ущерба, определяет комплекс технических и оперативных мероприятий (проводятся заблаговременно), а также план действий при реализации угроз. На его же плечи должны лечь составление бюджета мероприятий и обучение сотрудников правилам работы и поведения в необходимом объеме.

Аудит безопасности

Контроль эффективности проведения мероприятий — важнейшая составляющая обеспечения безопасности.

Метод проведения аудита — крайне интересная тема, выходящая за рамки статьи, но наиболее простой и эффективный способ — моделирование, теоретическое либо в рамках деловой игры.

Цель проведения аудита — избежание типовых технических ошибок. Ими могут являться: в области технической укрепленности — установка защитных конструкций, время вскрытия которых меньше времени реагирования оперативной группы, в области видеонаблюдения — установка камер, не позволяющих идентифицировать личность в расчетных воздействиях, в защите информации — незащищенность компьютерных сетей.

Но самой серьезной ошибкой является отсутствие системного подхода, поскольку любая из угроз может быть нейтрализована лишь с использованием комплекса оперативно-технических мероприятий.

Цена вопроса

Стоимость мероприятий разумнее всего определить до начала проведения работ. Руководитель волен принимать любые решения, но, принимая их, нужно всегда помнить о следующей негативной тенденции. Сегодня в России существует рынок специальных услуг по корпоративной разведке. Услуги эти непрестанно дешевеют, то есть стоимость нанесения неприемлемого ущерба любой компании становится все дешевле.

КОММЕНТАРИЙ

Бизнес директор Scarlett Сергей Машуков:

Как и любой бренд, обладающий высокой степенью востребованности у потребителя, Scarlett не избежал проблем в области интеллектуальной собственности.

Как известно, высокий спрос российского рынка на доступную бытовую технику порождает появление большого количества пиратской продукции. Мы регулярно сталкиваемся и с копированием нашего дизайна, и с неправомочным использованием товарного знака на продукции, даже отдаленно не напоминающей нашу. Попадая в квартиры потребителю, такой лже-Scarlett совсем не добавляет лояльности к нашей компании, и оставлять эту ситуацию бесконтрольной мы, конечно, не имеем права.

Мы стараемся выяснять, на какие фабрики ведет след продавцов контрафактной продукции, и регулярно проводим рейды для нейтрализации этих очагов пиратства и уничтожения найденной там продукции.

В последнее время изготовление контрафактной продукции распространилось и на комплектующие, отвечающие за безопасность функционирования домашней техники. В прошлом году мы, совместно с компанией Strix Limited (Великобритания), одним из двух мировых производителей лицензионных контроллеров для электрических чайников, проводили в отечественной прессе просветительскую программу. Целью программы было объяснение конечному потребителю опасности использования чайников с фальшивыми нелицензионными контроллерами, а также обозначение возможных последствий для дилеров, непредусмотрительно продающих подобную технику.

Мы понимаем, что в одиночку эффективно бороться на этом фронте не под силу ни нам, ни другим компаниям. Именно поэтому мы около года назад вошли в состав комитета по защите интеллектуальной собственности Содружества Русбренд.

Общими силами компаний — членов комитета проводится большая и полезная работа. В том числе совершенствование законодательства в области интеллектуальной собственности, организация семинаров для членов комитета и правоохранительных органов по вопросам борьбы с нарушениями прав на интеллектуальную собственность, разработка пособий по способам противодействия распространению «серого» импорта. Эта работа ведется в тесном взаимодействии с федеральными ведомствами, в том числе с Федеральной службой по интеллектуальной собственности, патентам и товарным знакам, что, конечно же, повышает ее эффективность.

компьютер, подключенный к сети Интернет, в среднем осуществляется около 400 атак в час, — делится данными Алексей Лукацкий. — Здесь и сканирование, и попытки его взлома, подбор паролей и т.д. Кстати, среднее время взлома пароля для Windows на сегодняшний день составляет 13-14 секунд. В данной ситуации уже не выглядит смешным факт, что 2% пользователей в мире в качестве пароля используют слово «пароль». Другая статистика: еще в 2003 году общий объем потерь от инцидентов в сфере информационной безопасности составил $660 млрд. Такую цифру достаточно сложно представить, поскольку далеко не каждая страна может похвастаться валовым продуктом в таком объеме.

Ситуация усугубляется еще одной гримасой быстроразвивающихся высоких технологий — появлением так называемых клик-хакеров, которые не имеют никакого представления о сути работы программ, сайтов и сетей, а просто механически используют для взлома совершенное программное обеспечение, предоставляющее удобный Windows-интерфейс. Впрочем, статистика говорит, что наиболее часто фиксируются именно непреднамеренные атаки, но ущерб от них тоже серьезный. Компьютер, зараженный при такой атаке вирусом, начинает сканировать другие компьютеры, что приводит к перегрузке интернет-канала, «зависанию» корпоративных машин, а иногда и выходу их из строя. Наличие в вирусе деструктивного кода часто приводит к полной потере данных.

Черви и люди

Помимо подготовленных атак Всемирная паутина кишит самостоятельными виртуальными сущностями, способными нанести вред как корпоративным сайтам, так и внутренним сетям компании. Если раньше вирусы распространялись достаточно медленно, перемещаясь из организации в организацию на дискетах, то сегодня это воспринимается как архаизм. Сегодня есть Интернет, и в нем правят бал черви. Именно они перегружают трафик и при недостаточной защите каналов могут блокировать работу внутренней сети компании. Яркий пример — действие червя Slammer, попавшего на атомную электростанцию в Огайо через несанкционированный канал, который был открыт в обход стандартных средств защи-

КОММЕНТАРИЙ

Владимир Федорович Веселов, заместитель генерального директора по инновациям и развитию компании «Ситроникс» (АФК «Система», ОАО «КНЦ»):

Встав на ноги за счет продажи оборудования, произведенного в России и частично купленного за рубежом, компания «Ситроникс» поставила себе задачу увеличить свое присутствие на рынке за счет собственных разработок. Поэтому сейчас на первый план выходит вопрос об интеллектуальной собственности. В России интеллектуальная собственность далеко не на первом месте по степени важности ее сохранения. Если посмотреть баланс российских компаний, то строка нематериальных активов редко когда бывает соответствующим образом заполнена. Существует прямая связь между нематериальным активом и потребительскими свойствами: если нематериальный актив отсутствует, то и потребительские свойства продукта будут далеко не такими, какими должны быть. Основная задача создания подразделения НИОКР — решить прежде всего эту проблему. Управление нематериальными активами позволяет компании «Ситроникс» создавать конкурентное преимущество для своего продукта, а стало быть, увеличивать продажи, амортизировать нематериальный актив и запускать его в создание новых продуктов. Если говорить вообще о безопасности в области интеллектуальной собственности, то это вопрос авторских прав. Мы ставим перед собой задачу защищать не только свою собственность, но и собственность разработчиков. В политике НИОКРа, которую сейчас формирует компания «Ситроникс», значительную часть составляет вопрос сотрудничества с теми российскими фирмами, которые имеют свои разработки.

Что касается налоговых рисков, необходимо сказать, что компания «Ситроникс» заявляет о себе как об абсолютно прозрачной компании. Но мы на себе ощущаем величину налогового давления. Это автоматически приводит к тому, что некоторые продукты производятся не в России, а в Китае, потому что это дешевле. Для того чтобы перейти в рентабельное состояние, торговой марке «Ситроникс», которая появилась в 2002 году, пришлось на время реорганизации концерна расстаться с частью производственных активов, и только сейчас, когда мы вышли на значительные объемы продаж, мы думаем о новых производственных линиях. Существенно пришлось сократить и численность персонала. После реструктуризации и перехода в безубыточное состояние за счет увеличения объемов продаж компания опять начинает расти. Сейчас налоговая ситуация оказалась достаточно сложной для фирм, которые занимаются разработкой нематериальных активов, поскольку они связаны с живым трудом, который в сегодняшней налоговой системе оказывается наиболее обложенным налогами.

Что касается информационной безопасности, то сегодня это наиболее актуальная тема в связи с развитием IT-технологий. В компании «Ситроникс» информационная безопасность осуществляется штатными IT-специалистами с применением наиболее эффективных средств обеспечения, существующих на рынке. Но, к сожалению, «гонка вооружений» среди программистов не может обеспечить стопроцентной безопасности. В скором времени мы надеемся предложить рынку две инновации, как в области компьютерной безопасности, так и в сфере коммуникаций. Для компьютеров мы, возможно, предложим разработку, которая позволит реализовать антивирус на аппаратном уровне. Для этого будет устанавливаться чип, являющийся «прививкой» против несанкционированного доступа, атак вредоносных программ, необнаруженных вирусов и возможных локальных эпидемий. Что касается сферы коммуникаций, то она сейчас интересна многим, в том числе и компании «Ситроникс», входящей в АФК «Система» вместе с МТС. Сейчас мы думаем над разработкой сотового телефона для МТС, который обеспечит конфиденциальный разговор.

ты. Его размножение привело к тому, что работа электростанции была нарушена, и произошло веерное отключение электричества.

— На сегодняшний день математически доказано, что можно создать так называемого активного червя Уорхолла, который в случае запуска распространится по всей Сети за 15 минут, — говорит Алексей Лукацкий. — Соответственно, ни один антивирусный производитель не сможет спасти вас от такого рода червя при его попадании в корпоративную сеть, поскольку даже если он успеет разработать сигнатуру атаки и сигнатуру этого вируса, он не успеет распространить его на всех своих заказчиков.

Пример с атомной электростанцией говорит о том, что ворота вирусу открыл человек. Это подтверждает истину, что самым уязвимым местом системы безопасности фирмы остаются собственные работники. Специалисты давно пришли к выводу, что система защиты организации должна быть комплексной, потому что только она способна оградить бизнес от главной опасности — человека, который может причинить вред случайно или преднамеренно, как находясь за пределами организации, так и будучи ее сотрудником. И это касается не только крупных организаций, но предприятий среднего и малого бизнеса. Возьмем для примера небольшое предприятие с небольшим числом работников.

— В такой фирме, как правило, каждый сотрудник отвечает за свою область, и информация, которой он обладает, находится полностью в его власти, т.е. имеет место децентрализация, когда каждый сотрудник отвечает за свое направление, — говорит Олег Чепиков. — Здесь информационные риски вполне осязаемы. Типичный пример — компания, занимающаяся продажами, один-два сотрудника которой обладают всей базой данных клиентов. Если они уходят и уносят с собой даже копию базы данных, компания может полностью потерять свой бизнес и закрыться. Таким образом, мы видим, что информационная безопасность — это вопрос не только технических средств, но и в очень большой степени — персонала.

Остро стоит и вопрос лояльности сотрудников. Лояльность в определенной степени зависит от величины дохода сотрудника. Хорошо оплачиваемый сотрудник с перспективами роста держится за свое место — ему есть все основания доверять. Поэтому стоит обратить внимание на низкооплачиваемых сотрудников.

Аудит

Как же оградить дело от всех угроз из внешней виртуальной среды и изнутри организации?

— Прежде всего, необходимо признать на уровне высшего руководства, что безопасностью необходимо заниматься, — считает ведущий системный разработчик компании Cisco Sistems Михаил Ка-

КОММЕНТАРИЙ

Начальник отдела маркетинга компании ЕВГО Тимофей Аркадьевич Антонюк

Интеллектуальная собственность нашей компании надежно защищена: торговая марка ЕВГО зарегистрирована, имеет патент и является полностью российской. Сейчас мы проходим процедуру регистрации на Украине, в Казахстане и в Беларуси. Уже в этом году мы будем иметь защищенный торговый знак в четырех республиках СНГ: в России, Украине, Казахстане и Беларуси.

От налоговых рисков, наверное, никакая российская компания не застрахована. Что касается нашей, то у нас возникают проблемы с зачетом НДС при поставках за границу или в страны СНГ. Поскольку сами компании не могут защитить себя от налоговых рисков, то безопасность частного бизнеса в этой области должно обеспечивать государство, то же можно сказать и о таможенной безопасности.

К вопросу об информационной безопасности: каждый сотрудник компании ЕВГО подписывает договор о неразглашении служебной информации. У нас существует проблема удаленности основного производства, которое находится в Хабаровске, от главного офиса московского филиала. Фактически все переговоры и деловая переписка идут не по телефону, а по Интернету. Для быстрого и своевременного обмена информацией у нас установлены частные локальные сети, которые связывают Москву и Хабаровск. Естественно, они имеют несколько степеней защиты, в первую очередь от доступа извне, а также от вирусов и спама. Для обеспечения информационной безопасности компании нашим штатным IT-специалистом используются самые современные технологии.

дер. — Нередко приходится слышать от своих потенциальных заказчиков фразы вроде «ура, нас в пятый раз взломали, теперь, может быть, нам дадут бюджет на информационную безопасность». Удивительно, но руководители словно не хотят слышать «тревожных звонков», не желают обеспечить безопасность собственной фирмы.

Иногда бывает и так, что у бизнесмена просто не доходят руки, ему просто физически некогда заниматься данным вопросом, и он снова и снова откладывает решение вопроса на завтра. Но если руководство упрямо не хочет тратить

ведущий системный разработчик компании Cisco Sistems Михаил Кадер

деньги или время на защиту собственного бизнеса, то рано или поздно с большой вероятностью может наступить момент, когда единовременный ущерб, причиненный киберпреступниками, многократно превысит стоимость любой системы защиты.

— ОАО «Российские железные дороги», одна из крупных монополий в России, использует информационные технологии достаточно активно. В 2004 году на нее было совершено 5 тыс. атак, и тот ущерб, который удалось предотвратить в результате их блокирования, измеряется одним миллиардом рублей, — рассказывает Алексей Лукацкий. — Мне лично неизвестно ни одного внедрения систем защиты, которое бы обошлись в эти деньги.

Все эти цифры и доводы приводят к мысли, что «промедление смерти подобно». Итак, с чего же начать?

Если речь идет об информационной безопасности, то перво-наперво стоит провести аудит системы безопасности, включая аудит существующих документов по системе безопасности, если они уже были разработаны на предприятии. В настоящее время на российском рынке предлагают свои услуги множество компаний, специализирующихся на информационном аудите и консалтинге предприятий. После проведенного приглашенными специалистами исследования состояния информационной системы руководитель, совместно с этими же специалистами, должен провести анализ рисков.

— Риски информационной безопасности начинают играть существенную роль прежде всего тогда, когда информация действительно обладает ценностью, причем ценностью с точки зрения либо ее конфиденциальности, либо ее целостности, либо ее доступности, — считает Олег Чепиков. — Конфиденциальность, целостность, доступность — это как раз те три критерия, которые являются областью и предметом рассмотрения информационной безопасности, и это то, на что направлено обеспечение информационной безопасности.

Важным этапом является разработка внутрикорпоративных нормативных документов по информационной безопасности (политика безопасности). Посредством их устанавливаются правила для сотрудников.

— С помощью политики безопасности руководство обязывает рядовых сотрудников не разбрасывать бумаги по столу, не использовать простые пароли, вести деловые переговоры в специально оборудованных комнатах и тому подобное, — поясняет Олег Чепиков. — Сотрудники с повышенными полномочиями, например, инструктируются об обязательном шифровании всей конфиденциальной информации, ее обязательном хранении только на отдельном диске и работе с ней исключительно на отдельном компьютере, хранении таких данных в закрытой комнате и с наклейкой: «Конфиденциально». Системным администраторам предписывается настраивать межсетевые экраны так, а не иначе, следить за регулярным обновлением антивирусных программ и не брать на себя полномочий специалиста по безопасности, если таковой имеется в организации.

После отработки нормативов можно приступать к реализации реального технического решения. Завершающим этапом работы над созданием надежной защиты организации станет аудит готовой системы. Если компания развивается, потребуется периодический системный мониторинг защиты и, возможно, внесение в нее корректировок. Как правило, такие работы связаны с изменением и расширением структуры предприятия, сетевым подключением к работе сотрудников, привлечением партнерских организаций, запуском услуг через Интернет. Скорее всего, может возникнуть вопрос: а нельзя ли обойтись без аудита?

— Конечно, можно поступить «не просто, а очень просто», купив и сконфигурировав «железки» руками неспециализированных мастеров, имеющих лишь общее представление о возможных «дырах» в системе защиты, — рассуждает Михаил Кадер. — Однако в этом случае нет гарантии, что все возможные входы и выходы информационной системы будут взяты под

начальник отдела защиты информации департамента информационно-технологического развития ОАО «Росбанк» Олег Чепиков

контроль. К тому же без правильной идеологии это может оказаться бессмысленным. При таком подходе руководитель должен быть готов к периодическим и, как всегда, несвоевременным проблемам.

Пытаясь минимизировать расходы, не следует забывать, что это приводит к одновременному увеличению риска нанесения ущерба. Плату за информационную безопасность (например, зарплата руководителя службы ИБ, который профессионально контролирует сеть и сотрудников) можно рассматривать как страховку, которую вы платите, чтобы в один прекрасный момент не обнаружились колоссальные убытки.

Минимизация рисков и страхование

Если что и стоит минимизировать, так это риски. Минимизация (или смягчение) рисков происходит при подключении к Интернету при посредстве специальных средств защиты, которые позволяют эти риски уменьшать. Несомненно, всегда остается вероятность заражения компьютера неизвестными вирусами, в том числе руками собственных сотрудников, приносящих на CD игрушки непонятного происхождения. Но ожидаемый ущерб от таких «бациллоносителей», по крайней мере, значительно меньше, чем от незащищенного компьютера, подключенного к Интернету: в неблагоприятные моменты вы имеете шанс собрать на него за 10 минут полный набор червей и вирусов. Чтобы снять с себя тревогу за сохранность информационных ресурсов, можно прибегнуть к услугам страховых компаний. Страхование рисков используется, когда, с одной стороны, риски очень маловероятны и, с другой — когда с ними уже практически ничего нельзя сделать. Например, землетрясение в Москве или разрушение двух зданий, в одном из которых хранится оригинал баз данных, а в другом — постоянно обновляемые копии (трагический пример — американские «Башни-близнецы»: многие компании, державшие в них офисы, ушли с рынка именно потому, что их информационные ресурсы имели именно такую структуру). Можно, конечно, построить десятиэтажный бункер под землей, но вряд ли клиенты будут с большой охотой посещать ваш офис, да и обойдется это недешево. Более вероятен пожар — статистика по ним ежегодно ухудшается. Сегодня страхование информации стоит недешево и требования к клиентам высокие, поэтому каждый руководитель должен решить сам, насколько высокую ценность имеют для компании ее информационные ресурсы и готов ли он уменьшать прибыльность своего дела ради исключения вероятности банкротства по причине их потери.

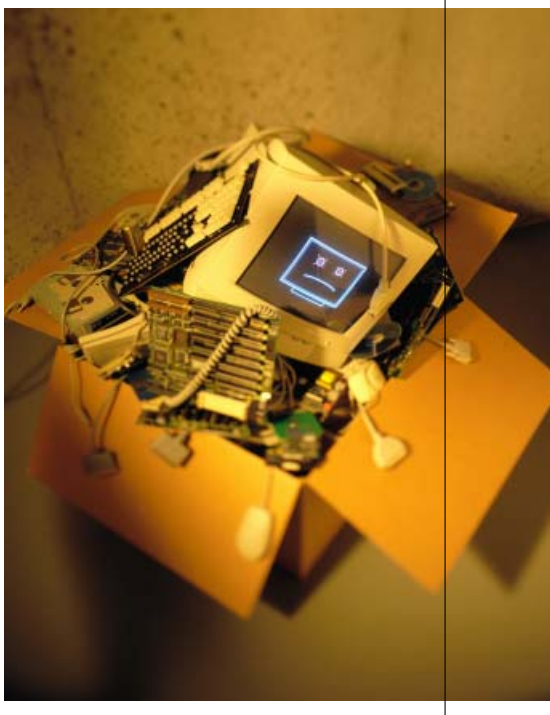
— Какой бы изощренной фантазией и предусмотрительностью не обладал бизнесмен, риски все равно остаются, — уверен Олег Чепиков. — Даже построив максимально эффективную систему безопасности, он должен либо принять этот факт, либо застраховаться от этого. Принятие остаточных рисков или их страхование — третьего не дано.

Стоимость защиты

Сколько бы мы не говорили о важности защиты бизнеса, всегда есть вопрос, который может кардинальным образом повлиять на решение руководителя. Это стоимость системы защиты. Принимающие решения часто задают подобный вопрос и к их удивлению и возмущению поставщики услуг и оборудования не дают им точных цифр. Но это происходит совсем не потому, что на отечественном рынке информационной безопасности нет настоящих профессионалов. Ориентировочные цифры, несомненно, могут быть названы, но в каждом случае нужно быть готовым к значительным отклонениям.

— Многих из нас испортило техническое образование, — иронизирует Олег Чепиков. — Мы стремимся загнать информационную безопасность в одну универсальную формулу, в которую мы могли бы подставлять только пару переменных и получать определенный и четкий ответ. Но информационная безопасность движется — это скорее «science and arts». Наука и искусство одновременно. Сюда входит и оценка рисков, просчет возможных видов атак и многое другое. В каждом индивидуальном случае затраты будут считаться иначе.

Понятно, что стоимость системы защиты не должна превышать стоимость возможного ущерба, который оценить достаточно сложно. Он зависит от текущей стоимости информации, от степени нарушения бизнес-процессов, от косвенных убытков и от других последствий. В настоящее время «модно» оценивать риски, исходя из уже имеющейся статистической базы данных. Но часто статистики нет, и приходится оценивать риски качественно, исходя из соображения здравого смысла и жизненного опыта, который есть у эксперта, проводящего оценку. Оценив риски, вероятность потерь в единицу времени умножают на единичные потери от данного события и получают величину потерь за какой-то период времени. Собственно стоимость системы защиты не должна быть больше, чем вероятные потери. Иногда применяют еще более хитрый прием, прибавляя к объему капиталовложений в систему защиты процент, недополученный вследствие невложения денег в банк или бизнес. То есть, по мнению сторонников данного способа, изъятие денег из бизнеса на оборудование системы безопасности должно автоматически увеличивать ее стоимость на недополученный процент (а эта сумма иногда достигает 50%!). К такой методе можно относиться по-разному, но в логичности ей не откажешь. Каждый судит и рядит по-своему.



Но, оценивая стоимость системы защиты, не стоит забывать о такой важном моменте, как требования регулирующих органов и органов надзора. Иногда приняв решение не ставить те или иные средства защиты, можно вообще потерять возможность принимать какие-либо решения, связанные с бизнесом.

Король внутренней сети

Вечный для бизнеса вопрос «Вложить или не вложить?» встает и при формировании штата специалистов, ответственных за информационную составляющую предприятия. Самый распространенный вариант штатного расписания — системный администратор, одной рукой вскрывающий «подавившийся» бумагой со скрепкой принтер, другой показывающий бухгалтерам, где находятся нужные им опции Word и периодически вспоминающий, что он назначен ответственным за информационную безопасность фирмы. Не нужно иметь технического образования, чтобы понять, что при таком положении дел о какой-то серьезной информационной безопасности не может идти и речи. Руководитель, действительно радеющий за защиту своих информационных ресурсов, имеет двух специалистов: системного администратора, занимающегося кропотливым трудом по поддержанию сети в рабочем состоянии, IT-директора. Последний решает стратегические вопросы, связанные с работой информационной системой предприятия и руководителя отделом информационной безопасности, проводит работу с сотрудниками, анализирует процессы, происходящие в информационной системе предприятия на предмет потенциальной опасности. Если у вас объем работ небольшой, риски информационной безопасности небольшие и связаны только с защитой от вирусов и от внешних угроз, вы можете полагаться на своего IT-специалиста, которому вы доверяете, и уверены, что если он даже куда-то уйдет, то ничего страшного не случится. Потому что при такой структуре он будет знать содержимое всех финансовых баз данных вашей компании. Избежать такой ситуации можно, только организовав собственную аудиторскую проверку с последующим прописанием правил работы сотрудников, которая должна проводиться именно специалистом по информационной безопасности. В результате полномочия должны быть жестко разделены. IT-специалист получит запрет открывать определенные файлы без специального разрешения руководителя, а при его получении — без контроля специалиста отдела безопасности, который должен напрямую подчиняться руководителю. В свою очередь, специалист по безопасности, не имея административных полномочий для доступа к определенным файлам, сможет проверять системные журналы, в которых отражаются все действия операционной системы, в том числе и все действия системного администратора. То есть даже если администратор почистит журналы, запись об этом событии в них останется.

КОММЕНТАРИЙ

пресс-секретарь компании «М.Видео» Надежда Киселева:

Как известно, для всех торговых сетей неизбежна проблема воровства в магазинах и на складах. Любую проблему всегда легче предупредить, чем потом бороться с ее последствиями, поэтому мы ввели специальные меры профилактики. В компании «М.Видео» ведется индивидуальный учет по складским площадям и по отделам в магазинах. Периодически, каждые две недели, в магазинах и на складах проводится инвентаризация. На всех складах и в магазинах компании используются электронные противокражные системы, как то:

* цифровые камеры видеонаблюдения;
* специализированные системы защиты. Например, на портативном аудио крепятся специальные датчики, которые, в случае незаконного выноса товара через электронные рамки, издают звуковой сигнал.

Кроме того, в каждом магазине действует подразделение службы безопасности, в обязанности которой входит предотвращение краж в магазинах.

Стоимость внедрения систем информационной безопасности для различных типов организаций в соответствии с потребностями среднестатистического предприятия

Размер бизнеса	Область деятельности	Численность сотрудников, человек	Разброс стоимости по рынку, $					
			1*	2*	3*	4*	5*	6*
Малый	Промышленность	От 100	4000	10000	23000	30000	39000	77000
	Оптовая торговля	От 50	4000	7000	15000	20000	28000	53000
	Розничная торговля	От 30	1500	3000	12000	16000	23000	43000
Средний	Промышленность	От 200	12000	22000	35000	55000	68000	138000
	Оптовая торговля	От 100	4000	10000	23000	30000	39000	77000
	Розничная торговля	От 60	4000	7000	15000	20000	28000	53000
Крупный	Промышленность	От 400	25000	50000	75000	105000	123000	343000
	Оптовая торговля	От 200	12000	22000	35000	55000	68000	138000
	Розничная торговля	От 120	12000	18000	31000	53000	63000	113000

1* — пакет включает: межсетевой экран Интернета
2* — пакет включает: межсетевой экран Интернета, антивирус
3* — пакет включает: межсетевой экран Интернета, антивирус, сетевую систему обнаружения вторжений
4* — пакет включает: межсетевой экран Интернета, антивирус, сетевую систему обнаружения вторжений, компьютерную систему предотвращения вторжений
5* — пакет включает: межсетевой экран Интернета, антивирус, сетевую систему обнаружения вторжений, компьютерную систему предотвращения вторжений, систему строгой аутентификации пользователей
6* — пакет включает: межсетевой экран Интернета, антивирус, сетевую систему обнаружения вторжений, компьютерную систему предотвращения вторжений, систему строгой аутентификации пользователей, защиту центра обработки данных от несанкционированной деятельности собственных сотрудников