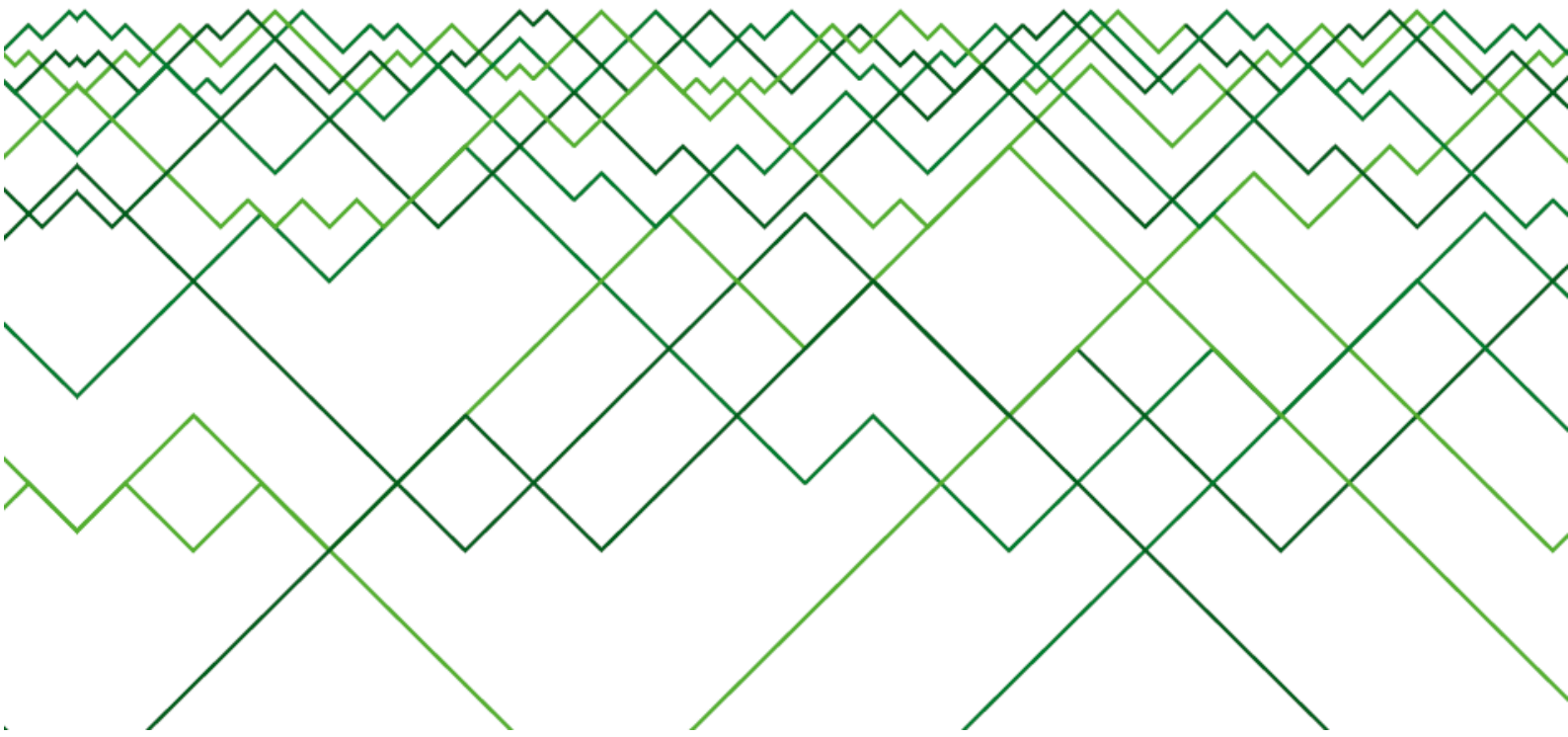
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аналитический Центр InfoWatch
www.infowatch.ru/analytics

Глобальное исследование утечек конфиденциальной информации в I полугодии 2013 года



INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Оглавление

Основные факты

- ✓ За первое полугодие 2013 год в мире зафиксировано, обнародовано в СМИ[1] и выявлено Аналитическим Центром InfoWatch **496** случаев утечки[2] конфиденциальной информации[3], что на **18%** превышает количество утечек за аналогичный период прошлого года.
- ✓ Скомпрометировано более **258 млн** записей, в том числе финансовые и персональные данные.
- ✓ Россия вышла на **второе место** по количеству опубликованных утечек, обогнав Великобританию. Число «российских» утечек в первом полугодии 2013 **выросло почти на треть**[4] – зарегистрировано **42 случая** утечки конфиденциальной информации из компаний на территории РФ.
- ✓ Доля утечек в госорганах и муниципальных учреждениях по всему миру остается стабильно высокой – **30%.** Именно госорганы, наряду с медицинскими учреждениями, являются основным источником утечек персональных данных.
- ✓ Количество утечек персональных данных из компаний среднего (от 50 до 500 ПК) размера и число скомпрометированных записей немногим отличаются от количества утечек и числа записей, связанных с крупными компаниями.
- ✓ Больше всего утечек информации связано с персональными данными – в **93,8%** случаев утекает именно эта информация.
- ✓ Обнародованный в СМИ ущерб (затраты на ликвидацию последствий утечек, судебные разбирательства, компенсационные выплаты), который понесли компании вследствие утечек информации в I полугодии 2013 года, составляет **3,67** млрд долларов.

[1] А также в блогах и форумах.

[2] Утечка конфиденциальной информации – инцидент информационной безопасности, действие или бездействие лица, имеющего легитимный доступ к конфиденциальной информации, которое повлекло потерю контроля над информацией или нарушение конфиденциальности этой информации.

[3] Конфиденциальная информация (КИ) – (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 также информацию, подпадающую под определение государственной, коммерческой, иных видов тайн.

[4] По сравнению с аналогичным периодом прошлого года.

Аннотация

Аналитический Центр компании InfoWatch представляет отчет об исследовании утечек конфиденциальной информации в I полугодии 2013 года.

Всестороннее исследование утечек конфиденциальной информации позволяет **оценить уровень защищенности информации от утечек** в коммерческих компаниях, государственных организациях, образовательных учреждениях. Причем эта оценка базируется не только на количестве утечек, но и на таком параметре, как число утекших записей. Так рост числа утекших записей в расчете на одну утечку, который мы наблюдаем в последнее время, говорит о недостаточной защищенности информации даже в большей степени, чем рост количества утечек.

В данном отчете авторы впервые в практике Аналитического Центра InfoWatch используют число утекших записей в качестве одной из основных метрик **для составления отраслевой карты утечек**. Сама карта утечек[5], содержащая сведения о количестве утечек и общем числе утекших записей, также составлена впервые. На одной диаграмме сведена информация об утечках персональных данных (ПДн) из компаний различного размера и разных отраслей.

В данном исследовании закладывается фундамент для более глубокого изучения вопросов защиты конфиденциальной информации **как в разрезе отраслей, так и в разрезе размеров бизнеса**.

Исследование утечек конфиденциальной информации в масштабе всего мира позволяет сопоставить общую картину утечек в более «продвинутых» (США, Великобритания) и менее развитых в плане регулирования темы информационной безопасности регионах (страны Европы). 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.

Следует уже сегодня подготовиться 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**. И в этом смысле анализ картины утечек в зарубежных странах, наиболее «продвинутых» в деле борьбы с утечками, будет более чем полезен для российского рынка.

Только так, на реальных примерах, отечественные компании смогут оценить значение и степень опасности утечки конфиденциальной информации для своего бизнеса, а законодатели и регуляторы – смоделировать воздействие на рынок тех или иных инициатив.

По сравнению с предыдущими исследованиями, авторы уточнили ряд спорных моментов. Введено деление компаний по отраслям и по размеру парка персональных компьютеров (ПК), скорректирована классификация каналов утечек.

[5] См. раздел «Отраслевая карта».

Методология

Исследование основывается на собственной базе данных, которая пополняется специалистами Центра с 2004 года. В базу InfoWatch включаются утечки, которые произошли в организациях в результате злонамеренных или неосторожных действий сотрудников и были **обнародованы в СМИ** или других **открытых источниках** (включая web-форумы и блоги). В настоящее время база утечек InfoWatch насчитывает несколько тысяч зарегистрированных инцидентов.

Классификация инцидентов в базе утечек осуществляется сотрудниками Аналитического Центра InfoWatch. В ходе наполнения базы каждая утечка (если возможно и такая информация есть в сообщении об утечке) классифицируется по ряду критериев: размер организации, сфера деятельности (отрасль), ущерб, тип утечки[6] (умысел), канал утечки[7], типы утекших данных и пр.

Данные об ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций в СМИ.

Исследование охватывает незначительное (не более 1-5%) число от реальных утечек, произошедших в мире. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества (категории) содержали достаточное или избыточное количество элементов (фактических случаев утечки). Так по критерию «размер компании» мы выделяем три категории (множества) – небольшие, средние, крупные, по критерию «тип утечки» выделяем два – умышленные и неумышленные и т. д. Такой подход к формированию предмета исследования **позволяет считать получившуюся выборку теоретической, а исследование на выборке 1-5% репрезентативным для генеральной совокупности**.

Для сохранения однородности выборки при составлении отраслевой карты мы целенаправленно вывели за рамки исследования утечки с несоразмерно большим количеством утекших персональных данных – например, если наблюдалось превышение среднего числа утекших данных на 3-4 порядка (всего 4 инцидента, в ходе которых «утекло» более 240 млн записей). Для составления отраслевой карты

[6] Мы разделяем утечки информации по признаку умысла (намерения) на умышленные (злонамеренные) и неумышленные (случайные). К умышленным утечкам относятся случаи утечки информации, когда пользователь, работающий с информацией, знал или предполагал возможные негативные последствия своих действий, был предупрежден об ответственности. Однако, в нарушение установленных правил работы с информацией, он совершил поступок, повлекший утрату контроля над информацией и нарушение конфиденциальности информации. При этом неважно, имели ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. Под случайными (неумышленными) утечками мы понимаем такие случаи, когда пользователь не знал и не предполагал наступления возможных негативных последствий, не был предупрежден об ответственности. Термины умышленные – злонамеренные и неумышленные – случайные (попарно) равнозначны и употребляются здесь как синонимы.

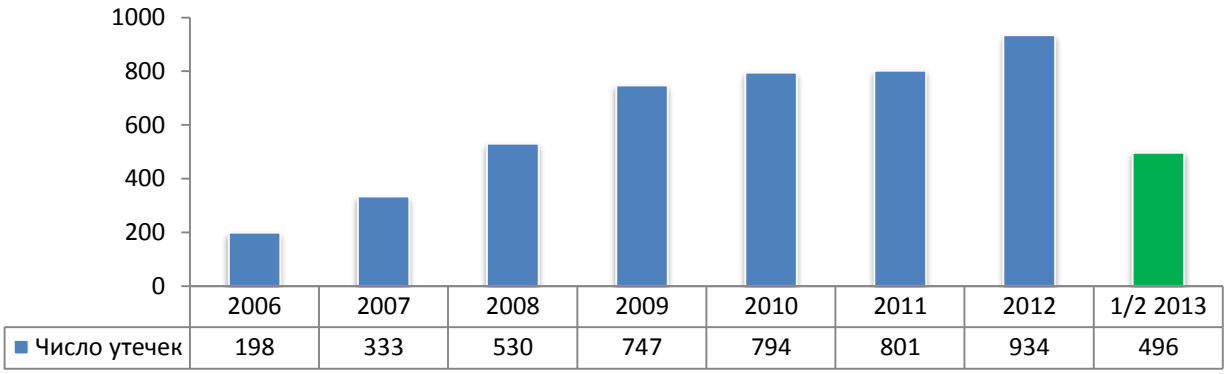
[7] Под каналом утечки мы понимаем сложный сценарий (действия (или бездействие) пользователя корпоративной информационной системы, направленные на оборудование или программные сервисы), в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. Классификация каналов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

утечки с незначительным (менее 100) количеством «ушедших» записей также 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 относящиеся к утечкам, в данном отчете не рассматриваются.

Общая статистика

За I полугодие 2013 года Аналитическим Центром InfoWatch зарегистрировано 496 (2,7 в день, 82,6 в месяц) случаев утечки конфиденциальной информации. Это на 18% больше, чем за аналогичный период 2012 года (419 утечек). В исследуемый период динамика роста утечек была на 2 процентных пункта (п. п.) выше, чем в 2012 году (тогда рост к 2011 году составил 16%). Если такая динамика сохранится, в 2013 году число утечек может впервые за годы наблюдений превысить отметку в 1000 случаев.



	2006	2007	2008	2009	2010	2011	2012	1/2 2013
Число утечек	198	333	530	747	794	801	934	496

Рис.1. Количество утечек информации, 2006 - ½ 2013 г.

Рост количества утечек мы традиционно связываем с повышенным вниманием регуляторов, государства, СМИ и других заинтересованных сторон к проблеме безопасности данных.

Данный фактор актуален и для России. По сравнению с аналогичным периодом 2012 года, число «российских»[8] утечек в первом полугодии 2013 выросло на 27%. Зарегистрировано 42 случая утечки информации из российских компаний и госорганов.

Баланс умышленных и случайных утечек (см. рис. 2) несущественно отличается от картины, выявленной в прошлом году. Доля умышленных утечек выросла на 3 п. п. Доля случайных увеличилась на 8 п. п.

Рост долей утечек обоих типов произошел за счет сокращения и перераспределения доли утечек категории «не определено». Соответственно, доля утечек этой категории снизилась.

[8] Утечек информации из компаний, расположенных на территории РФ.

В СМИ все чаще появляется информация с явным указанием типа утечки, должности злоумышленника или сотрудника, допустившего утечку по неосторожности. Во многих случаях источником такой информации являются сами пострадавшие компании, которые с помощью технических средств защиты выявляют инциденты и злоумышленников, ранее остававшихся незамеченными.

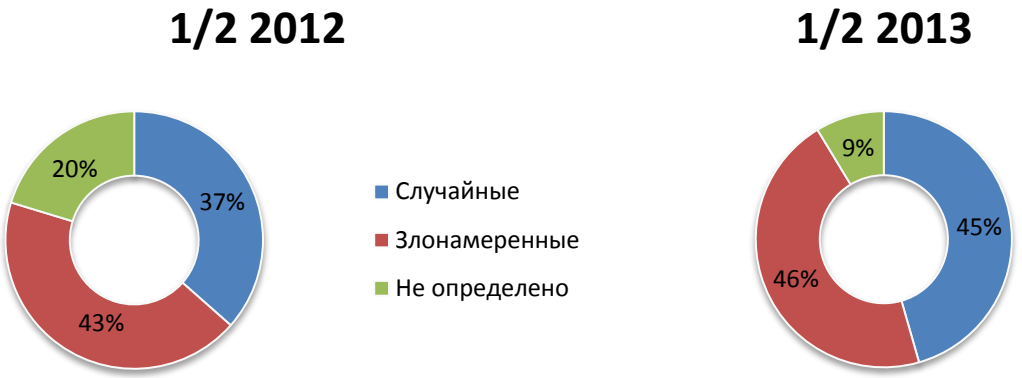
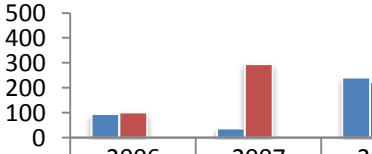


Рис.2. Соотношение случайных и умышленных утечек, ½ 2012 - ½ 2013 г.

Во многих случаях компании могут установить не только тип утечки (умышленно или случайно), но и виновника.

The New Zealand Herald. Более 80 000 жителей Крайстчерч (Новая Зеландия) стали жертвами утечки персональных данных по вине неосторожных действий членов Комиссии по землетрясениям. Данный инцидент стал одним из крупнейших нарушений конфиденциальности информации, когда-либо допущенных государственной организацией страны. Утечка произошла в результате ошибочной отправки на адрес бывшего подрядчика Комиссии электронного письма, содержащего заявления на компенсацию ущерба от землетрясения с указанием персональных данных жителей Крайстчерч.

Динамика случайных и злонамеренных утечек за последние 6 лет показана на гистограмме (рис. 3). Как видно из гистограммы, соотношение случайных и намеренных утечек, начиная с 2008 г., колеблется, но остается примерно одинаковым.



	2006	2007	2008	2009	2010	2011	2012	1/2 2013
Случайные	96	38	242	325	420	336	352	226
Умышленные	102	295	223	382	334	344	430	227
Не определено	0	0	65	40	40	121	152	43

Рис. 3. Динамика соотношения случайных и умышленных утечек, 2006 - ½ 2013 г.

9% утечек в категории «не определено» (43 зарегистрированных случая за исследуемый период) – это немало. Снижение доли утечек этой категории, скорее всего, продолжится, но сама категория «неопределенных» утечек не исчезнет – зачастую установить, была утечка умышленной или случайной, объективно не представляется возможным. Например, когда речь идет о краже ноутбуков, потере мобильных устройств или флешек. Не всегда ясно, действительно потерян носитель, или его владелец заявил об этом, чтобы скрыть факт разглашения конфиденциальных данных.

> *Пользователь, легитимно работая с информацией на корпоративном ноутбуке, обычно не ожидает негативных последствий, оставляя устройство в автомобиле. Кража ноутбука приведет к утечке данных (если информация на устройстве не зашифрована). При этом пользователь может инсценировать кражу, передав важную информацию конкуренту. Это уже умышленная утечка.*

Защититься от утечки типа «потеря устройств» или «кража носителей» можно лишь в случае, если организация занимает твердую позицию в вопросе политики использования мобильных носителей. Например, можно запретить использование мобильных носителей вообще или обязать использовать только шифрованные носители информации, принудительно шифровать информацию на корпоративных ноутбуках. Но на это идут далеко не все.

> *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.*

Сценарии утечек, связанные с потерей резервных копий, компрометацией данных при ремонте оборудования также выполняются лишь при отсутствии в компании жестко установленных правил обращения с информацией и носителями информации.

> ***Вывод:***
>
> *Рост количества утечек конфиденциальной информации продолжается. Причем темпы роста в этом году опережают аналогичные показатели прошлого года. Позитивной тенденцией следует считать сокращение доли утечек неопределенного характера в распределении утечек по умыслу. Это может означать, что компаниям удается все лучше детектировать утечки, определять их тип, выявлять виновных.*

Каналы утечек[9]

Канал утечек – параметр, который имеет прямое практическое приложение. В зависимости от частоты утечек по тому или иному каналу можно планировать внедрение средств защиты на предприятии, определить, какими каналами следует заниматься в первую очередь.

К сожалению, динамика изменения долей утечек по каналам не может рассматриваться в качестве показателя эффективности систем защиты от утечек. Доля утечек по каналам, которые можно перекрыть техническими средствами защиты, не сокращается. Наоборот, распространение технических средств защиты как бы «провоцирует» рост доли утечек через эти каналы.

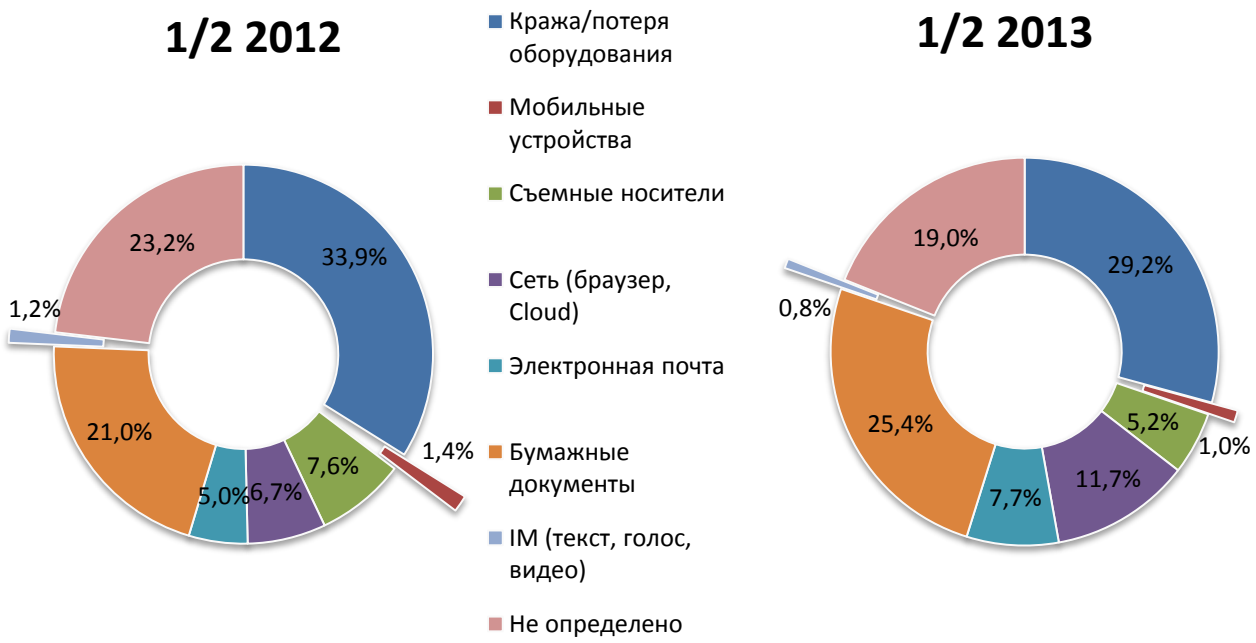


Рис. 4. Распределение утечек по каналам, ½ 2012 - ½ 2013 гг.

Наблюдается удивительная ситуация: если канал контролируется лучше, утечки по этому каналу регистрируются чаще – компании обнаруживают утечки, которые они ранее не замечали.

О все большем распространении средств борьбы с утечками также свидетельствует сокращение доли утечек неясной природы (категория «Не определено»).

> *Отсюда следует довольно парадоксальный вывод – распространение технических средств защиты ведет к увеличению доли утечек по каналам, которые контролируются этими средствами защиты. Компании-владельцы информации с помощью технических средств «ловят» все больше утечек, которые раньше оставались незамеченными.*

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

По итогам I полугодия 2013 года доля утечек через сеть (использование браузера для передачи информации, компрометация данных вследствие ошибочной публикации в веб), выросла почти вдвое (11,7% против 6,7% в первом полугодии 2012 г.). Утечки через электронную почту составляют 7,7% (что наполовину превышает долю утечек через e-mail за аналогичный период 2012 г.).

Растет доля утечек, связанных с бумажными документами (до 25,4% или на 4,4 п. п.), незначительно колеблется доля утечек через мобильные устройства (потеря и кража смартфонов, планшетов). Такая низкая доля утечек через мобильные устройства объясняется, во-первых, тем, что люди не используют мобильные для хранения информации, продолжая по инерции пользоваться разными другими накопителями информации, включая бумажные. Во-вторых, рискнем предположить, что мобильные устройства довольно плохо контролируются предприятиями, а посему утечки с них остаются нераскрытыми и неизвестными.

Наблюдается снижение доли канала «кража/потеря оборудования» на 5 п. п. при том, что с 2013 года мы относим к утечкам по этому каналу не только случаи компрометации данных при краже или сервисном обслуживании ПК, серверов, другого оборудования (в т. ч. СХД), но и компрометацию информации при потере ноутбуков.

Теперь рассмотрим, насколько отличается в разрезе каналов распределение умышленных и случайных утечек.

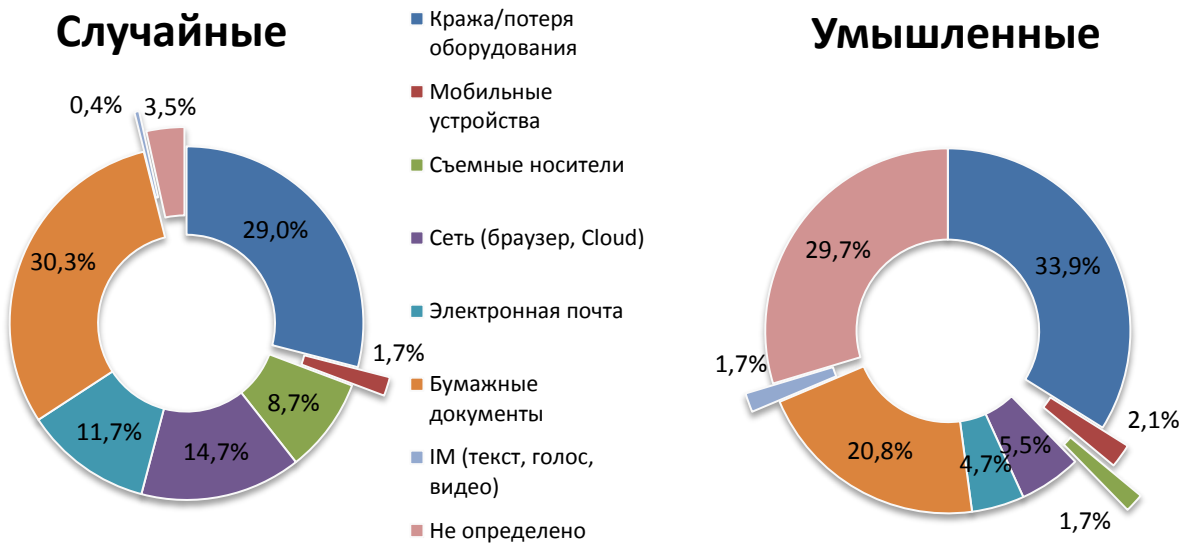


Рис. 5. Распределение случайных и умышленных утечек по каналам, ½ 2013 г.

Доля случайных и умышленных утечек, связанная с использованием мобильных устройств, остается незначительной. Во многом, это ответ на заявления некоторых экспертов о якобы чрезвычайной угрозе распространения мобильных устройств в корпоративной среде. Действительно, с мобильного устройства можно отправить конфиденциальный документ, и защищать этот канал нужно. Да и изучены эти утечки недостаточно, как мы отмечали выше. Однако «популярностью» этот канал явно не

пользуется – «большие» утечки чаще связаны с давно известными каналами – электронной почтой, сетью, бумажной документацией, кражей ноутбуков.

> *komonews.com. У шерифа округа Кинг (Вашингтон, США) из автомобиля был похищен корпоративный ноутбук, где находились персональные данные нескольких тысяч американцев (включая номера соцстрахования и водительских удостоверений). Руководство King County Sheriff's Office сообщило, что на 60 % компьютеров был уже установлен крипто-защитный софт, однако на похищенном ноутбуке не было программ по шифрованию данных.*

Логичным выглядит большая доля случайных утечек через съемные носители – флешки теряются часто. И это при том, что ограничить использование флешек или заблокировать USB-порты технически возможно. Почему это не делается – большой вопрос.

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.*

Соотношение доли случайных и умышленных утечек по каналам подтверждает тезис о том, что технические средства защиты пока лучше ориентированы на обнаружение и предотвращение случайных утечек. Доли умышленных утечек через электронную почту, сеть, съемные носители намного меньше долей случайных утечек по тем же каналам.

Остается упомянуть еще один, довольно экзотический канал – утечки информации через сервисы мгновенных сообщений. Данный канал представлен незначительными 0,4% на диаграмме случайных утечек. Между тем 1,7% злонамеренных утечек прошли именно по этому каналу – аргумент в пользу старой истины, что в информационной безопасности не бывает «мелочей» и неважных, периферийных каналов утечек.

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

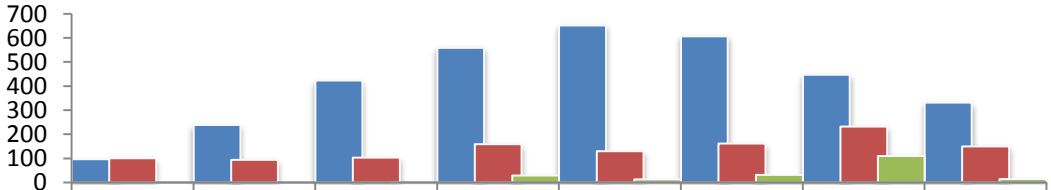
утечек. Компании пока не научились обеспечивать безопасность даже на этих каналах. При этом доля «новых» каналов – те же мобильные устройства – пока остается незначительной.

Отраслевая карта[10]

2012 год во всем мире стал годом утечек из государственных учреждений (см. Исследование утечек информации из компаний и госучреждений России 2012). Статистика за I полугодие 2013 года показывает, что государственные органы своего неуважительного отношения к проблеме утечек информации не изменили. Более того, доля утечек из государственных учреждений даже увеличилась за I полугодие 2013 года на 1 п. п., составив 30%.

Рис.6. Соотношение случайных и умышленных утечек, ½ 2012 - ½ 2013 гг.

Рост доли «коммерческих» утечек произошел за счет сокращения доли утечек из компаний «неопределенной» категории. Ретроспективный же анализ количества утечек по этому параметру дает нам следующую картину (см. рис. 7):



	2006	2007	2008	2009	2010	2011	2012	1/2 2013
Коммерческие	97	239	423	559	651	607	447	332
Государственные	101	94	104	159	130	162	232	150
Не определено			3	29	13	32	110	14

Рис. 7. Соотношение количества утечек по типу компании, 2006 - 1/2 2013 гг.

Обратим внимание, что с 2008 года доля утечек из госорганов и муниципальных организаций по отношению к доле утечек из коммерческих компаний изменялась

[10] В данном отчете мы впервые даем картину утечек информации в разрезе отраслевой принадлежности компаний.

незначительно (исключением явился послекризисный 2009 год). На этом фоне «бум» «государственных» утечек 2012-2013 годов выглядит неожиданным. Причем большинство утечек связано с компрометацией персональных данных (ПДн).

Распределение утечек по типу данных приведено на рис. 8. Еще год назад мы говорили о снижении доли ПДн в общей картине утечек (до 89,4%). Вынуждены констатировать, что утечек персональных данных вновь стало больше (93,8%).

С учетом самых крупных утечек (120 млн записей, утекших из Минфина Греции, 60 млн медицинских записей, скомпрометированных американской Службой внутренних доходов (Internal Revenue Service), ряд других случаев) количество утечек переваливает за 258 млн записей, утекших из различных организаций за первое полугодие 2013 года.

> *МОСКВА, 8 янв — 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.*

За исследуемый период зафиксировано лишь 4 случая утечек, где число записей превышало 1 млн, при этом совокупное число утекших записей в ходе этих четырех утечек составило более 240 млн (более 93% от числа всех записей). Поэтому, составляя отраслевую карту утечек ПДн, мы не включили крупнейшие утечки в выборку во избежание неверного представления отраслевой картины утечек. Также исключены из статистики случаи, когда «утекло» менее 100 записей.

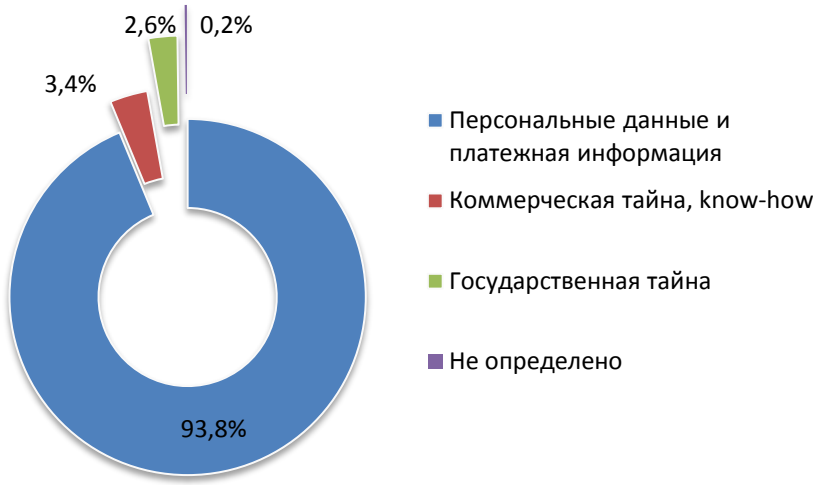


Рис.8. Распределение утечек по типам данных, ½ 2013г.

В отличие от утечек сведений, составляющих коммерческую или государственную тайну, утечки персональных данных обычно «обходятся» компаниям-владельцам информации дешевле. Так, лишь один случай кражи технологий может привести к многомиллионным убыткам.

> *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 в краже были обвинены три конкретных человека: два работника Sinovel Wind Group — Су Лиин (Su Liying) и Чжао ХайЧунь (Zhao Haichun) — и Деян Карабашевич, бывший сотрудник дочернего предприятия AMSC в Австрии.

Применительно к персональным данным ущерб в сотни миллионов долларов представить все-таки сложно. Однако именно утечки персональных данных являются своеобразным барометром уровня защищенности информации в той или иной отрасли.

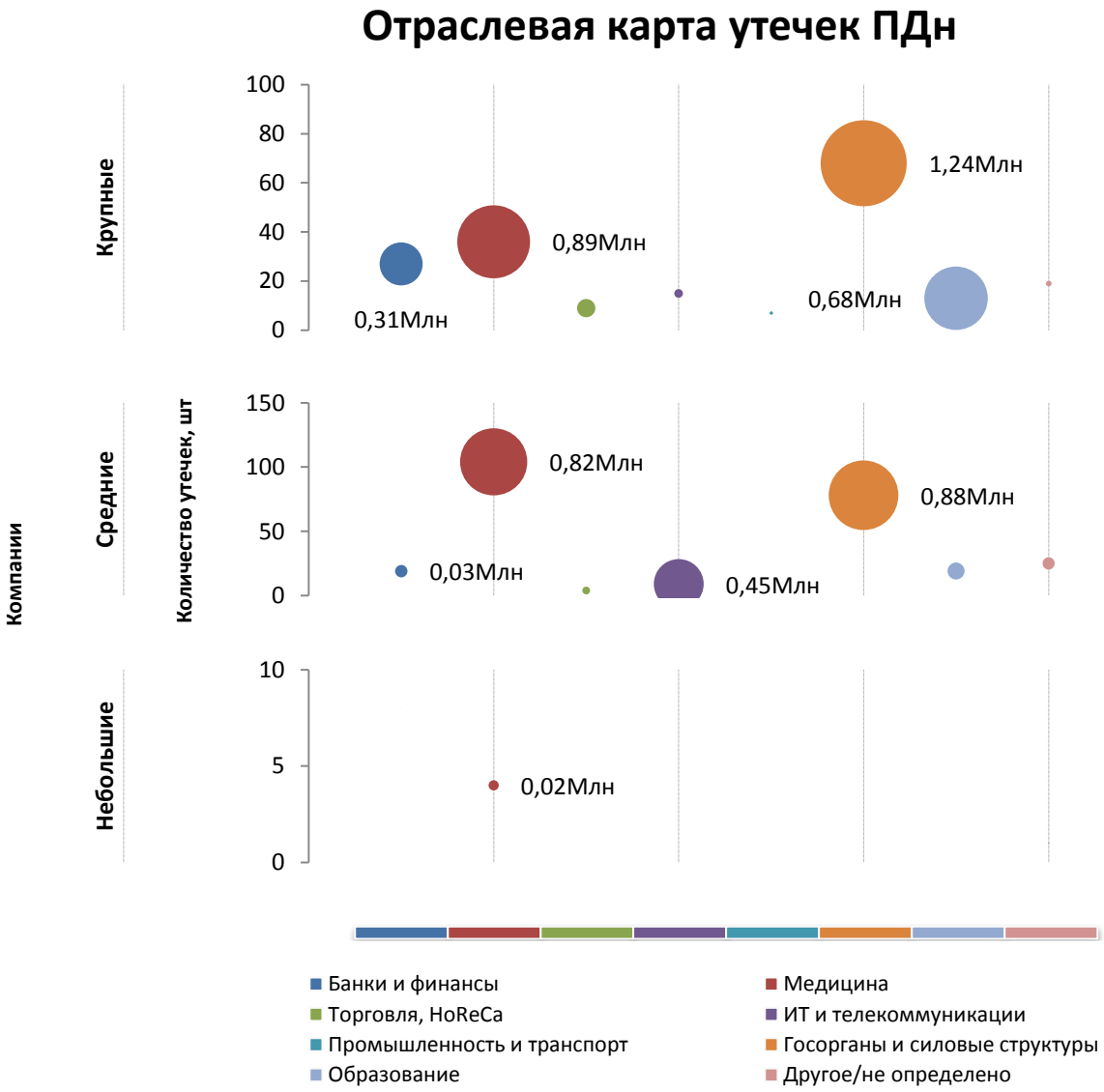


Рис. 9. Отраслевая карта утечек персональных данных, ½ 2013 г.

Соотношение количества утечек и объема утекших данных позволяет судить о том, в какой отрасли информацию защищают лучше, а в какой хуже. Если организации или госкомпании 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.

Отраслевая карта утечек персональных данных приведена на рис. 9. На диаграмме видно, что госорганы и муниципальные учреждения являются крупнейшими «поставщиками» новостей об утечках персональных данных. Нами зарегистрировано 68 случаев утечек ПДн из крупных[11] госорганов, 78 утечек из средних. В общей сложности только из госорганов утекло 2,12 млн записей о гражданах (на диаграмме суммарное количество утекших данных из той или иной отрасли обозначено размером «пузырька», а число утечек откладывается по вертикальной оси). [12]

На втором месте по количеству случаев утечки информации (149) располагаются медучреждения (1,73 млн утекших записей), на третьем (53 случая) – финансовые организации (0,33 млн утекших записей).

На рис. 10 показано среднее количество утекших записей (в млн) по каждой из отраслей. Госорганы и в этом разрезе занимают «достойное» место. Больше записей в расчете на одну утечку уходит только в ИТ- и телекоммуникационных компаниях, а также из образовательных учреждений (крупные утечки в университетах, образовательных центрах).

Рис. 10. Среднее число утекших записей на одну утечку, ½ 2013 г.

Сама по себе отраслевая карта утечек персональных данных довольно наглядна. Обратим внимание лишь на один важный факт: компании среднего размера (до 500 ПК) в большинстве отраслей как по числу утечек, так и по количеству утекших ПДн не отстают от крупных. А в некоторых отраслях (ИТ и телекоммуникации) даже превосходят.

Вывод:

[11] Размер компаний определяется по количеству персональных компьютеров, что более показательно, чем деление по обороту бизнеса. К крупным компаниям мы относим организации с числом ПК более 500, средние – 50-500 ПК, малые – менее 50 ПК.

[12] Возможно несовпадение цифр в тексте и диаграмме, так как при составлении диаграммы мы исключили единичные в своем роде случаи утечки (несопоставимо большой объем утекших ПДн). Кроме того, некоторые данные на диаграмме перекрыты другими «пузырьками» и не отображаются.

«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. Новый рост доли утечек персональных данных в общей картине утечек объясняется именно слабостью госорганов в деле защиты персональных данных. С другой стороны, 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 I половине 2013 года США традиционно заняли первую позицию по количеству утечек (312 или 62,9% от всех произошедших). Доля Америки по сравнению с предыдущим годом увеличилась на 5 п. п. Сюрпризом стало второе место России (42 утечки), которой удалось на 1 утечку опередить Великобританию.

Zabmedia. Оловяннинский мировой суд привлек к ответственности директора МУП «ЖКХ Ясная» (Забайкальский край) Александра Пешкова за то, что тот в нарушение законодательства о защите персональных данных обнародовал список должников с указанием фамилии, имени, отчества, адреса и суммы задолженности каждого. Список должников по состоянию на 1 апреля был размещен на стенде предприятия.

Традиционно в первой пятерке оказались Канада и Новая Зеландия. Еще одна неожиданность – шестое место Германии с 13 зафиксированными утечками.

Рис. 11. Распределение утечек по странам, ½ 2013 г.

Заключение и выводы

В I полугодии 2013 году Аналитическим Центром InfoWatch зарегистрировано **496** случаев утечки конфиденциальной информации, что на 18% больше, чем за тот же период прошлого года.

Почти треть утечек пришлась на госорганы и муниципальные учреждения. Увеличилась доля случаев, когда точно известен тип утечки (умышленная или нет), источник утечки (из какой компании ушла информация). Это говорит о готовности компаний не только раскрывать факт утечки (естественно, под давлением регуляторов и законодательства), но и проводить тщательные расследования причин инцидента.

По-прежнему большая часть утечек касается персональных данных — 93,8% случаев. За I полугодие 2013 года по всему миру скомпрометировано более 258 млн записей, в том числе финансовые данные, номера полисов социального страхования, медицинская информация, иные персональные данные.

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.

Все перечисленное заставляет признать, что уровень защищенности информации в мире (в том числе персональных данных) все еще очень низок. Распространение систем мониторинга и предотвращения утечек, противодействия внутренним угрозам позволяет в какой-то мере сгладить ситуацию в отдельных отраслях (банки и финансы, ИТ и телеком). Однако для остальных отраслевых вертикалей положение дел с защитой информации нельзя считать удовлетворительным.

Причем это касается как информации общего характера (персональные данные), так и критически важных для бизнеса сведений (коммерческая тайна, know-how).

Обнародованный в СМИ ущерб (затраты на ликвидацию последствий утечек, судебные разбирательства, компенсационные выплаты), который понесли компании вследствие утечек информации в I полугодии 2013 года, составляет 3,67 млрд долларов.

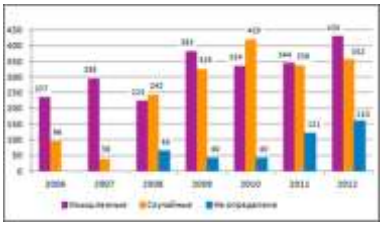
Напомним, что речь идет лишь о публичных утечках, ставших достоянием СМИ - это 1-5% от всех утечек. С учетом этого факта, размер возможного ущерба компаний от утечек идет на десятки, если не сотни миллиардов долларов.

Мониторинг утечек online

На сайте аналитического агентства InfoWatch регулярно публикуются:

- Отчеты по утечкам информации
- Самые громкие инциденты утечек с комментариями экспертов InfoWatch

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


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

- Почтовая рассылка
- Facebook
- Twitter
- RSS

Аналитическое агентство InfoWatch

www.infowatch.ru/analytics

Глоссарий

Утечка конфиденциальной информации *–инцидент информационной безопасности. Под утечкой мы понимаем такое действие или бездействие лица, имеющего легитимный доступ к конфиденциальной информации, повлекшее 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 государственной, коммерческой, иных видов тайн.*

Умышленные утечки *– к таковым относятся случаи утечки информации, когда пользователь, работающий с информацией, знал или предполагал возможные негативные последствия своих действий, был предупрежден об ответственности, однако, в нарушение установленных правил работы с информацией, он совершил поступок, повлекший утрату контроля над информацией и нарушение конфиденциальности информации. При этом неважно, имели 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 знал и не предполагал наступления возможных негативных последствий, не был предупрежден об ответственности. 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 оборудования. Нелегитимное использование оборудования не предполагается.*
- ✓ *Мобильные устройства – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства.*
- ✓ *Съемные носители – потеря/кража съемных носителей.*
- ✓ *Сеть – утечка через браузер (отправка данных в личную почту, формы ввода в браузере), нелегитимное использование FTP, облачных сервисов.*
- ✓ *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».*