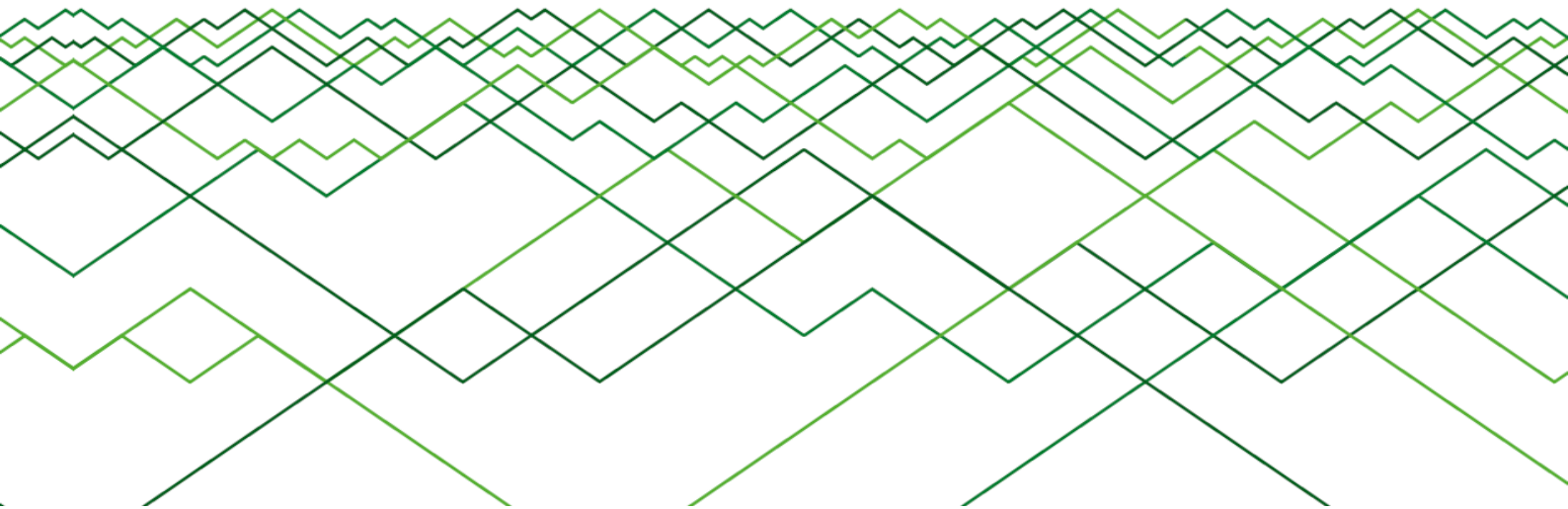
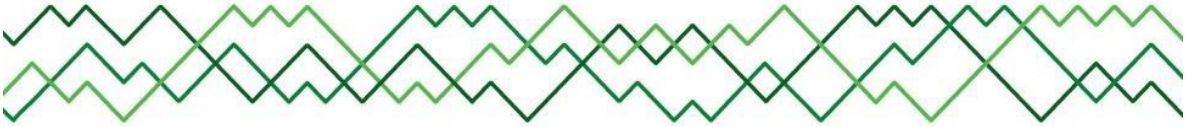
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

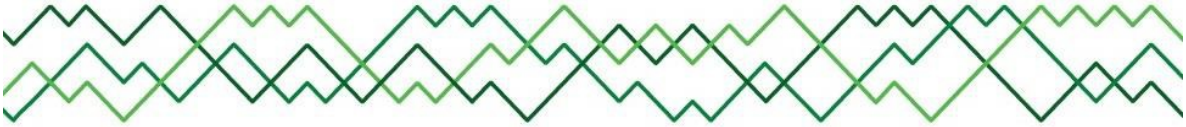
Аналитический центр InfoWatch
www.infowatch.ru/analytics

Глобальное исследование утечек конфиденциальной информации в I полугодии 2016 года





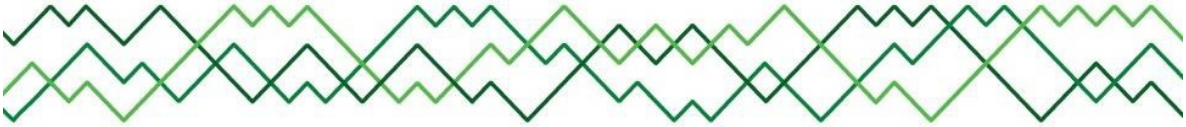
Оглавление



INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Только цифры

- ✓ В I полугодии 2016 года в мире обнародовано (в СМИ и иных источниках) и зарегистрировано Аналитическим центром InfoWatch **840** случаев утечки конфиденциальной информации, что на **16%** превышает количество утечек, зарегистрированных за аналогичный период 2015 года.
- ✓ В результате утечек скомпрометировано **1,06 млн** персональных данных (записей ПДн, платежных данных), - номера социального страхования, реквизиты пластиковых карт, иная критически важная информация.
- ✓ Внешние атаки стали причиной **33%** утечек данных. В **67%** случаев утечка данных произошла под воздействием внутреннего нарушителя.
- ✓ За I полугодие 2016 году зафиксировано **23** «мега-утечки». В результате каждой «утекло» более **10 млн** персональных данных. На «мега-утечки» пришлось **92%** всех скомпрометированных записей.
- ✓ В **67%** случаев виновными в утечке информации оказались сотрудники компаний. В **1%** случаев – высшие руководители организаций.
- ✓ Россия заняла второе место по числу утечек, ставших достоянием общественности. В исследуемый период зарегистрировано **110** случаев утечки конфиденциальной информации из российских компаний и государственных организаций.



Аннотация

Аналитический Центр компании InfoWatch представляет отчет об исследовании утечек конфиденциальной информации в I полугодии 2016 года.

Сообщения об утечках не сходят со страниц СМИ, что связано как с масштабом явления (сотни миллионов скомпрометированных данных), так и с громкими именами компаний, пострадавших от утечек: Alibaba, Amazon, American Express, Apple, Baidu, Blizzard Entertainment Inc, BMW, Credit Suisse Group AG, Dell, eBay, Etihad Airways, Facebook, Google, Huawei, id Software, IRS, LinkedIn, McDonald's, Microsoft, MySpace, Neiman Marcus Group, Nokia, Seagate Technology, Time Warner Cable, T-Mobile, Tumblr, Twitter, Uber, Valve, Verizon Communications Inc, Vodafone, VTech, Wal-Mart Stores Inc, Yahoo.

Не обошла беда правительственные учреждения, администрации регионов, министерства и силовые ведомства, полицейские департаменты. Утечки данных зарегистрированы в Госдепартаменте США, в Американской налоговой службе, в предвыборном штабе Дональда Трампа.

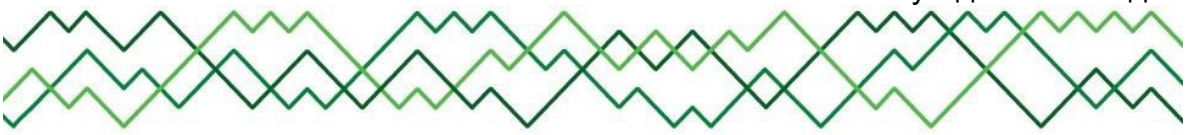
В I полугодии 2016 года мы впервые столкнулись с системными проявлениями «политического хактивизма» в виде атак на организации, ответственные за проведение выборов. В результате взломов были похищены десятки миллионов данных филиппинских, мексиканских, турецких, американских избирателей. Непрерывные скандалы, связанные со взломом серверов и утечкой данных, сопровождают текущую президентскую кампанию в США.

В своем исследовании утечек данных на глобальной выборке мы отталкиваемся от следующего предположения: число утечек данных будет расти а объемы скомпрометированной информации увеличиваться по мере того, как возрастает ценность информации в цифровом виде.

Динамика роста может отличаться от региона к региону (в зависимости от уровня развития цифровой экосистемы, ценности, полезности данных в цифровом виде). Но общемировой тренд на увеличение числа утечек и объемов скомпрометированных данных определяется не особенностями региона, а новыми возможностями, которые связаны с использованием информации в цифровом мире (перевод услуг в электронный вид, e-commerce, электронные деньги, интеллектуальная собственность в цифровом виде). Очевидно, чем больше таких возможностей в глобальном масштабе, тем выше интерес злоумышленников к цифровым данным.

Поэтому мы считаем, что анализ статики и динамики утечек данных на глобальной выборке позволяет не только привлечь внимание всех заинтересованных лиц к проблеме защиты данных, но и дает наглядное представление, например, о том, какой канал более других уязвим в настоящее время и почему, какую отрасль злоумышленники считают наиболее привлекательной, что опаснее – внешняя атака или действия злонамеренного инсайдера.

Авторы работы уверены, что выводы исследования будут интересны практикующим специалистам в области информационной и экономической безопасности, журналистам, собственникам и высшему менеджменту компаний, оперирующих



информацией ограниченного доступа (коммерческая, банковская, налоговая тайна), иными ценными информационными активами.

Методология

Исследование основывается на собственной базе данных, пополняемой специалистами Аналитического центра InfoWatch с 2004 года. В базу попадают публичные сообщения[1] о случаях утечки[2] информации из коммерческих и некоммерческих (государственных, муниципальных) организаций, которые произошли 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[6], тип утечки (по умыслу), канал утечки[7], типы утекших данных.

Утечки данных, произошедшие вследствие внешнего воздействия (таргетированная атака, фишинг, взлом веб-ресурса и пр.), долгое время оставались вне нашего внимания. С 2014 года такие утечки также добавляются в базу (наряду с утечками данных, которые связаны с действиями внутренних нарушителей). К списку критериев утечки добавлен вектор воздействия[8].

Также с 2014 года инциденты классифицируются по характеру действий нарушителя. Авторы исследования наряду с утечками выделяют случаи, когда сотрудник, имеющий легитимный доступ к данным, использует данные в целях мошенничества (манипуляции с платежными данными, инсайдерской информацией), когда сотрудник получает доступ к данным, которые не нужны ему для исполнения служебных обязанностей (превышение прав доступа).

Исследование охватывает не более 1%[9] случаев от предполагаемого совокупного количества утечек. Однако критерии категоризации утечек подобраны так, чтобы

---

[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, а также нарушение конфиденциальности информации под воздействием внешней атаки.

[3] Утечки данных разделяются на умышленные (злонамеренные) и неумышленные (случайные) в зависимости от наличия или отсутствия умысла у лица, которое спровоцировало утечку данных (см. Глоссарий). Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы.

[4] В данном исследовании авторы представляют картину утечек в разрезе виновных лиц. Впервые, наряду с внутренними нарушителями, в данную классификацию попадает внешний нарушитель.

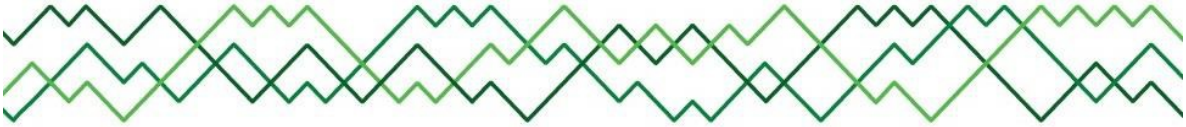
[5] Аналитики Центра InfoWatch классифицируют организации по размеру в зависимости от известного либо предполагаемого парка персональных компьютеров (ПК). Небольшие компании – до 50 ПК, средние - от 50 до 500 ПК, крупные – свыше 500 ПК.

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

[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. Каналы утечек определяются только для таких утечек, которые спровоцированы действиями/бездействием внутреннего нарушителя.

[8] Вектор воздействия – признак действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников, направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации информации, и действия внутренних злоумышленников, атакующих системы защиты изнутри (нелегитимный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.)

[9] С вероятностью, для России доля зафиксированных утечек от общего числа утечек, случившихся в нашей стране, значительно (на несколько порядков) меньше 1%.



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.

При составлении отраслевой карты и диаграмм раздела «Отраслевая карта» авторы целенаправленно вывели за рамки исследования утечки с несоразмерно большим (более 10 млн) количеством утекших персональных данных. Утечки с незначительным (менее 100) количеством «ушедших» записей также удалены из выборки. Это сделано для того, чтобы избежать искажения, которое неизбежно вносят крупные утечки в отраслевую картину утечек, другие распределения. Использование ограниченной выборки для построения диаграмм в названном разделе специально оговаривается.

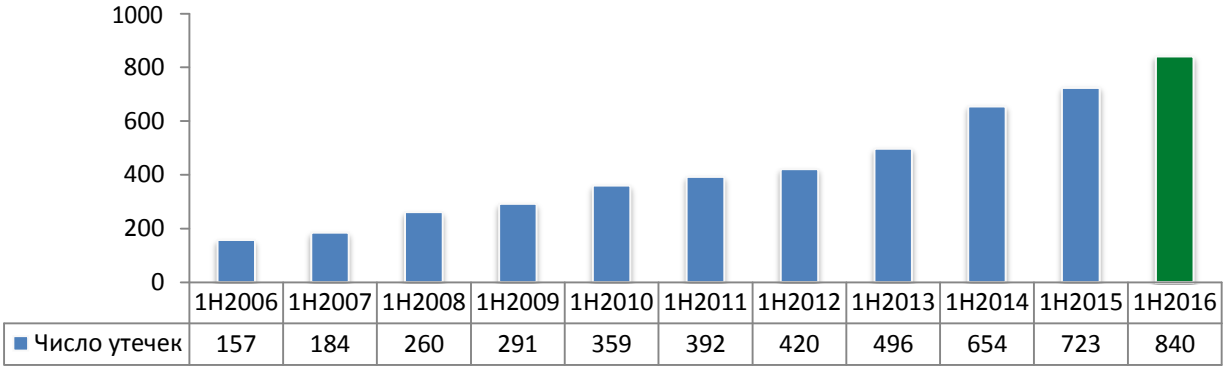
При формировании диаграмм (разрезов) из выборки исключены утечки, классифицированные по основному критерию разреза как неопределенные. Например, разрез по вектору воздействия (внешние атаки, действия внутреннего нарушителя) не содержит утечек, для которых вектор не удалось определить. То же самое справедливо для распределения по виновнику, умыслу и проч. Если данные исследуемого периода сравниваются с данными аналогичного периода прошлого года, выборка прошлого года скорректирована («неопределенные» утечки также удалены).

Случаи нарушения конфиденциальности информации (обнаруженные уязвимости), иные инциденты ИБ (DDoS-атаки), не повлекшие утечек данных, а также утечки с неясным источником данных (когда неизвестно, какой компании или организации принадлежали скомпрометированные данные) в выборку не попадают.

Авторы настоящего исследования не ставили перед собой цели посчитать все утечки, оценить реальный или возможный ущерб. В большей степени исследование направлено на выявление динамики процессов, характеризующих глобальную, отраслевую, региональную картину утечек.

Результаты исследования

За I полугодие 2016 года Аналитическим центром InfoWatch зарегистрировано 840 случаев утечки конфиденциальной информации (см. Рисунок 1). Это на 16% больше, чем за аналогичный период 2015 года (723 утечки).



	1H2006	1H2007	1H2008	1H2009	1H2010	1H2011	1H2012	1H2013	1H2014	1H2015	1H2016
Число утечек	157	184	260	291	359	392	420	496	654	723	840

Рисунок 1. Число зарегистрированных утечек информации, ½ 2006 – ½ 2016 гг.

В результате утечек скомпрометировано 1,06 млн персональных данных (записей ПДн и платежных данных), - номера социального страхования, реквизиты пластиковых карт, иная критически важная информация. Для сравнения - за весь 2015 год скомпрометированы 965,9 млн записей.

Зарегистрировано 506 (67%) утечек информации, причиной которых стал внутренний нарушитель. В 250 (33%) случаях утечка информации произошла из-за внешнего воздействия (см. Рисунок 2).

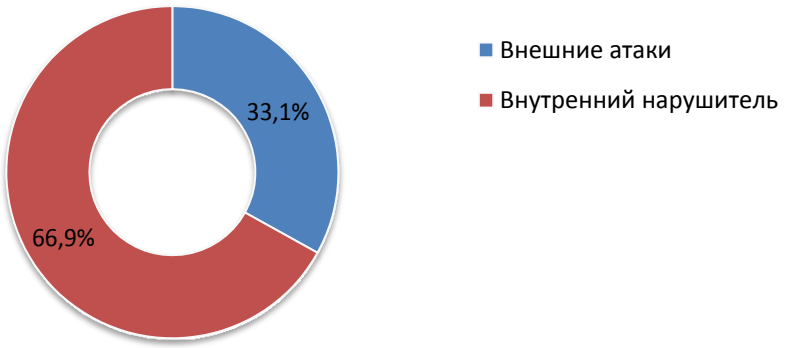
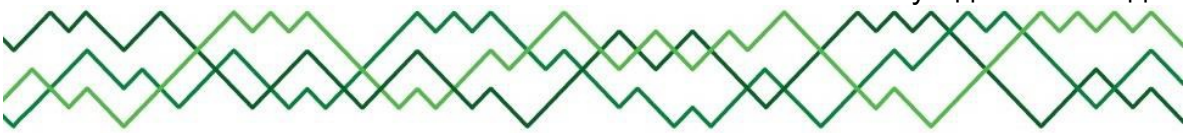


Рисунок 2. Распределение утечек по вектору воздействия[10], ½ 2016 г.

По сравнению с I полугодием 2015 года, изменений в распределении утечек по вектору не наблюдается. Ранее на протяжении нескольких лет мы отмечали

[10] Вектор воздействия – признак действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников, направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации информации, и действия внутренних злоумышленников, атакующих системы защиты изнутри (нелегитимный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.)



постепенное увеличение доли утечек под воздействием внешних атак. В исследуемом периоде доля утечек под воздействием внешних атак увеличилась всего на 1 п. п.

Таким образом, сделанный нами ранее прогноз на долгосрочный рост доли утечек под воздействием внешнего злоумышленника (с соответствующим сокращением доли утечек, спровоцированных злонамеренными или неосторожными действиями внутреннего нарушителя) не оправдался. Это, впрочем, не отменяет вывода исследований предыдущих лет о том, что «внешние утечки» по своей природе более разрушительны, чем утечки данных, спровоцированные внутренним нарушителем.

В I полугодии 2015 года в результате внешнего воздействия скомпрометировано 603 млн персональных данных (2,41 млн на утечку). Итогом воздействия внутреннего нарушителя стала компрометация 406 млн записей (0,80 млн на утечку).

Внешние атаки спровоцировали 16 из 23 зафиксированных «мега-утечек»[11]. На «мега-утечки» приходится 982 млн записей о персональных данных, скомпрометированных в результате утечек в I полугодии 2016 года (92% от общего числа).

> gazeta.ru: *Сайт филиппинской избирательной комиссии взломан группировкой LulzSec Philippines. Им удалось украсть данные о 55 млн филиппинцев и выложить их в сеть. Среди личных данных значатся имена, даты рождения, паспортные данные и даже отпечатки пальцев. Ранее этот же сайт взломали хакеры из группировки Anonymous Philippines. Злоумышленники утверждали, что эта акция направлена на привлечение внимания общественности к возможным нарушениям во время выборов.*

Многомиллионные утечки данных избирателей становятся своеобразной визитной карточкой нынешнего предвыборного цикла.

> databreaches.net: *Эксперт в области информационной безопасности Крис Викери (Chris Vickery) обнаружил в интернете базу данных, в которой содержались персональные данные 2 миллионов мексиканских избирателей. О своей находке Крис рассказал сотрудникам Национального избирательного института, которые непосредственно отвечают за организацию выборов в Мексике. Некоторое время спустя представители института заявили, что им удалось ликвидировать утечку, закрыв внешний (из интернета) доступ к базе данных.*
>
> *В конце апреля СМИ уже сообщали об утечке данных 93 млн мексиканских избирателей. Утечку обнаружил тот же Крис Викери на одном из облачных хранилищ, арендованных у компании Amazon. База содержала имена людей, их адреса проживания, даты рождения, данные о родителях, а также уникальный ID избирателя.*

Распределение утечек по виновнику за год практически не изменилось. Доля утечек под воздействием внешнего злоумышленника снизилась на 4 п. п. и составила 30%. В 67% случаев виновниками утечек информации были настоящие или бывшие сотрудники - 66% и 1% соответственно. Менее чем в 1% случаев зафиксирована вина руководителей организаций (топ-менеджмент, главы отделов и департаментов). Доля

[11] «Мега-утечки» - утечки информации, в ходе которых скомпрометированы свыше 10 млн записей персональных данных.

утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к охраняемой информации, составила 2% (Рисунок 3).

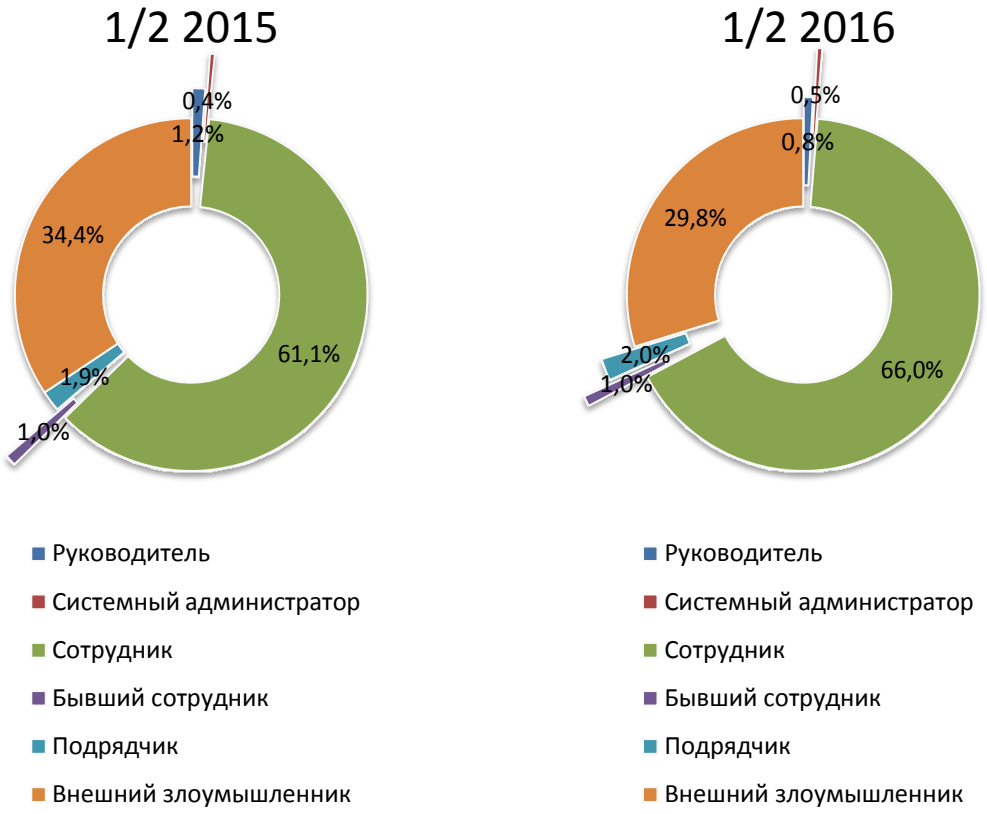


Рисунок 3. Распределение утечек по источнику (виновнику), ½ 2015 – ½ 2016 г.

Совокупная доля утечек персональных и платежных данных[12] выросла на 4 п. п. и составила 94%. При этом на персональные данные пришлось 88% утечек. В 6% случаев утекала платежная информация. Как правило, при утечке платежной информации речь идет о компрометации реквизитов платежных карт.

> *infowatch.ru: Российские пользователи Uber сообщили о взломе сервиса: их платежные карты используются для оплаты поездок в других странах мира. При этом самостоятельно изменить платежные данные или отвязать карту они не смогли. Оценить ущерб и масштаб утечки на данный момент в Uber затруднились, однако пообещали разобраться в случившемся.*
>
> *Нужно отметить, что это далеко не первый инцидент информационной безопасности, произошедший с данными пользователей Uber. Ранее, в октябре 2015 года, в сеть утекли фотографии более 600 водительских удостоверений американских водителей Uber, их регистрационные номера и*

[12] При классификации утечек определенные трудности связаны с распределением сообщений об утечках по признаку типа утекших данных. Персональные данные (ФИО, номер соцстрахования, ИНН и проч.) от платежной информации отделить непросто. Поэтому авторы исследования объединяют их в категорию «Персональные данные и платежная информация».

номера социального страхования, а в конце 2014 утечка затронула ПДн десятков тысяч пользователей сервиса по всему миру.

Причем за последние полгода возросло число утечек платежной информации, в ходе которых скомпрометировано свыше миллиона записей.

vladtime.ru: Хакеры взломали социальную кредитную сеть Webtransfer и получили доступ к данным 3,5 млн пользователей. В руках злоумышленников оказалась база данных сервиса, которая содержала информацию о всех клиентах сети. В результате атаки скомпрометированы имена и электронные адреса пользователей, номера пластиковых карт и телефонов, а также коды подтверждения финансовых операций. В июле 2015 года ЦБ РФ предположил, что социальная сеть является финансовой пирамидой. Сообщалось, что сеть массово задерживает выплаты денежных средств своим пользователям. О результатах проверки СМИ не сообщали.

По сравнению с I полугодием 2015 года, наблюдается незначительное (на 1 п. п.) уменьшение долей утечек информации, составляющей государственную и коммерческую тайну (Рисунок 4).

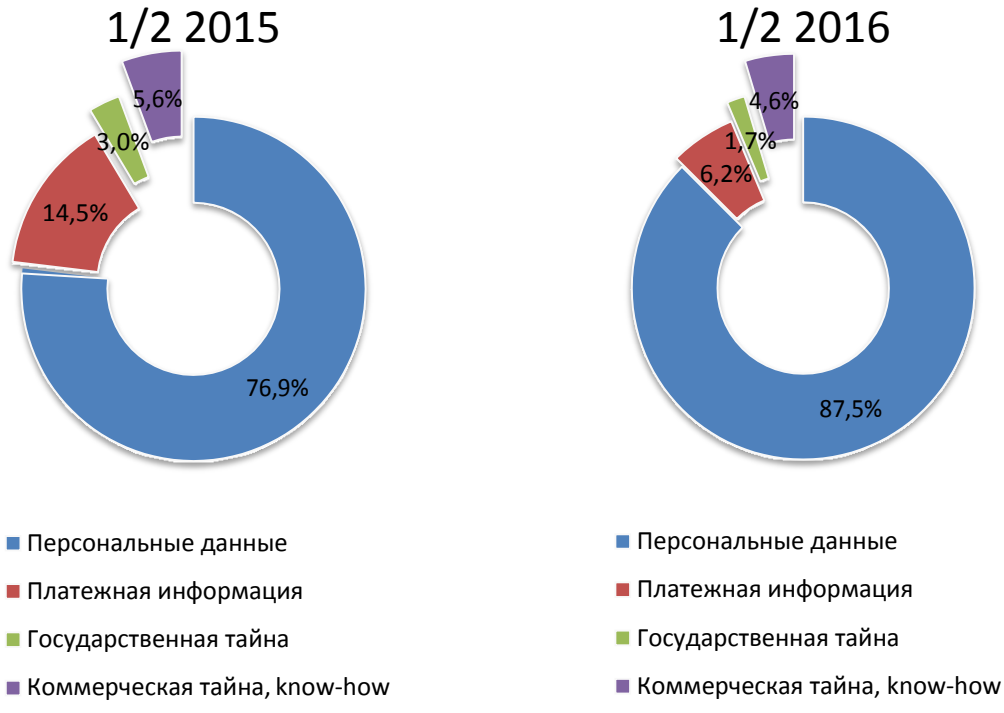


Рисунок 4. Распределение утечек по типам данных, ½ 2015 – ½ 2016 г.

Огромный объем скомпрометированных персональных данных и платежной информации, высокая доля утечек этих типов данных свидетельствует о растущей год от года ценности личной информации в цифровом виде. Причем, это касается не только персональных данных отдельных граждан, но и сведений о физических лицах – представителях организаций-контрагентов, которые (сведения) аккумулированы в клиентских базах коммерческих компаний.

Действия злоумышленников в основном укладываются в два сценария – кража личности (identity theft), в результате чего украденные персональные данные используются для получения кредитов, налоговых вычетов и пр., и хищение клиентских баз – агрегированных сведений о контрагентах компании, как правило, по заказу или в интересах конкурентов.

В 2016-м году доля утечек данных, сопряженных с последующим использованием скомпрометированной информации в целях мошенничества (банковский фрод) снизилась и составила 8%. Доля утечек данных, сопряженных с неправомерным доступом к информации (злоупотребление правами доступа, внутренний шпионаж), составила 11% (см. Рисунок 5).

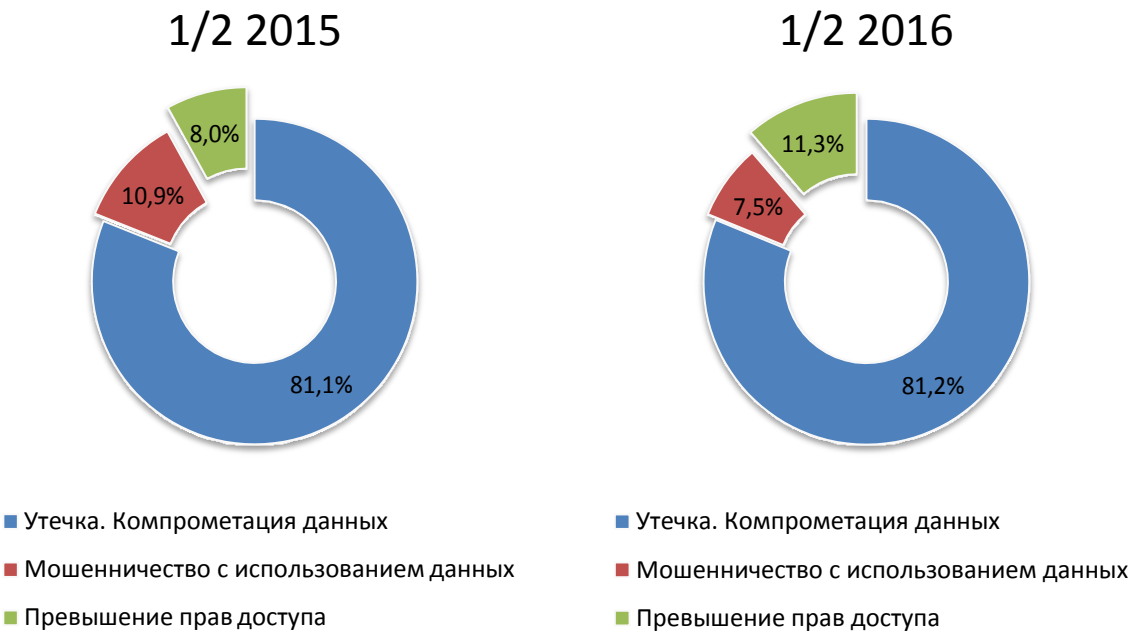


Рисунок 5. Распределение утечек по характеру, ½ 2015 – ½ 2016 г.

81% инцидентов, сопряженных с потерей контроля над информацией, относится к типу «классических» утечек, не сопряженных с дополнительными нарушениями – нет превышения прав доступа, нет использования в целях мошенничества. На диаграмме мы их обозначили как утечки, приведшие к компрометации данных[13].

Невозможно однозначно сказать, в каком случае последствия для владельца данных (коммерческой компании, государственного органа) будут более разрушительными. Не очевидно, что обычный хакер, которому посчастливится пробраться внутрь защищенного периметра, натворит меньших бед, чем профессиональный мошенник.

> *Motherboard: Хакер взломал сервер Минюста США и украл более 200 ГБ данных, в том числе имена, фамилии, номера телефонов, адреса*

[13] Отметим, что любая утечка данных приводит к их компрометации. Однако для методологического разделения «классических» утечек и утечек «с отягощением» (фрод с использованием утекшей информации, неправомерный доступ или превышения прав доступа – наиболее значимые внутренние угрозы на сегодняшний день) мы выделили эту условную категорию.

электронной почты 20 тыс. сотрудников ФБР и 10 тыс. сотрудников Министерства внутренней безопасности. По информации Motherboard, злоумышленнику удалось взломать аккаунт сотрудника Министерства внутренней безопасности, после чего хакер связался с оператором ФБР и, выдавая себя за легитимного пользователя, получил доступ к инфраструктуре Министерства юстиции.

Распределение случайных и умышленных утечек в I полугодии 2016 года и за аналогичный период 2015 года представлено ниже. Отметим незначительный рост доли умышленных утечек по отношению к случайным (см. Рисунок 6).

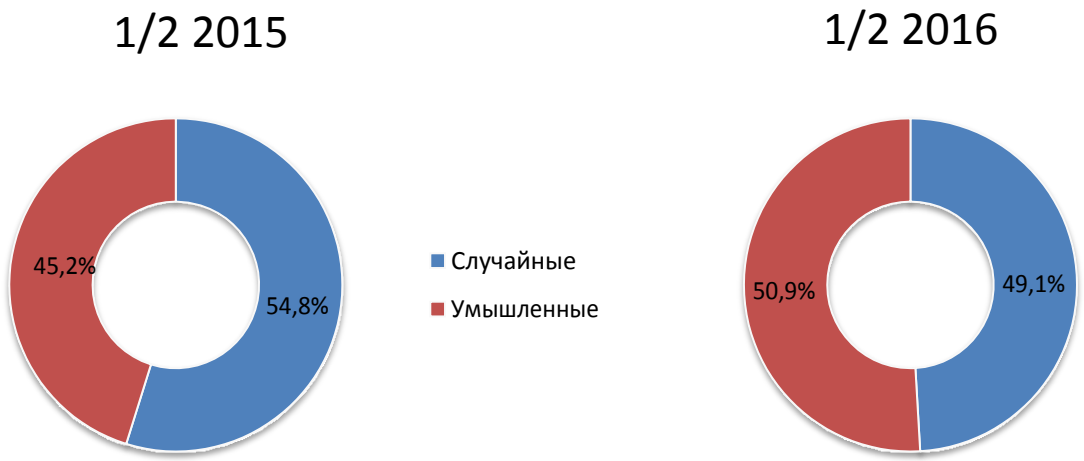


Рисунок 6. Соотношение случайных и умышленных утечек, ½ 2015 – ½ 2016 гг.

На протяжении нескольких лет мы наблюдаем относительную стабильность картины утечек. Существенными изменениями в пределах исследуемого периода можно считать увеличение объема скомпрометированных записей в расчете на утечку в 3,5 раза, трехкратный рост числа мега-утечек (с 8 до 23) по сравнению с I полугодием 2015 года, рост доли утечек персональных данных.

Вывод:

Во многом неожиданный трехкратный рост объема скомпрометированных данных свидетельствует о растущей день ото дня ценности данных в цифровом виде. Злоумышленники поняли это даже раньше, чем владельцы информации, которые до сих пор не всегда готовы оценить в деньгах свои информационные активы. Между тем очевидно, что дальнейшее развитие подходов к обеспечению информационной безопасности данных неизбежно потребует оценки стоимости активов, ясного представления, прежде всего, от владельцев информации, относительно того, какие данные для них важны, каковы финансовые потери в случае утечки этих данных.

Каналы утечек

В I полугодии 2016 года продолжилось увеличение доли утечек по таким каналам, как съемные носители, электронная почта. Снизились доли утечек данных в результате кражи/потери оборудования, через сеть, бумажные документы. Почти на 1 п. п. возросла доля утечек по голосовому каналу (см. Рисунок 7).

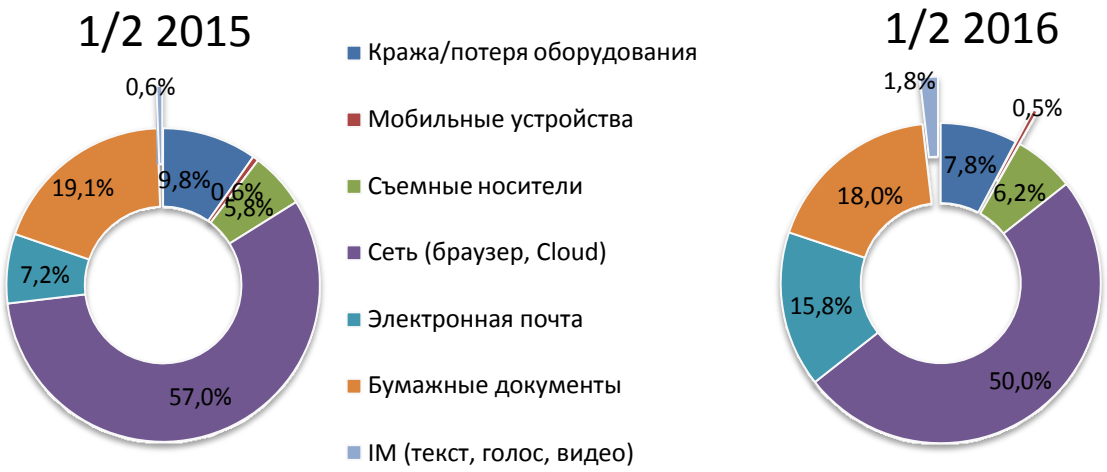


Рисунок 7. Распределение утечек по каналам, ½ 2015 – ½ 2016 гг.

При этом распределения умышленных и случайных утечек по каналам впервые за все время наблюдений не имеют драматических отличий (за исключением «электронной почты»). Например, доля умышленных утечек через бумажные документы отличается от доли случайных по тому же каналу лишь на 6 п. п. (**Ошибка! Источник ссылки не найден.**).

Рисунок 8. Распределение утечек по каналам, ½ 2016 г.

Для сравнения – по данным I полугодия 2015 года на бумажные документы пришлось всего 2% умышленных утечек при 23% случайных утечек по тому же каналу.

Сопоставимо меньшие доли умышленных утечек (по сравнению со случайными) зафиксированы по таким каналам, как съемные носители, электронная почта, бумажная документация. Именно эти каналы исторически наиболее чувствительны к применению технических средств защиты данных. Не секрет, что изначально системы предотвращения утечек контролировали как раз электронную почту, бумажные документы, копирование данных на флешки.

Увеличение доли случайных утечек свидетельствует о возрастающей эффективности таких решений, все большем проникновении систем защиты информации, благодаря которым и удается в итоге эти утечки обнаружить.

С другой стороны, внутренние злоумышленники все меньше используют эти каналы для совершения противоправных действий. «Продвинутый» нарушитель осведомлен, что современные средства контроля позволяют успешно перехватывать передачу конфиденциальной информации практически по всем перечисленным каналам, и не рискует понапрасну.

Сетевой канал выходит на первый план как по количеству утечек, так и по объему скомпрометированных данных. Большая часть (65%) утечек персональных данных (конкретно – наиболее «ликвидной» [14] платежной информации) приходится на сетевой канал (см. **Ошибка! Источник ссылки не найден.**).

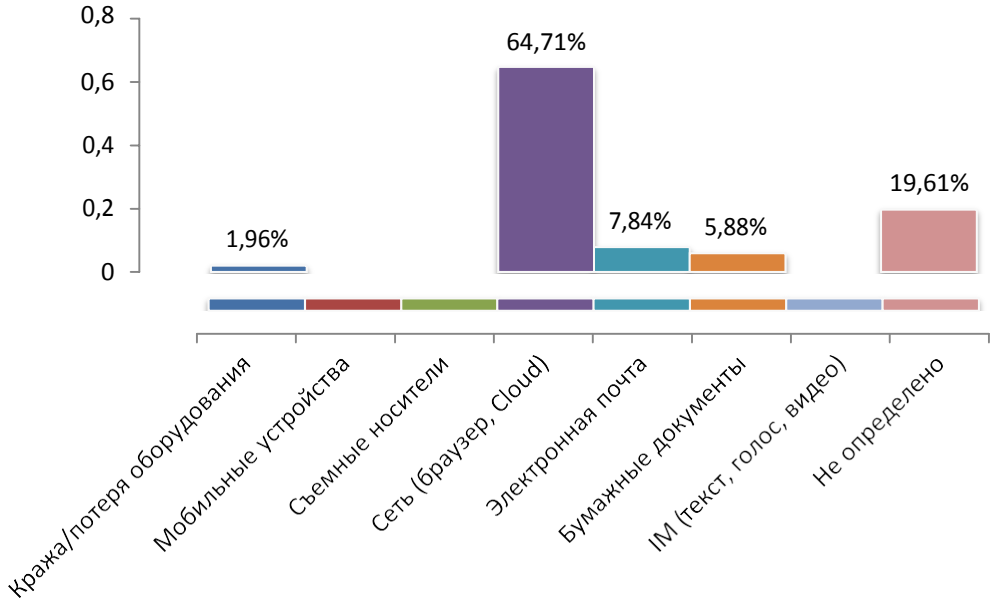
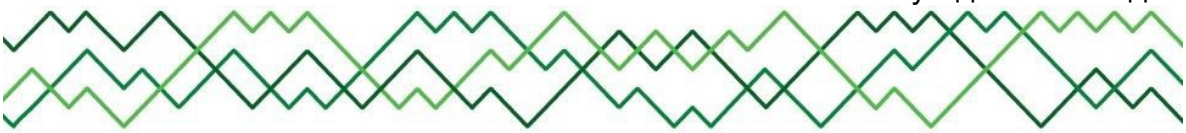


Рисунок 9. Утечки платежных данных, распределение по каналам, ½ 2016 г.

[14] Под «ликвидными» данными авторы понимают такие данные, использование которых может принести злоумышленнику финансовую выгоду в кратчайшей перспективе при минимальных издержках. Наиболее ликвидными данными по традиции считаются данные кредитных карт.



В случае с внутренними нарушителями компании имели дело со стандартными сценариями – сохранение конфиденциальной информации в облаках Box, OneDrive и пр., использование бесплатных почтовых аккаунтов (веб-почта).

Сценарии внешних взломов менее разнообразны. Хакеры, как правило, не слишком хорошо знакомы со структурой данных компании, с тем, где хранится наиболее ценная информация и что она собой представляет, потому «берут» все, что представляет хоть малейшую ценность. Как правило, это агрегированные базы персональных данных, платежная информация.

> *databreaches.net: Персональные данные 49 млн граждан Турции были украдены и опубликованы в сети. Ссылка на файл объемом 6,6 ГБ появилась в твиттере, но впоследствии была удалена. Файл содержит имена, адреса, даты рождения, сведения о родителях и о национальной принадлежности, другую чувствительную информацию граждан. В сообщении злоумышленников, взломавших базу данных, подчеркивается, что информация о гражданах была защищена очень слабо. Сама база была плохо проиндексирована, зашифрована с применением простого алгоритма, а единственным средством защиты выступал сложный пароль от интерфейса пользователя.*

Представление утечек в разрезе каналов, по которым уходит информация, имеет огромное практическое значение. В зависимости от частоты утечек по тому или иному каналу, можно разрабатывать модели угроз (отраслевые, региональные, применительно к конкретным типам данных), осуществлять внедрение средств защиты в компании или в отрасли, определить, каким каналам следует уделить повышенное внимание.

> ***Вывод:***
>
> ***Год назад мы говорили о тотальном преобладании сетевого канала в распределении утечек. Сегодня картина изменилась – случайные и умышленные утечки стабильно фиксируются практически на всех каналах (хотя, доля сетевого канала по-прежнему велика).***
>
> ***Это означает, что производители средств защиты информации адаптировались к новой реальности – смартфоны, планшеты, голосовые мессенджеры, - и готовы защищать информацию от утечек в том числе и по таким каналам, которые ранее считались «проблемными» (голосовые сообщения, фотографирование и передача изображений с помощью смартфонов, корпоративная почта на ноутбуке сотрудника за пределами периметра).***

Отраслевая карта

В I половине 2016 года доля утечек из государственных организаций возросла на 2 п. п. и составила 20%. До 80% снизилась доля утечек из коммерческих компаний (см. Рисунок 10).

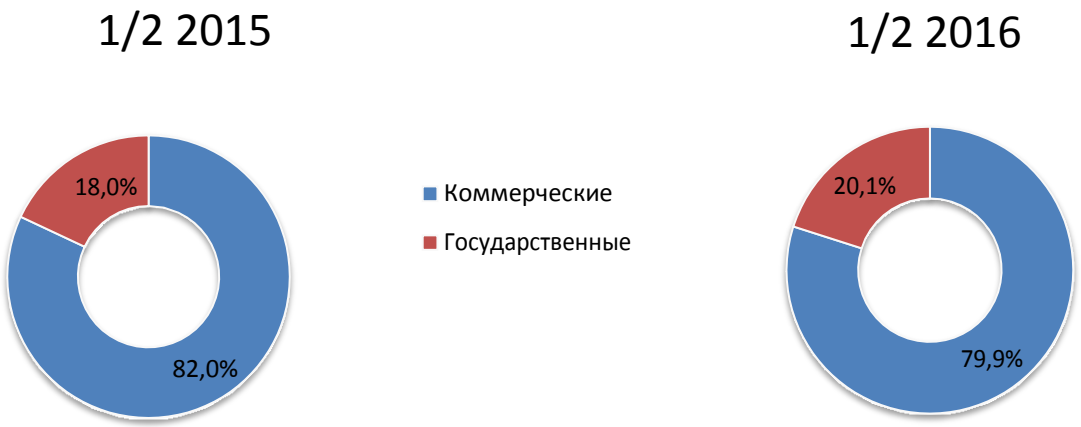


Рисунок 10. Распределение утечек по типу организации, ½ 2015 – ½ 2016 гг.

Чаще всего утечки фиксировались в медицине (23%), реже всего в муниципальных учреждениях (<3%). По объему скомпрометированных записей пальму первенства удерживают компании высокотехнологичного сегмента (интернет-сервисы, крупные порталы). На утечки из госорганов приходится 15% совокупного объема скомпрометированных данных, на утечки из муниципальных учреждений – 14% (см. Рисунок 11).

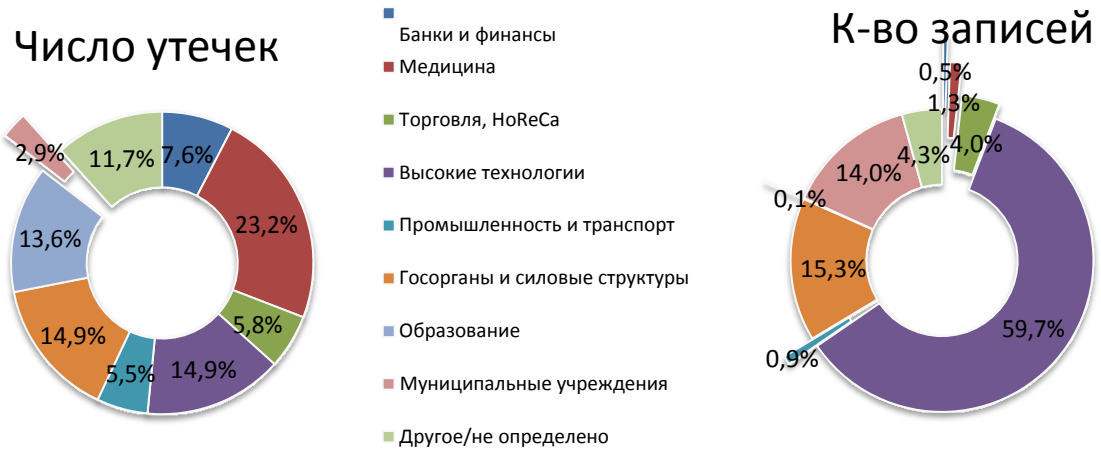


Рисунок 11. Распределение числа утечек и объема скомпрометированных персональных данных по отраслям, ½ 2016 гг.

Приведенные диаграммы дают лишь фактическую картину утечек и объемов скомпрометированных данных в отраслях. Важнее выяснить, какие отрасли в настоящий момент являются наиболее «привлекательными» для злоумышленников.

«Привлекательность» отрасли прямо обусловлена «ликвидностью» данных, которыми владеют компании данного сегмента[15]. Представление злоумышленников об уровне защиты данных в отрасли, также влияет на «привлекательность», но обратно пропорционально. «Привлекательность» отрасли для злоумышленника находит конечное воплощение в числе зафиксированных умышленных утечек информации. Проиллюстрируем это умозаключение формулой:

$$\text{Число умышленных утечек} \leftarrow \frac{\text{Ликвидность данных}}{\text{Представление об уровне защищенности информации}}$$

Если сделать выборку утечек одного типа информации (в нашем случае мы отобрали утечки персональных данных), то доля умышленных утечек в конкретной отрасли будет показателем привлекательности (а значит, уязвимости) этой отрасли для злоумышленника.

В I полугодии 2016 года таковыми следует признать торговые компании, банки. В этих отраслях более половины утечек, сопровождавшихся компрометацией персональных данных, носили умышленный характер (см. **Ошибка! Источник ссылки не найден.**).

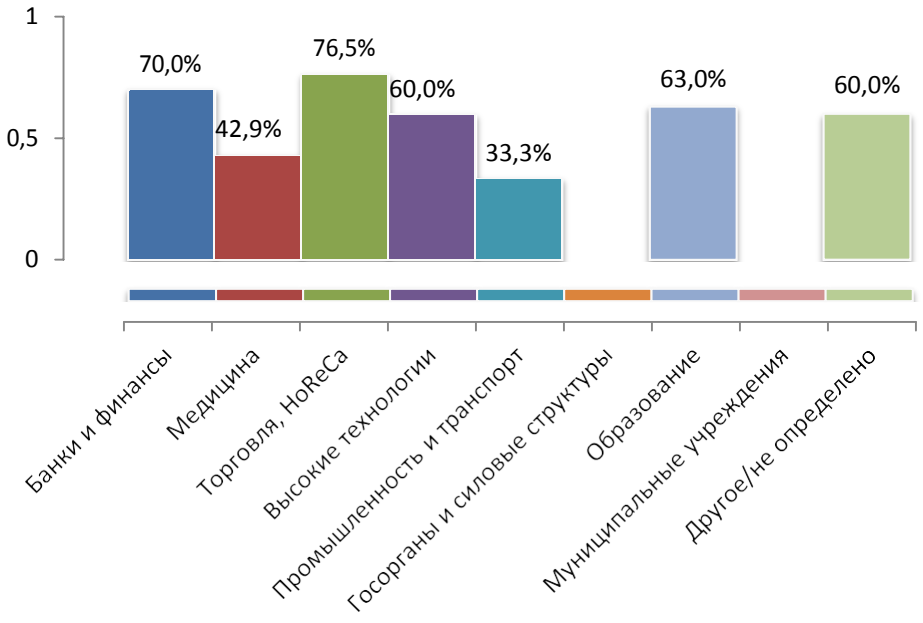


Рисунок 12. Доля умышленных утечек ПДн от общего количества утечек ПДн по отраслям, ½ 2016 г.

Определившись с наиболее уязвимыми отраслями, перейдем к картине утечек персональных данных для всех сегментов — так называемой «отраслевой карте». Сама по себе отраслевая карта утечек персональных данных наглядна. Размер

[15] Чем проще конвертировать украденную информацию в деньги, тем «привлекательнее» сегмент.

«пузырьков» показывает совокупное число скомпрометированных записей, их положение по вертикали – число утечек в отрасли[16] (см. **Ошибка! Источник ссылки не найден.**).

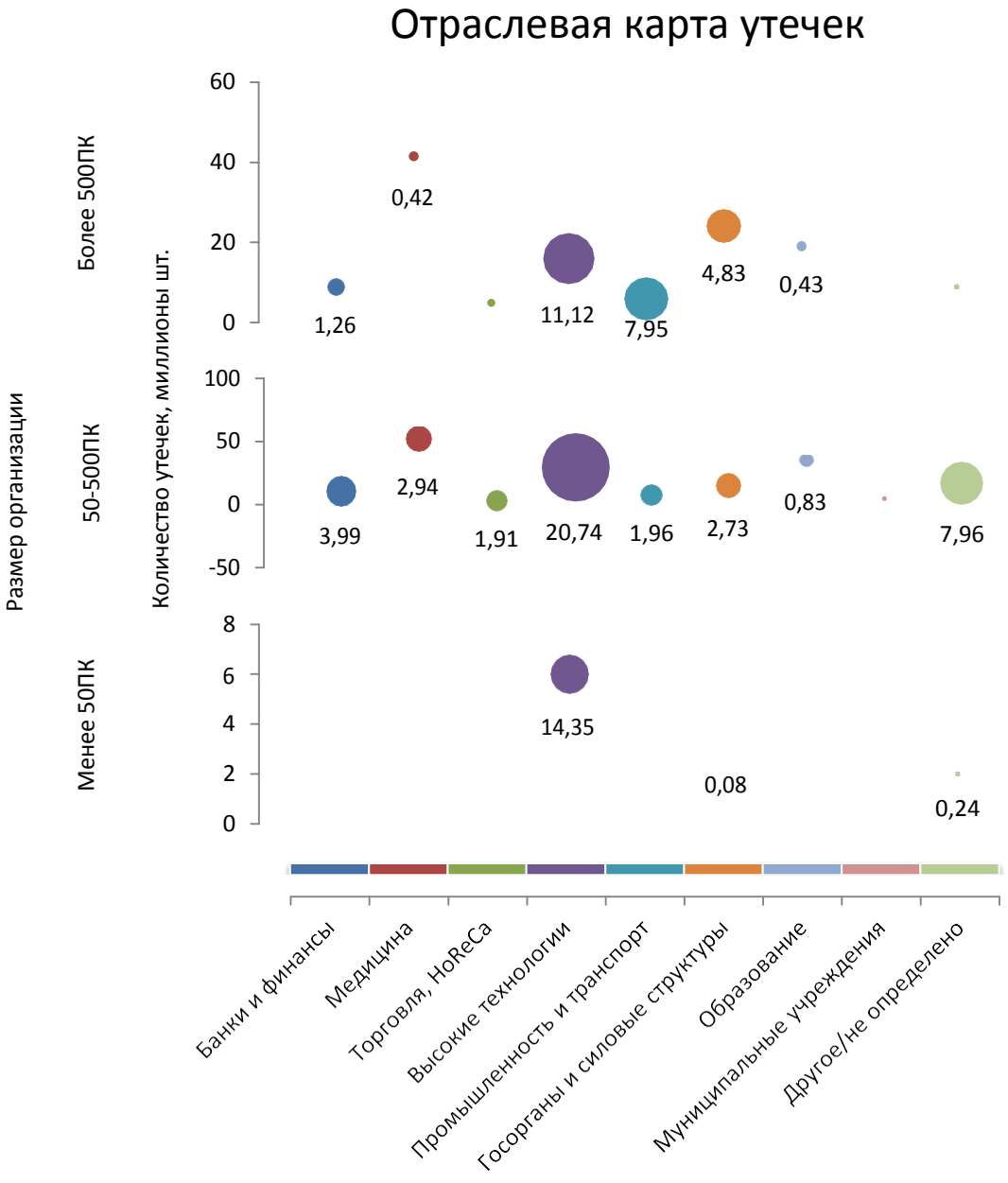


Рисунок 13. Отраслевая карта утечек персональных данных, млн, ½ 2016 г.

[16] В число утечек в отрасли включены утечки персональных данных, в результате которых точно известно о количестве скомпрометированных данных. При этом объем скомпрометированных данных для отрасли рассчитывается без учета «мега-утечек» - случаев компрометации данных, когда количество скомпрометированных данных превысило 10 млн записей.

Наибольший объем скомпрометированных данных пришелся на компании высокотехнологичного сегмента (включая интернет-сервисы). Со знаком минус «отличились» транспортные компании, банки.

В I полугодии 2016 года на долю компаний среднего размера (до 500 ПК) пришлось 57% от всех утечек данных. При этом доля среднего бизнеса в совокупном объеме скомпрометированных данных составляет 72% (см. **Ошибка! Источник ссылки не найден.**).

Рисунок 14. Распределение утечек по размеру организации ½ 2016 г.

Современные средства защиты от утечек все еще слишком дороги для среднего и малого бизнеса, что делает сегмент СМБ излюбленной мишенью для злоумышленников, промышляющих хищением персональных данных и платежной информации (записи о сотрудниках, клиентах, контрагентах, реквизиты банковских карт и пр.).

Вывод:

Наиболее «привлекательными» для злоумышленников и, как следствие, уязвимыми отраслями оказались: сегмент высоких технологий, торговля, финансовый сектор. Наибольший объем скомпрометированных данных (без учета «мега-утечек») пришелся на интернет-сервисы. Средний бизнес по-прежнему в большей степени подвержен утечкам персональных данных, чем крупные компании.

Региональные особенности

В распределении утечек по регионам в I полугодии 2016 года США традиционно заняли первую позицию по количеству утечек (451 или 54% от всех произошедших). Россия оказалась на уже привычном втором месте (110 утечек), которое досталось нашей стране еще по итогам I полугодия 2013 года. На третьем месте — Великобритания - 39 утечек (Рисунок 15).

Авторы исследования неоднократно отмечали, что современная глобальная картина утечек данных с незначительными изменениями воспроизводится во всех странах, где

оперируют информацией в электронном виде. Причем субъективно воспринимаемая ценность информации (как для злоумышленников, так и для владельцев) зависит не от географии, а от степени развития экосистемы, построенной вокруг данных – от уровня «диджитализации» региона.

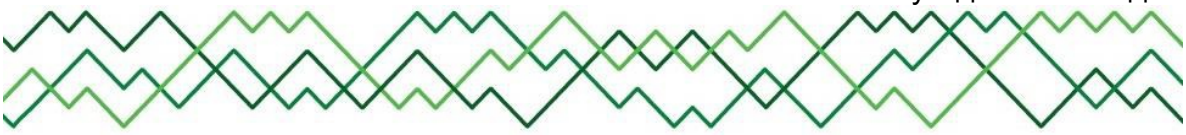
В странах, где персональные данные в электронном виде позволяют быстро и удобно получить государственные и прочие услуги, заменяют бумажные документы, велика вероятность, что эти данные будут использоваться неправомерно. Пример – США, где кража личности давно превратилась в обыденное преступление. Причем за кражей личности стоят, как правило, не квалифицированные хакеры, а обычные люди – медсестры, официанты, полицейские, - которые всего лишь хотят подзаработать немного денег на использовании чужих данных.

В менее развитых регионах ситуация иная. В количественном выражении утечек значительно меньше, но их масштаб, характер вполне сопоставим с «лучшими образцами» западного мира.

> *thehackernews.com: Пакистанские хакеры взломали один из самых популярных стриминговых сервисов Индии. В результате утечки данных в руках злоумышленников оказалась база данных пользователей сервиса, составляющая более 10 млн записей – имена, пароли, электронные адреса, даты рождения, другая личная информация посетителей ресурса. Украденную информацию хакеры разместили в открытом доступе.*

Информация об утечках все чаще появляется не только в отечественных СМИ, но и в прессе таких стран, как Индонезия, Вьетнам, Индия, что свидетельствует о проявляющемся интересе к теме утечек и безопасности данных в обществе и бизнес-структурах этих стран.

Рисунок 15. Распределение утечек по странам, ½ 2016 г.



Заключение и выводы

В 2014 году мы объявили о наступлении эры «мега-утечек»[17]. За прошедшие два года ситуация ухудшилась. В I полугодии 2016 года число зафиксированных мега-утечек достигло 23-х. На мега-утечки приходится основная часть скомпрометированных ПДн и платежных данных. Причем эта доля с каждым годом увеличивается.

Наиболее весомый вклад в увеличение объема скомпрометированных данных принадлежит внешним атакам. Однако наш прогноз на увеличение доли внешних атак не оправдался. Очевидно, что внешние атаки остаются наиболее разрушительным фактором, формирующим картину утечек. Но и внутреннего нарушителя пока еще рано сбрасывать со счетов.

В I полугодии 2016 года мы впервые столкнулись с компрометацией персональных данных в результате действий политических «хактивистов». Таким образом тема утечек данных пришла не только в бизнес, но и в политику, став, например, одним из заметных сюжетов текущей американской избирательной кампании.

Растет «квалификация» внутреннего нарушителя, который отказывается от использования электронной почты, сервисов мгновенных сообщений, съемных носителей. «Продвинутый» нарушитель осведомлен, что современные средства контроля позволяют успешно перехватывать передачу конфиденциальной информации по перечисленным каналам, и не рискует понапрасну. Его выбор — закрытые, неконтролируемые каналы, на которых средства защиты данных по тем или иным причинам не работают либо неэффективны.

Впрочем, данные свидетельствуют о том, что разработчикам средств защиты удалось в какой-то мере адаптировать свои решения к изменившейся инфраструктуре. Утечки фиксируются не только на «популярных» каналах, но и, например, при передаче информации через «голосовой» канал. Причем не только случайные (что и раньше отмечалось), но и умышленные.

Самыми «привлекательными» для злоумышленников и, как следствие, уязвимыми отраслями оказались сегмент высоких технологий, торговля, банки. Наибольший объем скомпрометированных данных (без учета «мега-утечек») пришелся на высокотехнологичные компании. Средний бизнес подвержен утечкам персональных данных в большей степени, чем крупные компании.

Тема утечек данных становится все более прозрачной, и это нельзя не приветствовать. Надеемся, в ближайшем будущем мы сможем говорить не только о самих утечках, типах данных, особенностях каналов, но и об оценке объектов защиты, скомпрометированных в результате инцидентов, о реальных финансовых потерях конкретных компаний вследствие утечек тех или иных типов данных. Представляется, что такая оценка еще более сблизит информационную безопасность и бизнес, позволит вывести задачу защиты информации на критичный для владельцев компаний уровень.

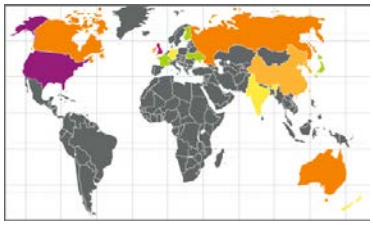
[17] Под «мега-утечками» авторы исследования понимают утечки данных, в результате которых объем скомпрометированных данных составил 10 млн записей и выше.

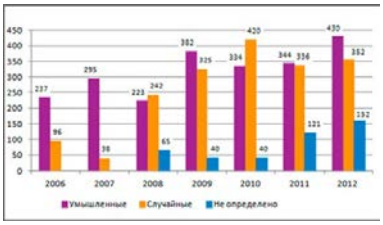
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

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.



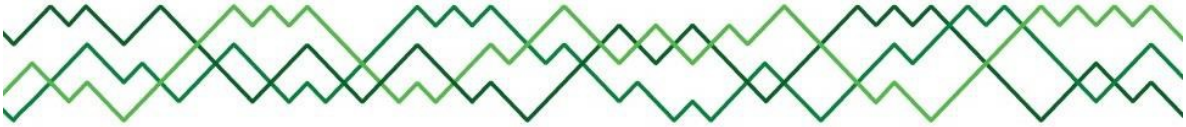


Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Twitter
- RSS

Аналитический центр InfoWatch

www.infowatch.ru/analytics



INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Глоссарий

Инциденты информационной безопасности — *в данном исследовании к этой категории авторы относят случаи компрометации информации ограниченного доступа вследствие утечек данных и/или деструктивных действий сотрудников компании.*

Утечка данных — *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.*

Деструктивные действия сотрудников — *действия сотрудников, повлекшие компрометацию информации ограниченного доступа: использование информации ограниченного доступа в личных целях, сопряженное с мошенничеством; нелегитимный доступ к информации (превышение прав доступа).*

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/неумышленные утечки — *к умышленным относятся такие утечки, 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.*

К неумышленным относятся 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. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы.

Вектор воздействия — *критерий классификации в отношении действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников – (Внешние атаки), направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации информации, и действия внутренних злоумышленников – (Внутренний нарушитель), атакующих системы защиты изнутри (нелегитимный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.)*

Канал передачи данных — *сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. На данный момент мы различаем 8 самостоятельных каналов:*

- ✓ *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».*