Информационная безопасность

КРОШИЛИН Сергей Викторович *- кандидат технических наук, доцент кафедры менеджмента и маркетинга Коломенского государственного педагогического института, лектор курсов МВА Академии народного хозяйства при Правительстве РФ*
тел. раб.: (496) 615-13-19;
e-mail: Krosh_sergey@mail.ru

МЕДВЕДЕВА Елена Ильинична *– кандидат экономических наук, доцент кафедры менеджмента и маркетинга Коломенского государственного педагогического института, лектор курсов МВА Академии народного хозяйства при Правительстве РФ*
тел. раб.: (496) 615-13-19;
e-mail: E_lenam@mail.ru

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРЕДПРИЯТИЯ: ВЫЯВЛЕНИЕ УГРОЗ И МЕТОДЫ ИХ УСТРАНЕНИЯ

Информационные технологии в настоящее время активно внедряются во все сферы деятельности. Быстро развивающийся рынок электронных информационных продуктов и услуг предлагает большое количество отечественных и зарубежных экономических информационных систем (ЭИС) различного назначения [1]. ЭИС – это не только компьютерная техника и применение новейших технологических достижений, но и совокупность внутренних и внешних потоков прямой и обратной информационной связи экономического объекта, методов, средств, специалистов, участвующих в процессе обработки информации и в выработке управленческих решений.

Важнейшим ресурсом современного предприятия, способным значительно повлиять на повышение его конкурентоспособности, инвестиционной привлекательности и капитализации, являются корпоративные информационные ресурсы и знания, которые сегодня призваны ***обеспечивать безопасность***.

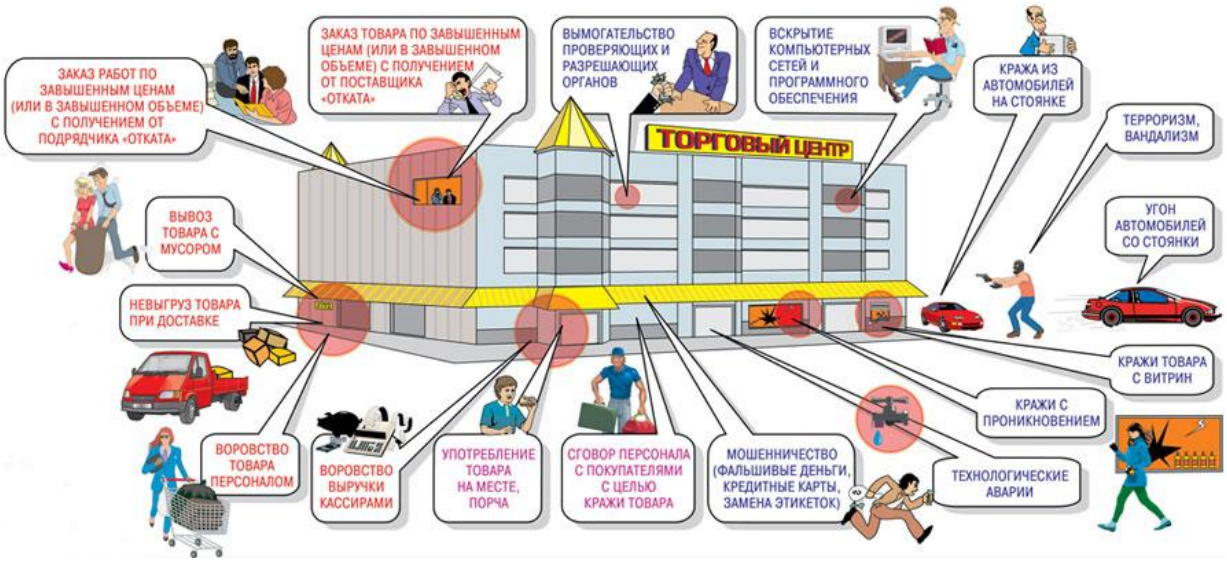
Экономическая и информационная безопасность бизнеса

Безопасность (с точки зрения экономики) – это интегральная системная характеристика сложных объектов, которая зависит от надежности элементов, устойчивости и стабильности показателей, управляемости параметров и живучести объекта в целом [2].

Если отойти от строго теоретического определения экономической безопасности, то можно дать более простое толкование этому термину через понятие «бизнес». Ведь что такое бизнес – это самостоятельная, осуществляемая с риском деятельность с целью получения систематической прибыли. Эту прибыль может или уже получает кто-то вместо вас. А, следовательно, возникают риски, которые формируются за счет целого списка потенциальных угроз для бизнеса.

Рассмотрим возможные угрозы для бизнеса на экономическом объекте «Торговый центр» (см. рис. 1), которых в настоящее время достаточно много.

Экономическая безопасность предприятия – это такое состояние коммерческой, финансовой, производственной и любой другой деятельности на предприятии, при которой невозможно или затруднительно нанести экономический ущерб данному предприятию.



Источник: http://g2engineering.ru/service/1191944536.htm

Рис. 1. Возможные угрозы экономической безопасности объекта «Торговый центр»

Современная «зависимость» бизнеса от ИТ: качество функционирования и обслуживания может серьезно сказаться на экономической безопасности предприятия, так как высокая степень централизации корпоративной информации делает ее особенно уязвимой и увеличивает риск утечки данных. Таким образом, одной из составляющих экономической безопасности является информационная. Информационная безопасность - это система, позволяющая выявлять уязвимые места организации, опасности, угрожающие ей, и справляться с ними.

Событие, которое может вызвать нарушение функционирования экономического объекта (фирмы, предприятия, организации и т.д.), включая искажение, уничтожение или несанкционированное использование обрабатываемой информации, называется угрозой. Возможность реализации угроз зависит от наличия уязвимых мест. Состав и специфика уязвимых мест определяется видом решаемых задач, характером обрабатываемой информации, аппаратно-программными особенностями обработки информации на предприятии, наличием средств защиты и их характеристиками.

Следует выделить два основных класса угроз информационной безопасности [2]:

1. ***Непреднамеренные или случайные действия***, выражающиеся в неадекватной поддержке механизмов защиты и ошибками в управлении (например, если пользователи пишут пароли на бумажках и приклеивают их к мониторам, ни о какой защите информации не может быть и речи).

2. ***Преднамеренные угрозы*** – несанкционированное получение информации и несанкционированная манипуляция данными, ресурсами и самими системами (например, попадание накопителей на жестких (оптических) дисках и магнитных лентах в руки посторонних лиц часто приводит к утечке конфиденциальной информации).

Сегодня, например, повсеместное распространение мобильных накопителей информации — таких как flash-диски, винчестеры с USB интерфейсом и т.д. обусловило появление нового класса угроз информационной безопасности. Несанкционированное использование таких устройств нелояльными сотрудниками может привести к утечке информации из корпоративной сети. Единственной альтернативой физическому отключению USB-портов может быть использование специальной системы защиты информации.

Большинство специалистов в области информационной безопасности считают мобильные накопители главной угрозой бизнеса сегодня (см. рис. 2) [3].

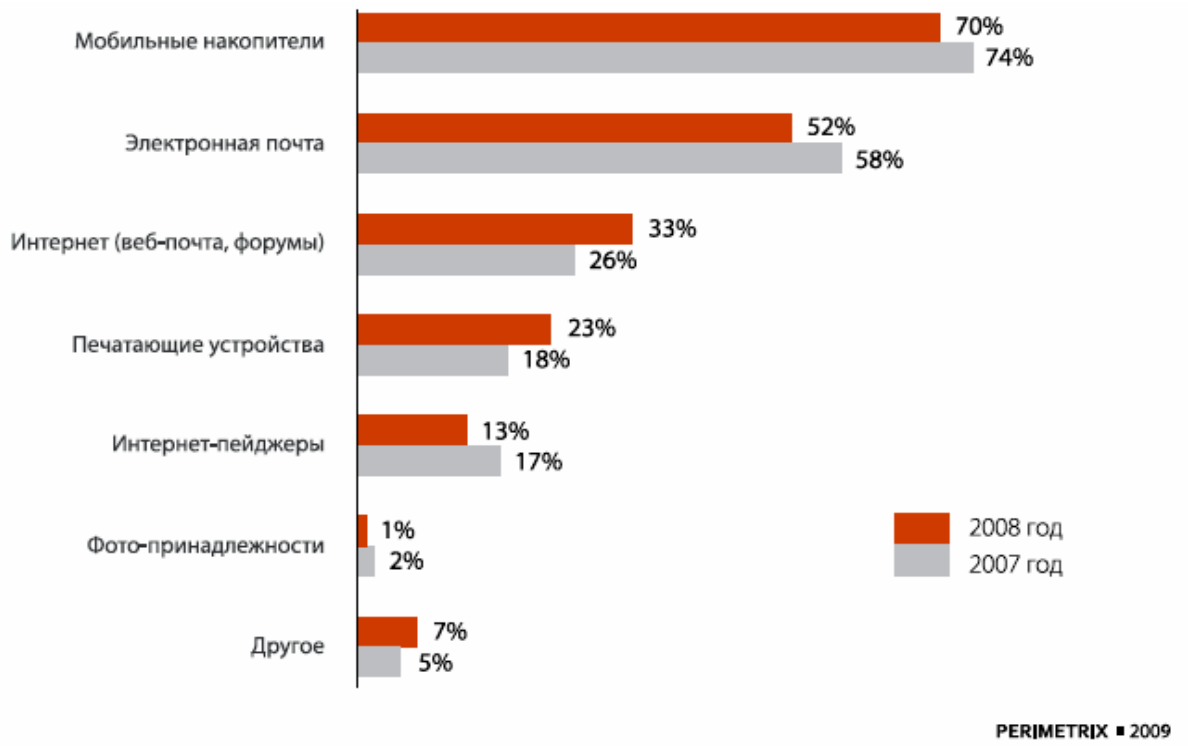


Рис. 2. Самые популярные каналы утечки

Электронная почта достаточно долго занимала лидирующие позиции в рейтинге самых опасных каналов утечки. Причина в том, что мобильные накопители являются менее заметными: крошечные запоминающие устройства, способные вмещать десятки гигабайтов данных, объем, сравнимый с возможностями жестких дисков. Их вместимость, мобильность и простота подключения — главные причины распространения как оружия инсайдеров. С другой стороны, за электронной почтой на большинстве предприятий зорко наблюдает служба безопасности. А также, очевидно, сложно таким образом переслать большой массив данных.

Просто запретить использование мобильных накопителей не всегда возможно, так как очень часто «флэшки» требуются по производственной необходимости. Это что-то вроде кухонного ножа: с одной стороны — самое распространенное орудие бытовых убийств, а с другой — незаменимый помощник в хозяйстве. Так что вариант с заклеиванием USB-порта ленточкой с голографической наклейкой здесь неуместен. Впрочем, сегодня уже есть широкий выбор специализированного ПО, способного предотвратить утечку программным способом, без таких экзотических средств.

Классификация угроз безопасности бизнеса

Классификация угроз безопасности может быть осуществлена разделением угроз на связанные с внутренними и внешними факторами [2].

Множество *непреднамеренных угроз*, связанных с ***внешними*** (по отношению к бизнесу) факторами, обусловлено влиянием воздействий, неподдающихся предсказанию (например, угрозы связанные со стихийными бедствиями, техногенными, политическими, экономическими, социальными факторами, развитием информационных и коммуникационных технологий, другими внешними воздействиями).

К ***внутренним*** *непреднамеренным* относят угрозы, связанные с отказами вычислительной и коммуникационной техники, ошибками программного обеспечения, персонала, другими внутренними непреднамеренными воздействиями. Отдельно следует выделить угрозы связанные с ***преднамеренными ошибками***, возникающие за пределами бизнеса. К таким угрозам относят следующее:

- несанкционированный доступ к информации, хранящейся в системе;
- отрицание действий, связанных с манипулированием информацией (например, несанкционированная модификация, приводящая к нарушению целостности данных);

- ввод в программные продукты и проекты “логических бомб”, которые срабатывают при выполнении определенных условий или по истечении определенного периода времени и частично или полностью выводят из строя компьютерную систему;
- разработка и распространение компьютерных вирусов;
- небрежность в разработке, поддержке и эксплуатации программного обеспечения, приводящие к краху компьютерной системы;
- изменение компьютерной информации и подделка электронных подписей;
- хищение информации с последующей маскировкой (например, использование идентификатора, не принадлежащего пользователю, для получения доступа к ресурсам системы);
- перехват (например, нарушение конфиденциальности данных и сообщений);
- отрицание действий или услуги (отрицание существования утерянной информации);
- отказ в предоставлении услуги (комплекс нарушений, вызванных системными ошибками, несовместимостью компонент и ошибками в управлении).

Под ***несанкционированным доступом*** (НСД) к ресурсам информационной системы понимаются действия по использованию, изменению и уничтожению исполняемых модулей и массивов данных системы, проводимые субъектом, не имеющим права на подобные действия.

К сожалению, приходится констатировать, что унифицированный подход к классификации угроз информационной безопасности отсутствует. И это вполне объяснимо, так как при всем том многообразии информационных систем, направленных на автоматизацию множества технологических процессов, которые затрагивают различные сферы человеческой деятельности, жесткая систематизация и классификация угроз неприемлема.

Наиболее приемлемой в настоящее время можно считать следующую классификацию (см. рис. 3).

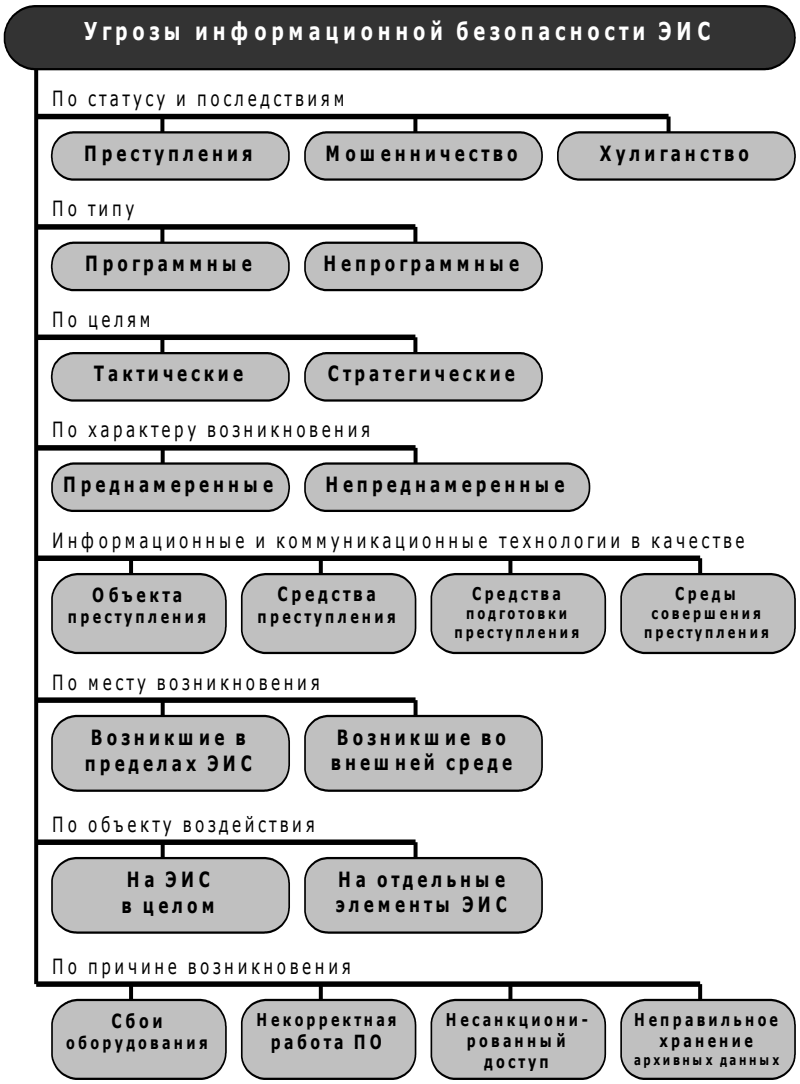


Рис. 3. Классификация угроз информационной безопасности

Как видно из рисунка, ***по составу и последствиям*** ПЗ представляются в виде преступлений, мошенничеств и хулиганств.

- Под *компьютерным преступлением* (КП) следует понимать комплекс противоправных действий, направленных на несанкционированный доступ, получение и распространение информации, осуществляемых с использованием средств вычислительной техники, коммуникаций и ПО.
- *Компьютерное мошенничество* отличается от других видов компьютерных нарушений тем, что его целью является незаконное обогащение нарушителя.
- *Компьютерное хулиганство*, на первый взгляд, является безобидной демонстрацией интеллектуальных способностей, но последствия подобных действий могут быть весьма серьезными, поскольку они приводят к потере доверия пользователей к вычислительной системе, а также к краже данных, характеризующих личную или коммерческую информацию.

По ***типу реализации*** можно различать *программные* и *непрограммные* злоупотребления. К программным относят злоупотребления, которые реализованы в виде отдельного программного модуля или модуля в составе программного обеспечения. К непрограммным относят злоупотребления, в основе которых лежит использование технических средств для подготовки и реализации компьютерных преступлений (например, несанкционированное подключение к коммуникационным сетям, съём информации с помощью специальной аппаратуры и др.).

Компьютерные злоумышленники преследуют различные цели и для их реализации используют широкий набор программных средств. Исходя из этого, представляется возможным объединение программных злоупотреблений ***по целям*** в две группы: *тактические и стратегические.* К тактическим относят злоупотребления, которые преследуют достижение ближайшей цели (например, получение пароля, уничтожение данных и др.). К группе стратегических относятся злоупотребления, реализация которых обеспечивает возможность получения контроля над технологическими операциями преобразования информации, влияние на функционирование компонентов ИС (например, мониторинг системы, вывод из строя аппаратной и программной среды и др.).

По характеру возникновения различают *непреднамеренные* и *преднамеренные* злоупотребления. Непреднамеренные угрозы связаны со стихийными бедствиями и другими неподдающимися предсказанию факторами, сбоями и ошибками вычислительной техники и программного обеспечения, а также ошибками персонала. Преднамеренные угрозы обусловлены действиями людей и ориентированы на несанкционированное нарушение конфиденциальности, целостности и/или доступности информации, а также использование ресурсов в своих целях.

При реализации угроз безопасности ***информационные и коммуникационные технологии*** могут выступать в качестве объекта преступления, средства преступления, средства подготовки преступления или среды совершения преступления.

По месту возникновения угроз безопасности ЭИС можно различать угрозы, возникающие в пределах ЭИС и угрозы, возникающие во внешней среде.

По объекту воздействия следует выделять угрозы, воздействующие на ЭИС в целом и угрозы, воздействующие на отдельные ее элементы.

По причине возникновения различают такие угрозы, как сбои оборудования, некорректная работа операционных систем и программного обеспечения, несанкционированный доступ и неправильное хранение архивных данных, вследствие чего они могут быть утеряны (уничтожены).

Реализация нарушителями угроз безопасности ЭИС приводит к нарушению нормального функционирования ЭИС и/или к снижению безопасности информации, определенное конфиденциальностью, целостностью и доступностью.

Структура и составляющие информационной безопасности

Таким образом, все перечисленное можно отобразить в виде схемы, которая дает полное представление о ***структуре информационной безопасности*** (ИБ) [1], которая предусматривает защиту информации от широкого спектра угроз для обеспечения непрерывности бизнеса, минимизации потерь и максимизации возврата от вложенных инвестиций. Каждая организация имеет информационные ресурсы (пункт 1) - знания и умения сотрудников, аппаратное и программное обеспечение, БД, документацию и прочие виды информации (пункт 2).

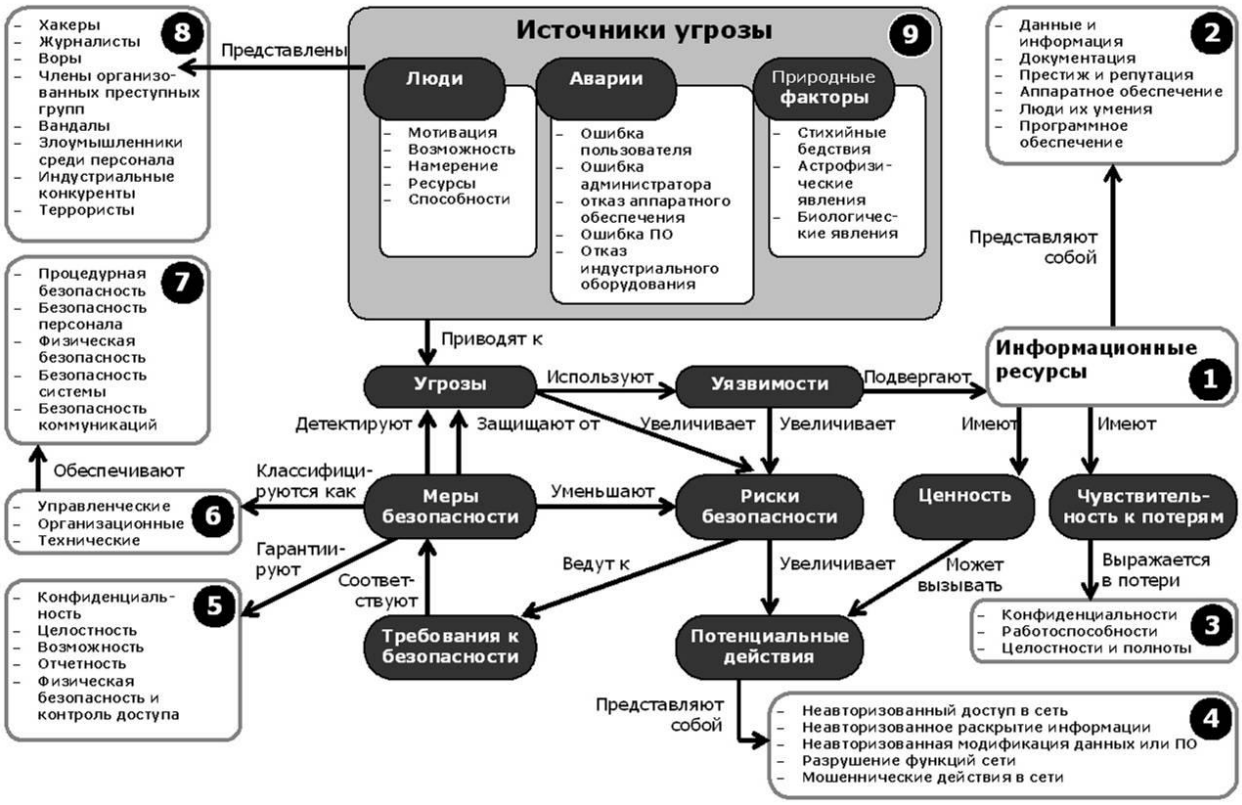


Рис. 4. Структура и составляющие информационной безопасности

Важной составляющей ресурса компании является информация о компании в обществе, которая формирует репутацию фирмы, степень доверия к ней со стороны клиентов, популярность бренда и т.д.

Информационные ресурсы подвержены потерям в виде нарушения конфиденциальности, работоспособности, целостности и полноты (пункт 3). Чем ценнее информация в компании, тем больше опасность вредоносных действий, направленных на завладение ею или на ее уничтожение. Вредоносные действия могут совершаться в виде неавторизованного доступа в сеть, неавторизованного раскрытия информации (утечки информации), модификации данных или ПО, а также мошеннических действий в сети (пункт 4).

Наличие описанных уязвимостей определяет угрозы безопасности, которые представляют собой риски, требующие введения мер безопасности. Степень риска определяет уровень затрат на меры безопасности. Меры безопасности должны гарантировать конфиденциальность, целостность, доступность информации, своевременную отчетность, физическую безопасность и контроль доступа (пункт 5). В свою очередь, меры безопасности могут быть техническими, организационными и управленческими (пункт 6).

Например, защита от вирусов может быть реализована технически - посредством установки антивируса, а может быть решена организационно путем запрещения выхода в интернет, самовольной установки ПО и использования мобильных накопителей информации.

Меры безопасности обеспечиваются различными системами безопасности: процедурной, физической, системной, коммуникационной и др. (пункт 7).

На рисунке показаны также источники угрозы: намеренные действия со стороны людей, возможные аварии (ошибки в работе пользователей, программ и оборудования), а также природные факторы (пункт 9).

Интересно, что в категорию вандалов и террористов (представляющих опасность с точки зрения кражи и повреждения информации) попадают также журналисты (пункт 8). Впрочем, очевидно, что в плане утечки корпоративной информации журналисты порой представляют не меньшую опасность для корпорации, чем шпионы. Недаром во многих компаниях общаться с журналистами имеют право лишь определенные категории сотрудников - обычно высший менеджмент и сотрудники отдела маркетинга.

Что можно предпринять для обеспечения информационной безопасности

Обеспечение информационной безопасности сводится к трем основным направлениям - это комбинация технических, административных и организационных мер. Прежде всего, нужно понять, что и от чего необходимо защитить. Знание природы бизнеса предприятия, особенностей бизнес-процессов, а также того самого инсайдера («врага») — самый важный шаг внедрения системы нейтрализации угроз информационной безопасности.

Традиционно защита была сферой компетенции ИБ/ИТ служб, которые зачастую выступали инициаторами, внедренцами и эксплуатирующей инстанцией таких проектов. Это, в свою очередь, наложило на проекты сильный отпечаток технократического подхода, слабо увязывавшего защиту с бизнесом организации. С точки зрения эффективности защиты и инвестиций, необходимо отталкиваться не от контроля информационной инфраструктуры и сетей передачи данных, а от контроля только критических бизнес-процессов. В рамках каждого внедрения системы нужно проводить глубокий предварительный анализ, призванный определить наиболее критичные, с точки зрения безопасности, бизнес-сценарии.

Важно заметить, что в процессе практической реализации ИБ стратегии компании питают слабость к точечным мерам, напоминающим пожаротушение. Например, «заткнуть» интернет-пейджеры или фильтровать электронную почту. Однако всегда найдутся альтернативные каналы. Из этого следует очевидный вывод — защита от утечек может быть всеобъемлющей, пронизывающей все бизнес-процессы.

Исходя из вышеизложенного, используя предложенную классификацию угроз безопасности, необходимо разрабатывать соответствующие методы и средства обеспечения информационной безопасности экономических информационных систем, среди них можно предложить следующие:

- совершенствование системы аутентификация пользователей;
- защита информации внутри фирмы (при пересылке и хранении);
- разработка эффективной системы защиты от внутренних угроз.

Совершенствование системы аутентификация пользователей. Аутентификация (или идентификация) пользователя выполняется каждый раз, когда пользователь вводит логин и пароль для доступа к компьютеру, в сеть или при запуске прикладной программы. В результате их выполнения он получает либо доступ к ресурсу, либо вежливый отказ в доступе.

Как правило, информационная инфраструктура современных предприятий гетерогенна. Это означает, что в одной сети совместно существуют серверы под управлением разных операционных систем и большое количество прикладных программ. В зависимости от рода деятельности предприятия это могут быть приложения электронной почты и групповой работы (GroupWare), CRM- и ERP-системы, системы электронного документооборота, финансового и бухгалтерского учета и т.д.

Количество паролей, которые необходимо помнить обычному пользователю, может достигать 5–6. Пользователи пишут пароли на бумажках и приклеивают на видных местах, сводя тем самым на «нет» все усилия по защите информации, либо постоянно путают и забывают пароли, вызывая повышенную нагрузку на службу поддержки. Если к этому добавить, что каждый пароль должен состоять не менее чем из 6–8 произвольных букв, цифр и спецсимволов и его необходимо периодически менять, то серьезность проблемы очевидна.

Оптимальное решение проблемы – специальное программное обеспечение, позволяющее хранить пароли в защищенной памяти электронных идентификаторов и в нужный момент извлекать их и предоставлять соответствующим системным или прикладным компонентам.

В качестве электронных идентификаторов могут использоваться USB-брелки или смарт-карты, что позволяет контролировать их обращение и организовать строгий учет в отличие от паролей, для которых это невозможно в принципе.

Такие системы существенно снижают риск утечки информации, связанный с ошибками персонала, а также с преднамеренными действиями нечестных или обиженных сотрудников и обеспечивают надежную аутентификацию пользователей при доступе к сетевым ресурсам.

Защита информации внутри фирмы. Современные корпорации сталкиваются с бурным ростом объемов данных, необходимых для их повседневной работы. Этот рост вызван потребностью иметь «на кончиках пальцев» финансовую, маркетинговую, техническую, статистическую и другую информацию для оперативного реагирования на изменения рыночной ситуации, поведение конкурентов и клиентов. Высокая степень централизации информации увеличивает риск утечки.

Информация в корпоративных сетях хранится на жестких дисках и магнитных лентах, и попадание именно этих носителей в руки злоумышленника создает наиболее серьезную угрозу информационной безопасности и может привести к тяжелым последствиям.

Приведем несколько возможных вариантов утечки конфиденциальной информации, хранящейся на жестких дисках и лентах: отправка серверов или жестких дисков в ремонт; перевозка компьютеров из одного офиса в другой; утилизация компьютеров, серверов, жестких дисков и лент; перевозка ленты в депозитарий и т.д.

Очевидно, что такие решения, как системы защиты периметра сети или системы аутентификации, в данном случае не работают, поскольку злоумышленник получает физический доступ к носителям информации.

Оптимальное решение проблемы – для защиты информации в процессе хранения необходима защита информации, размещенной на жестких дисках, на дисковых массивах и в хранилищах методом шифрования данных, а также шифрование данных на диске персональных компьютеров. Особое значение приобретает защита информации при резервном копировании.

Разработка эффективной системы защиты от внутренних угроз. Очевидно, что обиженный или недовольный сотрудник компании, имеющий легальный доступ к сетевым и информационным ресурсам и обладающий определенными знаниями о структуре корпоративной сети, может нанести своей компании гораздо больший ущерб, чем хакер, взламывающий корпоративную сеть через интернет. Этот факт подтверждает и статистика. Так, по различным оценкам, от 50 до 80 % атак, направленных на получение информации ограниченного доступа, начинается из локальной сети предприятия (интрасети) [4].

Особенную актуальность проблема внутренних угроз получила в связи с появлением и повсеместным распространением мобильных накопителей информации, подключаемых через USB-порты - таких как flash-диски, винчестеры с USB-интерфейсом и т.д. Любой сотрудник компании может практически незаметно пронести на территорию предприятия компактный носитель большого объема и скопировать на него всю интересующую его информацию.

Оптимальное решение проблемы – системы, блокирующие порты персонального компьютера, к которым могут подключаться внешние устройства, и возможность гибкой настройки прав доступа на основе списков контроля доступа. Такие системы могут запретить использование внешних накопителей информации и разрешить подключение каких-либо других внешних устройств, например, USB-ключей для аутентификации пользователей. Существующая возможность записи в журнал неудачных попыток подключения позволит выявить потенциально нелояльных сотрудников на ранних этапах.

Рассмотренные методы и средства преодоления угроз информационной безопасности нуждаются в дальнейшем совершенствовании и развитии, но даже относительно простые приведенные способы защиты позволяют существенно снизить риск несанкционированного доступа к информации, возможность ее порчи и кражи, что значительно повышает экономическую безопасность предприятия в целом.

Дадим несколько практических советов.

Практические рекомендации

Проблема весьма деликатна и дать универсальный совет на все случаи жизни достаточно тяжело. Механизмы защиты (или инструменты защиты) зависят от множества факторов, начиная от рода деятельности предприятия и территориального расположения офиса, заканчивая количеством персонала на предприятия и сложившимся отношением к информационной безопасности внутри предприятия. Однако, опираясь на опыт специалистов в данной области, можно дать несколько практических советов.

Во-первых, это проверка персонала при приеме на работу совместно блоком безопасности и блоком по управлению персоналом. Это не только тестирование, собеседование, определение личностных характеристик и наклонностей, но и проверка предыдущих мест работ, так называемое «наведение справок» по своим источникам информации. Это поможет отсеять «кротов-предателей» еще до тех пор, как они проникнуть в ВАШ бизнес.

Во-вторых, это грамотная пользовательская политика внутри корпоративной (компьютерной) сети. Разграничение прав и уровня доступа к отдельным видам информации, особенно к той, которая представляет коммерческую тайну, к клиентской базе данных (которая

сегодня является важным ресурсом предприятия), к финансово-бухгалтерской информации и т.д. Грамотная защита всего перечисленного поможет ВАМ избежать многих неприятностей.

В-третьих, постоянный контроль. Это не должна быть тотальная слежка за всем и вся, но персонал должен понимать, что его действия отслеживаются. Необходимо применять различные средства мониторинга сетевого трафика (например, TrafficInspector – наша коломенская разработка компании SmartSoft), анализа сетевой активности, кто и что посещает в Сети и куда уходят письма с корпоративного ящика. Камеры видеонаблюдения и фиксация телефонных звонков оказывают тоже очень положительный эффект в плане защиты. Так как понимание персонала того, что любое их действие фиксируется, заставляет по-другому относиться не только к вопросам безопасности, но и к эффективности работы на протяжении всего рабочего дня.

В-четвертых, это специализированные системы комплексной безопасности фирмы в виде информационных компьютерных систем, которые контролируют всё, начиная от финансовых показателей деятельности фирмы (базирующие на бухгалтерской информации), заканчивая анализом исходящих сообщений сотрудников по электронной почте. В этом случае часто встает вопрос: «Стоит ли инвестировать в технологии, которые все равно не смогут решить проблему?». Уже сейчас можно сказать, что индустрия разработки сделала большой шаг вперед по сравнению с концепцией «защиты от дурака». Недавно начали появляться системы класса РСКД (режим секретности конфиденциальных данных). Разработчикам еще предстоит предпринять много усилий не только для совершенствования своих решений, но и для информирования потенциальных заказчиков. А таких решений сегодня достаточно много, но о них мало кто знает. Эти системы используют технологию контентной фильтрации потока сетевых данных и выявлении конфиденциальной информации на основе вероятностных методов. Современной альтернативой является использование детерминистских методов, которые предполагают разметку всех конфиденциальных документов, и постоянный контроль над их использованием. В таких условиях контентная фильтрация становится дополнительной технологией, позволяющей автоматически категоризировать новые, неразмеченные документы. Но главным минусом таких систем является цена, а главное, сложность внедрения и необходимость детального изучения всего бизнеса со стороны внедренцев. Раскрытие всех особенностей своего бизнеса в России кому-либо равносильно потере бизнеса, так как мы уже писали выше «прибыль может или уже получает кто-то вместо вас».

Разумеется, невозможно создать абсолютную защиту – «щит» от всех и навсегда. Противостояние меча и щита — это непрекращающийся процесс совершенствования. В следующей статье мы хотим остановиться уже на «мече», т.е. на тех технологиях, которые помогают избежать возникновения угроз за счет их нейтрализации на ранней стадии – деловой (конкурентной) разведке, которая основывается на всестороннем анализе конкурентного поля предприятия.

Литература:

1. *Крошилин С.В., Медведева Е.И. Информационные технологии и системы в экономике: учебное пособие. - М.: ИПКИР, 2008. - 485с.*
2. *Крошилин С.В. Возможные угрозы безопасности экономических информационных систем и методы их устранения // Проблемы и методы управления экономической безопасностью регионов: Материалы межвузовской научной конференции профессорско-преподавательского состава, Коломна: КГПИ. - 2006. - С. 240-244.*
3. *Преображенский Е. Инсайдерские угрозы в России`09 // Управление персоналом // Корпоративная Периодика. -2009. - №7(209). - С. 6-10.*
4. www.it2b.ru – *Журнал «Технологии разведки для бизнеса»*

\