ZECURION
ANALYTICS

Утечки конфиденциальной информации

'12

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

Аннотация

Аналитический центр Zecurion Analytics представляет результаты очередного ежегодного исследования утечек конфиденциальной информации за 2012 год. Несмотря на постепенное ужесточение нормативного прессинга и грядущее увеличение штрафных санкций за утечки информации, ситуация в области защиты от внутренних угроз практически не меняется в лучшую сторону. Количество утечек по-прежнему высоко, что указывает на относительную слабость используемых компаниями средств защиты и недостаток внимания к проблеме со стороны топ-менеджмента. Мы также не можем сказать, что проблема утечек информации стала острее. Но лишь потому, что она и так стоит чрезвычайно остро. Существенные финансовые и репутационные потери от инцидентов внутренней безопасности оказывают ощутимое влияние на бизнес даже крупных компаний.

Данный отчёт предназначен для широкого круга заинтересованных лиц, специалистов в области защиты информации, руководителей компаний, представителей СМИ. Собранные в отчёте статистические данные могут быть полезны с практической точки зрения в ежедневной работе специалистов по информационной безопасности.

Ключевые выводы

- Ущерб от утечек конфиденциальной информации в 2012 году остался примерно на уровне прошлого года и составил $20,083 млрд. Средний ущерб от каждого инцидента — $24,34 млн.
- На долю России пришлось 4,4% от мирового количества зарегистрированных внутренних инцидентов информационной безопасности. Эта цифра могла быть ещё выше, если учесть инциденты с незначительным потенциальным ущербом.
- Планируемое в 2013 году ужесточение штрафных санкций за разглашение персональных данных в России и Евросоюзе приведёт к серьёзному увеличению финансового ущерба от утечек.
- Злоумышленники эффективно используют имеющуюся в их распоряжении информацию, утечка персональных данных даже одного человека может привести к серьёзным убыткам.
- Чаще всего информация утекает из образовательных заведений (20,1%), госсектора (16,9%), предприятий розничной и интернет-торговли (12,4%) и медучреждений (12,3%).
- Наиболее распространённые каналы утечек — это веб-сервисы (20,5%), ноутбуки и планшеты (16,5%), а также мобильные накопители (11,1%).

Методология исследования

При подготовке отчёта использовалась методология, максимально близкая к прошлогодней, что позволяет корректно выявлять актуальные тенденции в области внутренних угроз. Основу базы инцидентов информационной безопасности составляют сообщения из открытых источников, а также сведения об утечках, ставшие известными специалистам Zecurion в рамках ведения проектной деятельности. В данный отчёт попали описания инцидентов за 2012 календарный год, а также статистика прошлых лет для выявления тенденций в области внутренних угроз. Согласно действующей методике, в базу инцидентов не попадают атаки, реализованные исключительно внешними злоумышленниками без какого-либо содействия со стороны инсайдеров. Кроме того, в статистике не отражены инциденты, для которых потенциальный ущерб составляет менее $5 тыс.

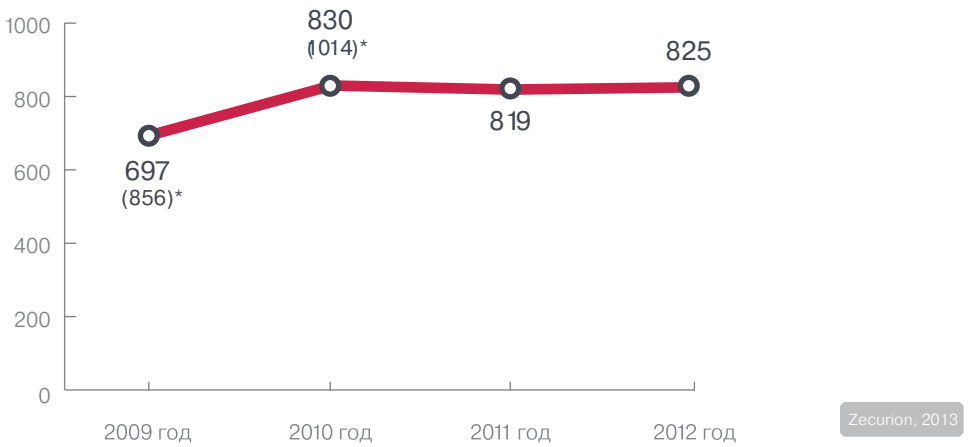
Потенциальный ущерб инцидентов рассчитывается по внутренней методике Zecurion Analytics, учитывающей тип и объём скомпрометированных данных, отраслевую специфику, особенности национального законодательства, а также реакцию на инцидент со стороны регулирующих органов, СМИ и общественности. Экспертная оценка ущерба может отличаться от реального значения ущерба как в сторону увеличения, так и в сторону уменьшения суммы.

Единственное существенное изменение по сравнению с прошлым годом касается порядка учёта типа скомпрометированной информации. Если раньше инцидент классифицировался только по одной из категорий, то теперь может попасть в несколько категорий одновременно. Согласно актуальной методике, учитывается наиболее критичный тип данных из утекшего информационного массива, если это можно определить. К примеру, если из организации утекает база данных, в которой хранятся номера кредитных карт, а также имена клиентов, их даты рождения и домашние адреса, утекшая информация классифицируется как утечка финансовых данных. Другой пример, если из учреждения утекает информация о состоянии здоровья граждан, а также номера их кредитных карт, инцидент учитывается в категориях «финансовые данные» и «медицинские данные» одновременно.

Источники утечек

При взгляде на динамику изменения числа утечек информации за последние годы можно отметить определённую стагнацию (см. рис. 1). За три года с 2010 по 2012 изменения укладываются в ничтожный двухпроцентный интервал. Объяснить данную ситуацию можно двумя обстоятельствами. Во-первых, существует некий порог «пресыщения» СМИ сообщениями об утечках (напомним, для сбора данных мы используем открытые источники, прежде всего, электронные СМИ). Во-вторых, в последние годы наблюдается тенденция раскрытия небольших по масштабу утечек информации. Подобные сообщения часто встречаются в блогосфере и региональных СМИ. Если по экспертной оценке ущерб от таких инцидентов незначителен (см. раздел «Методология исследования»), они не попадают в итоговый отчёт.

Рисунок 1 ▶
Количество зарегистрированных внутренних инцидентов информационной безопасности



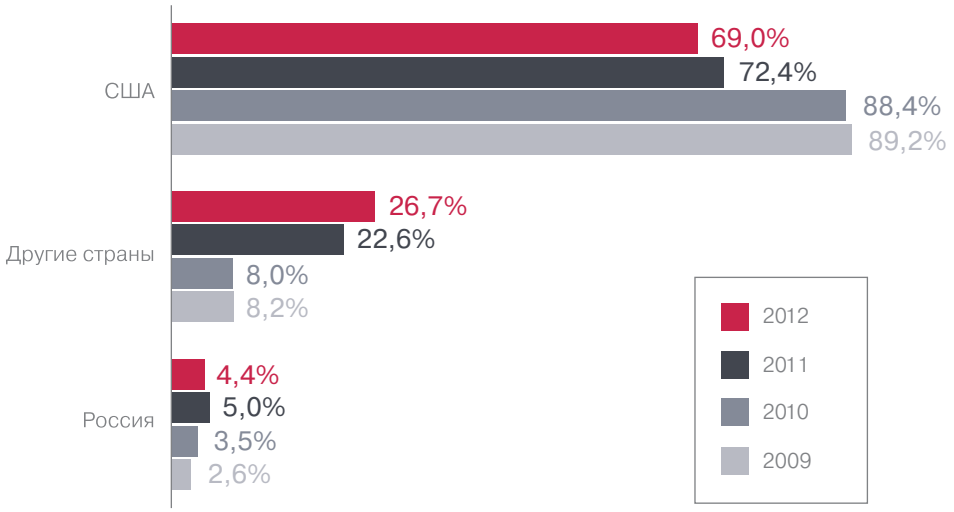
Необходимо также отметить, что приведённые выше цифры не являются абсолютными значениями количества утечек информации в мире. Учтены только инциденты, ставшие публичными. А таких, по оценкам Zecurion Analytics, не более 0,1% от общего их числа. Тем не менее, собранная статистическая база позволяет определять актуальные тенденции в области внутренних угроз.

Доля утечек из США (69% от общего числа) продолжает постепенно снижаться, хотя и не так радикально как в прошлые годы (см. рис. 2). В отношении географии утечек следует выделить ряд нюансов, которые не могут быть отражены одной цифрой. Мы наблюдаем серьёзный рост числа сообщений об инцидентах из стран, ранее появлявшихся в новостных лентах об утечках лишь эпизодически либо вообще не фигурировавших. Это объясняется не только повышением внимания к утечкам в указанных странах, но и более широким охватом СМИ и появлением сообщений об утечках в англоязычном интернете. Тем не менее, значительное число подобных инцидентов по-прежнему не попадает в рамки нашего годового отчёта из-за низкого потенциального ущерба. В противном случае доля США была бы ещё меньше.

Среди особенностей «национального инсайда» США следует отметить значительный удельный масштаб инцидентов. В США регистрируется много инцидентов, связанных с утечкой персональных данных большого числа людей. А в силу действующего законодательства и сложившейся практики реагирования на инциденты, это чревато внушительными потерями, не только потенциальными, но и фактическими.

* Данные за 2009 и 2010 годы были скорректированы в соответствии с актуальной методологией исследования. В скобках на графике приведены неадаптированные (по старой методике) цифры.

Рисунок 2 ▶
География утечек



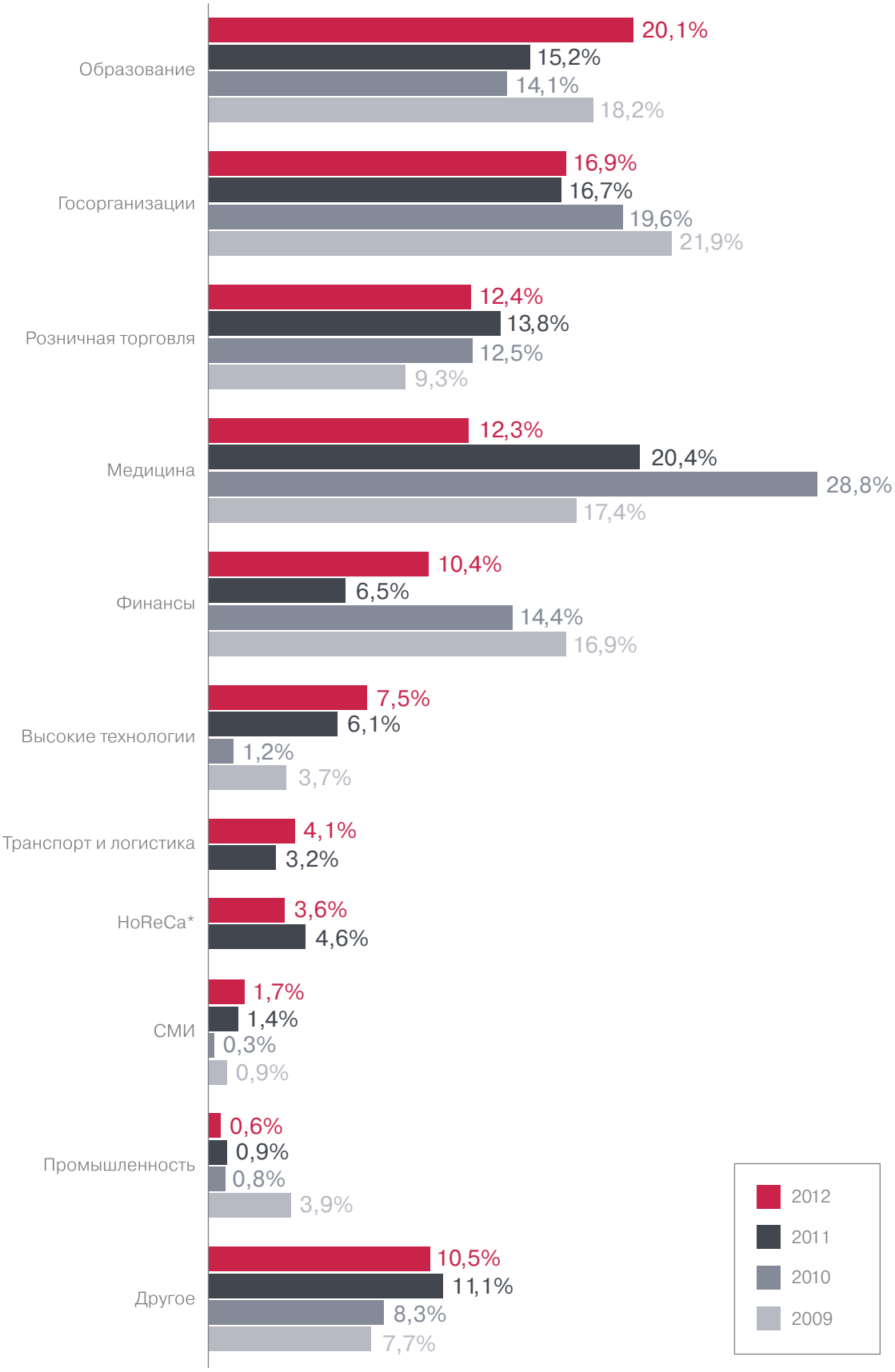
Zecurion, 2013

Число российских утечек с ощутимым потенциальным ущербом осталось примерно на уровне прошлого года (36 в 2012 году против 41 в 2011 году). Наиболее громкие из российских утечек информации будут подробнее рассмотрены в одном из следующих разделов. В категории «другие страны» существенные доли имеют Великобритания, Канада, Австралия, Индия.

Существенно поменялся отраслевой профиль утечек (см. рис. 3). Если в прошлом году больше всего утечек было зарегистрировано в отрасли здравоохранения, то по итогам 2012 года медучреждения оказались лишь четвёртыми после учебных заведений (20,1%), госорганизаций (16,9%) и предприятий розничной (в том числе через интернет) торговли (12,4%). В прошлом году мы отмечали одновременно большую долю «медицинских» утечек и высокую стоимость сведений, утекающих из поликлиник и больниц. Двух этих факторов вполне достаточно, чтобы сосредоточить самое пристальное внимание на защите информации в медучреждениях. Тем не менее, объяснять столь существенное сокращение доли только решительными мерами по укреплению безопасности было бы неправильно — ситуация вряд ли могла измениться столь кардинально за короткий промежуток времени. К тому же вновь повысилась (до 10,4%) доля утечек из организаций финансового сектора, хотя банки и страховые компании также обладают большими объёмами критичной внутренней информацией, а санкции регуляторов в финансовом секторе могут быть достаточно суровыми.

Доля утечек в госсекторе на протяжении нескольких лет находится на стабильно высоком уровне. Поэтому в очередной раз нельзя не отметить низкую заинтересованность в защите информации и, прежде всего, персональных данных. Убытки, связанные с ущербом репутации и потерей конкурентоспособности, для частных компаний гораздо выше, нежели для госучреждений, для которых само понятие «конкурентоспособность» в некоторых случаях просто неприменимо. Если сюда прибавить большие объёмы обрабатываемой информации и не всегда высокий уровень подготовки служащих, объяснение высокой доли госутечек можно считать законченным.

Рисунок 3 ▶
Отраслевая специфика утечек



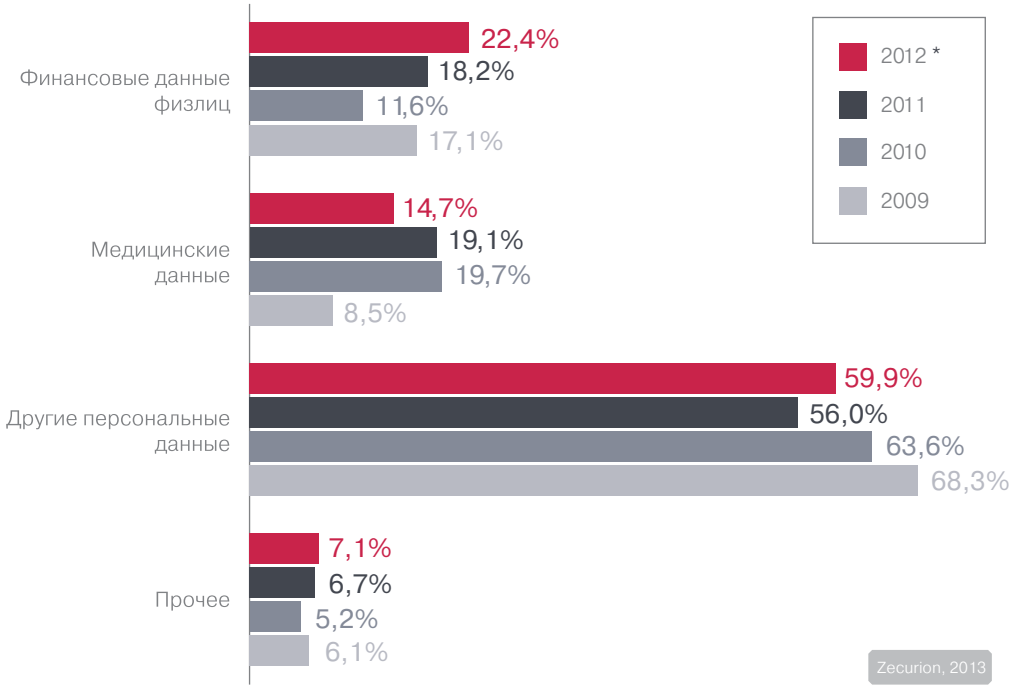
*HoReCa — Hotel, Restaurant, Cafe/Catering

Zecurion, 2013

Последствия утечек

Уменьшение числа утечек из медучреждений естественным образом сказалось и на уменьшении объёма скомпрометированных медицинских данных. Несмотря на прямую закономерность, необходимо всё же отметить, что не каждый инцидент информационной безопасности в сфере здравоохранения приводит к утечке медицинских данных. Нередко из больниц пропадает информация, не связанная с состоянием здоровья пациентов или медицинским обслуживанием. Верна и обратная логика. К примеру, сведения о здоровье граждан или номера полисов медицинского страхования могут утекать из госучреждений, органов социальной опеки и т. д. На рис. 4. приведены данные о характере скомпрометированной информации в 2012 году.

Рисунок 4 ▶
Какие данные утекают



Сведения об утечках других типов информации (коммерческой тайны, интеллектуальной собственности и пр.) встречаются реже. Периодически СМИ сообщают даже о случаях раскрытия гостайны, обнаружении документов с грифами секретности. Но далеко не всегда можно оценить ущерб таких утечек и понять, представляет ли загрифованная информация какую-то ценность вообще или нет. Кстати, по нашим наблюдениям, подобные утечки гостайны случаются не только и не столько по злому умыслу или на заказ (такие случаи вообще крайне редко становятся достоянием гласности), сколько из-за халатности.

Утечки коммерчески важной информации обычно происходят при увольнении сотрудников и особенно при переходах между конкурирующими компаниями. В прошлом году мы получили немало иллюстраций подобных утечек. Например, несколько топ-менеджеров AMD, включая вице-президента Роберта Фельдштейна, при переходе летом 2012 года в конкурирующую корпорацию Nvidia скопировали порядка 100 тыс. документов, содержащих конфиденциальные сведения о продуктах компании и соглашениях с партнёрами. На момент подготовки отчёта AMD подала судебный иск, однако судьба разбирательства ещё не была ясна.

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

Прежде чем перейти к оценке ущерба от утечек информации, скажем несколько слов о возможных негативных последствиях. Считается, что монетизировать (т. е. превратить в деньги) большинство типов персональных данных невозможно. Вследствие чего даже появляются призывы к максимальной публичной открытости и прекращению утаивания этой самой информации.

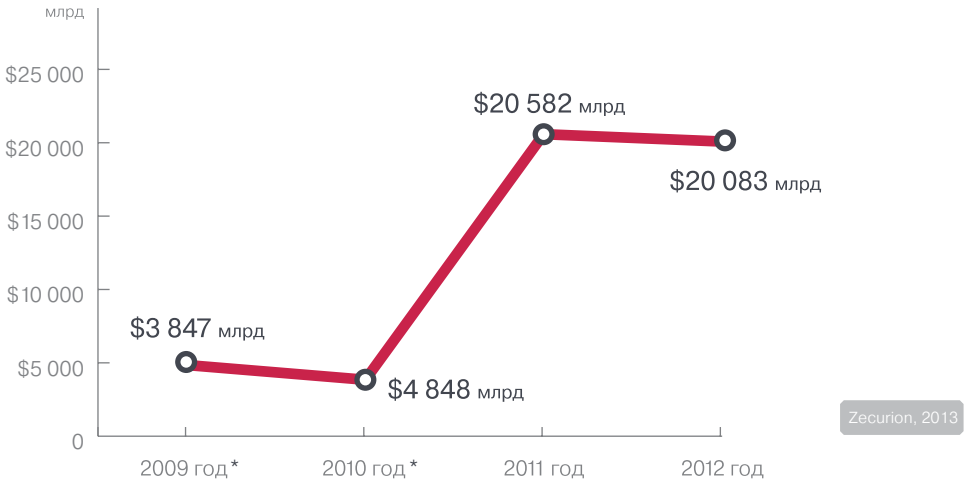
Конечно, борьбу за privacy не стоит превращать в самоцель и впадать в крайности, но мы рекомендуем соблюдать минимальные требования информационной безопасности и не разглашать самостоятельно ту информацию, которая не является изначально открытой (например, пароли к электронным аккаунтам). Взять, к примеру, аккаунт в социальной сети или блогосфере. Вряд ли у большинства пользователей там спрятаны действительно важные сведения вроде паспортных данных или фотографий интимного характера. Но и эти «никчёмные» аккаунты привлекают внимание злоумышленников. Ведь из них можно рассылать спам по списку контактов/френдов. А, значит, и монетизировать.

Ярким примером того, как утечка может быть монетизирована, является история корреспондента газеты «Ведомости» Валерия Кодачигова, опубликованная осенью прошлого года. Потеряв паспорт, Валерий поспешил обратиться в полицию и вскоре получил новый паспорт. Однако мошенники, в руки которых попал пропавший документ, успели взять на имя владельца кредиты в трёх банках на сумму примерно 400 тыс. рублей.

Безусловно, физический паспорт, который можно практически сразу использовать, более ценен для мошенников, чем голые данные. Но в преступном бизнесе и данные будут востребованы. По крайней мере, до тех пор, пока стоимость изготовления фальшивого паспорта заметно меньше, чем потенциальная выгода от его использования. К тому же надо учитывать, что у мошенников потребность в объёме паспортных данных гораздо выше, чем количество фактически изготовленных документов. Под разные задачи могут требоваться данные со специфическими характеристиками, например, человек из определённого региона или номер из заданного интервала. Если к мошенникам попадёт крупная база данных, большинство записей из неё, скорее всего, не будет использовано в преступных схемах. Но это вовсе не означает, что данные находятся в безопасности.

Общий ущерб от утечек информации, зафиксированных аналитическим центром Zecurion, составил $20,083 млрд (см. рис. 5). Несмотря на увеличение числа инцидентов, это на полмиллиарда меньше, чем в прошлом году ($20,582 млрд). Соответственно, удельный ущерб от утечки тоже снизился и составил $24,34 млн.

Рисунок 5 ▶
Ущерб от утечек



* Данные за 2009 и 2010 годы приведены для справки. Оценка ущерба проводилась по иной (нескорректированной) методике.

На протяжении нескольких лет мы наблюдали стабильное увеличение размера ущерба от утечек информации (единственное действительно ощутимое снижение ущерба было отмечено лишь в 2010 году). Тенденция была обусловлена одновременно увеличением количества инцидентов и ростом усреднённого ущерба. Нынешнее снижение суммы ущерба, к сожалению, слишком незначительно, чтобы можно было однозначно заявить о нисходящем тренде. Тем не менее, прекращение роста уже является положительным моментом. В целом, в отношении размера ущерба от утечек присутствует некая неопределённость и мы рассчитываем, что статистика следующего года поможем определить направление тренда, будет ли он растущим или падающим.

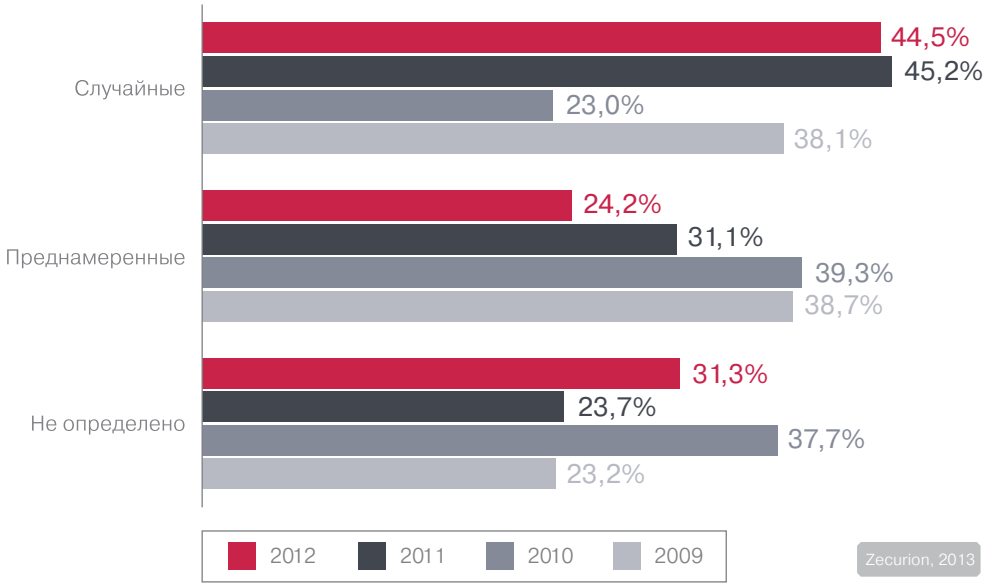
Хотя, признаться, ожидать дальнейшего снижения суммы финансовых потерь сложно. К этому нет предпосылок. Внимание к внутренним инцидентам не ослабевает, санкции регуляторов тоже не становятся мягче. Объективно, рассчитывать можно на сознательность организаций и действительное укрепление информационной безопасности. Хотя компании сегодня внимательнее относятся к вопросам безопасности, стремятся минимизировать собственные издержки, сопровождают пострадавших клиентов, оказывают им помощь консультативного характера и даже возмещают убытки, результаты подобной работы будут видны лишь несколько лет спустя.

Говоря об убытках, наносимых утечками информации, нельзя не упомянуть об одном уникальном инциденте, произошедшем в минувшем году. Речь идёт о громкой утечке документов из резиденции Папы Римского, т. н. Vatileaks. Считается, что именно это событие привело к отставке понтифика. Если оставить в стороне вопросы религии и этики, разглашение информации и последующее переизбрание Папы принесут, по всей видимости, неплохой доход в бюджет Ватикана. По крайней мере, в 2005 году, когда состоялись предыдущие выборы Папы, профицит бюджета страны увеличился на 224% по сравнению с 2004 годом.

Причины утечек

Человеческий фактор является одной из ключевых проблем информационной безопасности. Тем более в сфере внутренних угроз. Перефразируя известное высказывание И. В. Сталина, «каждая утечка имеет свою фамилию, имя и отчество». Но даже понимая, что за каждой утечкой стоит халатность или злой умысел инсайдера, не всегда получается определить, каким же образом информация оказалась скомпрометированной. Для уточнения деталей необходимо провести расследование инцидента. В свою очередь, расследование сложных случаев требует глубокой экспертизы журналов компьютерных систем, задействованных в передаче данных. Далеко не всегда пострадавшая от утечки компания может провести экспертизу или даже предоставить все необходимые журналы. Просто потому, что не располагает ими. А специальные технические решения для контроля перемещения информации распространены всё ещё не слишком широко. Поэтому весьма высока и доля неопределённости в статистике (см. рис. 6).

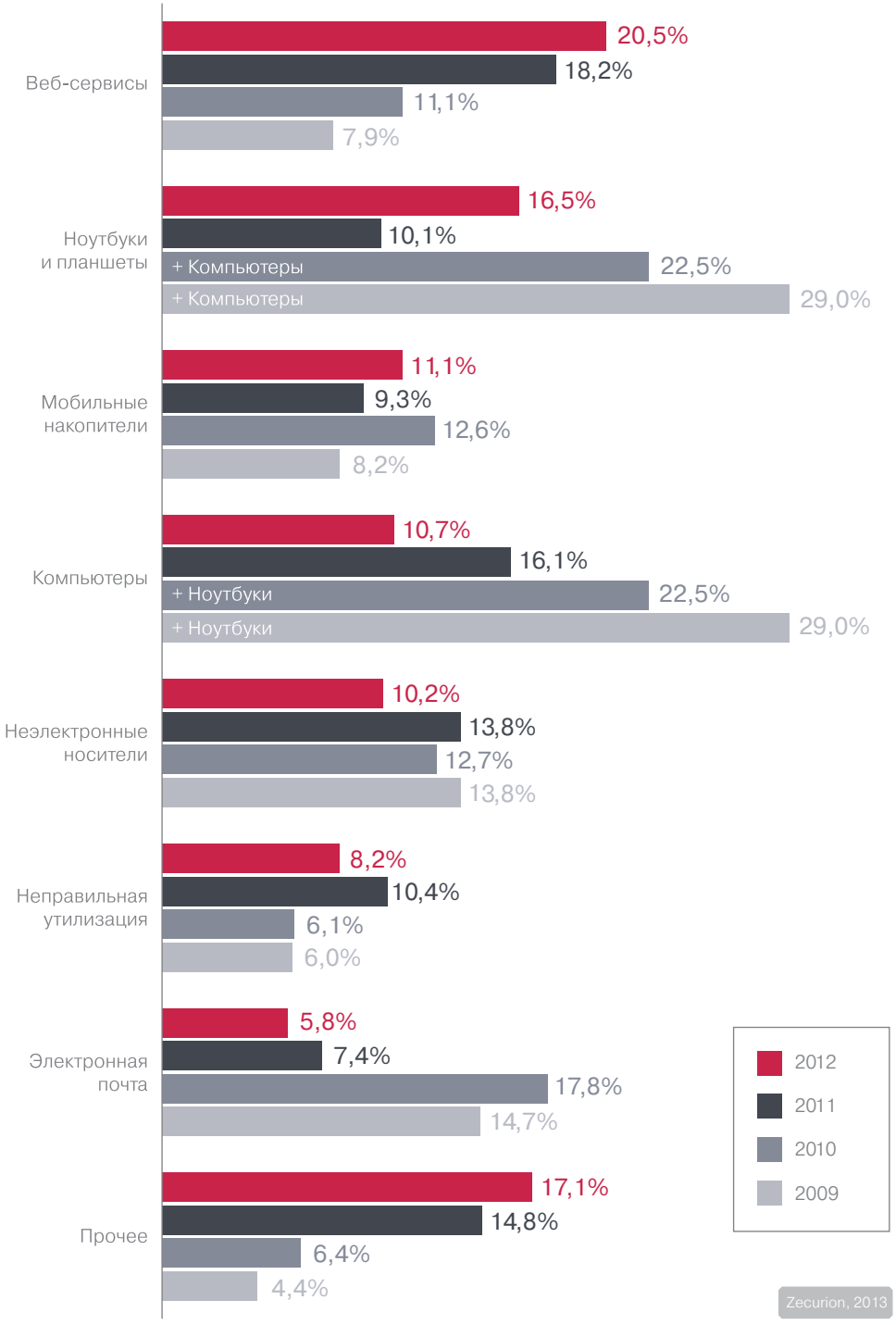
Рисунок 6 ▶
Наличие умысла в утечках информации



По статистике 2012 года, большая доля утечек по-прежнему происходит случайно, из-за ошибок или халатности собственных сотрудников. Одним из типичных сценариев в данной категории является утеря незашифрованных носителей с конфиденциальной информацией. Хотя доля умышленных утечек информации по статистике снизилась, одновременно возросла доля неопределённости. Выше уже говорилось о сложностях в расследовании инцидентов, поэтому вкратце можно резюмировать, что сегодня подготовленные атаки на информационные ресурсы становятся всё более изощрёнными и умелыми, а в отсутствие специальных технических средств контроля информационных потоков даже последующее изучение их является непростой задачей.

Не всегда получается детектировать и канал утечки данных (см. рис. 7). Однако мы можем выделить наиболее явную тенденцию — рост доли утечек через ноутбуки. Даже в корпоративной среде мобильные компьютеры вытесняют стационарные в силу большего универсализма при примерно равных технических возможностях и соизмеримой стоимости решений. Несмотря на схожее предназначение, с точки зрения безопасности использование мобильных и стационарных компьютеров принципиально различно.

Рисунок 7 ▶
Каналы утечки



Если уж из организации выносят системный блок, в большинстве случаев это классифицируется как кража со взломом. К примеру, в феврале прошлого года неизвестные пробрались в клинику города Юджин (США, штат Орегон) и вынесли оттуда компьютеры с персональными данными пациентов. Соответственно, при разборе подобных инцидентов необходимо учитывать аспекты не только информационной, но и физической безопасности.

В свою очередь мобильные компьютеры сотрудники сами часто выносят за пределы офиса, забывают в кафе, аэропортах и в других общественных местах. Соответственно, риски утечки сразу серьёзно повышаются. Кстати, с этого года в категорию мобильных компьютеров включены не только ноутбуки, но и планшеты, хотя доля зарегистрированных утечек через tablet PC пока мала.

Краткие прогнозы

В заключение оценим точность собственных прогнозов, данных в прошлогоднем отчёте, и попробуем понять, какие тенденции будут иметь место в ближайшие несколько лет.

Наш прогноз относительно роста стоимости утечек пока не оправдался. Но только пока. Одна из объективных причин состоит в том, что новый закон о защите персональных данных до сих пор находится на рассмотрении Европарламента. Однако в конце концов закон будет принят, и при сохранении нынешних формулировок виновникам разглашения информации будет угрожать серьёзный штраф, не говоря уже о других последствиях инцидента.

Готовиться к повышению штрафных санкций стоит не только компаниям, работающим на европейских рынках, но и сугубо российским фирмам. Доработки законодательства в части защиты персональных данных идут в России полным ходом, и уже в феврале 2013 года член Совета Федерации и председатель комиссии по развитию информационного общества Руслан Гаттаров сообщил, что штрафы за утечки персональных данных для юридических лиц должны исчисляться миллионами рублей.

В свою очередь оправдались ожидания уменьшения числа инцидентов, связанных с неправильной утилизаций носителей, в том числе неэлектронных. Хотя снижение доли выражается в единицах процентов, мы считаем, что это только начало устойчивого тренда. К тому же основным фактором снижения подобных утечек является внедрение организационных мер, то есть изменения в голове людей. А такие изменения, как известно, приживаются не быстро.

Подтвердились прогнозы и относительно роста спроса на продукты для шифрования данных. Продукты этого класса можно условно отнести к системам предотвращения утечек на этапе хранения. Отметим также интерес потребителей к продуктам для выявления мест несанкционированного размещения конфиденциальных данных. Вместе с модулем шифрования подобные решения являются полезным инструментом для предотвращения утечек. Найденные данные могут быть удалены, перемещены или зашифрованы.

Ещё один прогноз касался уменьшения числа непредумышленных утечек. И хотя их доля действительно снизилась, но несущественно. Это вполне закономерно, так как предпосылок для кардинального сокращения нет. Такой предпосылкой могло бы стать, к примеру, резкое повышение штрафов и ответственности, в том числе для физических лиц. Но, как известно, пока гром не грянет, мужик не перекрестится. В отсутствие таких сильных (хотя и явно репрессивных) мотиваторов ведётся планомерная работа в части обучения персонала аспектам защиты информации и расширение охвата технических средств, что и выливается в итоге в постепенное снижение доли случайных утечек. Надеемся, что в нынешнем году снижающийся тренд будет выражен ярче.

Громкие российские утечки

Концерн «Тракторные заводы»

Machinery & Industrial Group N.V.
Концерн Тракторные заводы

Доступ к коммерческой тайне конкурента даёт серьёзные преимущества не только в сфере высоких технологий (в предыдущих разделах исследования уже упоминался инцидент с утечкой 100 тыс. конфиденциальных документов из корпорации AMD). Горячий спор о краже коммерческой тайны разгорелся между российскими машиностроительными предприятиями, концерном «Тракторные заводы» (КТЗ) и ООО «ЧТЗ-Уралтрак», созданным на базе обанкротившегося Челябинского тракторного завода. По версии представителей КТЗ, гендиректор «ЧТЗ-Уралтрак», ранее работавший в КТЗ, организовал с помощью своих бывших коллег хищение конструкторской документации, касающейся серийно изготавливаемых изделий и перспективных разработок.

О возбуждении дела по факту хищения (ст. 183 УК, собирание сведений, составляющих коммерческую тайну, путём похищения документов, подкупа и угроз) в отношении неустановленной группы лиц стало известно в апреле 2012 года. А осенью представители МВД сообщили, что обвинение в незаконном разглашении сведений, составляющих коммерческую тайну, предъявлено начальнику отдела ОАО «Промтрактор», входящему в концерн «Тракторные заводы». По предварительным оценкам владельцев коммерческой тайны, им был нанесён крупный ущерб, свыше 50 млн рублей.

Министерство внутренних дел

Неправильная утилизация носителей информации является одним из распространённых сценариев утечки информации. К примеру, в 2011 году было установлено, что в 40% мусорных контейнеров офисных зданий в Лондоне можно найти конфиденциальные сведения. Случаются подобные инциденты и в России. Так, в апреле 2012 года близ Казани инспекторы Центрального территориального управления министерства экологии обнаружили несанкционированную свалку. Среди мусора оказались и личные дела военнослужащих расквартированной неподалёку воинской части МВД специального назначения. Её бойцы — участники контртеррористических операций на Северном Кавказе. Никаких претензий в части раскрытия персональных данных инспекторы военным не предъявили, зато пообещали привлечь к ответственности за загрязнение окружающей среды.

В ходе расследования, которое провела военная прокуратура, было установлено, что в компрометации служебных документов (личные дела военнослужащих-призывников, проходивших службу в 2006-2007 годах) виноват начальник квартирно-эксплуатационной службы воинской части. Именно он вывез мусор в лесной массив. Правда, осталось невыясненным, каким образом документы попали в бытовой мусор, и кто нарушил порядок работы с информацией. По сообщению Генеральной прокуратуры РФ в отношении проштрафившегося офицера и командира части были возбуждены административные дела и решался вопрос о возбуждении уголовного дела.

Мобильные операторы

Утечки информации из мобильных операторов обычно характеризуются большими объёмами данных, однако инцидент, зафиксированный летом 2012 года, выбивается из общей картины. Инсайдеры из ОАО «МТС» и ОАО «Вымпелком» сливали информацию о переговорах всего трёх абонентов — высокопоставленных российских чиновников. По версии Федеральной службы безопасности, расследовавшей дело, инсайдеры действовали с января 2010 по май 2012 года. В незаконном сборе и распространении информации оказались замешаны сотрудники технических центров МТС и «Вымпелкома», а также несколько других физических лиц и частных компаний.

Примечательна полярная реакция мобильных операторов на инцидент. В «Вымпелкоме» признали факт утечки информации через бывшего сотрудника. Утечка была обнаружена с помощью действующей в компании системе защиты конфиденциальной информации и персональных данных. Не понятно только, почему инцидент зафиксировали спустя 2,5 года после начала кражи информации. Тем не менее, оператор связи принёс свои извинения и пообещал возместить моральный ущерб клиентам после завершения расследования. В свою очередь в МТС заявили, что внутренней службой безопасности фактов утечки не выявлено.

Сайты-«купонаторы»

Пройдя пик своей популярности, скидочные сайты в России столкнулись с рядом трудностей, в том числе снижением потребительского спроса, жалобами и судебными исками по поводу недобросовестных поставщиков услуг и т. д. Очередным событием, ударившим по репутации «купонаторов», стала утечка баз пользователей, всего 760 тыс. человек. У 92 тыс. человек из базы помимо имён и адресов электронной почты указаны также номера мобильных телефонов. Продавец базы просил за информацию немного – всего $500, рассчитывая, вероятно, заработать на количестве проданных экземпляров. Тем не менее, данный инцидент является крупнейшей публичной утечкой информации в России в 2012 году по количеству затронутых людей.

Представители наиболее популярных купонных сервисов, что не удивительно, отрицают факты и даже возможности утечек информации из их компаний. Неопровержимых доказательств того, что утечка действительно произошла из какого-то конкретного сервиса или сервисов до сих пор нет. Тем не менее, косвенные признаки указываю именно на скидочные сайты. Если бы это была база, к примеру, интернет-магазинов, там было бы больше телефонных номеров, а также адреса доставки. Достоверность базы проверили корреспонденты газеты «Ведомости», прозвонившие несколько человек. Имена ответивших на звонки совпали с указанными в базе. Однако никто из них не смог сказать, на каком сайте оставлял свои персональные данные.

Следственный комитет

В декабре 2012 года на сайте Следственного комитета России в открытом доступе появились тексты обращений граждан через интернет-приёмную. Всего около 30 тыс. сообщений, оставленных за 2,5 года, оказалось в разделе «Новости». Наиболее вероятные причины инцидента — ошибки при разработке сайта или халатность обслуживающих его технических специалистов. Хотя в пресс-службе ведомства заявили о том, что имел место технический сбой.

Первыми об инциденте сообщили корреспонденты газеты «Ведомости». Помимо СМИ живой интерес к утечке проявили представители Роскомнадзора, поскольку при обращении граждане оставляют также свои персональные данные. По оценкам юристов, пострадавшие от утечки информации граждане вполне могут рассчитывать на возмещение ущерба. Впрочем, надо понимать, что ущерб ещё надо доказать, а желающих судиться со Следственным комитетом вряд ли будет много.

Интересно, что при расследовании прошлогодней громкой утечки текстов SMS оператора сотовой связи «МегаФон» представители Следственного комитета говорили о необходимости ужесточить ответственность за разглашение персональных данных в сети.

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 Analytics
analytics@zecurion.com

Александр Ковалёв
Заместитель генерального директора
marketing@zecurion.com

129164, Российская Федерация, Москва,
Ракетный бульвар, 16
Тел.: +7 495 221-21-60
www.zecurion.ru