ZECURION
ANALYTICS

Утечки конфиденциальной информации

Итоги 2013 года

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

Аннотация

Год утечек и разоблачений — таким запомнится 2013 год благодаря Эдварду Сноудену и раскрытой им информации. Тема утечек конфиденциальных данных муссировалась в СМИ насколько активно, что ею всерьёз заинтересовались все слои общества.

Оборотная сторона медали — на фоне сноуденовского шума вокруг секретных документов американского правительства утечкам данных из коммерческих организаций, реально затрагивающим большое количество людей, уделялось совсем мало внимания. Между тем, в прошедшем году произошло сразу несколько инцидентов, которые претендуют на попадание в число крупнейших.

Данный отчёт агрегирует информацию об инцидентах внутренней безопасности, произошедших в государственных учреждениях и коммерческих организациях в 2013 году и даёт целостную картину ситуации в отрасли. Отчёт адресован широкой аудитории — специалистам по защите информации, руководителям компаний, представителям отраслевых СМИ. Собранные при подготовке отчёта статистические данные могут иметь практическую ценность для специалистов, чьи профессиональные интересы лежат в области защиты информации.

Ключевые выводы

- Суммарные убытки компаний от утечек информации выросли за год почти на четверть и составили свыше $25 млрд. Виной тому — ряд крупнейших инцидентов внутренней безопасности, зарегистрированных в 2013 году.
- В среднем организации теряют $31,23 млн от каждой крупной утечки. В России убытки несколько меньше. При этом максимальные потери от одного инцидента составили около 4 млрд руб.
- Доля российских утечек в мировой статистике — 6%. Это на треть больше, чем год назад.
- Большинство фиксируемых утечек (36,9%) является следствием человеческих ошибок или халатности, но не злого умысла. Что, впрочем, не умаляет серьёзности последствий.
- Чаще всего утечки конфиденциальных данных происходят на предприятиях розничной торговли (16,2%), в медучреждениях (16%) и госсекторе (15,5%).

Методология исследования

Отсутствие кардинальных изменений в области защиты от внутренних угроз в прошедшем году позволило оставить методологию ежегодного отчёта об утечках конфиденциальной информации без изменений. Основу отчёта составляет база инцидентов информационной безопасности, собранная из открытых источников (СМИ), а также в рамках ведения проектов по защите конфиденциальных данных специалистами Zecurion.

Инциденты хронологически распределены по календарным годам. В данном отчёте приведены данные с 2011 по 2013 гг. включительно. Со статистическими данными за 2010 год и ранее можно ознакомиться из отчётов предыдущих лет (http://www.zecurion.ru/press/analytics/).

Потенциальные убытки от инцидентов рассчитываются по внутренней методике Zecurion Analytics, учитывающей тип и объём скомпрометированных данных, отраслевую специфику, особенности национального законодательства, а также реакцию на инцидент со стороны регулирующих органов, СМИ и общественности. Экспертная оценка убытков может отличаться от их реального значения как в сторону увеличения, так и в сторону уменьшения суммы. Инциденты, для которых оценочный ущерб составляет менее $5 тыс. исключаются из рассмотрения и влияния на статистические показатели не оказывают.

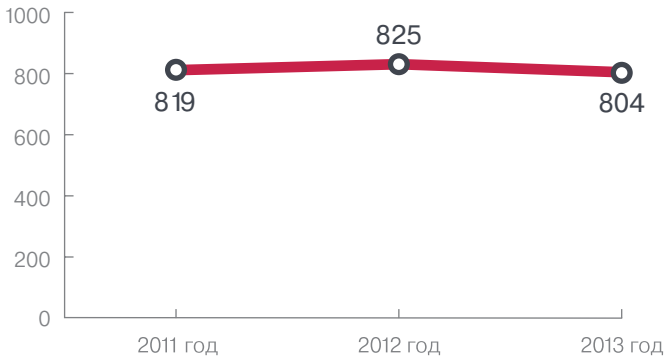
Преемственность методологии и наглядный ретроспективный анализ позволяют делать объективные выводы о нынешней ситуации и строить предположения относительно перспектив развития отрасли в будущем.

Источники утечек

Количество значимых инцидентов внутренней безопасности, зарегистрированных в 2013 году, изменилось незначительно (см. рис. 1). Тенденция к выравниванию числа инцидентов из года в год отмечалась и в предыдущих отчётах. Основная тому причина — насыщение средств массовой информации сообщениями об утечках.

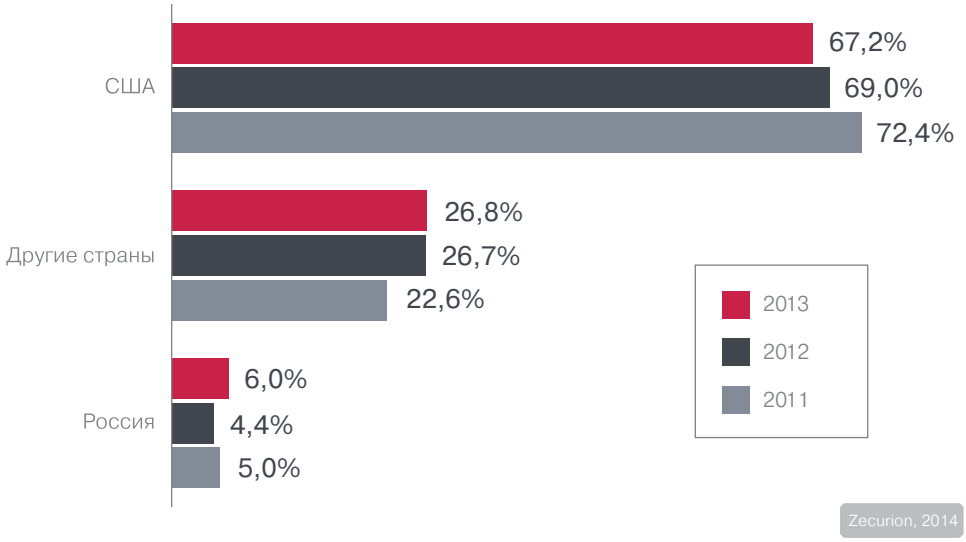
Говоря о количестве зафиксированных утечек, нельзя не отметить, что реальное количество инцидентов и в отдельных странах, и в мире в целом на порядки выше. Однако большая часть из них никогда не становится публичными, а в некоторых случаях остаётся скрытой даже от самих владельцев информации.

Рисунок 1 ▶
Количество зарегистрированных внутренних инцидентов информационной безопасности



Географическое распределение утечек (см. рис. 2) в целом соответствует прошлогоднему профилю — примерно две трети инцидентов приходятся на США. В других странах больше всего от утечек пострадали британцы и канадцы. Кроме того, не менее десятка инцидентов произошло в Индии, Австралии, Германии и Новой Зеландии.

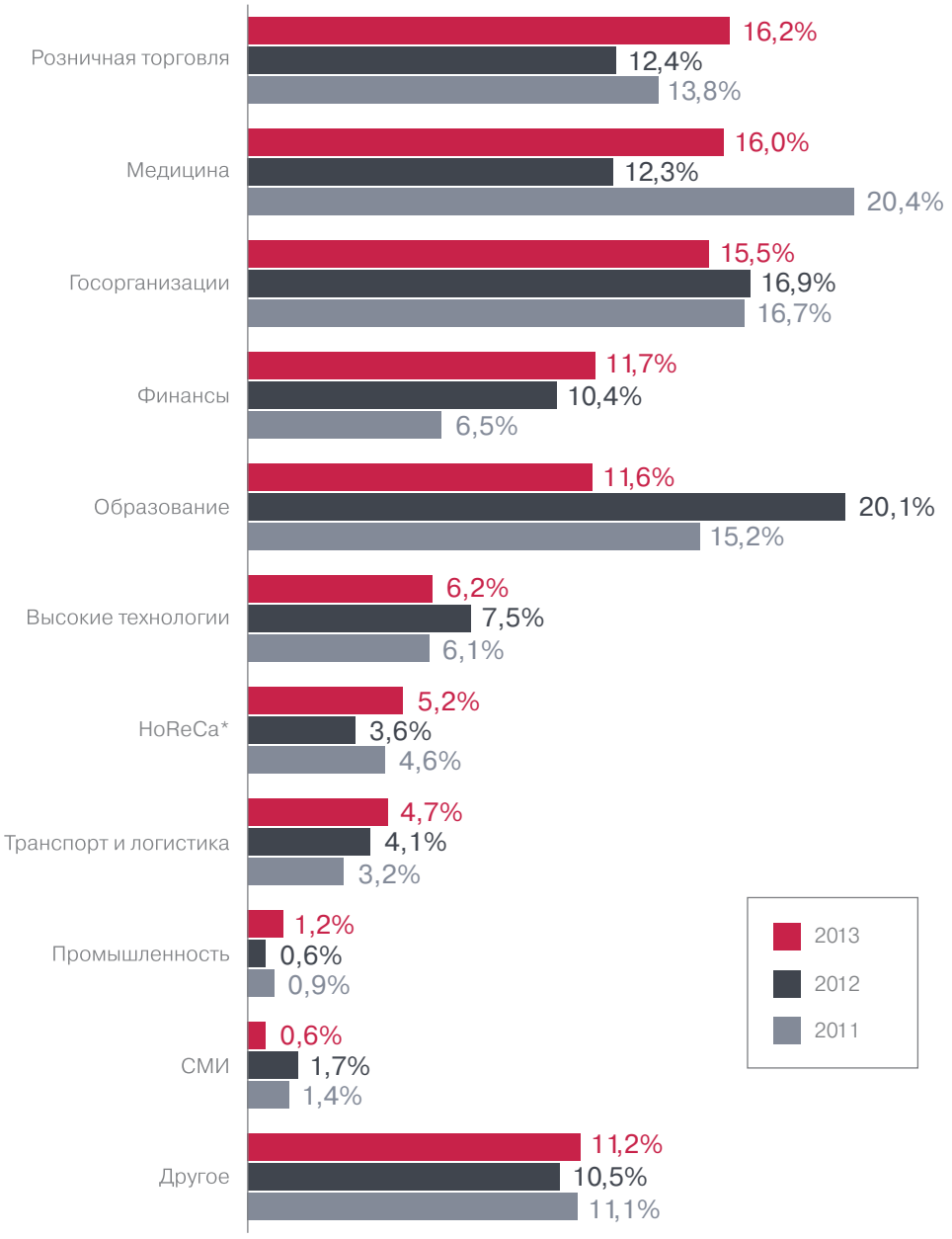
Рисунок 2 ▶
География утечек



Что касается ситуации в России, увеличилось не только количество инцидентов (48 в 2013 году), но и тяжесть их последствий. В рамках опроса руководителей служб информационной безопасности об опыте использования DLP-решений, проведённом в конце 2013 года, респонденты рассказывали даже о миллионных (в долларах США) убытках.

В прошлом году заметно изменился отраслевой профиль инцидентов (см. рис. 3). Если в 2012 году наибольшее число внутренних инцидентов произошло в сфере образования, то в 2013 году учебные заведения не вошли даже в лидирующую тройку — их доля сократилась с 20,1% до 11,6%.

Рисунок 3 ▶
Отраслевая специфика утечек



*HoReCa — Hotel, Restaurant, Cafe/Catering

Zecurion, 2014

Сразу три отрасли в 2013 году претендуют на звание ведущей по количеству утечек. Это розничная торговля (16,2%), организации здравоохранения (16%) и госучреждения (15,5%). Интересно, что госсектор в отношении защиты конфиденциальной информации является наиболее стабильным. Изменение его доли за последние годы минимально. Печальная статистика, указывающая на то, что «воз и ныне там». Между тем, во многих государственных организациях ведутся объёмные реестры и базы персональных данных граждан, доступ к которым имеет значительное число служащих. Поэтому повышаются и риски случайной компрометации данных или целенаправленного их слива.

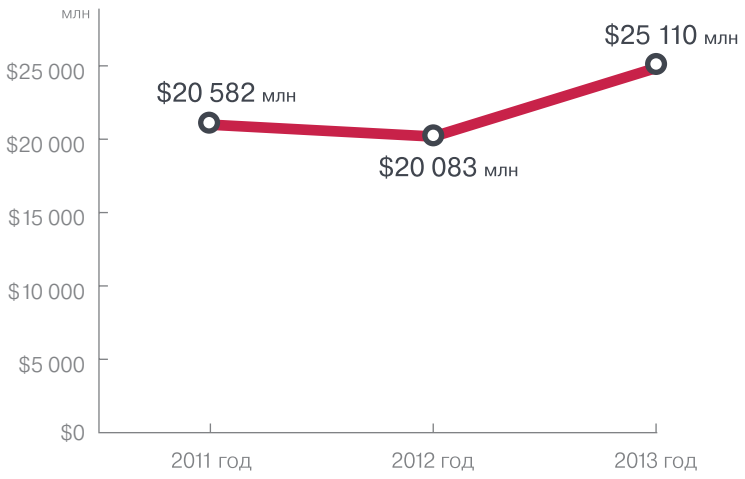
Доля утечек из высокотехнологичных компаний была бы заметно выше, если пересчитать по отраслям не количество утечек, а число затронутых людей. Виной тому — крупнейший в истории инцидент в корпорации Adobe Systems. Осенью 2013 года в интернете всплыла база данных пользователей различных сервисов Adobe. По первоначальным оценкам, в базе было менее 3 млн аккаунтов. Однако детальное изучение найденного дампа показало, что на самом деле в базе содержится свыше 150 млн записей. Даже если принять во внимание некоторое количество неактуальных или одноразовых аккаунтов, масштаб утечки впечатляет.

Кстати, одна из главных проблем в данном случае заключается не только, и не столько в том, что злоумышленники смогут авторизоваться на сайте Adobe под чужим именем, а в том, что пользователи часто используют одно и то же сочетание логина (или адреса электронной почты) и пароля для доступа к различным системам и сервисам. А здесь уже открывается широкое поле для махинаций. Возможные последствия для пользователей варьируются от прямых денежных убытков при использовании сетевых финансовых сервисов и служб удалённого банковского обслуживания до банального вымогательства за возврат аккаунтов в социальных сетях и прочих сервисах. При этом продажа электронных адресов спамерам выглядит одним из самых безобидных вариантов.

Последствия утечек

Финансовая оценка последствий внутренних инцидентов информационной безопасности является для специалистов вопросом актуальным, но в то же время нетривиальным. Даже скрупулёзное расследование и тщательная обработка инцидента не всегда дают полную картину, особую сложность представляет оценка упущенной выгоды. Тем не менее, конкретные цифры убытка, пусть даже ориентировочные, необходимы в ежедневной работе для анализа рисков и обоснования использования тех или иных мер защиты информации.

Рисунок 4 ▶
Убытки от утечек информации



Общие убытки от утечек информации в мире в 2013 году составил рекордные $25,11 млрд. Это самое большое значение за всё время ведения статистики. Благодаря ряду крупных утечек, от которых пострадало большое количество людей, за год убытки выросли ровно на четверть. Средний убы-

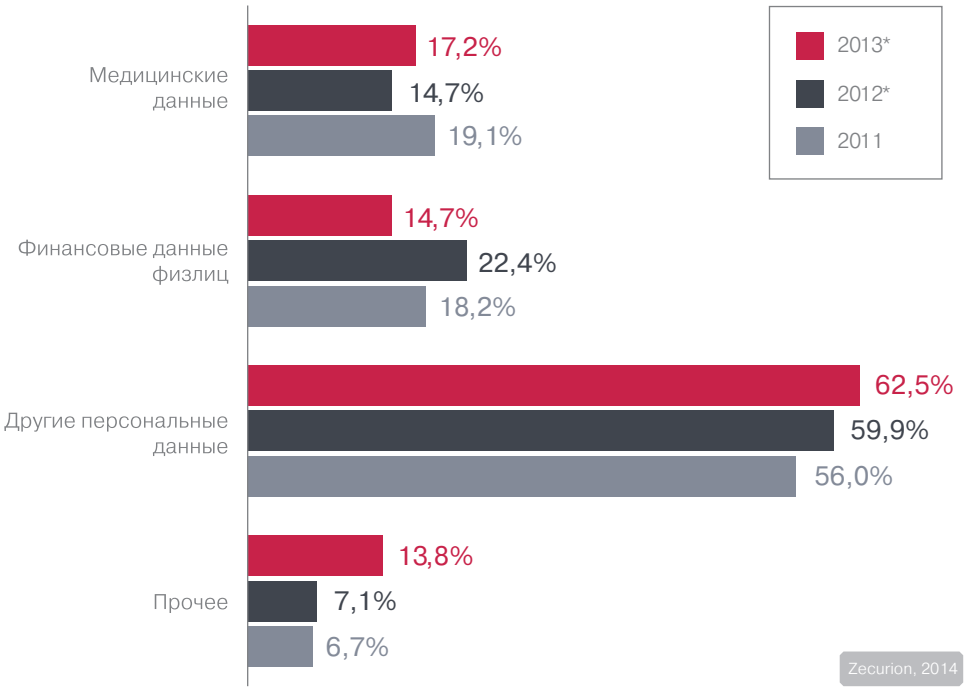
ток за прошедший год вырос ещё значительнее и составил $31,23 млн. Т. е. каждый внутренний инцидент в среднем отнимал у владельца информации примерно 1 млрд руб.

В наиболее «дорогих» инцидентах нередко оказываются замешанными топ-менеджеры компаний. Так, летом 2013 года полиция Тайваня задержала трёх топ-менеджеров корпорации HTC, связанных с разработкой продуктов. Одно из выдвинутых обвинений — передача конфиденциальной информации по перспективным разработкам конкурирующим фирмам. При этом не лишним будет напомнить, что на протяжении долгого времени дела HTC идут не самым лучшим образом, финансовые показатели ухудшаются, а в 3 квартале 2013 года компания зафиксировала чистый убыток около $100 млн. Использование служебного положения — типичный кейс для целенаправленных утечек.

В оценку финансовых потерь, приведённую на рис. 4, не включены последствия сноуденовских разоблачений. Между тем, по разным оценкам убытки США от утечки информации через бывшего сотрудника спецслужб составляют до нескольких десятков миллиардов долларов.

Последствия утечки информации сильно зависят от типа данных, которые утекают (см. рис. 5). Среди «прочих» данных чаще всего оказываются скомпрометированными учётные записи пользователей различных web-сервисов и информационных систем. Гораздо реже встречаются утечки государственной или коммерческой тайны, интеллектуальной собственности. Хотя происходят они регулярно, сведения о подобных инцидентах попадают к журналистам редко. Пример Эдварда Сноудена с его 1,7 млн секретных документов — скорее исключение.

Рисунок 5 ▶
Какие данные утекают



Впрочем, время от времени подобные нестандартные инциденты просачиваются в прессу. Один из примеров — утечка тактических схем футбольного клуба «Бавария» перед матчем 13-го тура бундеслиги с принципиальным соперником, «Боруссией» из Дортмунда. Подробный план на предстоящую игру был опубликован журналом Bild за несколько дней до матча. Однако

* Сумма долей утечек превышает 100%, поскольку в некоторых случаях информация классифицировалась по нескольким категориям одновременно.

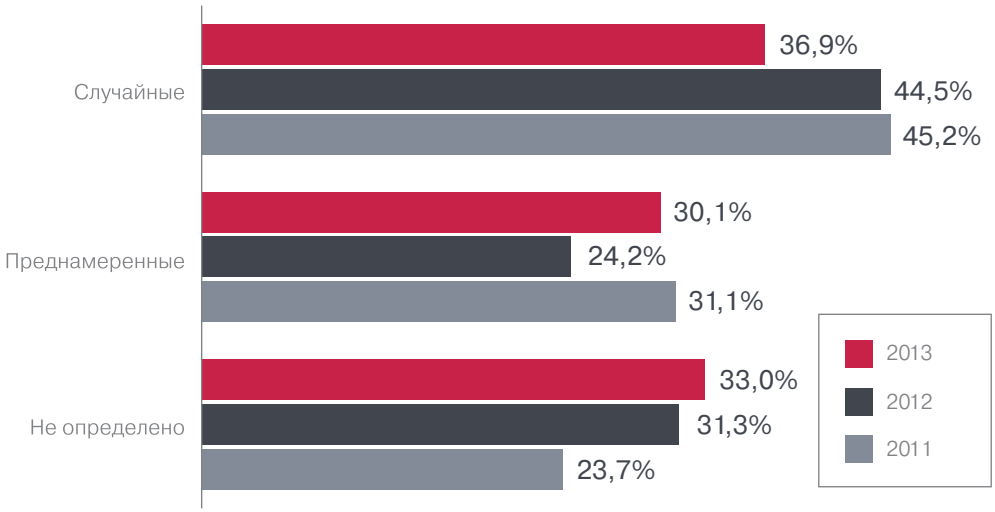
футболистам «Боруссии» информация не помогла — «Бавария» разгромила соперника со счётом 3:0, а игроки и работники клуба заявили, что инцидент не повлияет на атмосферу внутри команды. Действительно ли можно нормально относиться к существованию инсайдера в коллективе — большой вопрос, однако на спортивных достижениях баварцев инцидент действительно не отразился.

Приведённый выше пример доказывает, что существуют утечки, предотвратить которые обычными техническими средствами невозможно. Сколь бы совершенными ни были средства контроля информации, всегда существует возможность запомнить часть сведений в голове. Поэтому наравне с техническими средствами нельзя забывать и об организационных моментах.

Причины утечек

Несмотря на то, что в конфиденциальной информации всегда кто-то заинтересован (иначе конфиденциальной она и не являлась бы), большинство инцидентов, учитываемых в нашей статистической базе, происходит без злого умысла, по воле случая или из-за халатности людей. Эта тенденция сохраняется на протяжении уже многих лет. Отчасти она объясняется используемой методологией — ведь в базу утечек попадают случаи, о которых стало известно публично. А когда речь идёт о целенаправленном инсайде, воровстве данных засланным или подкупленным сотрудником, участники заинтересованы в сохранении конфиденциальности, и раскрыть утечку может разве что владелец информации, если вовремя её диагностирует.

Рисунок 6 ▶
Наличие умысла в утечках информации

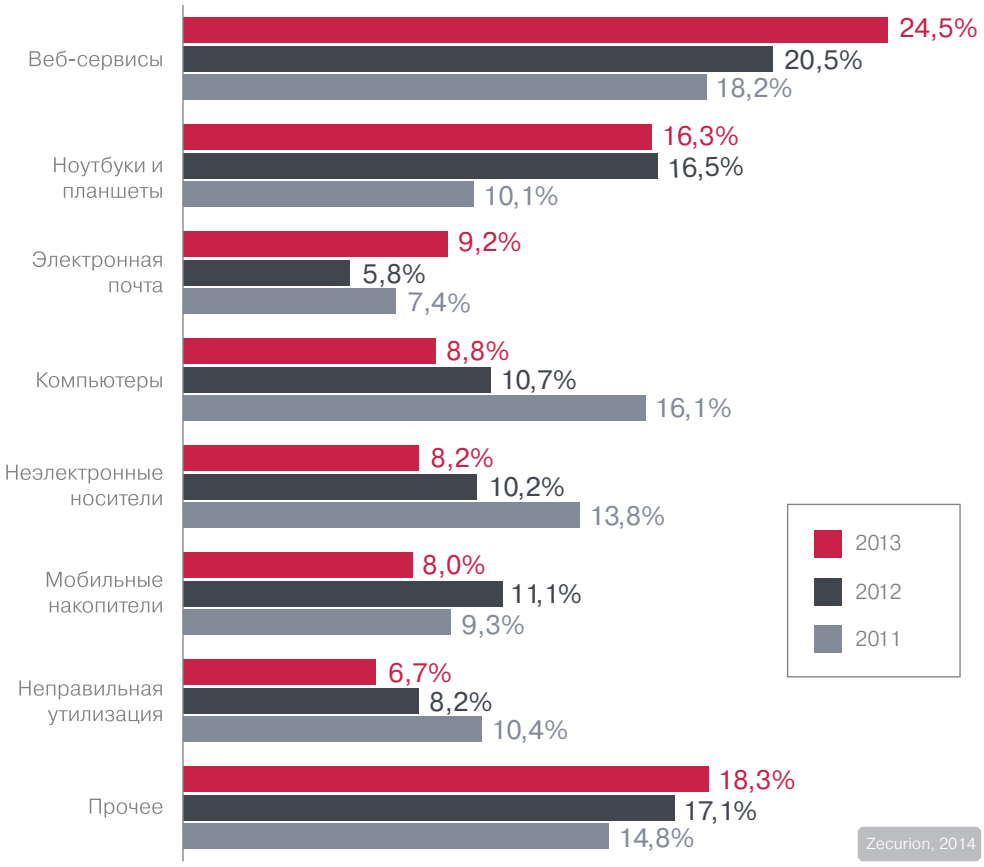


Zecurion, 2014

Тем не менее, в 2013 году доли случайных и преднамеренных утечек выровнялись (см. рис. 6). Существуют также инциденты, для которых определить умысел сложно. В тех ситуациях, когда к утечке одновременно привели и преднамеренные действия сторонних лиц, и халатность собственных сотрудников (например, случаи социальной инженерии), это классифицировалось как умышленный инцидент. Большое число целенаправленных утечек указывает на то, что компании недостаточно внимания уделяют защите информации, даже не смотря на существенные финансовые потери от утечек (см. предыдущую главу).

Статистика утечек по различным каналам приведена на рис. 7. Расклад аналогичен прошлому году. Единственное заметное изменение — более чем полуторакратный рост числа утечек через электронную почту. В отчётах об утечках прошлых лет отмечалось, что почта хорошо контролируется автоматизированными техническими средствами, в том числе DLP-системами. Однако уровень проникновения DLP-систем по-прежнему остаётся на низком уровне (для России этот показатель в конце 2012 года составлял 20% в организациях среднего и крупного бизнеса — см. отчёт «Внутренняя безопасность в регионах России и странах СНГ 2013» http://www.zecurion.ru/press/analytics/).

Рисунок 7 ▶
Каналы утечки



Несмотря на давно наступивший цифровой век, экстравагантные сегодня носители информации представляют сложность не только для ИТ-специалистов, вынужденных обеспечивать их поддержку или конвертировать в современные форматы хранения данных, но и для специалистов по информационной безопасности. Даже отслужив свой срок, такие носители создают проблемы. Летом 2013 года в США к утечке данных почти 300 тыс. человек привела некорректная утилизация микрофиш. Интересно, что микрофиши были переданы компании, специализирующейся на уничтожении различных нецифровых носителей информации. Случаи, когда виновниками утечек становятся подрядчики, к сожалению, остаются достаточно распространёнными.

Краткие прогнозы и выводы

В отчётах прошлых лет прогнозировался рост убытков от утечек, что объяснялось в том числе планируемыми изменениями в законодательстве не только отдельных стран, но и Евросоюза. Прогноз оказался точным, в 2013 году организации потеряли от утечек на 25% больше, чем в прошлом году.

При этом в силу естественных сложностей, а также инертности и забюрократизированности процесса законотворчества, новые нормативные документы до сих пор ещё не приняты либо не вступили в силу. Таким образом некоторый резерв увеличения убытков в отрасли сохраняется. Вообще, штрафные санкции составляют одну из небольших статей потерь компаний в инцидентах информационной безопасности, однако в некоторых случаях речь идёт о значительных суммах. Так, финансовая компания Citigroup прошедшей осенью заплатила 30-миллионный штраф за утечку коммерческой информации. Аналитик Citigroup за день до официальной публикации выслал конфиденциальный отчёт о деятельности одного из поставщиков Apple нескольким крупным клиентам. В результате избранные компании могли избавиться от акций Apple до значительного снижения их котировок.

Подтвердился и тренд к снижению количества утечек вследствие неправильной утилизации носителей информации. В данном случае проблема носит прежде всего организационный характер, и может быть решена с минимальными финансовыми затратами. Правда, как мы уже могли убедиться, искоренить её вовсе пока не получилось.

Широкое внедрение средств шифрования данных, популярность которых отмечалась в прошлогоднем отчёте, позволило снизить количество случайных и халатных утечек, а также утечек через мобильные накопители. Обратная сторона улучшения статистики — увеличение числа преднамеренных краж информации, приносящих, обычно, заметно большие убытки.

Если говорить о перспективах, стоит готовиться к увеличению краж инсайдерской информации из банков. Мошеннические схемы, связанные с эмиссией и эквайрингом пластиковых карт, а также удалённым банковским обслуживанием, оказываются чрезвычайно эффективными. Они позволяют злоумышленникам быстро монетизировать полученную информацию, а цепочки исполнителей, каждый из которых выполняет свою достаточно узкую функцию — замести следы и минимизировать собственные риски, когда несанкционированные списания со своих счетов обнаружат клиенты банков.

Вообще, возможности инсайдеров, в плане получения конфиденциальной информации намного превосходят возможности внешних злоумышленников, использующих программы-шпионы или взламывающие сети и ИТ-системы. Взлом не только труднее осуществить, но и легче обнаружить его следы специалистам по информационной безопасности. А шпионское ПО имеет ограниченный радиус действия, т. к. его внедрение в изолированные сегменты сети в большинстве случаев всё равно требует привлечения человека-инсайдера, имеющего доступ к закрытым ресурсам.

Громкие российские утечки*

Mail.ru

В начале января 2013 года выяснилось, что все файлы, которыми обмениваются пользователи сервиса ICQ, принадлежащего Mail.ru Group, фактически находятся в открытом доступе. Виной тому — новая схема передачи файлов, введённая разработчиками после приобретения сервиса у AOL. Если раньше файлы передавались напрямую от пользователя к пользователю, то теперь файл сохранялся на сервере Mail.ru, а получателю отправлялась лишь ссылка для скачивания. При этом скачать файл по прямой ссылке мог кто угодно, никаких дополнительных проверок получателя не проводилось.

Сами ссылки имели определённый вид и отличались 6-значным кодом. Соответственно задача получения файлов свелась к перебору этих кодов в известном диапазоне. Одновременно с новостью в интернете появился и простейший скрипт для автоматизированной генерации ссылок и скачивания файлов. Пользователи наперебой начали выкладывать коллекции заинтересовавших их файлов.

Особенной популярность пользовались фотографии интимного характера. Однако среди прочего встречалась и легче монетизируемая информация, в том числе тексты договоров, сканы паспортов и других документов.

МТС

Ещё одна январская утечка, благодаря которой пользователи узнали интригующие подробности взаимоотношения сотрудников сотового оператора с контент-провайдерами. Вкратце, речь шла о возможном прикрытии и санкциях к нечистоплотным провайдерам, использующим вредоносное ПО для неправомерного списывания денег со счетов абонентов, подменяющих посадочные страницы, скрывающих стоимость услуг и т. д. Какие решения принимались в каждом из случаев можно узнать из переписки, доступной в интернете. Наиболее интересные места блоггеры широко растиражировали.

Кто выложил переписку в открытый доступ и зачем это сделал — не ясно. Хотя ограничения в области информационной безопасности, накладываемые на сотрудников МТС, тем слабее, чем выше должность. В частности, некоторые сотрудники используют личную почту (публичные почтовые сервисы вроде Gmail или Mail.ru) для переписки по рабочим вопросам. А ведь защищённость подобных сервисов вызывает множество вопросов, не говоря уж о возможном контроле со стороны иностранных спецслужб.

Помимо переписки, касающейся сомнительного для пользователей контента, в почтовом архиве было обнаружено немало другой чувствительной к утечке информации. Заинтересованные лица этой информацией, скорее всего, воспользовались, но широкую публику коммерчески важные документы оператора не впечатлили.

* Только публично известные. Информация об инцидентах, ставших известными в рамках ведения проектной деятельности специалистами Zecurion, по соглашению с заказчиками не разглашается.

Сбербанк

Конфиденциальные бумажные документы, выброшенные в обычный мусорный бак — распространённый случай утечки в других странах, однако нечасто на такие «мелочи» обращают внимание в России. Весной прошлого года, наконец, обратили. Жители Зеленограда обеспокоились, когда увидели банковские документы, раздуваемые ветром по дворам. Как выяснилось, документы пропали из ближайшего отделения Сбербанка — уборщица высыпала толстые стопки ненужных бумаг в обычный мусорный бак, а поднявшийся ветер разнёс их по округе.

Среди утилизированных бумаг оказались заявления клиентов на выпуск пластиковых карт, заполненные анкеты, подписанные договоры банковского обслуживания, выписки и прочие документы, которые можно классифицировать как банковскую тайну и персональные данные. По сведениям пресс-службы кредитной организации, «Сбербанк» отстранил заведующую отделением и её заместителя от занимаемых должностей и инициировал служебное расследование, о результатах которого позднее не сообщалось.

Страховая компания «Цюрих»

Впечатляющая утечка информации, случившаяся в первой половине 2013 года, угрожала страховой компании многомиллионными убытками. В руки неизвестных злоумышленников попала база данных более чем 1 млн человек — клиентов СК «Цюрих». При этом база была исключительно актуальной и включала сведения обо всех клиентах, заключавших договоры с января 2012 по февраль 2013 года.

Самостоятельно найти источник утечки и устранить её последствия в компании не смогли и обратились за помощью в правоохранительные органы. По одной из версий, базу скопировал уволившийся сотрудник. Установлено, что новые владельцы базы искали на неё покупателя. О случаях продажи базы точных сведений нет, и убытки страховщиков можно посчитать, лишь зная процент аномального оттока клиентов. При этом следует иметь в виду, что негативный эффект от утечки может ощущаться на протяжении нескольких лет.

ФосАгро

Бывший начальник отдела продаж одного из крупнейших в мире производителей минеральных удобрений нанёс убытки своему работодателю на сумму более $2 млн. Доказательства вины и убытков были получены в рамках расследования уголовного дела московской прокуратурой. Кстати, дело стало одним из первых в уголовно-судебной практике по защите коммерческой тайны организаций.

Пользуясь служебным положением, сотрудник передавал конфиденциальную информацию заинтересованным иностранным компаниями, в том числе прямым конкурентам холдинга. Среди информации, которую передавал инсайдер, данные об объёмах производства некоторых материалов, условия продажи продуктов, цены, сведения о взаимоотношениях с клиентами и т. д.

Необходимо также отметить, что бывший сотрудник сливал информацию в течение двух лет, что указывает на слабость или даже отсутствие мер защиты информации в крупной коммерческой организации. При таких условиях в компании вполне могут быть и другие нечистоплотные работники, а поимку единичного инсайдера стоит расценивать как случайность.

О компании Zecurion

Zecurion (www.zecurion.ru) — крупнейший 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). В рейтинге CNews Analytics компания Zecurion уверенно удерживает первое место среди разработчиков DLP с 2011 года и входит в число 30 крупнейших ИТ-компаний России в сфере защиты информации. 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 её жизненного цикла — от создания до записи в архив или удаления. Благодаря инновационным подходам и ориентированности решений на требования бизнеса комплексные системы Zecurion используются более чем в 7000 организаций. Компанию Zecurion поддерживают более 100 бизнес-партнёров из различных регионов России и СНГ, стран Азии и Тихоокеанского региона, Европы и США.

ZECURION
ANALYTICS

Контактная информация

Владимир Ульянов
Руководитель аналитического центра Zecurion

Телефон: +7 909 691-22-12
analytics@zecurion.com

Ксения Головко
Заместитель руководителя пресс-службы

Телефон: +7 967 091-65-50
pr@zecurion.com

129164, Российская Федерация, Москва,
Ракетный бульвар, 16

Телефон/факс: +7 495 221-21-60
www.zecurion.ru