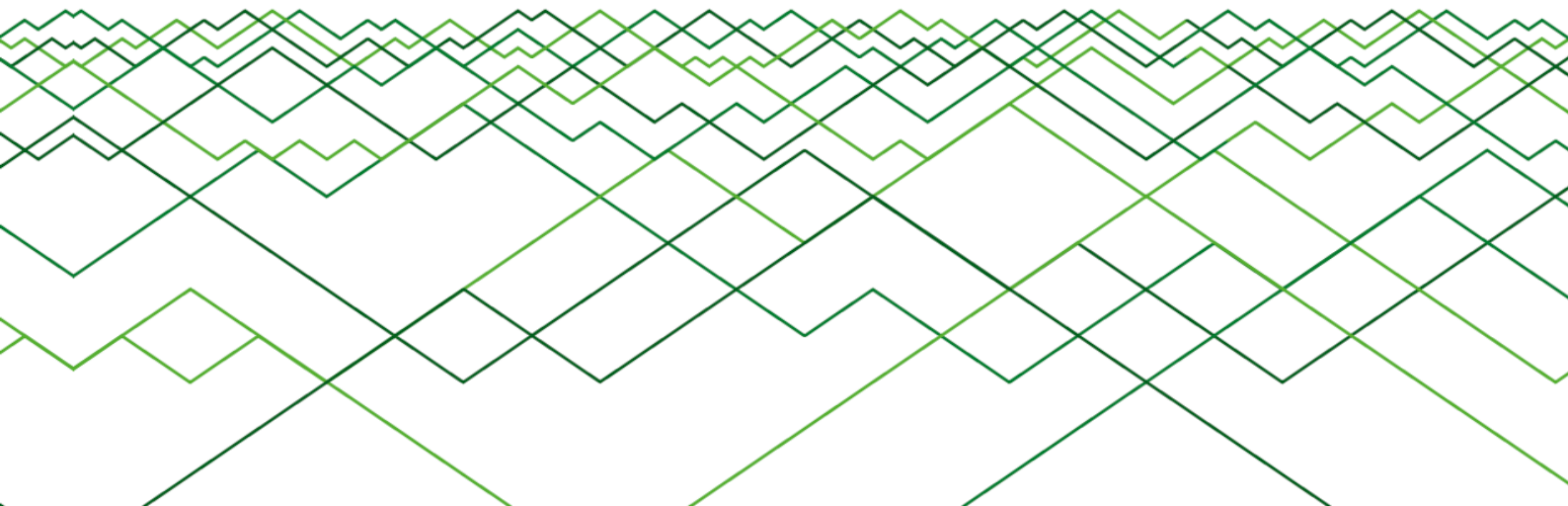
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Аналитический центр InfoWatch
www.infowatch.ru/analytics

Глобальное исследование утечек конфиденциальной информации в 2016 году



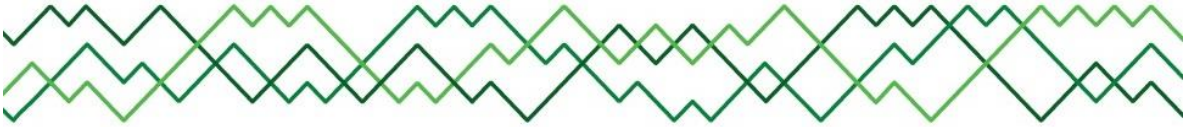
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Оглавление

INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Только цифры

- ✓ В 2016 году в мире было обнародовано (в СМИ и иных источниках) и зарегистрировано Аналитическим центром InfoWatch **1556** случаев утечки конфиденциальной информации, что на **3,4%** превышает количество утечек, зарегистрированных в 2015 году.
- ✓ Внешние атаки стали причиной **38%** случаев утечек данных. Доля утечек информации вследствие внешних атак выросла на шесть процентных пунктов (п. п.) по сравнению с аналогичным показателем 2015 года.
- ✓ **93%** утечек были связаны с компрометацией персональных данных и платежной информации. Всего за исследуемый период было скомпрометировано более **3,1 млрд** записей — в три раза больше, чем было зафиксировано в 2015 году.
- ✓ В 2016 году было зафиксировано **44** «мега-утечки», в результате каждой из которых «утекло» не менее **10 млн** единиц персональных данных. Совокупно на «мега-утечки» пришлось **94,6%** всех скомпрометированных записей.
- ✓ В **36%** случаев виновными в утечке информации оказывались сотрудники, а в **2,2%** случаев — высшие руководители организаций.
- ✓ По итогам 2016 года Россия заняла второе место в мире по числу известных случаев утечек. В исследуемый период было зарегистрировано **213** случаев утечки конфиденциальной информации из российских коммерческих и государственных организаций. Число «российских» утечек по сравнению с данными 2015 года выросло на **80%**.



Аннотация

Аналитический центр компании InfoWatch представляет ежегодный отчет об исследовании утечек конфиденциальной информации.

В 2016 году мы впервые столкнулись с системными проявлениями «политического хактивизма». В результате взломов были похищены десятки миллионов данных филиппинских, мексиканских, турецких, американских избирателей. Непрерывные скандалы, связанные с утечкой данных, сопровождали предвыборную гонку нынешнего президента США и, возможно, решили ее исход.

Внешние атаки стали причиной компрометации данных пользователей онлайн-платформ Facebook, Foursquare, GitHub, iCloud, LinkedIn, MySpace, Snapchat, Telegram, Tumblr, Twitter. Сложно назвать хотя бы один интернет-сервис, чьи пользователи в 2016 году не пострадали от действий внешних или внутренних злоумышленников.

Любая крупная компания с «громким» именем гарантированно «получает» первые полосы в СМИ в случае, если есть хоть малейший намек на утечку данных по ее вине. В этом году такого внимания удостоились Alibaba, AliExpress, Amazon, American Express, Apple, AT&T, Baidu, BMW, Cisco, Credit Suisse, Dell, Deutsche Telekom, Experian, Google, Huawei, владельцы сети отелей Hyatt и Marriott, KFC, Microsoft, Nokia, Oracle, T-Mobile, Toyota, Uber, Valve, Vodafone, Walmart, Yahoo.

Масштабы утечек и, как следствие, сопутствующих финансовых потерь поистине огромны — по данным компании FireEye, только на участников одной хакерской группировки FIN6 пришлась компрометация 20 млн кредитных карт, что принесло хакерам более 400 млн долл. США.

Не обошла беда и правительственные учреждения, администрации регионов, министерства и ведомства, включая силовые, полицейские структуры. Утечки данных были зарегистрированы в Госдепартаменте и Олимпийском комитете США, в американской налоговой службе, в предвыборных штабах Дональда Трампа и Хиллари Клинтон.

Общемировой тренд увеличения числа утечек информации и объемов скомпрометированных данных определяется не особенностями того или иного региона, а новыми возможностями, которые связаны с использованием информации в цифровом мире, включая перевод услуг в электронный вид, e-commerce, электронную валюту, интеллектуальную собственность в цифровом виде.

Очевидно, что чем больше появляется таких возможностей, тем выше становится интерес злоумышленников к цифровым данным. Анализ утечек данных на глобальной выборке дает наглядное представление о сегодняшней картине угроз, связанных с компрометацией данных. Например, о том, какой канал более других уязвим в настоящее время и почему, какую отрасль злоумышленники считают наиболее привлекательной и 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 организаций, оперирующих информацией ограниченного доступа (коммерческая, банковская, налоговая тайна), иными ценными информационными активами.

Методология

Исследование проводится на основе собственной базы данных, пополняемой специалистами Аналитического центра InfoWatch с 2004 года. В базу попадают публичные сообщения[1] о случаях утечки[2] информации из коммерческих, некоммерческих (государственных, муниципальных) организаций, госорганов, которые произошли вследствие умышленных или неосторожных действий[3] сотрудников и иных лиц[4]. База утечек InfoWatch насчитывает несколько тысяч зарегистрированных инцидентов.

В ходе наполнения базы каждая утечка классифицируется по ряду критериев, таких как размер организации[5], сфера деятельности (отрасль), размер причинённого ущерба[6], тип утечки (по умыслу), канал утечки[7], типы утекших данных, вектор воздействия[8].

Инциденты также классифицируются по характеру действий нарушителя. Наряду с «простыми» утечками авторы исследования выделяют следующие типы «квалифицированных» утечек:

- 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).

По оценке авторов, исследование охватывает не более 1% случаев предполагаемого совокупного количества утечек из-за высокого уровня латентности инцидентов, связанных с компрометацией информации. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества (совокупности категорий) содержали

---

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

[2] Утечка информации (данных) – утрата контроля над информацией (данными) в результате внешнего воздействия (атаки) а также действий лица, имеющего легитимный доступ к информации или действий лица, получившего неправомерный доступ к такой информации.

[3] Утечки данных разделяются на умышленные (злонамеренные) и неумышленные (случайные) в зависимости от наличия вины в действиях лица, которые привели к утечке данных. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы.

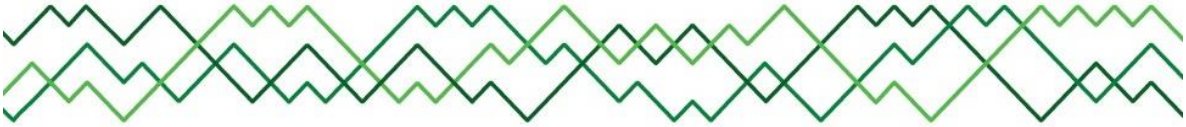
[4] Авторы классифицируют утечки по виновнику (источнику) инцидента. Наряду с внутренними нарушителями, в данную классификацию попадает внешний нарушитель.

[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 (совокупность действий пользователя корпоративной информационной системы, направленных на оборудование или программные сервисы), в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. Каналы утечек определяются только для таких утечек, которые спровоцированы действиями 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 ресурсам, неправомерные действия с инсайдерской информацией и проч.).



достаточное или избыточное количество элементов — фактических случаев утечки. Такой подход к формированию поля исследования позволяет считать полученную выборку теоретической, а выводы исследования и выявленные с учетом данной выборки тренды — репрезентативными для генеральной совокупности.

При формировании диаграмм по отдельным разрезам из выборки исключены утечки, классифицированные по основному критерию разреза как неопределенные. Например, разрез по вектору воздействия, куда входят утечки под воздействием внешних атак и внутреннего нарушителя, не содержит утечек, для которых вектор не удалось определить. То же справедливо для распределений по виновнику, умыслу и другим критериям.

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

Случаи нарушения конфиденциальности информации и иные инциденты информационной безопасности (ИБ), например DDoS-атаки, не повлекшие утечек данных, а также утечки с неясным источником данных, когда неизвестно, какой организации принадлежали скомпрометированные данные, не включаются в выборку.

Авторы настоящего исследования не ставили перед собой задач определить точное количество произошедших утечек, оценить причинённый ими реальный или возможный ущерб организациям. Исследование направлено на выявление динамики процессов, характеризующих глобальную, отраслевую и региональную картину происшествий, связанных с утечками информации.

Результаты исследования

В 2016 году Аналитическим центром InfoWatch было зарегистрировано 1556 случаев утечки конфиденциальной информации (см. Рисунок 1). В результате утечек было скомпрометировано более 3,1 млрд записей персональных данных (записей ПДн), — номера социального страхования, реквизиты пластиковых карт и иная критически важная информация.

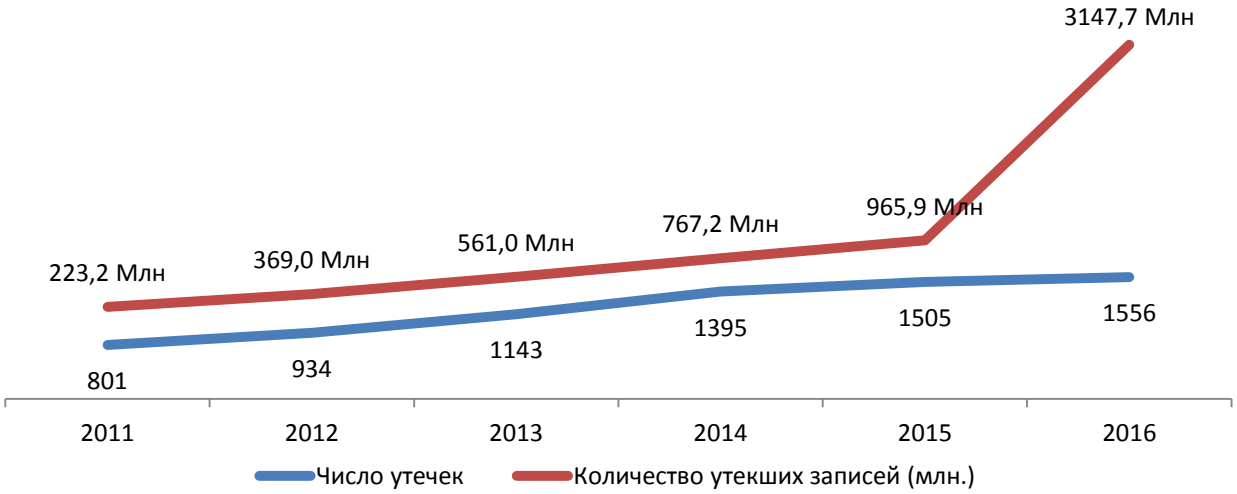


Рисунок 1. Число утечек информации и объем персональных данных, скомпрометированных в результате утечек. 2011 - 2016 гг.

Количественный рост утечек в 2016 году замедлился (Рисунок 2). Если в 2015 году этот показатель составил 7,9%, то в 2016 году число утечек выросло на 3,4%.

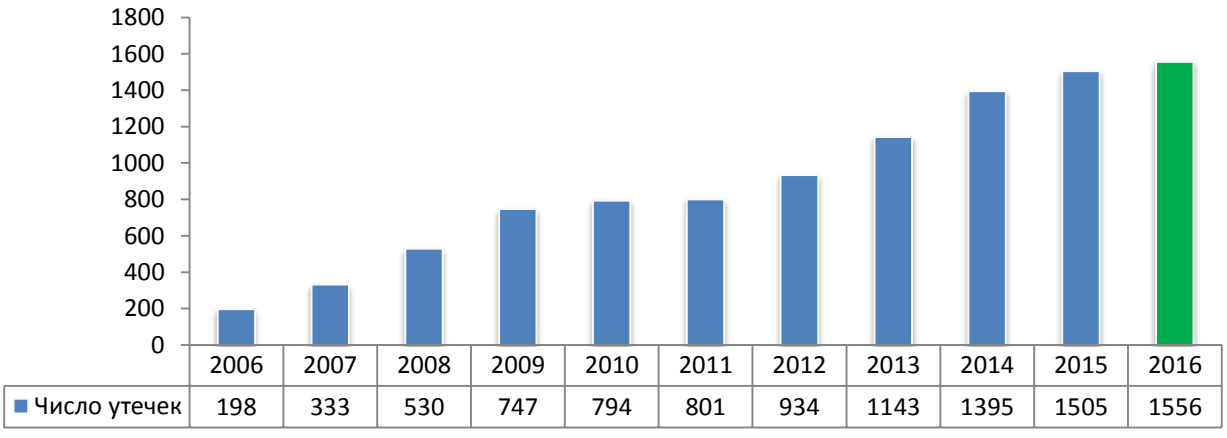


Рисунок 2. Число зарегистрированных утечек информации, 2006 -2016 гг.

В 2016 году впервые за все время наблюдений мы зафиксировали трехкратное увеличение объема данных, скомпрометированных в результате утечек, и столь же существенный рост числа скомпрометированных записей персональных данных в расчете на одну утечку (см. Рисунок 3). Причем увеличение объемов скомпрометированных данных не связано только с одной или несколькими крупными

утечками — в противном случае можно было бы говорить о случайном всплеске. На деле же было зафиксировано 79 утечек, в результате каждой из которых скомпрометировано более 1 млн записей.

Таким образом, в 2016 году картина утечек претерпела существенные изменения. Мы входим в эпоху массовой компрометации данных. Основной фактор, определяющий современную картину — количественный и качественный рост утечек.

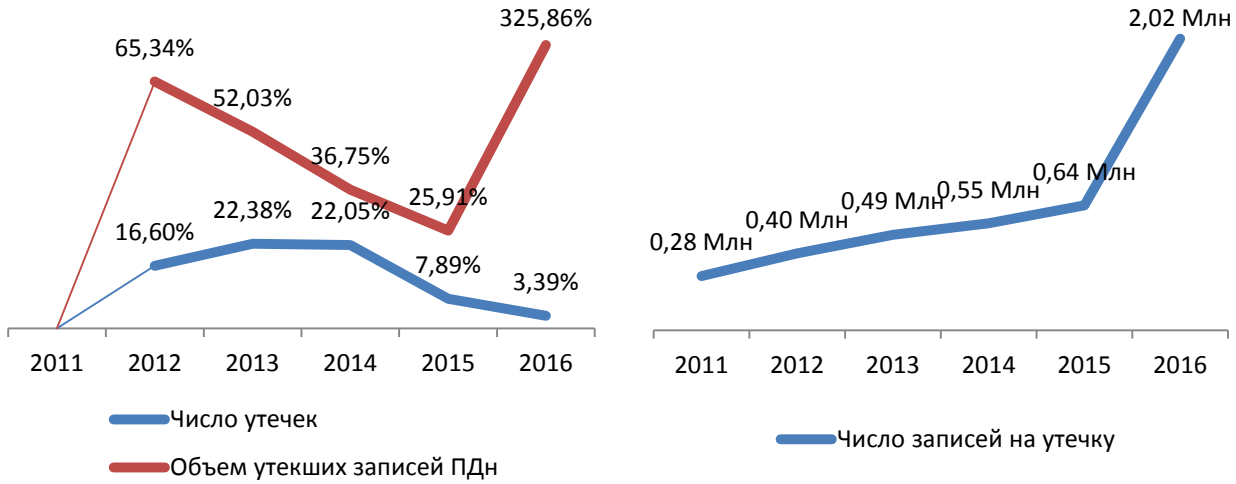


Рисунок 3. Динамика роста числа утечек и объема записей ПДн. Объем персональных данных, скомпрометированных в ходе одной утечки. 2011 -2016 гг.

В 2016 году было зарегистрировано 540 (38,2%) утечек информации, причиной которых стал внешний злоумышленник. В 873 (61,8%) случаях утечка информации произошла вследствие действий внутреннего нарушителя (см. Рисунок 4).

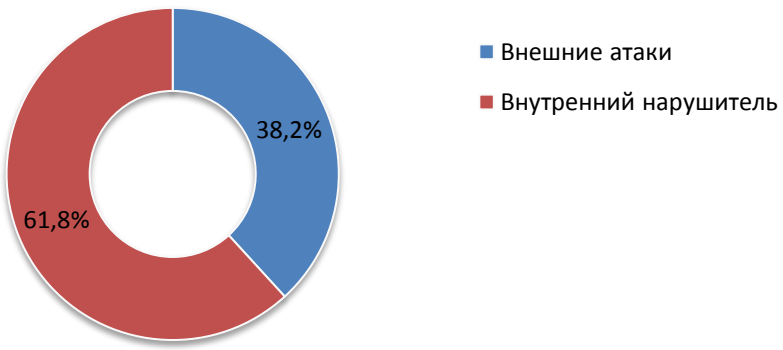


Рисунок 4. Распределение утечек по вектору воздействия[9], 2016 г.

[9] 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.)

Доля утечек под воздействием внешних атак оказалась более чем на 6 п. п. выше аналогичного показателя 2015 года (тогда на долю утечек под воздействием внешних атак пришлось 32% утечек). В результате, в 2016 году по вине внешнего злоумышленника было скомпрометировано 2,53 млрд. записей ПДн — это составляет 80% от совокупного объема скомпрометированных за год записей. Внешние атаки спровоцировали 34 из 44 зафиксированных случаев «мега-утечек»[10].

> *databreaches.net: Внешним злоумышленникам удалось украсть личную и финансовую информацию о 203 млн клиентов Experian. Хакеры получили доступ к личной информации — именам, датам рождения, адресам, телефонным номерам и прочим данным. Дамп базы данных был выставлен на продажу, в результате чего любой желающий мог купить эту информацию за 0,8082 биткоина (около $640 по текущему курсу).*

Утечки данных под воздействием внешних атак отличаются большим объемом компрометируемых данных. В среднем, на одну «внешнюю» утечку приходится 4,69 млн скомпрометированных записей ПДн. Для сравнения — в результате одной утечки данных по вине или неосторожности внутреннего нарушителя было скомпрометировано в среднем 0,56 млн записей ПДн. Атаки «извне» имеют еще одну характерную черту — злоумышленники «выносят» из атакуемого периметра все, до чего могут дотянуться.

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

Не менее интересен «информационный эффект», связанный с внешними утечками. Любая крупная утечка требует от пострадавшей организации публичной реакции. Далеко не всегда пресс-службам организаций удается с честью решить эту задачу. Иногда утечка выступает поводом для отставки руководителей организации, государственных служащих.

> *Thesmokinggun.com: Персональные данные членов палаты представителей США от демократической партии были похищены и размещены в глобальной сети Интернет. Ссылка на файл Excel с данными политиков появилась в твиттере хакера с ником Guccifer 2.0, который ранее взял на себя ответственность за взлом сети Национального комитета демократической партии. Тогда Guccifer 2.0 выложил около 20 тысяч электронных писем национального комитета демократов на портале WikiLeaks. Утечка предположительно стала причиной заявления председателя комитета демократов Дебби Вассерман-Шульца о намерении уйти в отставку.*

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

Впрочем, это не означает, что утечки, случившиеся в результате недозволенных действий внутреннего нарушителя менее разрушительны, чем утечки, произошедшие в результате внешнего воздействия. Основные отличия результатов внутреннего воздействия от внешнего заключаются в характере последствий для организации-жертвы.

Если эффект «внешней» утечки можно сравнить с ковровой бомбардировкой, то «внутренняя» утечка ближе к точечному бомбометанию — под угрозой оказывается критически важная информация, а размер потенциального финансового ущерба практически не ограничен и может достигать стоимости всего бизнеса пострадавшей компании.

> *bloomberg.com: Британские букмекерские компании 888 Holdings Plc и Rank Group Plc отказались от поглощения William Hill — еще одного крупного участника игорного рынка, за 4,1 млрд долларов США. Основная причина срыва переговоров — утечка данных на стороне William Hill.*

В связи с особенностями природы внутренних утечек необходимо обратить внимание на проблему «привилегированных» пользователей — топ-менеджмента, системных администраторов, иных сотрудников, чьи права доступа к информации практически не ограничены, включая самих специалистов по информационной безопасности. Контролировать действия таких сотрудников чрезвычайно сложно, а последствия, к которым приводят ошибки или злонамеренная деятельность «высокопоставленных» нарушителей, по масштабу можно сравнить со стихийным бедствием.

> *Руководство компании Hitsniffer, специализирующейся на веб-аналитике, объявило о приостановке бизнеса из-за кражи клиентских баз компании одним из бывших сотрудников.*

В 2016 году в 36% случаев виновниками утечек информации были настоящие (33,9%) или бывшие (2,1%) сотрудники организаций. Более чем в 2% случаев была зафиксирована вина руководителей (топ-менеджмент, главы департаментов и отделов) и системных администраторов. Доля утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к охраняемой информации, составила 6% (см. Рисунок 5).

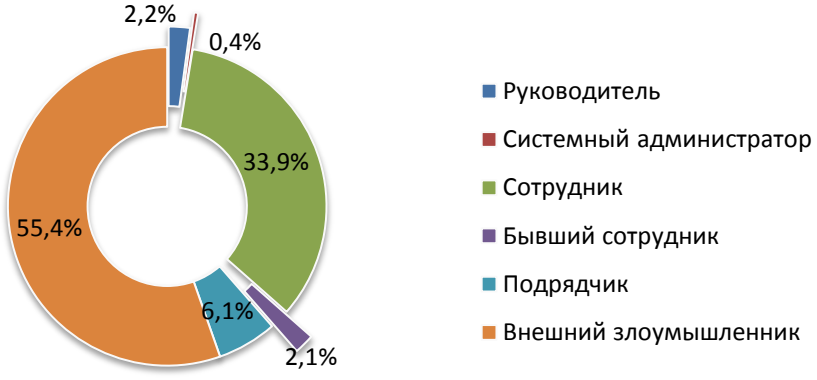


Рисунок 5. Распределение утечек по источнику (виновнику), 2016 г.

Доля утечек персональных и платежных данных в распределении утечек по типу информации осталась на уровне прежних лет, составив 93% (см. Рисунок 6).

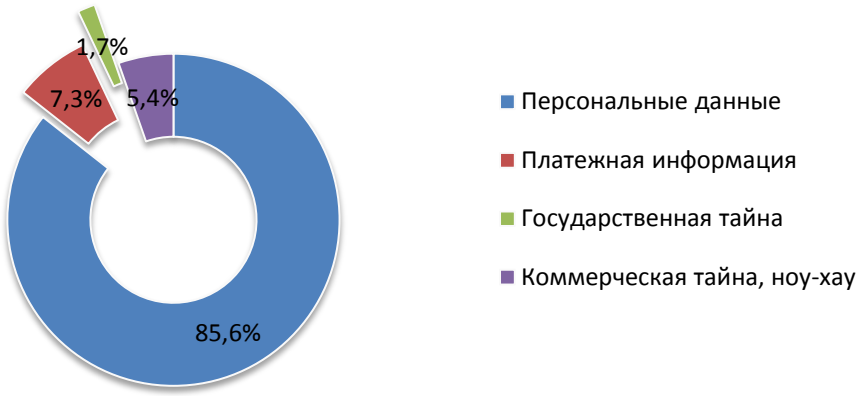


Рисунок 6. Распределение утечек по типам данных, 2016 г.

В 2016 году доля утечек данных, сопряженных с последующим использованием скомпрометированной информации в целях мошенничества (как правило, банковский фрод) снизилась на 3,3 п. п. до 7%.

Рисунок 7. Распределение инцидентов по характеру, 2016 г.

10% инцидентов классифицированы как нарушения, сопряженные с получением несанкционированного доступа к информации (превышение прав доступа, манипуляция с информацией, которая не нужна сотруднику для исполнения служебных обязанностей).

Вывод

Трехкратное увеличение объема скомпрометированных данных свидетельствует о растущей день ото дня ценности информации в цифровом виде. Причем если количественный рост утечек прогнозировать сложно — не исключено, что он попросту остановится, то сценарий, при котором объем скомпрометированных данных растет год от года, следует считать наиболее вероятным.

Каналы утечек

В 2016 году сократилась доля утечек в результате потери оборудования (на 4,8 п. п.), а также по таким каналам, как «электронная почта» (на 1 п. п.) и «бумажные документы» (на 7 п. п.). Доли утечек через съемные носители, мобильные устройства остались на уровне 2015 года. Доля «сетевого» канала выросла на 11,6 п. п. (см. Рисунок 8).

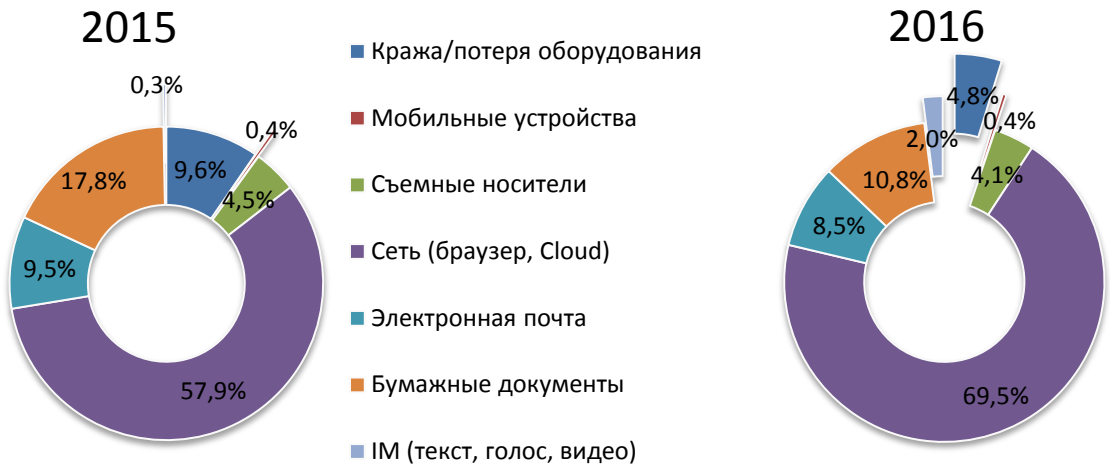


Рисунок 8. Распределение утечек по каналам, 2015 – 2016 гг.

В распределении утечек данных в результате случайных действий сотрудников наиболее заметны утечки через электронную почту — 23,7%, бумажные носители — 16,2%, съемные носители — 6,7% и в результате кражи или потери оборудования — 5,3%. На сетевой канал приходится 47,1% всех зафиксированных случайных утечек.

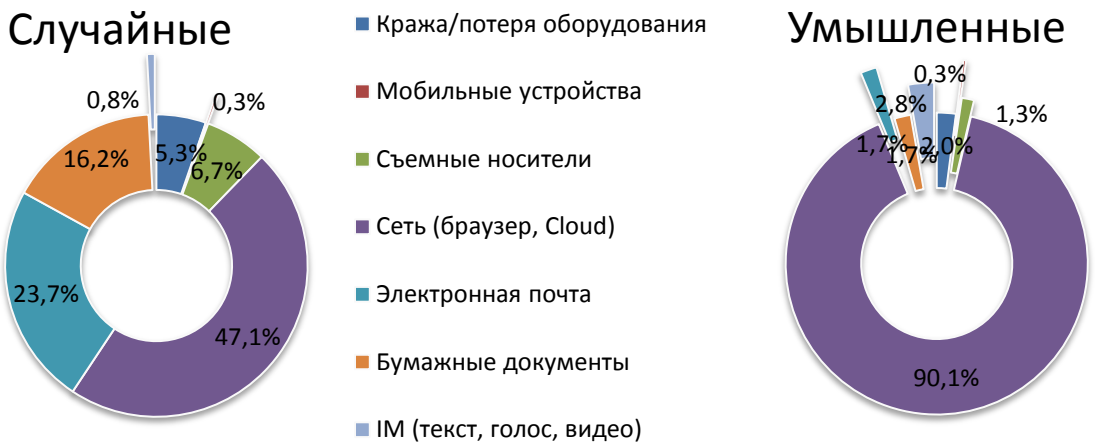


Рисунок 9. Распределение случайных и умышленных утечек, 2016 гг.

Распределение умышленных утечек информации характеризуется преобладанием сетевого канала. Более 90% случаев намеренной компрометации данных связаны с неправомерной передачей или разглашением информации с использованием сети Интернет (в том числе веб-сервисов, электронной почты и иных интернет-ресурсов).

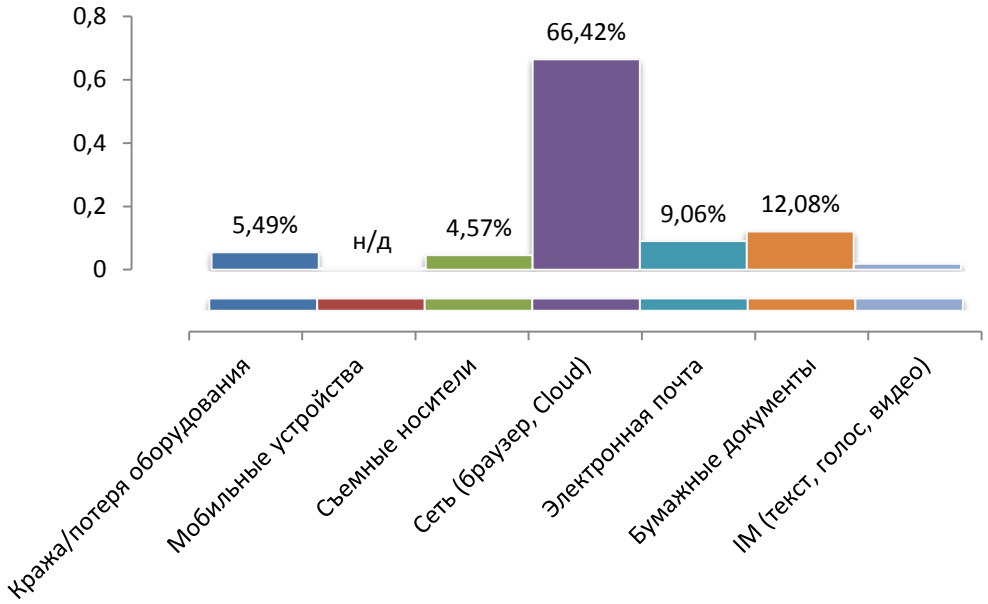


Рисунок 10. Утечки персональных данных, распределение по каналам, 2016 г.

Сетевой канал выходит на первый план как по общему объему скомпрометированных персональных данных, так и по количеству утечек. Большая часть (>66%) утечек персональных данных приходится на сеть (см. Рисунок 10).

В случае с внутренними нарушителями компании имели дело с разнообразными сценариями — сохранением конфиденциальной информации в облаках Box, OneDrive и других, использованием бесплатных почтовых аккаунтов (веб-почта).

Сценарии внешних взломов менее вариативны. Хакеры, как правило, не слишком хорошо знакомы со структурой данных организации, например, с тем, где хранится наиболее ценная информация и что она собой представляет, поэтому «берут» все, что представляет ценность.

> 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.*

Сетевой канал следует признать наиболее «популярным» применительно и к случайным, и к умышленным утечкам. «Сетевые» утечки характеризует высокий уровень критичности данных, огромные объемы скомпрометированной информации.

РИА Новости: В результате хакерской атаки на инфраструктуру французской компании DCNS, которая занимается строительством подводных лодок, похищены 22,4 тыс. страниц секретной документации. Французская госкомпания DCNS участвует в проекте по строительству шести субмарин класса Scorpene для индийского флота и одновременно строит 12 подлодок по заказу ВМФ Австралии. В результате утечки описание коммуникационных систем, подводных датчиков, систем боевого управления, навигационных систем и систем пуска торпед оказались в руках австралийского издания и, возможно, третьих лиц.

Небольшая доля умышленных утечек через мобильные устройства, съемные носители, электронную почту и бумажные документы объясняется тем, что злоумышленники все меньше используют эти каналы для совершения противоправных действий. «Продвинутый» нарушитель осведомлен, что современные средства контроля позволяют успешно перехватывать передачу конфиденциальной информации по этим каналам, и не рискует понапрасну.

Вывод

Доминирование сетевого канала в распределении случайных и умышленных утечек свидетельствует, во-первых, о растущем значении этого канала для бизнеса. Число коммуникационных сервисов, «завязанных» на сеть, огромно. Количество ошибок сотрудников, работающих с этими сервисами, год от года только увеличивается. Как следствие, растет доля случайных утечек при передаче информации по сети и публикации данных в интернете.

С другой стороны, злоумышленники все реже используют заведомо контролируемые каналы передачи информации — электронную почту, сервисы мгновенных сообщений. В этом смысле сеть все еще остается каналом передачи данных, где возможности систем контроля и защиты в целом превосходят возможности злоумышленников.

Отраслевая карта

По сравнению с данными 2015 года, распределение утечек по типу организации не претерпело критических изменений (см. Рисунок 11).

Рисунок 11. Распределение утечек по типу организации, 2015 - 2016 гг.

Чаще всего фиксировались утечки данных из медицинских организаций (25,8%), реже всего — в сфере промышленности и транспорта (3,9%). По объему скомпрометированных записей пальма первенства принадлежит компаниям высокотехнологичного сектора, прежде всего крупным интернет-сервисам и торговым онлайн-площадкам. На долю таких организаций приходится почти три четверти (73,6%) от всего объема скомпрометированных в2016 году данных. Заметна доля торговых компаний, отелей и ресторанов — 11,9%. На государственные органы и муниципальные учреждения приходится 9,9% от всего объема скомпрометированных данных (см. Рисунок 12).

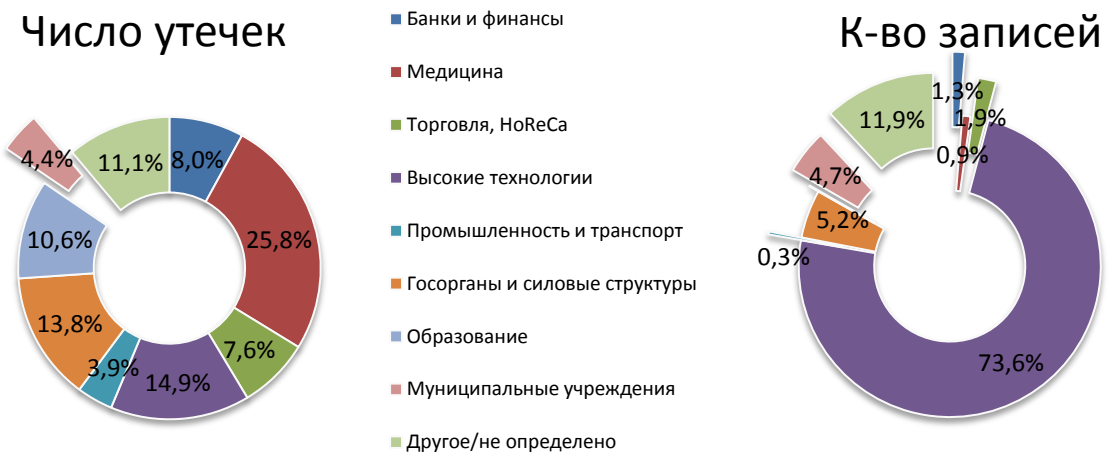


Рисунок 12. Распределение числа утечек и объема скомпрометированных персональных данных по отраслям, 2016 г.

Приведенные диаграммы дают фактическую картину, общее представление об утечках информации и объемах скомпрометированных данных в различных отраслях. Важнее выяснить, какие сегменты в настоящий момент являются наиболее «привлекательными» для злоумышленников.

«Привлекательность» отрасли прямо обусловлена «ликвидностью» данных, которые обрабатывают компании этого сектора[11]. Представление злоумышленников об уровне защиты данных в отрасли влияет на «привлекательность» обратно пропорционально. Проиллюстрируем это формулой:

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

Показателем «привлекательности» можно считать число умышленных утечек в конкретной отрасли. Отраслевое распределение умышленных утечек одного типа даст нам ответ на вопрос, какие сегменты наиболее «привлекательны» для злоумышленника (и наиболее уязвимы).

В 2016 году,как и годом ранее, наиболее «привлекательными» оказались торговые, транспортные компании, к которым добавились финансовые учреждения.

> securitylab.ru: *В результате хакерской атаки были украдены персональные данные порядка 6 млн клиентов крупнейшего в Британии оператора сотовой связи Three UK. Скомпрометированная информация включает имена, номера телефонов, адреса и даты рождения.*

В этих отраслях более половины утечек, сопровождавшихся компрометацией персональных данных, носили умышленный характер (см. Рисунок 13).

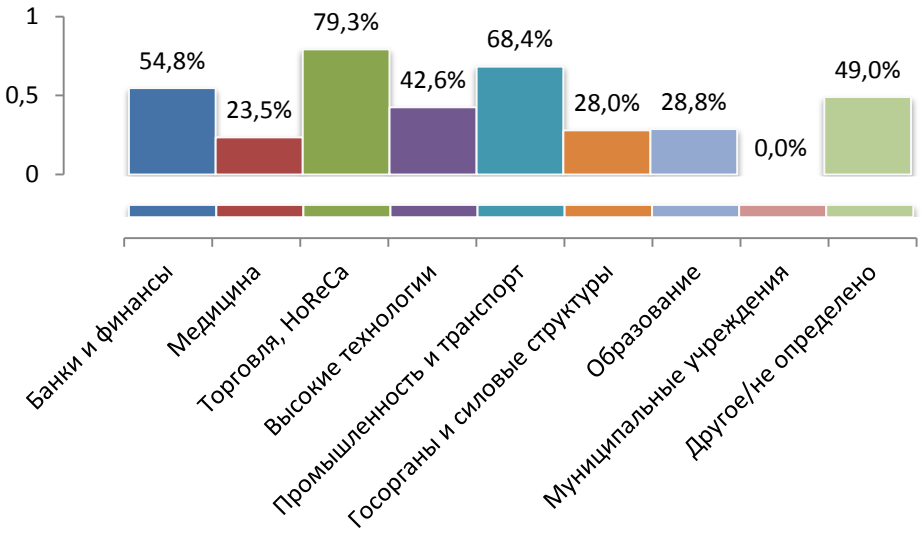


Рисунок 13. Доля умышленных утечек ПДн от общего количества утечек ПДн по отраслям, 2016 г.

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

Если перестроить уже приведенное распределение в зависимости от вектора атаки, мы получим наглядное представление о «привлекательности» конкретной отрасли для внешнего и внутреннего злоумышленника (см. Рисунок 14).

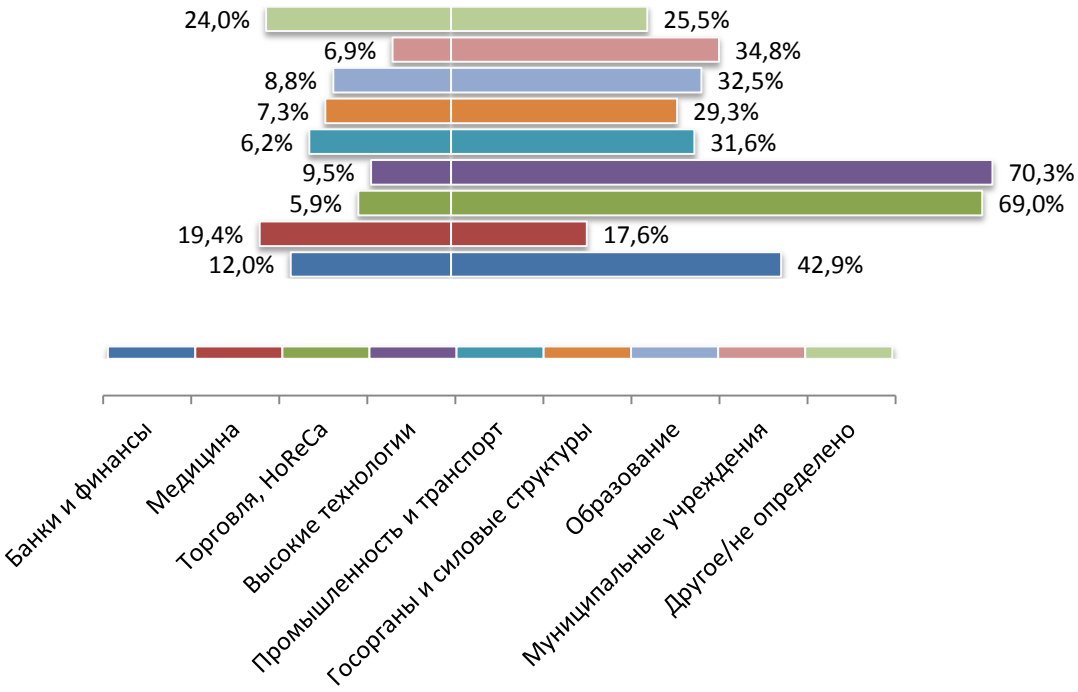


Рисунок 14. Доля умышленных утечек ПДн под воздействием внутреннего (слева) и внешнего (справа) злоумышленника от общего числа утечек ПДн по отраслям, 2016 г.

Как видно из диаграммы, высокотехнологичные компании, наряду с транспортным и банковским сектором, чаще всего становились жертвами внешних атак, направленных на хищение данных. Доля ПДн, украденных внутренними злоумышленниками, в этих отраслях незначительна.

С другой стороны, от злонамеренных действий внутреннего нарушителя чаще всего страдали медучреждения и банки. Одна из основных причин — чрезвычайно высокая ликвидность данных, с которыми работает персонал медицинских и финансовых учреждений.

> databreaches.net: *Данные 9,3 млн клиентов программ медицинского страхования были украдены и выставлены на продажу. Хакеры оценили базу данных в 750 биткоинов — 500 тыс. долларов США. Среди скомпрометированных данных были номера социального страхования, адреса и мобильные телефоны граждан.*

Более объемно картину утечек иллюстрирует отраслевая карта (см. Рисунок 15). Размер «пузырьков» показывает совокупный объем скомпрометированных записей — млн ПДн (по всем компаниям сегмента), положение «пузырьков» по вертикали

отражает число утечек в отрасли[12]. В зависимости от размера пострадавшей компании, карта разбита на три диаграммы — небольшие, средние и крупные организации.

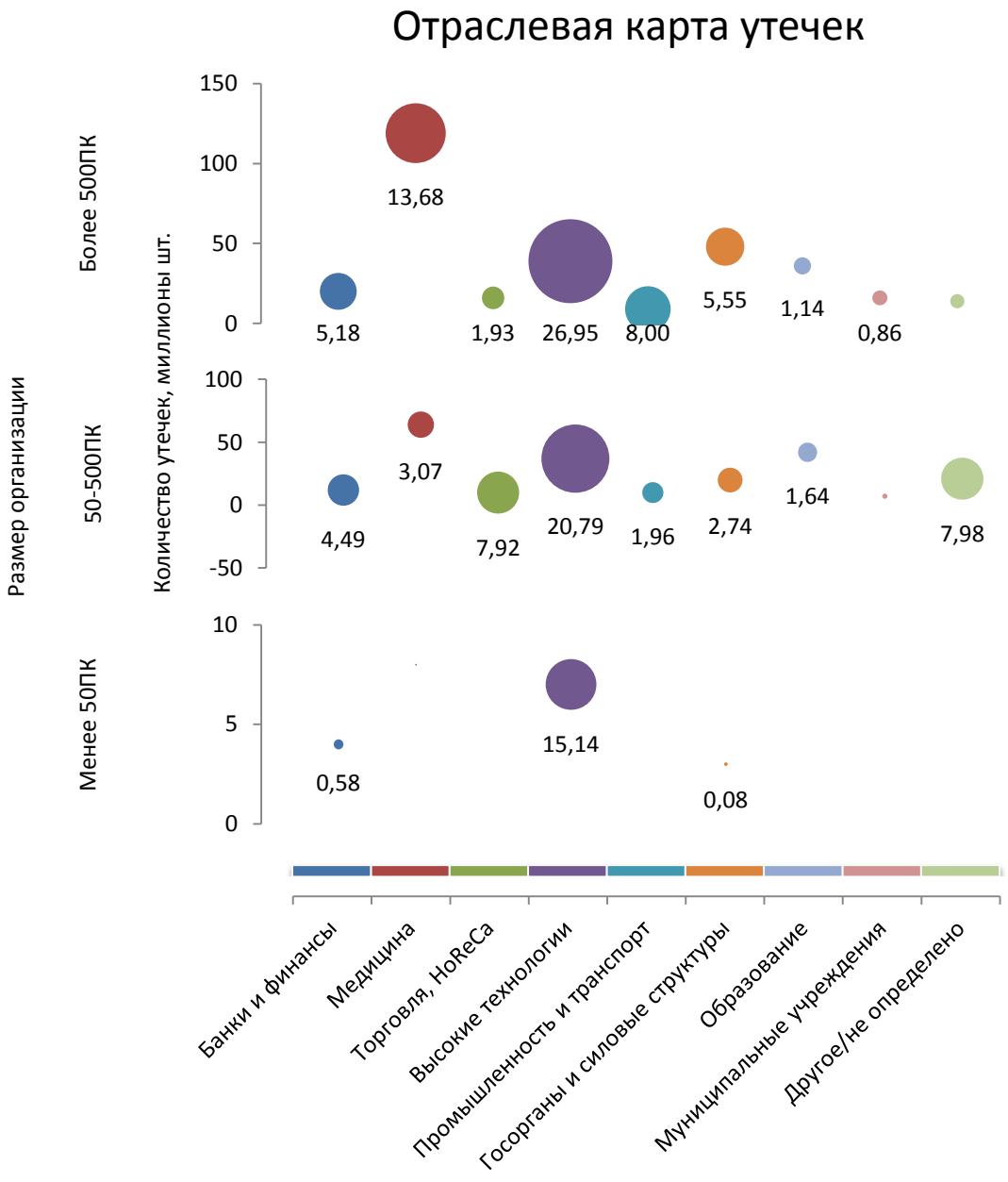


Рисунок 15. Отраслевая карта утечек персональных данных, млн единиц, 2016 г.

Наибольший объем скомпрометированных персональных данных приходится на высокотехнологичные компании (интернет-сервисы, провайдеры цифровых услуг,

[12] 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.

операторы сотовой связи). Эти компании можно назвать пионерами в использовании цифровых технологий обработки и хранения данных. Лидерство по показателю объема скомпрометированных данных — лишь следствие, плата за использование передовых подходов к работе с информацией.

В 2016 году распределение утечек между средними (до 500 ПК) и крупными (более 500 ПК) организациями получилось примерно одинаковым как по числу утечек, так и по объему скомпрометированных данных (см. Рисунок 16).

Рисунок 16. Распределение утечек по размеру организации 2016 г.

Крупные компании допускают чуть больше утечек в количественном выражении, при этом объем потерянных данных в расчете на одну утечку у них несколько ниже, чем у компаний среднего размера. Вероятно, в этой связи следует отметить недостаточность финансирования, выделяемого на защиту информации от утечек в сегменте малого и среднего бизнеса.

Вывод

В ближайшее время вряд ли следует ожидать каких-то серьезных изменений в отраслевой картине утечек. Оба фактора, так или иначе влияющих на динамику утечек в разрезе конкретных отраслей — это ликвидность и защищенность данных, — отличает завидная устойчивость. Представление о том, что банки, страховые компании обрабатывают наиболее ликвидную информацию, сложилось очень давно. Мнение о надежности или слабости систем защиты в той или иной отрасли также не подвержено особым колебаниям. В итоге мы имеем стабильную картину «привлекательности» и, как результат, понимание того, какая отрасль в настоящее время наиболее уязвима.

Накладывая данное понимание на реальную динамическую картину утечек, можно с уверенностью прогнозировать рост числа и мощности внешних атак в отношении высокотехнологичных компаний, медицинских учреждений и компаний, связанных с медстрахованием, а также финансовых организаций.

Региональные особенности

В распределении утечек по регионам в 2016 году традиционно первую позицию по количеству утечек заняли США (838 случаев или 57% от всех произошедших). Россия вновь оказалась на уже привычном втором месте. При этом в 2016 году на долю России пришлось 213 случаев компрометации данных — почти в два раза больше, чем годом ранее.

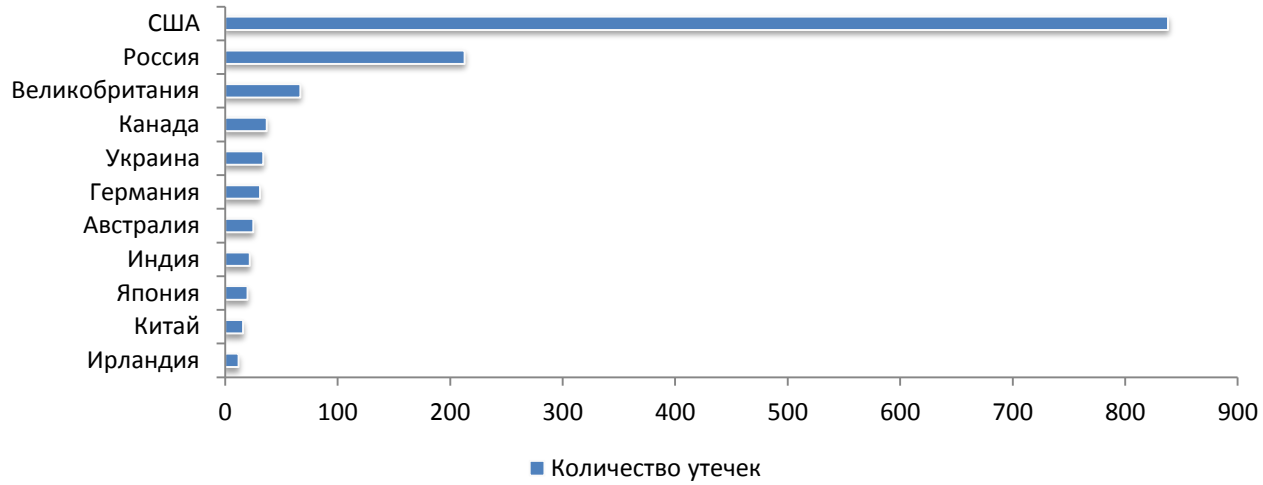


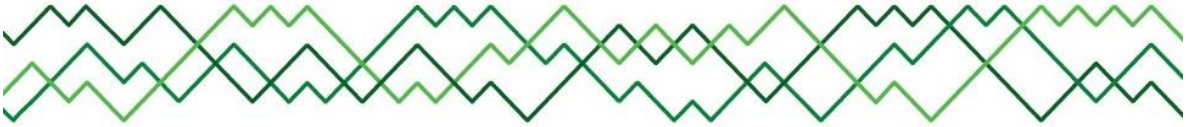
Рисунок 17. Распределение утечек по странам, 2016 г.

Авторы исследования уже отмечали, что современная глобальная картина утечек данных с незначительными изменениями характерна для всех стран, где оперируют информацией в электронном виде. Различия между регионами и странами коренятся в ментальной плоскости, вопросах восприятия утечек данных, оценке последствий, возможного ущерба, опасности утечек. Так информация об утечках все чаще появляется в прессе таких стран, как Индонезия, Вьетнам и Индия — государств, ранее не попадавших в нашу выборку.

> economictimes.indiatimes.com: *Платежные данные 3,2 млн клиентов 19 индийских банков оказались скомпрометированы в результате утечки. Журналисты назвали эту утечку крупнейшей в стране.*

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, например — медсестры, официанты или полицейские, которые всего лишь хотят подзаработать немного денег на использовании чужих данных.

В менее развитых регионах ситуация несколько иная. В количественном выражении утечек там происходит значительно меньше, зато их масштаб и характер вполне сопоставимы с «лучшими образцами» утечек данных в странах западного мира.



Заключение и выводы

На протяжении последних двух-трех лет мы стали свидетелями того, как картина утечек изменилась кардинальным образом. Сегодня положительную динамику изменения объема скомпрометированных данных полностью определяют утечки под воздействием внешнего нарушителя — «внешние» утечки. На долю внешних утечек приходится более 94% от всего объема скомпрометированных данных. Трехкратный рост этого показателя (объем украденных данных) в 2016 году, таким образом, напрямую связан с внешними утечками.

Однако из приведенных выше примеров следует, что утечка даже единственного документа может поставить под угрозу сам факт существования или смысл деятельности организации. Как правило, виновниками таких утечек становятся представители высшего руководства организации и иные привилегированные пользователи. Отметим, что как раз доля утечек информации по вине привилегированных пользователей в 2016 году существенно выросла.

Сетевой канал полностью доминирует в распределении умышленных утечек, а также год от года увеличивает долю в распределении случайных утечек. Виной тому, во-первых, рост коммуникационных сервисов, то есть возможностей для обработки, хранения и передачи информации в электронном виде. С другой стороны, злоумышленники давно отказались от использования контролируемых каналов передачи информации — электронной почты, съемных носителей.

Примечательно перераспределение утечек между средними и крупными компаниями. Если ранее мы говорили о том, что средний бизнес является «поставщиком» данных для злоумышленников, то в этом году ситуация несколько выровнялась — средний бизнес по-прежнему весьма чувствителен к атакам извне, в целом хуже противостоит современным угрозам ИБ, однако заметного разрыва более не наблюдается. Вероятно, средние компании стали уделять больше внимания вопросам безопасности собственных данных и информации о своих клиентах.

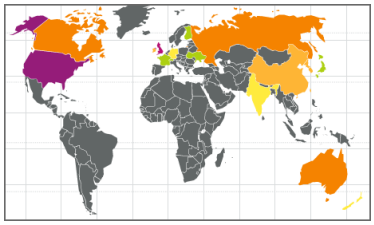
Однако при всех заметных позитивных тенденциях, общий вывод исследования неутешителен. Мы вступаем в эпоху массовой компрометации данных. Перефразируя известное выражение, дело не в том, взломают ли какую-то конкретную компанию в принципе, а в том, КОГДА ее взломают. Владельцам бизнеса, сотрудникам служб информационной безопасности стоит задуматься уже сейчас о том, что именно необходимо защищать как наиболее ценный актив, от кого защищать и как именно это сделать. Обеспечить безопасность всего ото всех уже вряд ли получится.

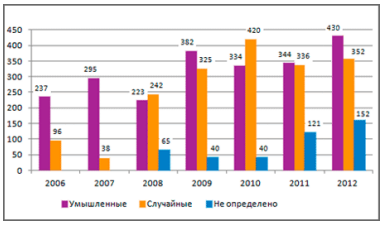
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

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 утрату контроля над информацией (данными) в результате внешнего воздействия (атаки) а также действий лица, имеющего легитимный доступ к информации или действий лица, получившего неправомерный доступ к такой 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».*