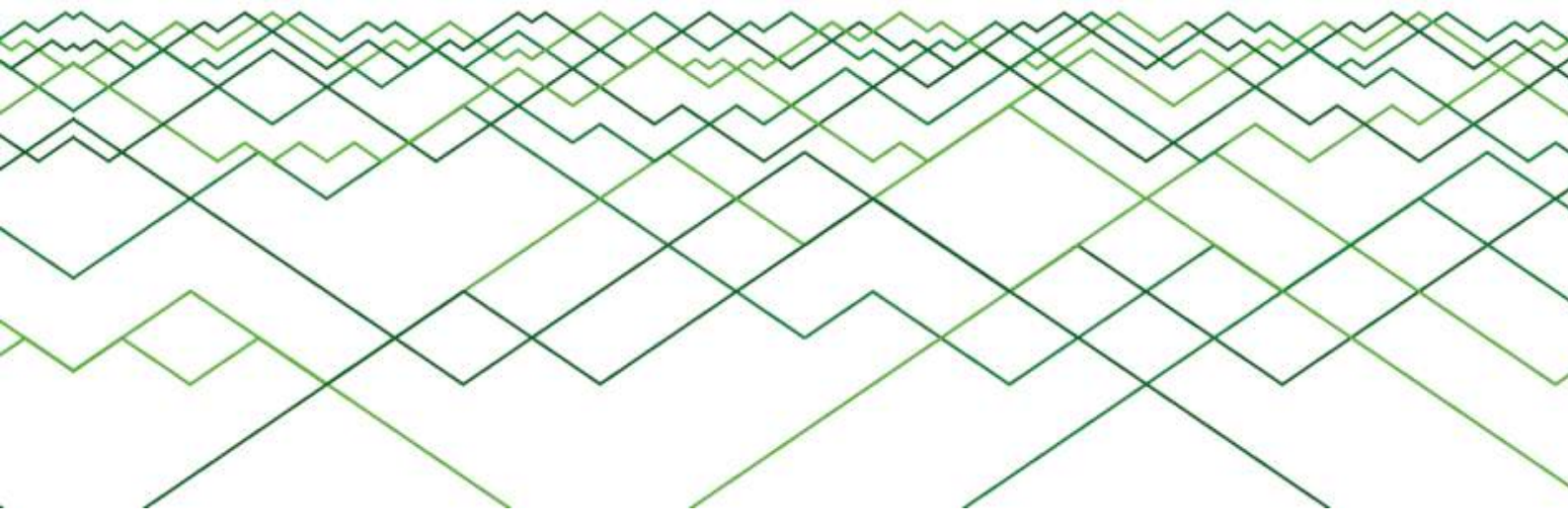
INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Аналитический Центр InfoWatch
www.infowatch.ru/analytics

Глобальное исследование утечек конфиденциальной информации в 2013 году



Оглавление

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Только цифры

- ✓ В 2013 году в мире зафиксировано, обнародовано в СМИ и зарегистрировано Аналитическим Центром InfoWatch **1143** случая утечки конфиденциальной информации, что на **22%** превышает количество утечек, зарегистрированных в прошлом году.
- ✓ Скомпрометировано более **561 млн** записей, в том числе финансовые и персональные данные.
- ✓ Россия вышла на **второе место** по количеству опубликованных утечек, обогнав Великобританию. Число «российских» утечек в 2013 году **выросло на 78%** – зарегистрировано **134 случая** утечки конфиденциальной информации из российских компаний и государственных организаций.
- ✓ Доля утечек в госорганах и муниципальных учреждениях по всему миру остается стабильно высокой – **31%.** Госорганы, наряду с медицинскими учреждениями, являются основным источником утечек персональных данных.
- ✓ Больше всего утечек информации связано с персональными данными – в **85%** случаев утекает именно эта информация.
- ✓ Обнародованный в СМИ ущерб (включая затраты на ликвидацию последствий утечек, судебные разбирательства, компенсационные выплаты), который понесли компании вследствие утечек информации в 2013 году, составляет **7,79** млрд долларов.

Аннотация

Аналитический Центр компании InfoWatch представляет отчет об исследовании утечек конфиденциальной информации в 2013 году. По мнению авторов работы, всесторонний анализ сообщений об утечках конфиденциальной информации дает возможность оценить уровень защищенности информации в коммерческих компаниях, государственных организациях, образовательных учреждениях; позволяет сопоставить общую картину утечек в более «продвинутых» (США, Великобритания) и менее развитых в плане регулирования темы информационной безопасности (далее ИБ) регионах.

В 2013 году более 70% утечек данных, ставших предметом исследования, пришлось на «англосаксонские» страны, где коммерческие компании и государственные органы обязаны уведомлять регуляторов и пострадавших граждан о произошедшей утечке. Однако такое распределение выборки вовсе не значит, что выводы данного исследования будут бесполезны для других стран. Проблема защиты конфиденциальной информации актуальна во всем мире по причине высочайшего уровня конкуренции как в развитых (с точки зрения ИБ), так и в развивающих тему безопасности странах.

Глобальный характер киберпреступности сводит на нет все рассуждения о возможности «собственного» пути развития ИБ в различных странах. Достаточно вспомнить такой «популярный» вид мошенничества с персональными данными, как кража личности. Еще пять лет назад такие преступления были распространены только в США (и странах со схожей социальной системой). Сегодня сотрудники российских банков неправомерно оформляют кредиты на чужие, украденные паспортные данные, сканы паспортов продаются на форумах и в социальных сетях.

> *kp.ru: 34-летняя женщина, используя копии чужих документов, оформила на них потребительские кредиты на 305 тысяч рублей. Дама работала кредитным экспертом в одном из отделений Сбербанка России. Воспользовавшись доступом к персональным данным клиентов финансового учреждения, подозреваемая незаконно оформила два потребительских кредита на сумму 130 и 175 тысяч рублей. Впоследствии путем обмана своих коллег, с кредитных счетов, оформленных на указанных граждан, предприимчивая сотрудница банка перевела денежные средства на свой личный счет.*

Картина по утечкам других видов данных в мировом масштабе также имеет больше общего, чем различного. Таким образом, «Развивающиеся» в плане ИБ страны рано или поздно встретятся лицом к лицу с реальностью, характерной сегодня для «развитых» держав – США, Великобритании. Коммерческим компаниям и госорганам «отстающих» стран следует уже сейчас готовиться к новым вызовам информационной безопасности, как то растущее год от года влияние фактора внутренних угроз, усилившееся внимание законодателей и регуляторов к вопросам защиты конфиденциальной информации и персональных данных.

В этом смысле анализ картины утечек в зарубежных странах, наиболее «продвинутых» в деле борьбы с утечками, будет более чем полезен как для

российского рынка (который, условно, можно считать «догоняющим», по отношению к тем же США), так и для стран со схожей в вопросе защиты информации ситуацией.

Методология

Исследование основывается на собственной базе данных, пополняемой специалистами Центра с 2004 года. В базу Аналитического Центра InfoWatch включаются публичные сообщения[1] о случаях утечки[2] информации из коммерческих и некоммерческих (государственных, муниципальных) организаций вследствие злонамеренных или неосторожных действий[3] сотрудников, иных лиц[4]. База утечек InfoWatch насчитывает несколько тысяч зарегистрированных инцидентов.

В ходе наполнения базы каждая утечка (если возможно и такая информация есть в сообщении об утечке) классифицируется по ряду критериев: размер организации[5], сфера деятельности (отрасль), размер ущерба, тип утечки (по умыслу) [6], канал утечки[7], типы утекших данных[8] и пр. Данные об ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций в СМИ.

Исследование охватывает не более 4-8%[9] случаев от предполагаемого совокупного количества утечек. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества (категории) содержали достаточное или избыточное количество элементов (фактических случаев утечки). Такой подход к формированию поля исследования позволяет считать получившуюся выборку теоретической, а выводы исследования и выявленные на выборке тренды репрезентативными для генеральной совокупности.

Для сохранения однородности выборки при составлении отраслевой карты[10] мы целенаправленно вывели за рамки исследования утечки с несоразмерно большим количеством утекших персональных данных (например, если наблюдалось

---

[1] Сообщения об утечках данных, опубликованные официальными ведомствами, СМИ, авторами записей в блогах, интернет-форумах, иных открытых источниках.

[2] Утечка информации (данных) - действие или бездействие лица, имеющего легитимный доступ к конфиденциальной информации, которое (действие) повлекло потерю контроля над информацией или нарушение конфиденциальности этой информации.

[3] См. тип утечки по умыслу.

[4] В данном исследовании авторы впервые представляют картину утечек в разрезе виновных лиц.

[5] Аналитики Центра InfoWatch классифицируют организации по размеру в зависимости от известного либо предполагаемого парка персональных компьютеров (ПК). Небольшие компании – до 50 ПК, средние - от 50 до 500 ПК, крупные – свыше 500 ПК.

[6] Мы разделяем утечки информации по признаку умысла (намерения) на умышленные (злонамеренные) и неумышленные (случайные) см. Глоссарий. Термины умышленные – злонамеренные и неумышленные – случайные (попарно) равнозначны и употребляются здесь как синонимы.

[7] Под каналом утечки мы понимаем такой сценарий (действия (или бездействие) пользователя корпоративной информационной системы, направленные на оборудование или программные сервисы), в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. Классификация каналов утечек приведена в глоссарии.

[8] Предметом настоящего исследования являются исключительно сообщения об утечках персональных данных

[9] В ходе исследования мы столкнулись с явным свидетельством того, что уровень латентности (доля утечек, оставшихся неизвестными широкой публике) в мире серьезно снизился. Потому экспертная оценка процентной доли известных утечек по сравнению с утечками, оставшимися за рамками внимания данного исследования, повышена с 1-5% до 4-8%.

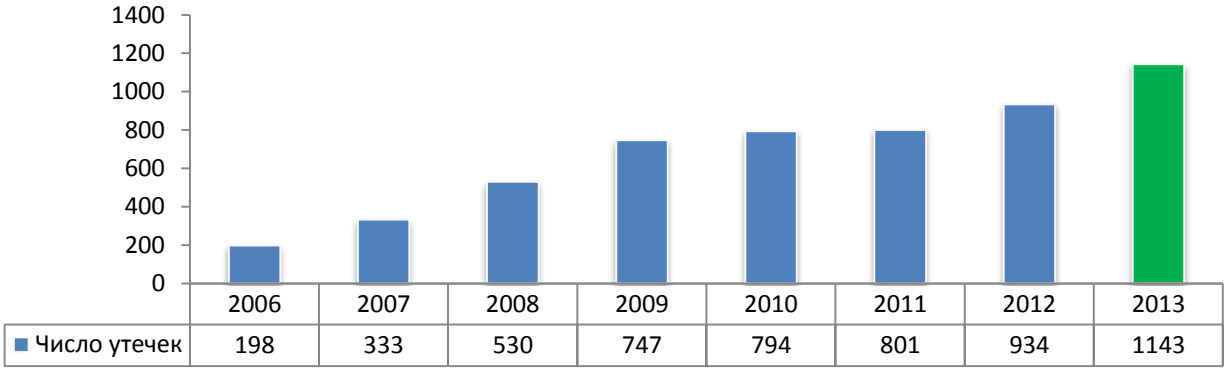
[10] В данном отчете мы впервые оцениваем степень защищенности информации в различных отраслях на примере утечек персональных данных.

превышение среднего числа утекших данных на 3-4 порядка). Для составления отраслевой карты утечки с незначительным (менее 100) количеством «ушедших» записей удалены из выборки.

Случаи нарушения конфиденциальности информации, произошедшие в результате внешних компьютерных атак, а равно иные инциденты ИБ (DDoS, фишинг, несанкционированный доступ к информации, саботаж сотрудников и пр.), не повлекшие утечек данных, в исследовании не рассматривались.

Общая статистика

В 2013 году Аналитическим Центром InfoWatch зарегистрировано 1143 (3,1 в день, 95,2 в месяц) случая утечки конфиденциальной информации (см. Рисунок 1). Это на 22,3% больше, чем в 2012 году (934 утечки). В исследуемый период динамика роста утечек была на 5,7 процентных пунктов (п. п.) выше, чем в 2012 году (тогда рост к 2011 году составил 16,6%). Впервые за годы наблюдений число утечек превысило отметку в 1000 случаев.



	2006	2007	2008	2009	2010	2011	2012	2013
Число утечек	198	333	530	747	794	801	934	1143

Рисунок 1. Число зарегистрированных утечек информации, 2006 -2013 гг.

В поле внимания СМИ все чаще попадают утечки, остававшиеся ранее неизвестными («уход» информации из государственных органов, компрометация больших объемов платежных данных – номера кредитных карт, срок действия и даже CVC, утечки коммерческой тайны из крупных компаний с мировым именем).

> *justice.gov: Министерство юстиции США обвинило китайского производителя турбин Sinovel Wind Group в краже технологий у американской AMSC. Ущерб AMSC от действий китайцев оценивается в 800 миллионов долларов. Вместе с компанией были обвинены два работника Sinovel Wind Group — Су Лиин (Su Liying) и Чжао ХайЧунь (Zhao Haichun) — и Деян Карабашевич, сотрудник дочернего предприятия AMSC в Австрии.*

Баланс случайных и умышленных утечек (см. Рисунок 2) отличается от картины, выявленной в 2012 году. Доля случайных утечек выросла на 8,1 п. п. Доля злонамеренных, наоборот, немного уменьшилась (на 1,8 п. п.).

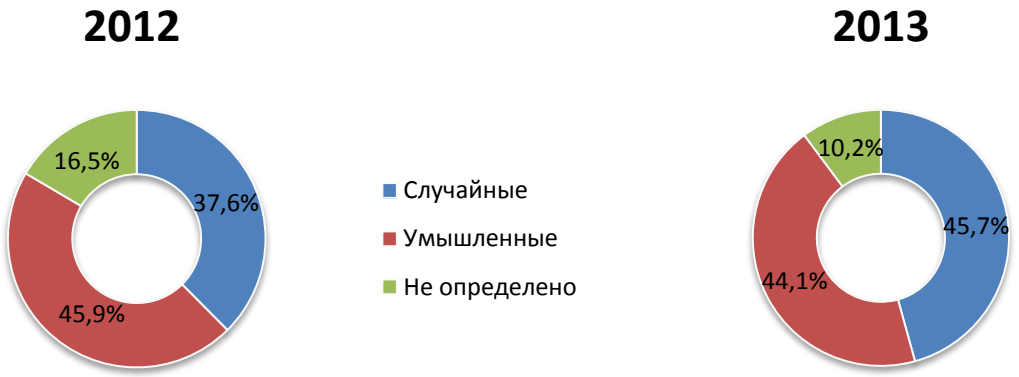


Рисунок 2. Соотношение случайных и умышленных утечек, 2012 - 2013 гг.

Снижение доли утечек «неопределенного» типа авторы исследования связывают с распространением технических средств защиты от утечек (в том числе решений класса DLP). С помощью подобных программных продуктов пострадавшие компании выявляют источник утечки, канал, виновного.

> *engadget.com: Дизайнеров HTC подозревают в краже коммерческой тайны и мошенничестве. Среди подозреваемых вице-президент по дизайну продуктов Томас Чин (Thomas Chien). Он скачивал, а потом отправлял третьим лицам по электронной почте файлы, связанные с Sense 6.0 UI. Трое сотрудников обвиняются в махинациях с комиссионными за дизайн корпуса HTC One. Дизайн разрабатывался в недрах HTC, но мошенники через подставную фирму, которая якобы его разработала, затребовали с HTC $334 тыс.*

В распределении по виновнику утечки[11] доля случаев, когда виновника не удалось определить, составила всего 15% (см. Рисунок 3).

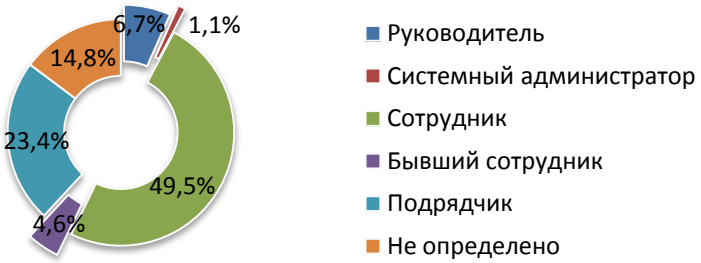


Рисунок 3. Распределение утечек по источнику (виновнику), 2013 г.

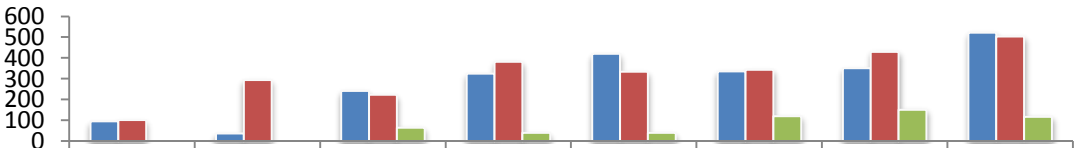
В половине случаев виновниками утечек информации были сотрудники компаний – настоящие или бывшие (49,5% и 4,6% соответственно). Велика доля утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к

[11] Лицо, неумышленно допустившее утечку информации, либо совершившее злонамеренные действия, следствием которых явилась компрометация охраняемой информации.

охраняемой информации (23,4%). В 6,7% случаев виновными оказались высшие руководители организаций (топ-менеджмент, главы отделов и департаментов).

> *vz.ru: Американский суд обязал независимого директора Сбербанка, ранее входившего в попечительский совет бизнес-школы «Сколково», члена совета директоров компании Goldman Sachs Раджата Гупту выплатить штраф в размере 13,9 млн долларов, сообщили в Комиссии США по ценным бумагам и биржам (SEC). По версии следствия, Гупта раскрыл детали закрытой финансовой отчетности Goldman Sachs за 2008 год в ходе переговоров с Раджаратнамом об инвестициях в Goldman Sachs компании Berkshire Hathaway в размере пяти миллионов долларов.*

Динамика случайных и умышленных утечек за последние 8 лет показана на гистограмме (см. Рисунок 4).



	2006	2007	2008	2009	2010	2011	2012	2013
Случайные	96	38	242	325	420	336	352	522
Умышленные	102	295	223	382	334	344	430	504
Не определено	0	0	65	40	40	121	152	117

Рисунок 4. Динамика числа случайных и умышленных утечек, 2006 -2013 гг.

Доли случайных и умышленных утечек примерно равны (разница в пределах погрешности, обусловленной методологией исследования)[12]. Такая картина наблюдается с 2008 года – признак сбалансированности факторов, влияющих на картину утечек.

В 2013 году более 70% утечек зарегистрированы в англосаксонских странах, где компании обязаны раскрывать случаи компрометации данных, а проникновение средств защиты от утечек (по крайней мере, в крупных компаниях) составляет, по разным оценкам, 20-50%[13]. С большой вероятностью, можно говорить о появлении тренда на повышение уровня прозрачности темы утечек информации в мировом масштабе.

Иначе говоря, факторы, влияющие на распределение утечек (в различных разрезах) в нашей выборке, в горизонте 2-3 лет стабилизировались. Потому при объяснении возросшего числа утечек в 2013 году авторы исследования испытали определенную сложность.

[12] На этапе классификации утечек возможно неверное определение некоторых параметров регистрируемого случая. В связи с этим, авторы исследования считают, что погрешность по отдельным разрезам (долям) составляет 1-3% от всего числа элементов выборки в данной категории..

[13] См., например, исследование The Radicati group, inc. Data Loss Prevention Market, 2010-2014. http://www.radicati.com/wp/wp-content/uploads/2010/12/Data-Loss-Prevention-Market-2010-2014-Executive-Summary.pdf

Единственно возможное объяснение существенного роста числа зарегистрированных утечек – снижение уровня латентности (доли скрытых утечек по отношению ко всем случившимся утечкам) утечек данных за счет повышения прозрачности темы защиты данных в «развитых» с позиции ИБ странах.

Иначе говоря, прирост числа утечек информации в 2013 году не связан с радикальными изменениями природы внешних (заинтересованность злоумышленников) или внутренних (ослабление защиты в компаниях, пострадавших от утечек) факторов. Но с тем, что доля скрытых утечек сокращается.

Второй немаловажный момент, повлиявший на увеличение доли известных утечек (и рост числа утечек, зарегистрированных авторами исследования в 2013 году) связан с тем, что восприятие средств защиты в компаниях, стремящихся обезопасить себя от утечек, кардинально изменилось. Compliance как основной драйвер бизнеса в англо-американском ИБ отходит на второй план. На смену «бумажной» безопасности приходит реальная работа по обеспечению защиты – считают в Gartner[14].

Вывод:

В 2013 году авторы данного исследования впервые за весь период наблюдения (с 2004 года) фиксируют снижение доли скрытых утечек в мировом масштабе. Темпы роста числа утечек в 2013 году опережают аналогичные показатели прошлого года, однако этот факт скорее внушает оптимизм. В основе выявленного тренда повышение прозрачности темы утечек информации и смена парадигмы восприятия средств защиты – компании применяют технические решения не только для того, чтобы выполнить требования регуляторов, но и для реального обеспечения информационной безопасности. Что позволяет этим компаниям все лучше детектировать утечки, определять их тип, выявлять виновных.

Каналы утечек[15]

Изучение случаев утечек в разрезе каналов, по которым уходит информация, имеет прямое практическое значение. В зависимости от частоты утечек по тому или иному каналу, можно рекомендовать внедрение средств защиты в компании или в отрасли, определить, какими каналами следует заниматься в первую очередь. Также на основе распределения утечек по каналам можно сделать выводы об уровне защиты информации в зависимости от отраслевой специфики или размера организации[16].

В 2013 году авторы исследования выявили две разнонаправленные тенденции на каналах, которые можно контролировать с помощью технических средств защиты. Сокращается доля утечек по таким каналам, как потеря оборудования (-6,4 п. п.), мобильные носители (-1 п. п.), при увеличении доли утечек через сеть (+7,1 п. п.) и электронную почту (+4,6 п. п.). Доля утечек бумажных документов изменилась

[14] Gartner Says Compliance Is No Longer a Primary Driver of IT Risk and Security Measures. http://www.gartner.com/newsroom/id/2571115

[15] Определение канала утечки и расшифровки отдельных каналов даны в глоссарии

[16] См. другие исследования Аналитического Центра InfoWatch.

незначительно (-0,4 п. п.). Увеличился процент утечек по голосовому и видеоканалу (+1,1 п. п.) (см. Рисунок 5).

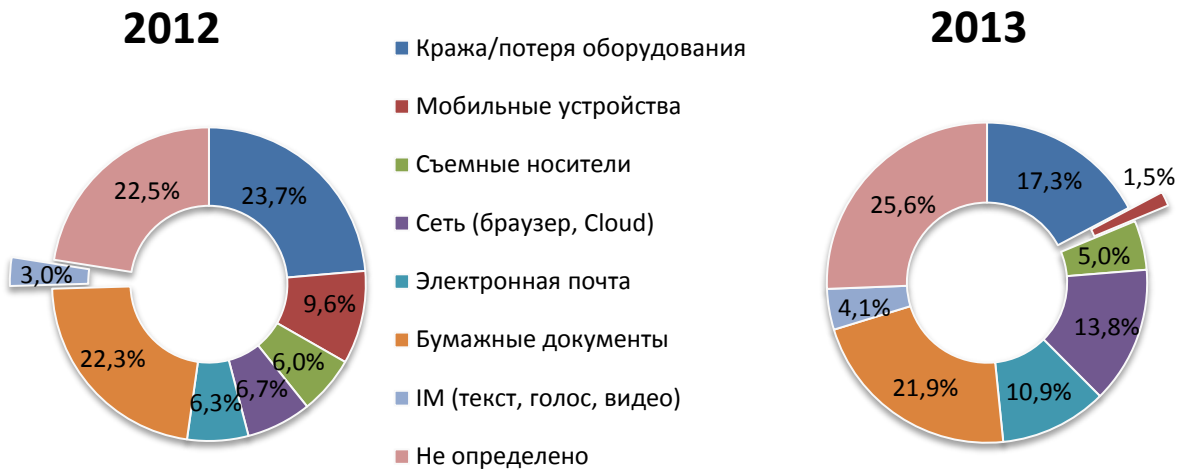


Рисунок 5. Распределение утечек по каналам, 2012 - 2013 гг.[17]

Обратим внимание, что первая группа каналов (потеря оборудования, мобильные носители) «закрывается» средствами шифрования информации, в то время как вторую группу (сеть и электронная почта) традиционно относят к каналам, где наиболее эффективно проявляют себя контент-ориентированные средства защиты (решения класса DLP).

Перераспределение каналов, таким образом, можно объяснить возросшим проникновением защитных решений как первой (шифрование, контроль устройств), так и второй (контент-ориентированные системы) категории. За счет применения шифрования утечек становится меньше (например, в случае потери ноутбука или флешки с зашифрованной информацией компрометации данных не происходит). И наоборот, если шифрование не применялось, уместно говорить о полноценной утечке информации.

> idradar.com: *Сотрудник Governor's Office of Information Technology потерял USB-накопитель, на котором хранились личные данные почти 19 тыс. работников госучреждения. Электронный документ, записанный на флешке, содержал имена, фамилии, номера социального страхования (SSN), как нынешних, так и бывших сотрудников.*

С другой стороны, все большее распространение решений класса DLP позволяет компаниям регистрировать утечки, ранее остававшиеся незамеченными – отсюда рост доли утечек по электронной почте и сети, иным каналам связи.

[17] Снижение доли утечек по каналу «мобильные устройства» связано с тем, что с 2013 года мы не классифицируем по данному каналу утечку информации вследствие потери ноутбуков, иных переносных устройств. Такие случаи относятся к категории «Кража/потеря оборудования».

databreaches.net: Британская Информационная комиссия (Information Commissioner's Office) оштрафовала Банк Шотландии (Bank of Scotland) на 75 тысяч фунтов стерлингов за рассылку факсов с конфиденциальной информацией по неправильным номерам. Установлено, что сотрудники банка ошибались номерами с февраля 2009 по 2012 годы. По неверным номерам направлялись платежные ведомости, банковские выписки и ипотечные заявки. В документах содержались имена и контактные данные клиентов.

Рост утечек через сеть объясняется возрастающей популярностью технологий обнаружения конфиденциальной информации (Discovery или Crawler) в файловых хранилищах и на сетевых ресурсах[18]. Утечки такого плана ранее также оставались неизвестными.

Если проанализировать соотношение случайных и умышленных утечек, гипотеза о все большем распространении DLP-систем становится еще более очевидной. Известно, что DLP-системы успешнее всего проявляют себя в деле выявления и предотвращения случайных утечек информации. Огромные доли (19,2% через сеть и 15,7% через электронную почту) зафиксированных случайных утечек там, где DLP-системы наиболее эффективны – подтверждение этой гипотезы (см. Рисунок 6). Умышленных утечек по этим каналам регистрируется значительно меньше – 8,3% и 5,8% соответственно.

Рисунок 6. Распределение случайных и умышленных утечек по каналам, 2013 г.

Примечателен довольно небольшой (17% и 17,5% соответственно) процент неумышленных и злонамеренных утечек, которые пришлись на канал «кража/потеря оборудования» (при том, что с 2013 года мы классифицируем потери ноутбуков и иных переносных устройств, кроме смартфонов, по этому каналу). И это на фоне

[18] К каналу «сеть» мы, помимо прочих, относим такие утечки, когда пользователь нелегитимно получил доступ к охраняемой информации своей компании через инранет и/или неправомерно сохранил охраняемую информацию на своем ресурсе (ПК, файловое хранилище и проч.).

разговоров о слабости организационных мер, применяемых в отношении корпоративных пользователей мобильных ПК.

> ihotdesk.co.uk: *Новое исследование Sony's VAIO Digital Business показало, что за последние 12 месяцев было потеряно более 1 млн ноутбуков, содержащих ценные корпоративные данные организаций. В опросе приняли участие представители 600 компаний Великобритании. 46% респондентов сообщили, что они намеренно игнорируют политики безопасности компании и продолжают использовать личные устройства, если фирма предлагает использовать нестандартные, по их мнению, технологии.*

Доля случайных и умышленных утечек, связанная с использованием мобильных устройств, остается незначительной. Во многом, это ответ на заявления о якобы чрезвычайной угрозе распространения мобильных устройств в корпоративной среде. Действительно, с мобильного устройства можно отправить конфиденциальный документ, и защищать этот канал нужно. Однако «популярностью» этот канал явно не пользуется – «большие» утечки чаще связаны с давно известными каналами – электронной почтой, сетью, бумажной документацией, кражей ноутбуков[19].

Доля умышленных утечек через съемные носители меньше, чем доля неумышленных, однако ущерб, который несут компании вследствие инцидента, измеряется порой сотнями тысяч или миллионами долларов. Как правило, умышленные утечки через съемные носители связаны с кражей чувствительной информации – коммерческих секретов, ноу-хау.

> www.pcper.com. *Бывшие сотрудники AMD перед уходом в NVIDIA скопировали на флеш-диск более 100 тыс. файлов с конфиденциальной информацией, принадлежащей AMD. После обнаружения утечки специалисты AMD выяснили, что вся операция была заранее спланирована. Инсайдеры решили покинуть AMD, прихватив с собой коммерческие секреты компании, для чего проникли на защищенные компьютеры и в течение шести месяцев собирали информацию. В числе сотрудников, обвиняемых в краже данных, упоминают Роберта Фельдштейна, бывшего вице-президента AMD по стратегическому развитию.*

Остается упомянуть еще один, довольно экзотический канал – утечки информации через сервисы мгновенных сообщений. Данный канал представлен незначительными 1,7% на диаграмме случайных утечек и 1,6% на диаграмме злонамеренных. Однако само появление таких утечек – аргумент в пользу старой истины, что в информационной безопасности не бывает «мелочей» и неважных, «периферийных» каналов.

> ***Вывод:***
>
> *Статистика инцидентов свидетельствует, что на утечки по «традиционным» каналам – почта, e-mail, бумажная документация, кража и потеря оборудования – по-прежнему приходится львиная доля случайных*

[19] В 2013 году мы не относим к числу утечек через канал «мобильные устройства» потери и кражи ноутбуков. С этим связано уменьшение доли утечек по данному каналу по сравнению с данными 2012 года.

утечек. При этом доля «новых» каналов (те же мобильные устройства, голос и видео) пока остается незначительной. Соотношение каналов случайных и умышленных утечек в целом подтверждает тезис о значительном проникновении систем защиты в корпоративной среде. Именно наличие средств защиты информации обусловливает неоднородность распределения «популярных» каналов случайных и умышленных утечек.

Отраслевая карта

2012 год во всем мире стал годом утечек из государственных учреждений (см. Исследование утечек информации из компаний и госучреждений России 2012). Статистика 2013 года показывает, что государственные органы своего неуважительного отношения к проблеме утечек информации не изменили. Доля утечек из государственных учреждений в 2013 году увеличилась на 3 п. п., составив 31,4% (см. Рисунок 7Рисунок 6).

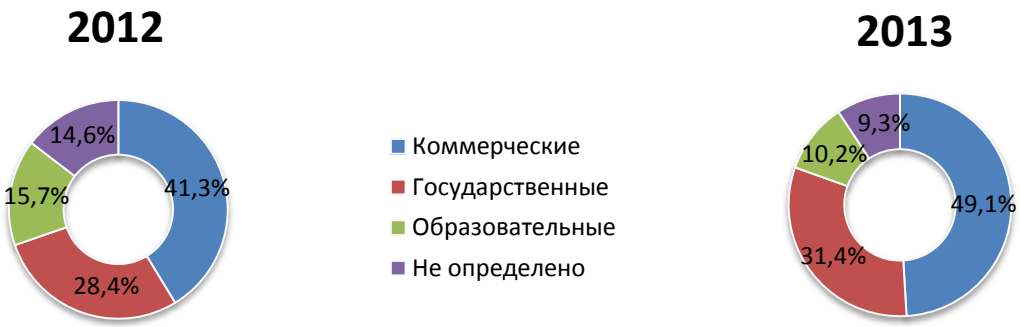


Рисунок 7. Распределение утечек по типу организации, 2012 - 2013 гг.

Рост доли «коммерческих» утечек произошел за счет сокращения доли утечек из компаний «неопределенной» категории. Распределение утечек по типу данных приведено на диаграмме (см. Рисунок 8).

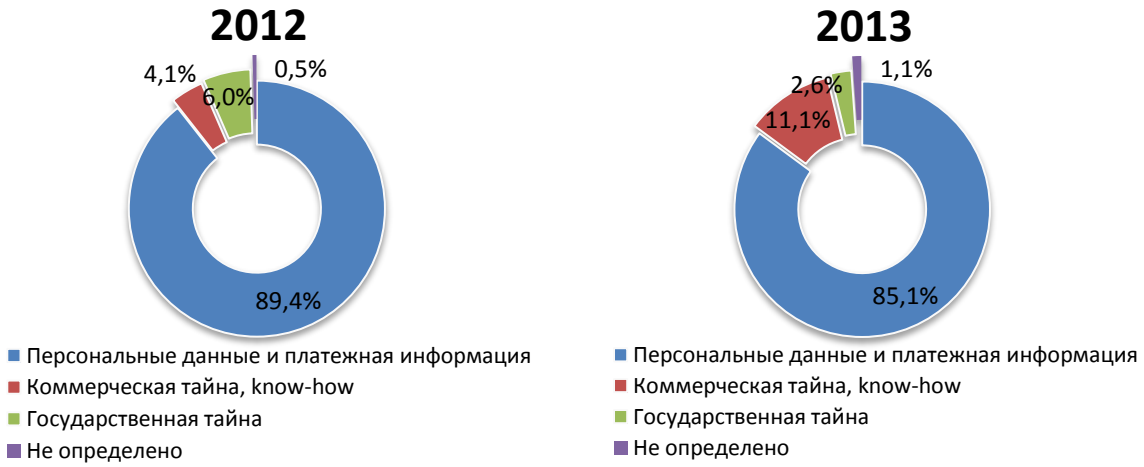


Рисунок 8. Распределение утечек по типам данных, 2012-2013 гг.

Еще год назад мы говорили о снижении доли персональных данных в общей картине утечек (до 89,4%). В 2013 году доля персональных данных вновь уменьшилась (до 85,1%).

> corp.cnews.ru: *Ответственность за недавнюю утечку данных из трех корейских организаций взяли на себя топ-менеджеры этих компаний. От*

утечки пострадали более 100 млн клиентов крупнейших игроков финансового рынка Кореи - KB Financial Group, NongHyup Financial Group и Lotte Group. В ходе утечки скомпрометированы имена и фамилии, номера телефонов и адреса электронной почты, номера пластиковых карт и даты истечения срока действия, номера соцстрахования клиентов.

С учетом самых крупных утечек (120 млн записей, «ушедших» из Минфина Греции, 60 млн медицинских записей, скомпрометированных американской Службой внутренних доходов (Internal Revenue Service), более 100 млн данных пользователей, скомпрометированных в ходе атаки на Target) количество утечек переваливает за 561 млн записей, утекших из различных организаций в 2013 году.

РИА Новости. *Более 120 миллионов записей данных о налогах греческих граждан украли сотрудники компании в одном из пригородов Афин, сообщает сайт газеты «Этнос». По оценке специалистов, на «черном рынке» такой объем персональных данных можно продать за 100 тысяч евро.*

Соотношение количества утечек и объема утекших данных позволяет судить о том, в какой отрасли информацию защищают лучше, а в какой хуже. Если организации в определенной отрасли плохо справляются с относительно простой задачей сохранить в безопасности персональные данные, можно с уверенностью утверждать, что уровень защиты конфиденциальной информации в этой отрасли чрезвычайно низок.

На следующей диаграмме (см. Рисунок 9) отчетливо видно, что ситуация с защитой персональных данных в государственных органах более чем плачевна. За год из организаций этой категории утекло 247 млн. записей.

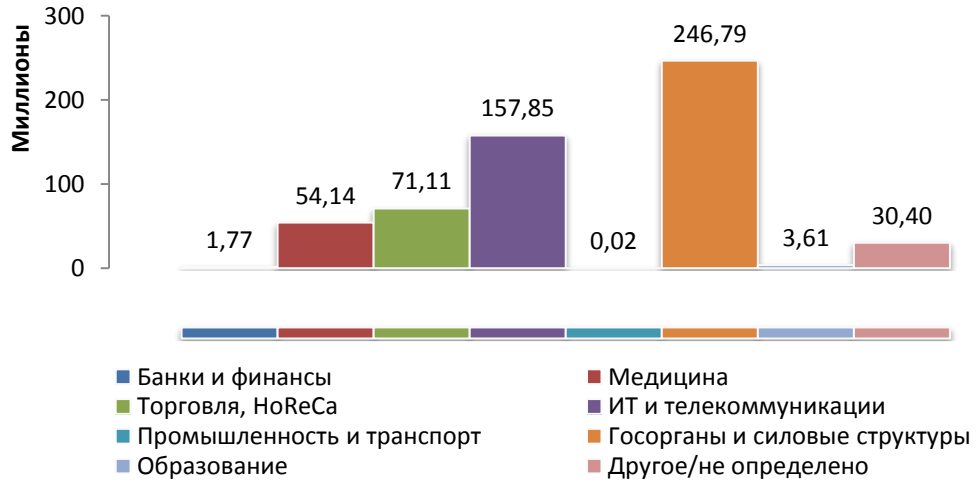


Рисунок 9. Количество скомпрометированных записей персональных данных по отраслям 2013 г., млн

На втором месте представители сферы ИТ и телекома (в основном, операторы), которые не уберегли 157 млн записей абонентов.

saharasamay.com: *Один из крупнейших операторов мобильной связи Германии Vodafone заявил о похищении личных данных 2 миллионов своих*

клиентов. Речь идет об именах, датах рождения, адресах абонентов, а также данных об их банковских счетах. В Vodafone отмечают, что злоумышленник имел доступ к конфиденциальной информации компании. Был ли подозреваемый сотрудником немецкого мобильного оператора и какой пост он занимал, собеседница уточнить не смогла.

Третье место (практически целиком за счет декабрьской утечки данных клиентов американских ритейловых сетей) осталось за торговыми компаниями и сегментом HoReCa.

krebsonsecurity.com: 70 миллионов имен, адресов электронной почты и телефонных номеров клиентов американского ритейлера Target (Target Corp. TGT:US) скомпрометированы в ходе атаки на инфраструктуру компании, сообщает сегодня в своем блоге Брайн Кребс. Реальный масштаб атаки раскрыт самой компанией Target в официальном заявлении 10 января. Пострадавшим клиентам Target пообещала бесплатно отслеживать все транзакции в течение года, чтобы предотвратить несанкционированное списание денежных средств. В базе Target, помимо номеров кредитных карт и персональных данных, хранилась номера соцстрахования (SSN) пользователей скидочной программы ритейлера.

На следующей диаграмме (см. Рисунок 10) показано среднее количество утекших записей (в млн) по каждой из отраслей. Госорганы и в этом разрезе занимают «достойное» место. Хотя, в расчете на одну утечку, больше записей уходит в том же ритейле и телекоммуникационных компаниях.

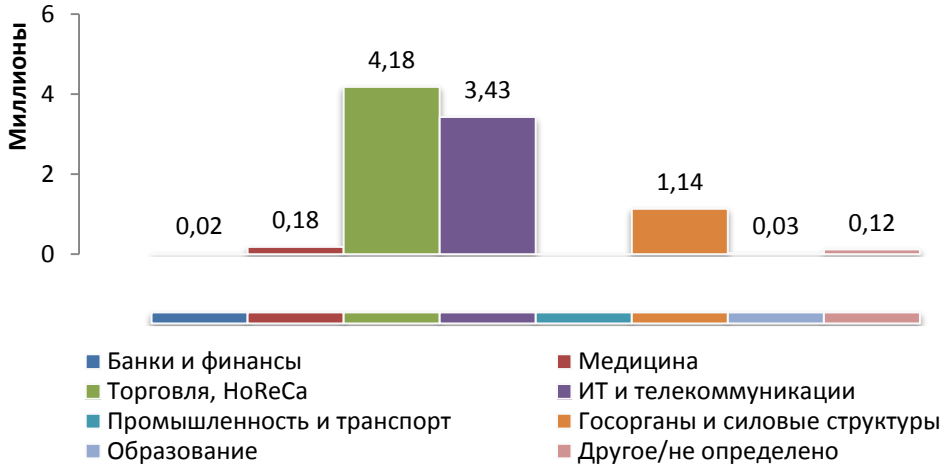


Рисунок 10. Среднее число утекших записей на одну утечку, 2013 г.

Утечки персональных данных являются своеобразным барометром уровня защищенности информации в той или иной отрасли. Потому в данном исследовании мы сформировали отраслевую карту утечек на основе сведений об утечках только одной категории информации – персональных данных. Сумма ущерба для каждого случая утечки берется из сообщений об утечках – это либо экспертная оценка, либо прямое высказывание представителей компании относительно масштаба материальных потерь. Сама по себе отраслевая карта утечек персональных данных довольно наглядна (см. Рисунок 11).

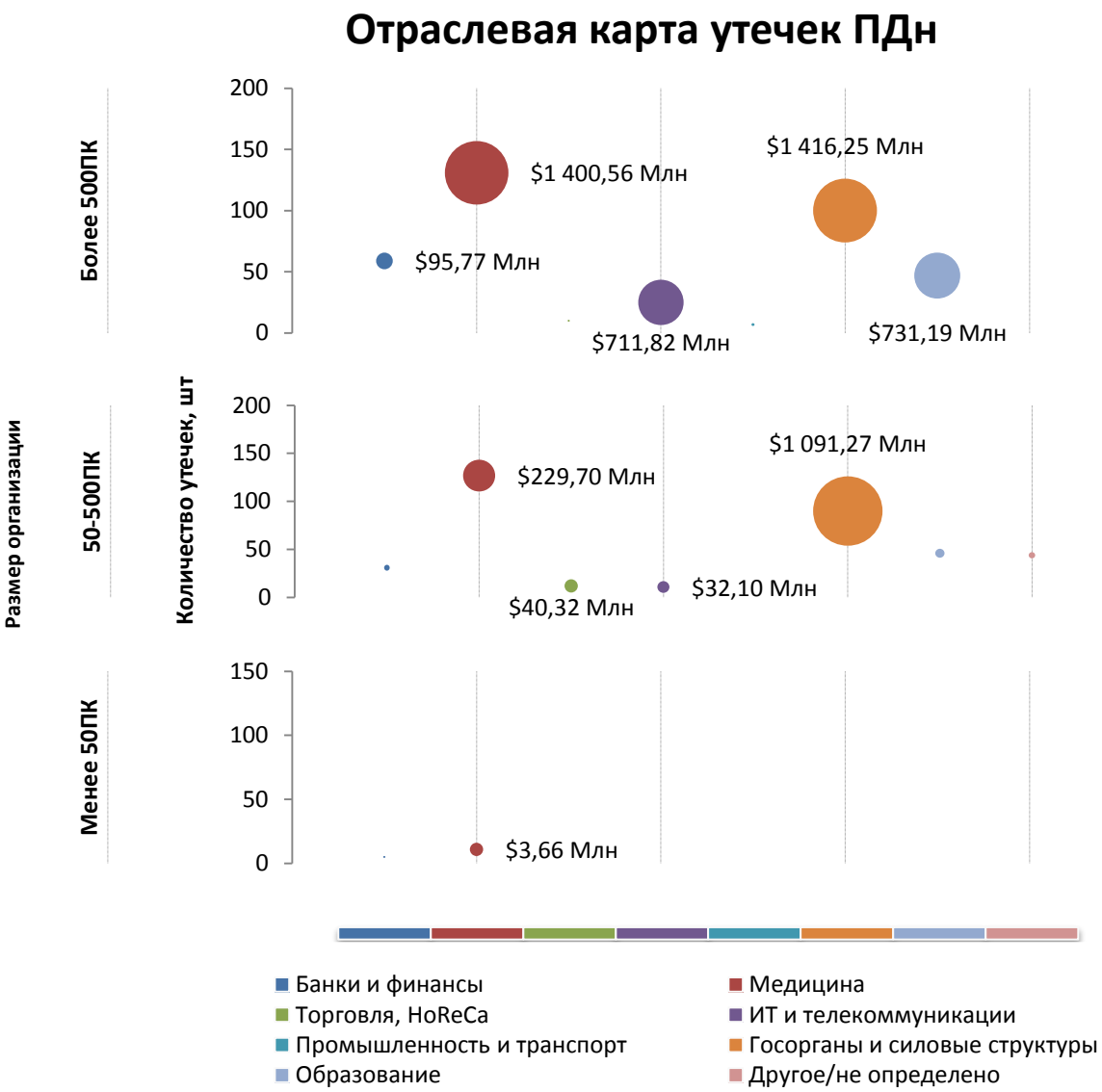


Рисунок 11. Отраслевая карта утечек персональных данных, 2013 г.

Обратим внимание лишь на один важный факт: компании среднего размера (до 500 ПК) в большинстве отраслей как по совокупному ущербу, так и по количеству утекших ПДн не отстают от крупных.

Вывод:

«Бум» утечек из госорганов и муниципальных организаций продолжается. Причем утекают персональные данные граждан. Защита такой информации – прямая обязанность госорганов, однако справляются они с этой задачей плохо, причем по всему миру. Огромное число утечек происходит из организаций среднего размера. Это говорит о том, что вопрос защиты ПДн от утечек для среднего бизнеса сегодня столь же актуален, как и для крупного.

Региональные особенности

В распределении утечек по регионам в 2013 году США традиционно заняли первую позицию по количеству утечек (679 или 59,41% от всех произошедших). Доля Америки по сравнению с предыдущим годом увеличилась на 2,2 п. п. По итогам года подтвердилось второе место России (134 утечки), которое досталось нашей стране еще по итогам I полугодия 2013 года.

> *Известия: В июле 2013 года произошла утечка базы данных клиентов международной страховой компании «Цюрих». Злоумышленники похитили полные данные более чем на 1 млн клиентов, заключивших за последние 1,5 года договоры страхования. В СК «Цюрих» размер возможного ущерба не комментируют.*
>
> Учитывая рост бизнеса компании[20] и выручку российского подразделения за 2012 год[21], эксперты InfoWatch оценивают ущерб от данного инцидента (включая репутационные потери и недополученную прибыль) в **2-2,5 млрд. руб.**, в том числе **4,4 млн руб.** - затраты на расследование и ликвидацию последствий инцидента.[22]

На третьем месте оказалась Великобритания (80 утечек). В первую пятерку впервые попала Германия с 48 утечками, и Канада, где зарегистрировано 33 утечки.

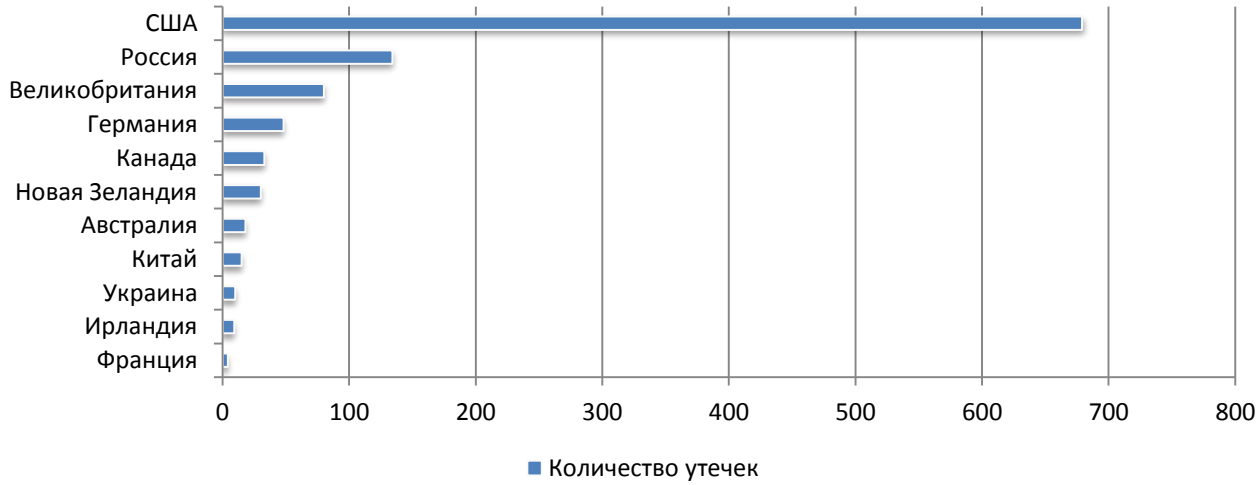


Рисунок 12. Распределение утечек по странам, 2013 г.

Даже на первый взгляд, ситуация с утечками данных в масштабах всего мира неоднородна. В англосаксонских странах утечкам придается огромное значение, а в восточной Европе и Азии бизнес и регуляторы еще не осознали, что утечки – серьезный фактор, влияющий на развитие и само существование бизнеса.

[20] http://www.zurich.com/internet/main/SiteCollectionDocuments/financial-reports/half-year-report-2013-en.pdf

[21] ООО СК «Цюрих» Форма №2-страховщик по ОКУД http://zurich.ru/upload/accounting/form2ooo.pdf
ЗАО «Цюрих надежное страхование» Форма №2-страховщик по ОКУД http://zurich.ru/upload/accounting/zao-form2.pdf

[22] Ущерб рассчитан по методике компании InfoWatch.

Впрочем, как авторы отмечали ранее, степень защищенности информации растет не только в «аглосаксонском» мире, но и в таких государствах, как Бразилия, Индия, Китай, страны Юго-Восточной Азии и Ближнего Востока. В 2013 году мы впервые зарегистрировали информационные сообщения об утечках данных в этих регионах.

> *city-of-hotels.ru: Гостиничные сети Китая не смогли защитить данные своих постояльцев. Как сообщает издание South China Morning Post, персональная информация о тысячах клиентов китайских отелей оказалась в широком доступе. Купить базу данных о бронировании номеров предлагалось на популярной китайской торговой платформе Taobao. За 8 гигабайт продавцы просили 2000 юаней. По информации китайских СМИ в сеть могла попасть персональная информация о бронировании как минимум 450 тыс. номеров, включая имена, адреса, места работы, телефонные номера из более 4500 отелей.*
>
> *www.todayszaman.com: Начальник Центрального банка Турции уволил 11 сотрудников Центробанка, в том числе трех топ-менеджеров, в связи с подозрением в том, что они поделились секретной информацией с организацией, участвующей в шпионской деятельности, пишет турецкая газета Today's Zaman.*

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Заключение и выводы

В 2013 году Аналитическим Центром InfoWatch зафиксирован самый большой (с 2008 года) рост числа сообщений об утечках конфиденциальной информации. Впервые за годы наблюдений число утечек превысило отметку в 1000 случаев. Этот рост авторы исследования традиционно связывают с повышенным вниманием регуляторов, государства, СМИ и других заинтересованных сторон к проблеме безопасности данных. И этого внимания в 2013 году было более чем достаточно, как в мире, так и в России.

Однако в истекшем году проявился еще один существенный фактор – снижение доли скрытых утечек информации. В результате зафиксированный рост утечек в большей степени обязан своим появлением как раз тому, что скрытых утечек стало меньше, а прозрачность темы утечек информации, наоборот, выросла.

Также следует отметить, что у компаний, заинтересованных в защите собственной информации, изменилось отношение к средствам защиты. Теперь технические решения применяются не только для того, чтобы выполнить требования регуляторов, но и для реального обеспечения информационной безопасности. В итоге это позволяет компаниям все лучше детектировать утечки, определять их тип, выявлять виновных.

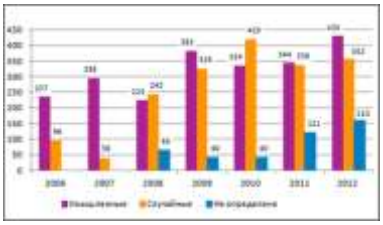
На утечки по «традиционным» каналам – почта, e-mail, бумажная документация, кража и потеря оборудования – по-прежнему приходится львиная доля случайных утечек. При этом доля «новых» каналов (те же мобильные устройства, голос и видео) пока остается незначительной. Соотношение каналов случайных и умышленных утечек в целом подтверждает тезис о значительном проникновении систем защиты в корпоративной среде.

«Бум» утечек из госорганов и муниципальных организаций продолжается. Причем утекают персональные данные граждан. Защита такой информации – прямая обязанность госорганов, однако справляются они с этой задачей плохо, причем по всему миру. Огромное число утечек происходит из организаций среднего размера. Это говорит о том, что вопрос защиты ПДн от утечек для среднего бизнеса сегодня столь же актуален, как и для крупного.

Мониторинг утечек на сайте InfoWatch

На сайте Аналитического Центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

Кроме того на сайте представлены статистические данные по утечкам информации за прошедшие годы, оформленные в виде динамических графиков.


Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Twitter
- RSS

Аналитический Центр InfoWatch

www.infowatch.ru/analytics

Глоссарий

Утечка конфиденциальной информации – *под утечкой мы понимаем действие или бездействие лица, имеющего легитимный доступ к конфиденциальной информации, которое (действие) повлекло потерю контроля над информацией или нарушение конфиденциальности этой информации.*

Конфиденциальная информация – *(здесь) информация, доступ к которой осуществляется строго ограниченным и известным кругом лиц с условием, что информация не будет передана третьим лицам без согласия владельца информации. В данном отчете в категорию КИ мы включаем информацию, подпадающую под определение персональных данных.*

Умышленные утечки – *случаи утечки информации, когда пользователь, работающий с информацией, предполагал возможные негативные последствия своих действий, осознавал их противоправный характер, был предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду. В результате создались условия для утраты контроля над информацией и/или нарушения конфиденциальности информации. При этом неважно, повлекли ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя.*

Неумышленные утечки – *к таковым относятся случаи утечки информации, когда пользователь не предполагал наступления возможных негативных последствий своих действий и не преследовал личной выгоды. При этом неважно, имели ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя.*

Канал утечки – *сложный сценарий (действия пользователя корпоративной информационной системы, направленные на оборудование или программные сервисы), в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. На данный момент мы различаем 8 самостоятельных каналов утечки:*

- ✓ *Кража/потеря оборудования (сервер, СХД, ноутбук, ПК), – компрометация информации в ходе обслуживания или потери оборудования.*
- ✓ *Мобильные устройства – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.*
- ✓ *Съемные носители – потеря/кража съемных носителей (CD, флеш-карты).*
- ✓ *Сеть – утечка через браузер (отправка данных в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов, нелегитимная публикация информации на веб-сервисе.*
- ✓ *Электронная почта – утечка данных через корпоративную электронную почту.*
- ✓ *Бумажные документы – утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации).*
- ✓ *IM – мессенджеры, сервисы мгновенных сообщений (утечка информации при передаче голосом, текстом, видео при использовании сервисов мгновенных сообщений).*
- ✓ *Не определено - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки».*