Динамика безопасности: от внешних угроз – к внутренним

В. Ульянов, *руководитель аналитического центра Perimetrix*
vladimir.ulyanov@perimetrix.com

Первое ежегодное исследование российской компании Perimetrix показало, что современные организации опасаются, прежде всего, внутренних угроз информационной безопасности (ИБ). Утечки конфиденциальной информации, халатность сотрудников и инсайдеры вызывают у отечественных компаний панический страх, несравнимый с впечатлениями от классических угроз ИБ – вирусов, хакеров и спама.

Согласно статистике, авиация является самым безопасным видом транспорта, на котором происходит наименьшее количество аварий. Но, не взирая на статистику, огромное количество людей бояться летать, испытывая так называемую аэрофобию. По мнению психологов, их поведение объясняется стандартной человеческой реакцией – людям свойственно преувеличивать опасность экзотических угроз и преуменьшать важность угроз обыденных.

Похожая ситуация долгое время наблюдалась и в информационной безопасности. Традиционные угрозы ИБ (прежде всего, вредоносное ПО и хакеры) всегда являлись эдакой экзотикой, поскольку даже крупные компании сталкивались с ними не чаще одного раза в несколько месяцев. Однако именно от этих типов угроз они пытались защититься в первую очередь.

Проблема заключалась в том, что опасность обыденных типов угроз катастрофически недооценивалась. Специалисты по безопасности думали о вирусах, однако забывали о том, что каждый сотрудник компании посылает десятки конфиденциальных писем в день, и всего лишь одна ошибка в адресе способна привести к серьезным последствиям. Пытаясь построить периметральную защиту от внешних вторжений, они не вспоминали о вечно пропадающих ноутбуках, содержащих гигабайты проприетарной информации. А, создавая защищенный web-сайт, они не понимали, что вся защита пойдет лесом, если какой-нибудь глупый сотрудник случайно опубликует секретные сведения в общем доступе.

Исследование Perimetrix показало, что эта нездоровая ситуация постепенно начинает меняться.

Методология исследования

Опрос проводился с 10 января по 10 февраля нынешнего года. В исследовании приняли участие сотрудники 472 российских организаций, которые отвечали на вопросы по электронной почте, в телефонных беседах, при личном интервью, а также заполняли online-анкеты на одном из сайтов по информационной безопасности. Легко видеть, что выборка респондентов (рис. 1) имеет небольшой уклон в сторону крупных и средних компаний. Кроме того, среди респондентов исследования преобладают компании с высоким количеством рабочих станций на одного сотрудника. Впрочем, уровень компьютеризации компании практически не влияет на сравнительную опасность информационных угроз.

Вертикальное распределение респондентов (рис. 2) вполне типично для опросов, проводимых «компьютерной» компанией. Лидирующие

доли (26 % и 21 %) заняли отрасли финансов и телекоммуникаций, которые являются основными потребителями ИТ-решений в целом и систем безопасности в частности. За ними расположился активно развивающийся ТЭК (19 %), а также государственные структуры (14 %). На долю каждого из остальных рынков пришлось не более 7 % респондентов.

Добавим, что практически половина (48 %) респондентов исследования являлись руководителями ИТ-отделов на своих предприятиях. 36 % опрошенных возглавляют отдел ИБ, а оставшиеся 16 % приходятся на рядовых специалистов по информационным технологиям и безопасности.

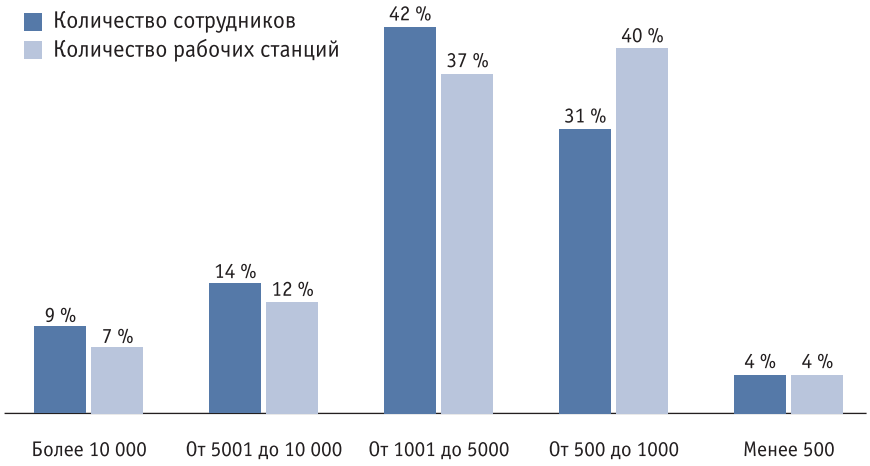

Рис. 1. ***Количество сотрудников и рабочих станций в организациях-респондентах***

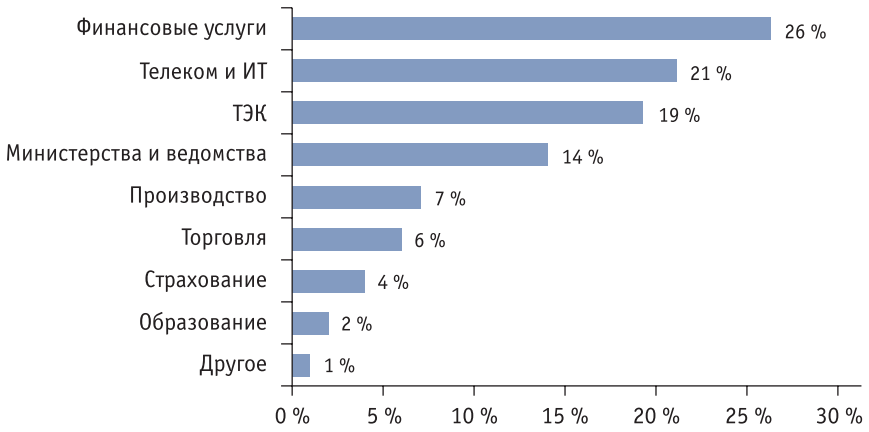

Рис. 2. ***Вертикальное распределение участников опроса***

Угрозы ИБ: общий взгляд

Первый содержательный вопрос исследования Perimetrix касался общей опасности как внешних, так и внутренних угроз ИБ. Респондентам предлагалось выделить до четырех угроз, представляющих максимальную опасность для их организации. Полученное распределение угроз показано на рис. 3 (темным выделены внутренние угрозы).

Первое место в рейтинге заняла главная угроза внутренней безопасности – утечка информации – которую отметили абсолютное большинство (76 %) респондентов. На втором месте оказалась халатность служащих (67 %), что также совсем неудивительно, поскольку утечки часто происходят именно по этой причине. Добавим, что в категорию «халатность» входит и излишнее рвение сотрудников, которое в некоторых случаях приводит к печальным последствиям. Например, желание поработать с конфиденциальными сведениями дома может обернуться украденным ноутбуком, либо скомпрометированным письмом на бесплатном почтовом сервисе.

Вирусы и прочее вредоносное ПО набрали 59 % голосов, хакеры – 47 %, а спам, соответственно, 46 %. О чем говорит это распределение? Прежде всего, угрозы внешней безопасности по-прежнему весьма актуальны, и пренебрегать ими ни в коем случае нельзя. Однако в настоящее время эти угрозы уже нельзя рассматривать как основной приоритет, поскольку опасность инсайдерских утечек информации становится все более и более серьезной.

Рис. 3. ***Наиболее опасные угрозы ИБ (возможно выбрать до четырех вариантов)***

Последний тезис лучше всего пояснить на примере. В случае хакерской атаки убытки компании будут измеряться стоимостью времени простоя тех или иных информационных систем (или неинформационных систем – сотрудников). Для крупной корпорации эта стоимость может оказаться весьма большой – однако и осуществить атаку на нее будет чрезвычайно трудно.

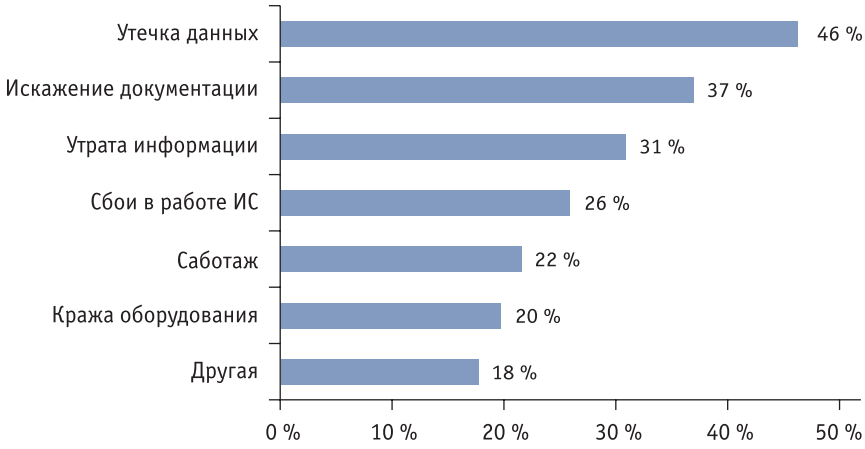

Рис. 4. ***Наиболее опасные угрозы внутренней ИБ***

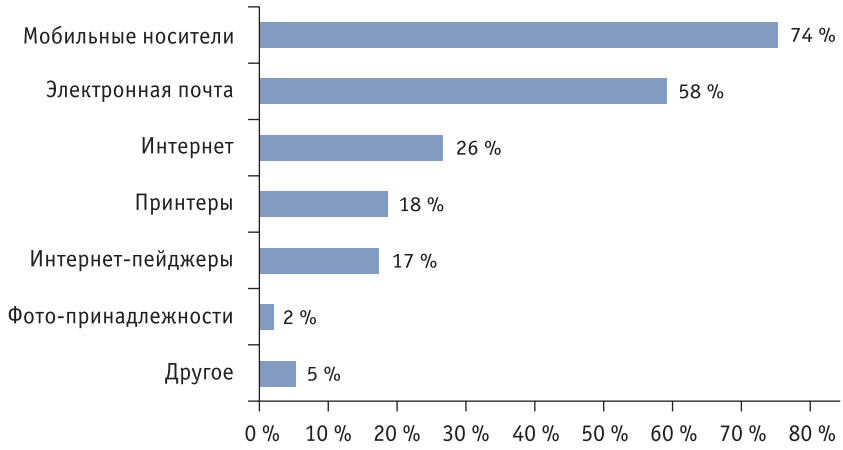

Рис. 5. ***Наиболее опасные каналы утечки***

Убытки в результате утечек определяется целым рядом факторов. Если «утекла» проприетарная информация – бизнес-планы, интеллектуальная собственность или документация по проектам – ущерб может быть практически каким угодно, все зависит от типа и количества потерянных данных. Если же компания теряет персональные сведения клиентов, то этот ущерб можно примерно оценить – он складывается из расходов на расследование инцидента, оповещение пострадавших, выплаты штрафов регуляторам и репутационных издержек. По данным Ponemon Institute, ущерб от потери персональных данных одного человека в США в 2007 году составлял примерно 197 долл. Другими словами, утечка базы данных всего лишь с 5 тыс. записей приводит компанию к миллионным потерям.

В России ситуация несколько иная: в нашей стране пока не работают нормативы, обязывающие оповещать жертв утечек. Как следствие, главной строкой расходов в случае утечки персональных данных являются репутационные потери, которые, впрочем, становятся действительно большими, только если сведения об инциденте появились в российских СМИ. Таким образом, основную опасность для российских компаний представляют утечки «другой» информации – информации, составляющей коммерческую тайну. Но даже этого вполне достаточно, чтобы считать саму угрозу основной.

Тут, правда, необходимо добавить, что целью хакеров и вирусов также может быть конфиденциальная информация компании. И более того, вероятность такого развития событий растет с каждым календарным годом. Здесь важно понимать, что получить доступ к информации снаружи значительно труднее, чем сделать это изнутри. Как следствие, собственные сотрудники компании всегда опаснее хакеров, просто потому, что доступ к информации имеется у них по умолчанию.

Угрозы внутренней ИБ: чем опасны инсайдеры?

Впрочем, утечка информации является далеко не единственной внутренней угрозой (рис. 4). Сотрудники компании могут не только вынести сведения за пределы фирмы, но и изменить (искажение документации), удалить (саботаж) или даже потерять (утрата информации) данные сведения. На этом список внутренних угроз не исчерпывается – в нем также присутствуют аппаратные или программные сбои (по вине сотрудников) и кража оборудования.

Однако именно утечку информации можно признать самой опасной внутренней угрозой – ее отметили 46 % респондентов. Почему именно эта угроза получила максимальное количество голосов? Все объясняется крайне просто – среди перечисленных угроз только инсайдерский «слив» и кража оборудования дают сотруднику прямую финансовую выгоду. При этом украсть у компании нематериальный актив (информацию) на порядок проще, чем вынести из офиса какое-нибудь техническое устройство.

Другой характерной чертой угрозы утечек является ее вариативность. Если инсайдер хоть немного знаком с информационными технологиями, он придумает десятки способов перенести информацию наружу. С точки зрения безопасности, крайне трудно перекрыть все эти способы, не создавая при этом помех для нормальной работы сотрудников.

Действительно, самым простым вариантом инсайда можно признать копирование информации на мобильный носитель, например, флешку. Каким образом можно защититься от данной угрозы? Физическая блокировка портов является элементарным, но при этом и крайне грубым способом, поскольку мешает выполнению прямых служебных обязанностей. Как следствие, компаниям приходится внедрять более хитрые системы, решающие проблему комплексно, а не перекрываю-

щие отдельные направления утечек. Традиционные «канальные» решения неэффективны, а, кроме того, реализовать фильтрацию по всем каналам невероятно трудно.

Зато вполне реально выделить из всех каналов наиболее опасные. Как показало исследование Perimetrix (рис. 5), такими каналами являются мобильные носители и электронная почта (74 % и 58 % соответственно). На третьем месте расположились другие интернет-каналы (26 %), а далее идут принтеры (18 %), IM (17 %), а также «экзотика» – фото-принадлежности (2 %). По-видимому, инсайдерам не слишком удобно орудовать фотоаппаратами.

Получившееся распределение вполне неплохо объясняется аналитически. Опасность мобильных носителей очевидна, поскольку именно они воспринимаются стандартным человеком как основное средство транспортировки файлов. Весьма опасна и электронная почта – главный инструмент работы любого компьютеризированного сотрудника. Но почта, в отличие от мобильных носителей, редко позволяет пересылать файлы очень большого размера.

Значительное отставание Интернета и IM-программ также не должно удивлять – оба канала не являются основными средствами транспортировки и, кроме того, они часто перекрываются службой информационной безопасности, чтобы сотрудники не вели личные беседы на рабочем месте.

Логичным следствием обилия каналов утечки является большое количество самих утечек. Здесь ситуация выглядит очень печально: по данным Perimetrix, только одна компания из 20 (!) не допустила ни одной утечки информации за последний год. Более того, 7 % российских фирм умудрились потерять информацию 25 раз и более (рис. 6).

Показательно, что 26% респондентов затруднились дать точный ответ на поставленный вопрос. Этот, казалось бы, довольно большой показатель значительно ниже общемировых параметров. По данным исследования консалтинговой фирмы PricewaterhouseCoopers (PwC) «The Global State of Information Security 2007», точного количества инцидентов не знают 40 % организаций, причем их доля выросла почти в полтора раза за последний год.

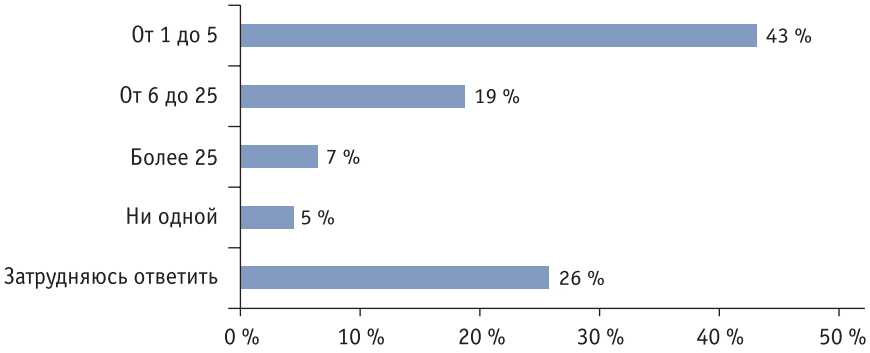

Рис. 6. ***Количество утечек конфиденциальной информации в 2007 году***

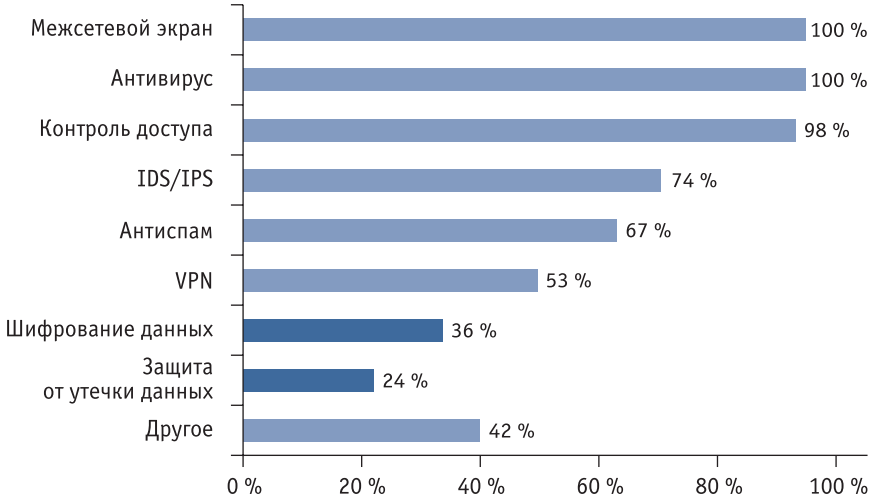

Рис. 7. ***Популярные решения по информационной безопасности***

«Мне кажется, что рост количества сомневающихся компаний говорит о положительной динамике рынка, – считает директор по развитию бизнеса компании Perimetrix Алексей Доля. – Несколько лет назад специалисты заявляли о том, что они знают ситуацию в своей ИТ-инфраструктуре, однако теперь у них уже не осталось таких иллюзий. Очевидно, что без предварительного и беспристрастного анализа нельзя построить действительно эффективную защиту».

Как защититься от угроз?

Вполне логично, что следующий вопрос исследования Perimetrix касался текущего положения дел в системе информационной безопасности респондентов. Как выяснилось (рис. 7), практически 100 % организаций уже используют антивирусную защиту, систему контроля доступа и межсетевые экраны, однако практически не применяют специализированных решений для защиты от утечек информации.

Действительно, только 36 % компаний имеют решения по шифрованию данных, которые не предотвращают, а лишь снижают риски утечки информации. В категорию «защита от утечки данных» (24 %) входят сразу несколько классов решений: системы контентной фильтрации, пассивного мониторинга (логирования), контроля портов рабочих станций и того же шифрования ноутбуков. Ни один из перечисленных классов решений нельзя назвать комплексной системой защиты класса DLP – по данным Perimetrix, проникновение таких систем в России по-прежнему близко к нулю.

Добавим, что полученные результаты прекрасно согласуются со списком основных угроз ИБ – защитившись от внешней стороны проблемы, компании стремятся избежать и внутренних инцидентов. И действительно, все опрошенные орга-

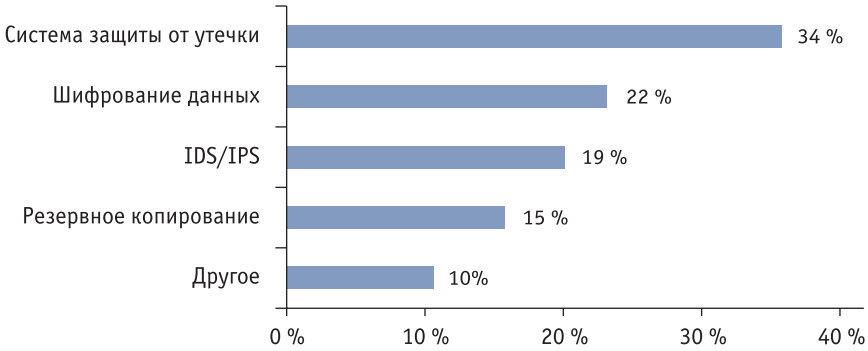

Рис. 8. ***Планы по наращиванию систем ИБ в ближайшие три года***

низации используют антивирусы и межсетевые экраны, а значит, они в той или иной степени защищены от вирусов и хакеров. Решения для борьбы со спамом, системы обнаружения/предотвращения вторжений и VPN-системы также широко распространены среди отечественных компаний.

Таким образом, максимальную актуальность сегодня приобретают внутренние угрозы безопасности, от которых пока мало кто защищен. Логично предположить, что ситуация будет меняться, и все большее количество компаний решат внедрить защитные системы. По мнению аналитического центра Perimetrix, эти изменения могут произойти уже в течение ближайших лет (рис. 8).

Легко заметить, что две первые позиции списка занимают классы продуктов, ориентированных на внутреннюю безопасность компании. Особо выделим шифрование – эта мера часто недооценивается, поскольку она не позволяет полностью защитить компанию от самой страшной внутренней угрозы – инсайдеров. Вместе с тем, важность шифрования трудно переоценить, поскольку почти половина утечек (49 % по данным Ponemon Institute) происходят вследствии кражи различных носителей. А шифрование, как известно, является единственным способом избежать неприятных последствий в результате подобных инцидентов.

Но если решение для шифрования информации можно внедрить сравнительно быстро и дешево, то реализация комплексного проекта по защите от утечек предполагает серьезную подготовительную работу. И, прежде всего – классификацию всех имеющихся корпоративных данных. В противном случае даже самая продвинутая система не сможет отличить приватные сведения от всех прочих.

Классификация информации весьма полезна и сама по себе, в отрыве от внедрения каких-либо систем. Во-первых, она увеличивает производительность труда (за счет снижения затрат на поиск), во-вторых – оптимизирует использование ИТ-ресурсов и, в-третьих – предоставляет качественную картину о положении дел в организации. Однако несмотря на очевидные преимущества, классификация используется крайне редко – только 13 % компаний провели ее в течение последнего года, а 40 % – вообще никогда не проводили. Основным фактором, препятствующим классификации, является временная динамика – более половины (52 %) респондентов отметили, что классификацию трудно поддерживать с течением времени.

«Наше исследование показало, что абсолютное большинство (77 %) специалистов относятся к классификации данных положительно, – отметил директор по маркетингу Perimetrix Денис Зенкин. – Почему же они так редко ее проводят? Основная причина в том, что у организаций отсутствуют инструменты для решения данной задачи, а ручная классификация слишком сложна и трудоемка. Мне представляется, что качественная система защиты от утечек должна содержать в себе подобные инструменты, поскольку без классификации она просто не сможет работать».

С другой стороны, классификацию можно рассматривать как важный фактор, подстегивающий клиентов к внедрению систем защиты от утечек. Благодаря классификации, организации не только минимизируют издержки от утечек, но и получают прямую выгоду для бизнеса, которую нетрудно оценить количественно.

Заключение

В целом, исследование компании Perimetrix показало, что российские компании достаточно неплохо защищены, но только с одной стороны. Внедряя защиту от внешних угроз на протяжении последних лет, компании забывали о внутренней проблеме и оставались уязвимыми для инсайдеров. Как следствие, лишь считанные проценты организаций избежали утечек в прошедшем году, а свыше четверти фирм зарегистрировали 6 и более внутренних инцидентов. Масштаб проблемы огромен, особенно если учесть, что даже одна утечка интеллектуальной собственности может привести компанию к многомиллионным потерям.

Существует целый комплекс причин, из-за которых сформировалась такая ситуация. Основная масса факторов лежит в исторической плоскости – решения по внешней безопасности появились на рынке значительно раньше и говорили о них гораздо больше. Добавим, что недооценка некоторых классов решений (прежде всего, шифрования и классификации данных) во многом объясняются и человеческой психологией.

Впрочем, не стоит посыпать голову пеплом – ситуация в отрасли постепенно начинает меняться. Специалисты прекрасно осознают несовершенство своей системы безопасности и будут активно с этим бороться. Около трети компаний (34 %) планируют внедрить комплексные системы защиты в течение ближайших трех лет, а четверть организаций (22 %) собираются использовать шифрование. Эти меры позволят вывести информационную безопасность на новую ступень развития, которая предполагает всестороннюю защиту информации, а не ИТ-инфраструктуры. ■