ЗИ

АКАДЕМИЯ
СОВРЕМЕННЫХ
ИНФОКОММУНИКАЦИОННЫХ
ТЕХНОЛОГИЙ

ЗИ **Защита информации**

ЗИ.2 Утечки конфиденциальной Информации 2011
(количество частей – 1, число страниц - 17)

ЗИ.2

ZECURION
ANALYTICS

Утечки конфиденциальной информации 2011

www.zecurion.ru | analytics@zecurion.com | +7 (495) 221-21-60

Аннотация

Аналитический центр Zecurion Analytics представляет результаты очередного ежегодного исследования об утечках конфиденциальной информации за 2011 год. Несмотря на серьезные изменения в профиле угроз, которые отмечают специалисты Zecurion Analytics, проблема утечек остается актуальной для большинства современных компаний. Стабильно высоким на протяжении последних лет сохраняется и число публичных инцидентов ИБ, а финансовый ущерб организаций неизменно растет.

Анализ инцидентов подтверждает, что защищенность компаний находится на крайне низком уровне. Отсутствие адекватных политик безопасности и современных технических средств защиты делает бизнес уязвимым перед внутренними угрозами. Часто причинами утечек становятся не подготовленные инсайдеры или тщательно спанированные атаки внешних злоумышленников, а банальная халатность сотрудников и низкая осведомленность в вопросах защиты информации.

Наш отчет адресован широкой аудитории, в т. ч. руководителям компаний, ИТ- и ИБ-подразделений, представителям СМИ. Мы также надеемся, что данное исследование будет интересно специалистам по информационной безопасности с практической точки зрения и поможет лучше понять профиль угроз, подобрать адекватные средства защиты.

Ключевые выводы

- Оценочный ущерб от публичных инцидентов информационной безопасности в 2011 году превысил $20 млрд (в среднем $25,13 млн на каждый инцидент). При этом были скомпрометированы персональные данные свыше 350 млн человек.

- Наибольшее число инцидентов (45,2%) происходит вследствие ошибок или халатности персонала, низкой осведомленности сотрудников компаний по вопросам информационной безопасности.

- Больше всего информации утекает из медицинских организаций (20,4%), госучреждений (16,7%), образовательных заведений (15,2%), предприятий розничной торговли (13,8%).

- Большое число утечек медицинских данных (19,1% всех утечек) связано с их высокой востребованностью среди мошенников.

- Чаще всего информация утекает через ноутбуки и мобильные накопители (суммарно 19,4%), веб-сервисы (18,2%), компьютеры (16,1%), а также неэлектронные носители (13,8%). По мнению специалистов Zecurion, внедрение средств шифрования и контроль печати документов поспособствует сокращению количества инцидентов.

- Количество публичных инцидентов в России стабильно растет. В 2011 году их зарегистрировано 41. Аналитический центр Zecurion связывает данный факт с ужесточением регулирования обработки персональных данных.

Методология исследования

В основу отчета легла база инцидентов информационной безопаности, собранная специалистами Zecurion из публикаций в открытых источниках в течение 2011 календарного года. Из числа инциднетов были исключены те случаи, когда потенциальный ущерб от утечки данных составлял менее $5 тыс. Кроме того, в отличие от исследований прошлых лет, в базу не добавлялись инциденты, реализованные исключительно внешними злоумышленниками без всякого содействия со стороны инсайдеров.

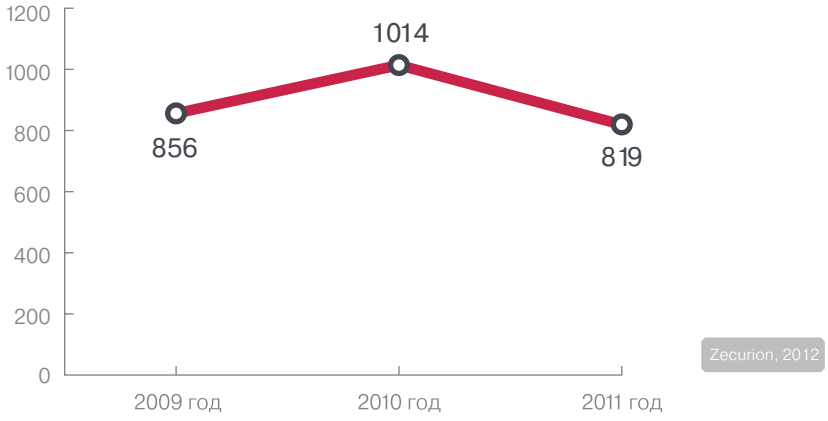
Потенциальный ущерб оценивался по внутренней методике Zecurion Analytics, учитывающей тип и объем скромпрометированных данных, отраслевую специфику, особенности национального законодательства, а также реакцию на инцидент со стороны регулирующих органов, СМИ и общественности.

Методология ежегодных исследований утечек не является жесткой и меняется в соответствии с реалиями сегодняшнего дня, сохраняя, тем не менее, преемственность для корректного определения актуальных тенденций в области информационной безопасности. В этой связи в отчете показана динамика показателей на основании данных прошлых лет. В тех случаях, когда данные прошлых лет не являются показательными, приведены только свежие цифры.

Источники утечек

Общее количество зарегистрированных утечек заметно уменьшилось по сравнению с прошлым годом (см. рис. 1). Однако эти цифры не должны никого вводить в заблуждение. Объясняется данный факт не реальным снижением числа утечек, а изменением критериев отбора инцидентов (см. раздел «Методология исследования») по сравнению с прошлыми годами.

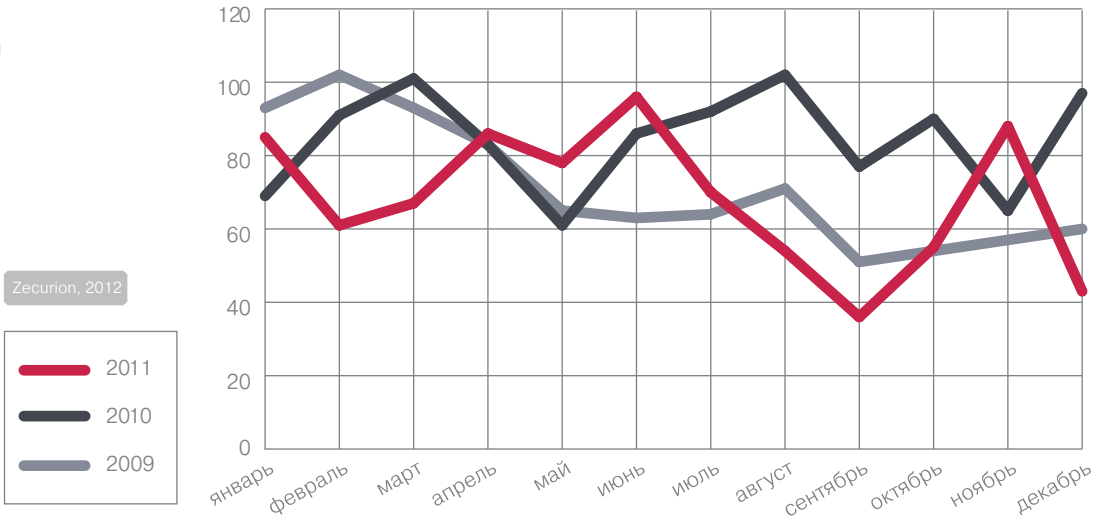
Рисунок 1 ▶
Количество зарегистрированных инцидентов информационной безопасности



Кроме того, необходимо учитывать, что публичными становится лишь незначительная доля инцидентов (не более 0,1%, по оценкам Zecurion Analytics). Выборка является достаточно репрезентативной для выявления актуальных трендов, однако не позволяет делать выводов о точном количестве инцидентов информационной безопасности в мире.

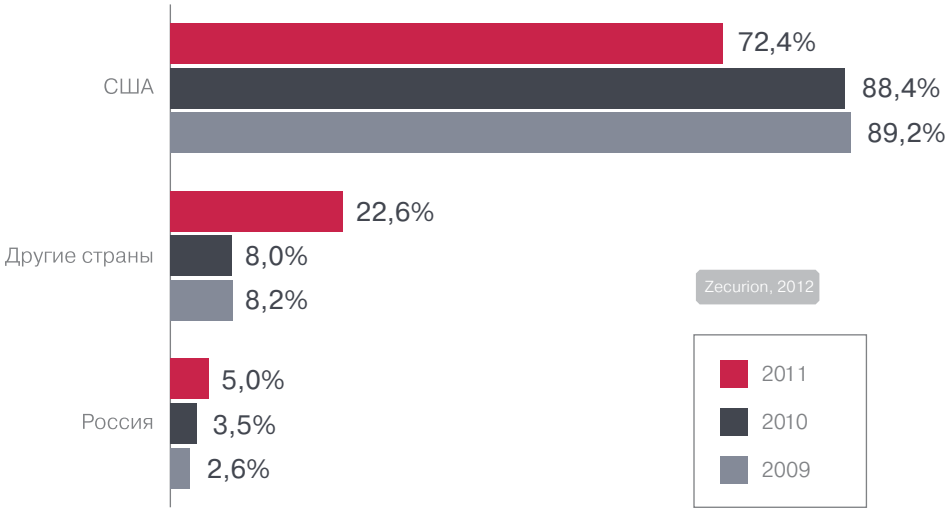
Наименее активным с точки зрения утечек в 2011 году был период с июля по октябрь. На рис. 2. представлено распределение утечек по месяцам.

Рисунок 2 ▶
Динамика утечек по месяцам



Говоря о географии инцидентов (см. рис. 3), необходимо отметить увеличение доли России и других стран за счет сокращения доли утечек из США. По мнению Zecurion Analytics, это положительная тенденция. Чем шире будут освещаться инциденты, тем сильнее будут мотивированы компании защищать конфиденциальные сведения, свои и своих клиентов. Стабильный рост доли публичных инцидентов в России связан, прежде всего, с реализацией закона «О персональных данных». О наиболее громких российских инцидентах будет рассказано в следующих разделах данного отчета. Среди прочих стран существенный процент имеет Великобритания.

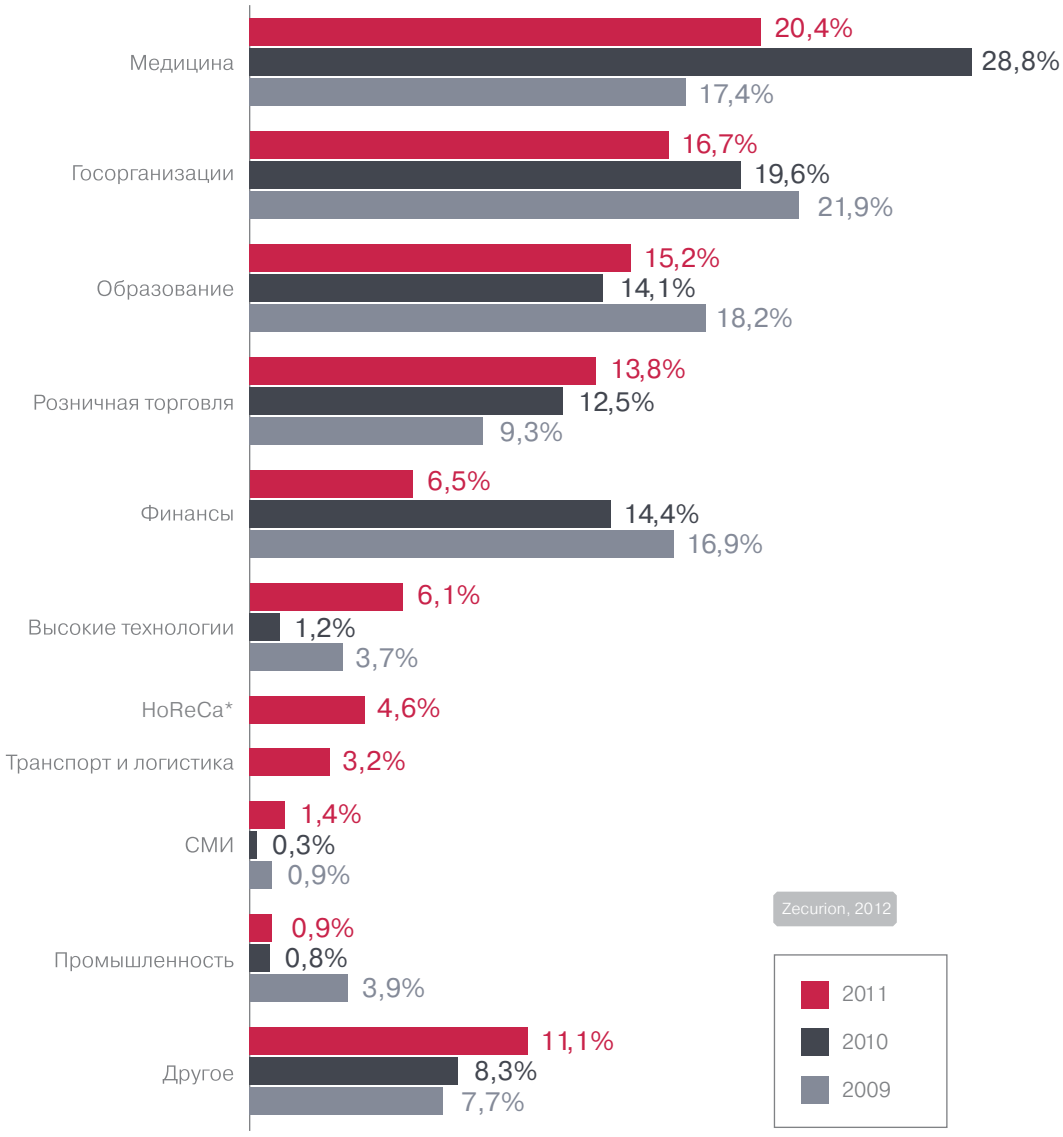
Рисунок 3 ▶
География утечек



В безусловном лидерстве США нет ничего удивительного. Достаточно жесткое законодательное регулирование, серьезные санкции за сокрытие утечек, пристальное внимание к вопросам защиты информации со стороны СМИ и щепетильность американцев в отношении собственных персональных данных предопределяют большое количество публично раскрытых инцидентов.

Отраслевое распределение (см. рис. 4) претерпело некоторые изменения по сравнению с прошлыми годами, однако никаких революционных сдвигов не произошло. В связи с увеличением доли в отдельные категории были выделены транспортные и логистические компании (3,2% всех зарегистрированных инцидентов) и предприятия общественного питания (4,6%). Отметим снижение доли финансовых компаний — показатель того, что к защите информации, в т. ч. банковской тайны, организации стали относиться внимательней.

Рисунок 4 ▶
Отраслевая специфика утечек



*HoReCa — Hotel, Restaurant, Cafe/Catering

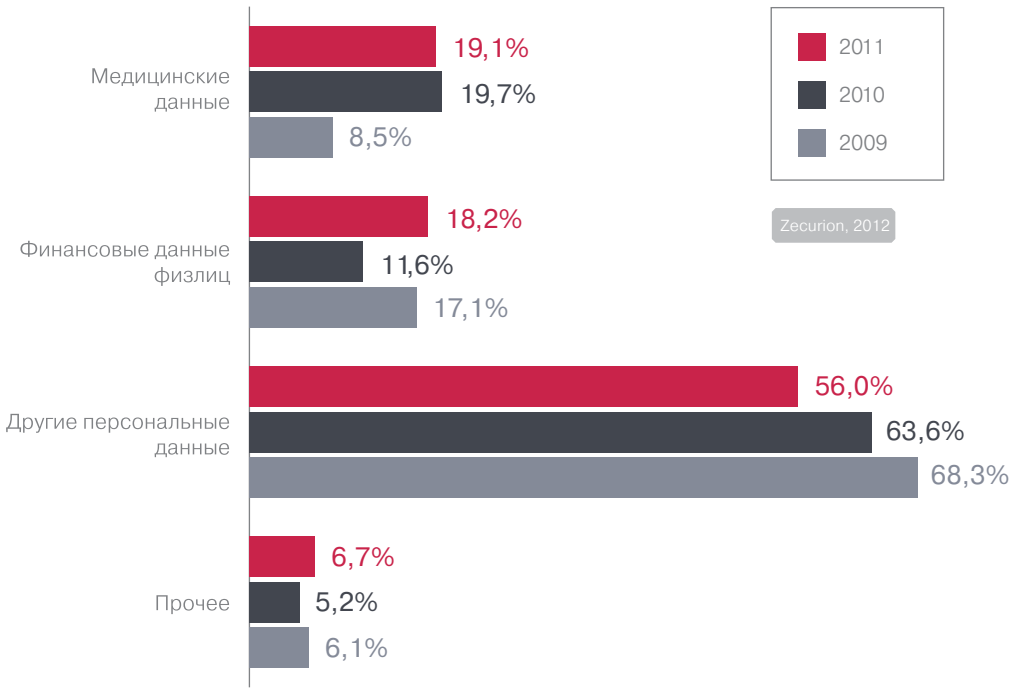
Вновь увеличилась доля высокотехнологичных компаний. Причиной здесь может быть, как ни парадоксально, именно высокая квалификация сотрудников. Даже если мы говорим о непреднамеренных утечках. Пренебрежение элеменарными мерами защиты информации из-за уверенности, что «со мной такого не произойдет» нередко выливается в шокирующие инциденты. К примеру, в 2008 году в британском Кэнноке, ИТ-аналитик на автостоянке у паба потерял флэшку с учетными данными для доступа к порталу Government Gateway (британский вариант электронного правительства), поставив под угрозу персональные данные 12 млн человек.

Стабильно высокой остается доля утечек из госучреждений. Если в коммерческих организациях серьезным препятствием для внедрения мер по обеспечению информационной безопасности часто является финансовый аспект, в государственных организациях причины утечек иные. Для госучреждений характерны большие объемы обрабатываемой конфиденциальной информации, в том числе персональных данных и большое количество сотрудников с доступом к этим данным. Как следствие, выше вероятность ошибки, которая может привести к непреднамернной утечке; проще внедрение злонамеренного инсайдера или подкуп нелояльного работника. Кроме того, финансовые последствия утечек из госорганов, как правило, ниже и ложатся бременем не на кошельки владельцев бизнеса, а на бюджеты разных уровней. Поэтому и мотивация менеджеров к защите информации не так высока.

Последствия утечек

На протяжении 3 лет ведения статистики мы видим стабильное снижение доли персональных данных, при этом серьезный всплеск в 2011 году наблюдается в категории финансовой информации (см. рис. 5). В результате количество скомпрометированных медицинских и финансовых данных сравнялось. Число утечек коммерческой и гостайны, интеллектуальной собственности и других типов данных (категория «Прочее») относительно невелико. Однако каждая такая утечка, как правило, имеет серьезные репутационные последствия и несет внушительные финансовые потери.

Рисунок 5 ▶
Какие данные утекают

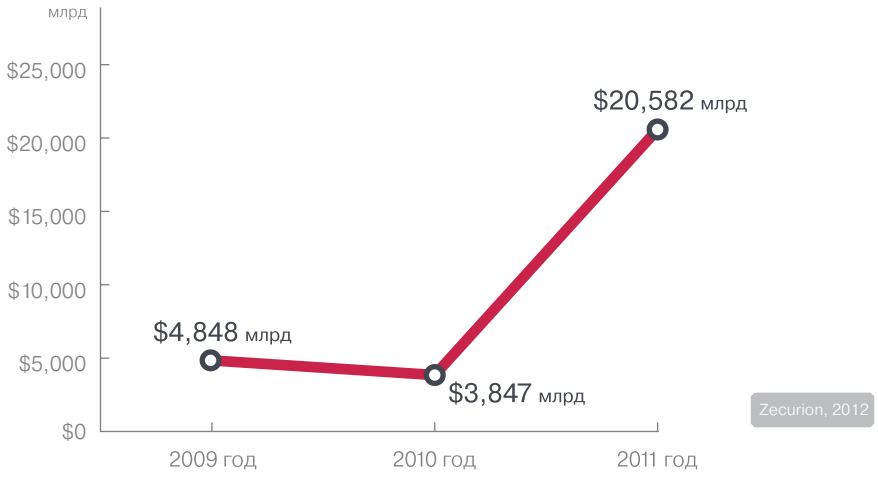


Примечательно, что в отраслевом распределении доля финансовых компаний составляла всего 6,5% (см. рис. 4). Это указывает на то, что большое количество финансовых данных утекло из других отраслей, прежде всего предприятий розничной торговли (еще один восходящий тренд), медицинских и образовательных учреждений.

Наиболее высокорисковыми активами из перечисленных являются, вследствие их высокой ценности, медицинские данные. Это отражается, к примеру, в стоимости данных на черном рынке. Согласно отчету «The financial impact of breached protected health information», выпущенному ANSI (American National Standards Institute), каждый медицинский идентификационный номер можно продать примерно за $50, в то время как номер социального страхования (SSN) только за $1. В том же исследовании отмечается, что при утечке медицинских данных через инсайдеров в 90% случаев это делается преднамеренно и только в 10% — случайно. Хотя в целом, по статистике, превалируют именно случайные утечки. Это еще один показатель востребованности данных среди мошенников.

Общий ущерб от зарегистрированных утечек информации в 2011 году, по оценке Zecurion Analytics, составил $20,582 млрд (см. рис. 6). В среднем, каждая утечка обошлась в $25,13 млн. Суммарное число скомпрометированных записей персональных данных составило свыше 350 млн.

Рисунок 6 ▶
Ущерб от утечек



Изменение масштаба ущерба по сравнению с 2009-2010 годами связано с корректировкой методики оценки ущерба в соответствии с современными международными практиками.

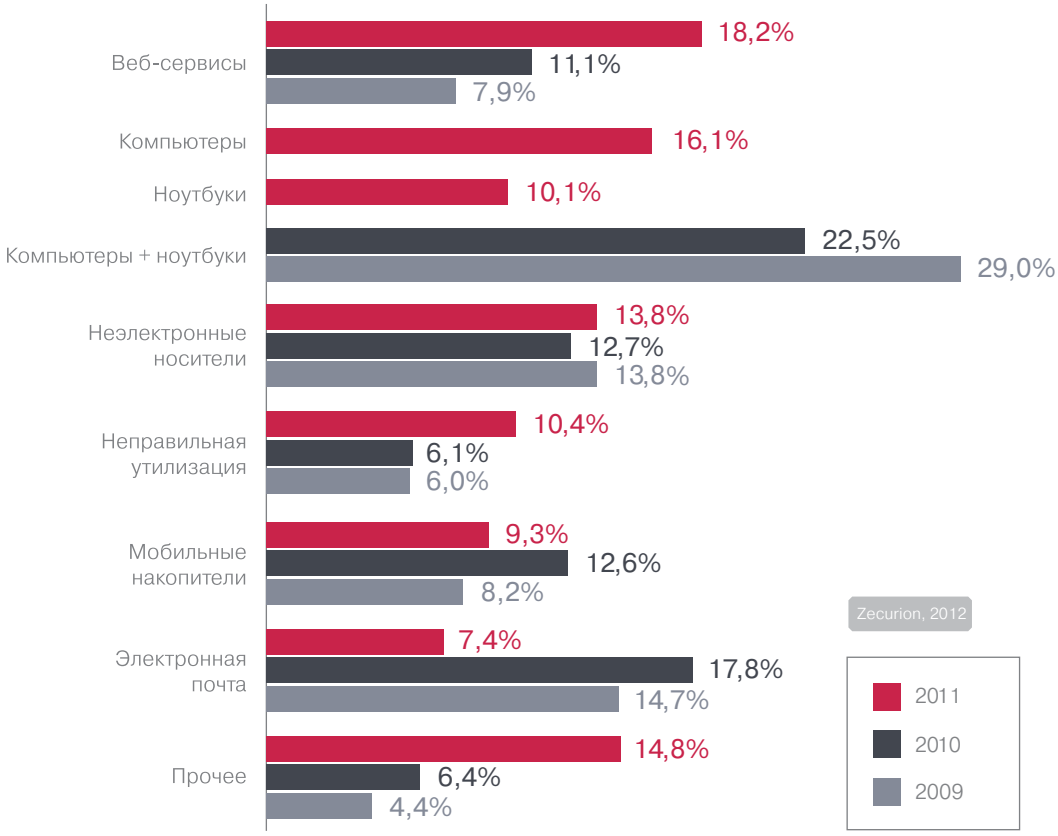
Причины утечек

Этот раздел является, пожалуй, наиболее интересным с практической точки зрения. Зная мотивацию инсайдеров и наиболее уязвимые каналы утечек (см. рис. 7), можно сосредоточить усилия на их фильтрации и предложить адекватные меры защиты. При этом следует помнить, что даже единственный открытый канал может привести к утечке информации, поэтому «лоскутные» мероприятия по безопасности могут быть оправданы только несоизмеримо высокими расходами на тотальный контроль.

В нынешнем отчете мы специально разделили категорию «компьютеры и ноутбуки» на две. С точки зрения информационной безопасности ноутбуки ближе к мобильным устройствам и носителям информации. Исходя из статистики инцидентов, наиболее частым сценарием является утеря/кража

лэптопа. Стационарные же компьютеры, хотя и хранят в большинстве случаев те же данные, что и ноутбуки, менее уязвимы перед подобными сценариями утечек и могут защищаться иными техническими средствами. Для стационарных компьютеров актуальна защита от утечек через локальные порты и по сетевым каналам. В то же время для ноутбуков, помимо этого, критически важным является шифрование.

Рисунок 7 ▶
Каналы утечки



В отдельную категорию выделены утечки, произошедшие вследствие неправильной утилизации носителей информации (10,4%). При этом физически неправильно утилизироваться могут как мобильные накопители (диски, флэшки, магнитные ленты), так и оборудование (серверы, компьютеры). В последнем случае конфиденциальная информация часто утекает при смене владельца. Виной тому отсутствие должных процедур безвозвратного удаления данных либо физического уничтожения носителей, что в некоторых случаях даже дешевле.

По-прежнему высока доля утечек через бумажные носители (13,8%). Таким образом, функция контроля печати, несомненно, будет востребована среди заказчиков DLP-систем. В то же время надо отметить, что бумажные носители гораздо чаще неправильно утилизируются. Таким образом, неправильная утилизация является сценарием одинаково губительным как для электронных носителей, так и для бумажных источников информации. В 2011 году сотрудники американской ассоциации NAID (National Association for Information Destruction) в буквальном смысле исследовали содержимое мусорных баков ряда крупнейших городов мира. Результаты шокировали. К примеру, в Лондоне конфиденциальные документы обнаружили более чем в 40% мусорных контейнеров коммерческих компаний.

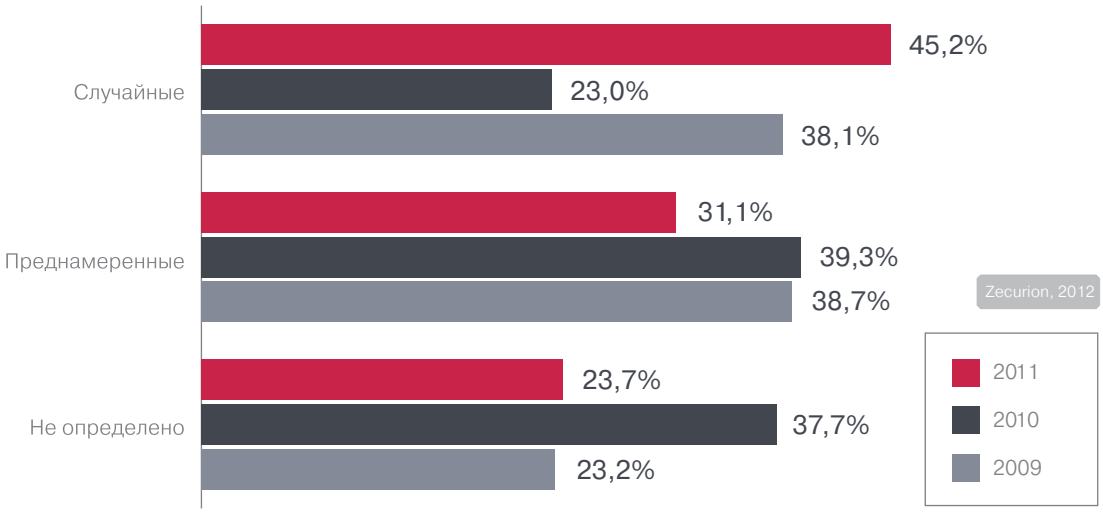
В отношении бумажных носителей также существует проблема «декласс-сификации», когда ненужные в делопроизводстве документы перестают считаться конфиденциальными. При этом бумаги могут превращаться в черновики, перемещаться между отделами компании и даже попадать к клиентам.

На протяжении последних лет стабильно растет доля веб-сервисов. Вероятно, компании сталкиваются со сложностями в соблюдении баланса защиты и удобства работы. Ограничение пользователя в правах доступа к различным ресурсам сети вполне допустимо. Нередко такая мера действительно способствует улучшению ситуации с безопасностью. В то же время многие пользователи сегодня способны обойти ограничения, найти альтернативные точки входа в социальные сети или на сайты знакомств. Поэтому более эффективной мерой следует признать контроль всего канала утечки, а не выборочный запрет на посещение ресурсов.

Из других тенденций отметим снижение доли канала «электронная почта» (7,4% в 2011 году против 17,8% в 2010 году). По мнению экспертов Zecurion, причин тому несколько. Во-первых, элекронная почта достаточно успешно фильтруется большинством продуктов класса DLP. Во-вторых, возрасла квалификация и осведомленность корпоративных пользователей. Большинство прекрасно осознает, что корпоративная переписка может не только контролироваться специализированными DLP-системами, но и часто архивироваться распространенными почтовыми серверами и просматриваться в профилактических целях или в рамках расследования инцидентов.

Относительно большая доля неопределенности (см. рис. 8) обусловлена трудностью в определении истинных причин утечек. Был ли похищен компьютер или накопитель ради «железа» или записанной на нем информации? Является ли техническая ошибка специалиста действительно случайной или преднамеренной?

Рисунок 8 ▶
Наличие умысла в утечках информации



Высокая доля случайных утечек соответствует статистике последних лет, однако, по оценкам Zecurion Analytics будет снижаться в будущем с ростом осведомленности пользователей и широким внедрением DLP-систем.

Краткие прогнозы

Прежде всего, мы прогнозируем дальнейший рост стоимости утечек. Данный тренд связан как с ростом ценности информации, так и с ужесточением законодательства в области защиты информации, прежде всего персональных данных. В январе нынешнего года Еврокомиссия предложила ряд радикальных изменений в области защиты информации. Нововведения направлены одновременно на снижение общих издержек бизнеса (предполагаемая экономия составит около $3 млрд) и ужесточение ответственности, в том числе и финансовой, за утечки данных.

Далее, мы ожидаем падение доли непреднамеренных утечек. Причин тому несколько. Во-первых, современные DLP-системы, в основу которых положены вероятностные методы, позволяют достаточно эффективно такие утечки отслеживать и блокировать. Также растет осведомленность персонала по вопросам информационной безопасности, поэтому механизмы социальной инженерии постепенно становятся менее эффективными. Наконец, внедрение средств шифрования поможет минимизировать утечки при случайной утере носителей с информацией.

Мы также надеемся на уменьшение в перспективе количества утечек из-за неправильной утилизации носителей (как электронных, так и бумажных). Проблема в данном случае носит скорее организационный характер. Поэтому ее решение не должно стать слишком обременительным для большинства компаний.

Что касается технических средств защиты, мы ожидаем рост популярности продуктов для шифрования. Данный класс решений отличают относительная простота внедрения и низкая совокупная стоимость владения. При этом решения позволяют устранить широкий пласт утечек, связанных с воровством/утерей мобильных и резервных накопителей, ноутбуков, взломом сети внешними злоумышленниками, несанкционированным доступом к информационным ресурсам и других.

Громкие российские утечки

МегаФон

В июле 2011 года произошла утечка SMS сообщений одного из крупнейших российских сотовых операторов. Сообщения тысяч абонентов мог увидеть любой пользователь поисковой системы «Яндекс». Как заявляют очевидцы, среди прочих были и сообщения достаточно откровенного содержания.

Представители оператора сотовой связи объяснили инцидент тем, что «произошел технический сбой, в результате которого в поисковую базу „Яндекса“ попало некоторое количество сообщений клиентов, отправленных через сайт „МегаФона“». Но «сбой не затронул SMS-сообщения клиентов, отправленные через телефоны и другие мобильные устройства». Со своей стороны «Яндекс» объяснил ситуацию отсутствием файла robots.txt, в котором указываются страницы, которые не должен индексировать поисковый робот системы.

В Роскомнадзоре квалифицировали данный инцидент как нарушение тайны связи компанией «МегаФон». Т. е. были нарушены условия лицензии, обязывающие сотовых операторов осуществлять деятельность в соответствии с законами и правовыми актами. По закону нарушение лицензионных условий может привести к штрафу для юридического лица в размере от 30 до 40 тыс. руб. В итоге Арбитражный суд Москвы удовлетворил иск в отношении компании «МегаФон» и оштрафовал оператора сотовой связи на 30 тысяч рублей.

МТС

Одной из самых массовых утечек в России стало появление в открытом доступе данных 1,6 млн абонентов компании МТС. Обнародованная база включала в себя персональные данные жителей Санкт-Петербурга и Башкирии.

Первым инцидент обнаружил житель Уфы Федор Пономарев. Как рассказал г-н Пономарев, он случайно увидел данные в Яндексе. При этом нашел свой номер телефона, сотовые и домашние номера своих друзей, паспортные данные. После этого возмущенный уфимец написал жалобу в Роскомнадзор. Экспертами было установлено, что в интернете оказались данные владельцев телефонных номеров с кодами 917 и 911. Среди других в базе был обнаружен номер высокопоставленного чиновника из Роскомнадзора по Башкирии. Корреспондентам «Ведомостей» чиновник пообещал разобраться в ситуации.

В МТС заявили, что утечка была незначительной, а сама база устаревшей. Тем не менее, персональные данные абонентов продолжают периодически «всплывать» на различных интернет-сайтах.

RusLeaks

Одна из самых скандальных историй минувшего года связана с проектом RusLeaks. Российские хакеры создали сеть сайтов-клонов, на которых выложили более 200 баз данных граждан РФ. В их число попали база ГИБДД, база МВД со сведениями людей, объявленных в розыск, учет ФСБ, данные о юридических лицах и индивидуальных предпринимателях, данные из системы Госзаказа, реестр владельцев недвижимости, реестр владельцев автотранспорта и др.

По информации от владельцев ресурса, на его создание их сподвигло желание избавить страну от коррупции. С их точки зрения, частную информацию необходимо обнародовать для общественного контроля. Это, впрочем, не помешало создателям продавать ключи доступа к системе.

Справедливости ради следует отметить, что базы, к которым предоставлялся доступ, могли быть приобретены или найдены в свободном доступе и ранее. Авторы проекта сделали лишь удобную оболочку для поиска.

Российские интернет-магазины

Летом 2011 года Роскомнадзор выявил около 80 интернет-магазинов, которые компрометировали персональные данные своих покупателей. В большинстве случаев утечки были связаны с неправильной настройкой видимости страниц сайтов для поисковых роботов. По итогам проведенных ведомством проверок, в прокуратуру были переданы дела только по 15 магазинам, а административные дела возбуждены в отношении еще меньшего числа нарушителей.

Тем не менее, инцидент весьма показателен. О существовании файла robots.txt узнали даже далекие от создания сайтов люди, а многие веб-разработчики и их клиенты наконец озаботились вопросами элементарной безопасности.

ВКонтакте

Осенью прошлого года участники «ВКонтакте» обнаружили, что собственный поисковой сервис социальной сети начал выдавать сканы паспортов пользователей по соответствующему запросу. Администрация сети оперативно сообщила о причинах такого поведения сервиса. Оказывается, виной всему галочка видимости «Документ доступен другим пользователям в поиске», которая по умолчания была включена. Ответственность за некорректные настройки социальная сеть возложила на своих пользователей. По мнению Владислава Цыплухина, начальника пресс-службы «ВКонтакте», именно пользователи определяют настройки видимости своих данных, а потому никакой вины соцсети в утечке нет.

Позиция пользователей основывалась на том, что большинство людей мало что понимает в настройках безопасности. После продолжительных препирательств администация «ВКонтакте» все же пошла навстречу пожеланиям общественности и в настройках по умолчанию сняла спорную галочку.

Пенсионный фонд России

Очередной жертвой поисковиков осенью 2011 года стал Пенсионный фонд России. Из-за технической ошибки на сайте Тверского отделения фонда в общий доступ попал файл с персональными данными граждан. В файле содержались ФИО, индивидуальные номера налогоплательщиков (ИНН), сведения о размере взносов в фонды обязательного медицинского страхования, страховой и накопительной частей пенсии.

Интересно, что представители Пенсионного фонда заявили, что эти сведения не классифицируются как персональные данные, сославшись на то, что в файле отсутствовали номера паспортов и другие сведения, по которым можно идентифицировать человека.

Обнаружили утечку, как водится, случайно. Один из тверичей искал в интернете сведения о себе и наткнулся на злополучный файл. После того, как «дыра» на сайте Пенсионного фонда была закрыта, данные оставались доступны в течение некоторого времени через кэш поисковых систем.

О компании Zecurion

Zecurion (www.zecurion.ru) — ведущий российский разработчик систем защиты информации от внутренних угроз. DLP-продукты Zecurion позволяют минимизировать риски умышленной и случайной утечки корпоративной информации.

Компания Zecurion более 10 лет профессионально занимается вопросами информационной безопасности. С 2001 года Zecurion является лидером в области шифрования данных, а с 2005 года разрабатывает инновационные решения для защиты от утечек информации. Среди современных продуктов, представленных на рынке DLP, решения Zecurion признаны самыми технологичными (по версии аналитического центра Anti-Malware.ru). По оценке CNews Analytics за 2011 год компания Zecurion вошла в число 30 крупнейших ИТ-компаний России в сфере защиты информации, заняв первое место среди разработчиков DLP. В 2012 году компания провела ребрендинг, прекратив использование старого названия SECURIT.

Линейка продуктов Zecurion реализует полный спектр защиты информации от инсайдеров: контроль всех потенциальных каналов утечки, ведение архива действий сотрудников, защиту данных в процессе использования и хранения, а также управление доступом пользователей к корпоративной сети, приложениям и конфиденциальной информации. Использование DLP-решений компании обеспечивает комплексную защиту информации от утечек на протяжении всего ее жизненного цикла — от создания до записи в архив или удаления. Благодаря инновационным подходам и ориентированности решений на требования бизнеса комплексные системы Zecurion на текущий момент используются более чем в 7000 организаций. Компанию Zecurion поддерживают более 100 бизнес-партнеров из различных регионов России и СНГ, стран Азии и Тихоокеанского региона, Европы и США.

ZECURION
ANALYTICS

Контактная информация

Владимир Ульянов
Руководитель аналитического центра
Zecurion Analytics

vladimir.ulyanov@zecurion.com

Алена Щеблыкина
Менеджер по связям с общественностью
Zecurion

Моб.: +7 (925) 787-06-37
alena.shcheblykina@zecurion.com

129164, Российская Федерация, Москва,
Ракетный бульвар, 16

Тел.: +7 (495) 221-21-60

www.zecurion.ru