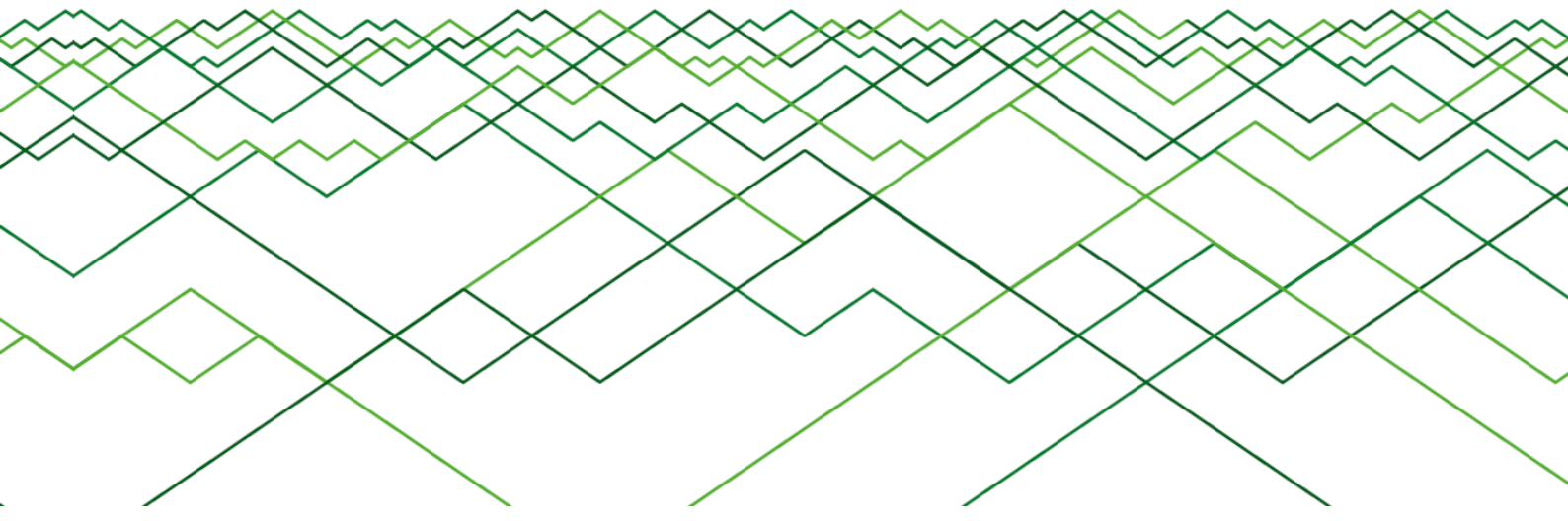
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аналитический центр InfoWatch
www.infowatch.ru/analytics

Глобальное исследование утечек конфиденциальной информации в I полугодии 2015 года



INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Оглавление

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Только цифры

- ✓ В I полугодии 2015 года в мире обнародовано (в СМИ и иных источниках) и зарегистрировано Аналитическим центром InfoWatch **723** случая утечки конфиденциальной информации, что на **10%** превышает количество утечек, зарегистрированных за аналогичный период 2014 года.
- ✓ Внешние атаки стали причиной **32%** утечек данных. Доля таких утечек выросла на 9 п. п. по сравнению с показателем I полугодия 2014 года.
- ✓ **90%** утечек связаны с компрометацией персональных данных. За исследуемый период скомпрометированы более **262 млн** записей, в том числе платежная информация.
- ✓ За I полугодие 2015 году зафиксировано **8** «мега-утечек». В результате каждой «утекло» более **10 млн** персональных данных. На «мега-утечки» пришлось **83%** всех скомпрометированных записей.
- ✓ В **58%** случаев виновными в утечке информации оказались сотрудники компаний. В **1%** случаев – высшие руководители организаций.
- ✓ Транспортные компании, наряду с интернет-сервисами, ретейлерами и медицинскими учреждениями, являются основным источником утечек персональных данных.
- ✓ Россия заняла второе место по числу утечек, ставших достоянием общественности. В исследуемый период зарегистрировано **59** случаев утечки конфиденциальной информации из российских компаний и государственных организаций. Число «российских» утечек по сравнению с аналогичным периодом 2014 года сократилось на **39%**.

Аннотация

Аналитический Центр компании InfoWatch представляет отчет об исследовании утечек конфиденциальной информации в I полугодии 2015 года. Авторы исследования на протяжении многих лет занимаются выявлением и анализом факторов, влияющих на формирование глобальной картины утечек данных. Особое внимание уделяется изучению последствий, которыми оборачиваются утечки данных.

Сообщения об утечках не сходят с полос ведущих СМИ, что связано как с масштабом явления (миллионы скомпрометированных данных), так и с громкими именами компаний, пострадавших от утечек. В числе таких организаций только за I полугодие 2014 года: Anthem, Apple, AT&T, British Airways, DreamWorks, Electronic Arts, Equifax, FIA, Google, HBO, HSBC, HTC, JP Morgan Chase, Kia Motors, Lenovo, Lufthansa, Microsoft, Morgan Stanley, NVIDIA, PayPal, PwC, Samsung, Starbucks, Tele2, Toyota, Twitter, Uber, United Airlines, Yahoo, ВТБ-24, МТС, РЖД, СОГАЗ.

Не обошла беда правительственные учреждения, администрации регионов, министерства и силовые ведомства, полицейские департаменты. Утечки данных зарегистрированы даже в АНБ и ЦРУ. В связи с утечками упоминались известные политики Дмитрий Медведев, Хилари Клинтон, Джеб Буш.

> *Ведомости: Число пострадавших от кибератаки на кадровое управление правительства США (U.S. Office of Personnel Management – OPM) возросло до 18 млн. Персональные данные настоящих и бывших сотрудников управления оказались скомпрометированы. Данные ведомства хранились в дата-центре министерства внутренних дел наряду с данными многих других федеральных структур. Возможно, число жертв увеличится, так как злоумышленники получили доступ к данным формы SF86, где содержится информация о членах семей госслужащих.*

Российская картина утечек стремительно приближается к американской. Многомиллионных утечек данных под воздействием внешних атак в России пока не зафиксировано. А вот мошенничество с чужими персональными данными в исполнении сотрудников банков, страховых компаний, салонов сотовой связи происходит чуть ли не ежедневно. Такие правонарушения стали нормой для нашей страны, хотя некоторое время назад казались экзотикой.

Авторы исследования уверены, что всесторонний анализ глобальной картины утечек (где преобладают случаи утечек в зарубежных странах, наиболее «продвинутых» в плане информационной безопасности) полезен как для российского рынка, так и для стран со схожей в вопросе защиты информации ситуацией. Результаты 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).

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Методология

Исследование основывается на собственной базе данных, пополняемой специалистами Аналитического центра InfoWatch с 2004 года. В базу Центра включаются публичные сообщения[1] о случаях утечки[2] информации из коммерческих и некоммерческих (государственных, муниципальных) организаций вследствие злонамеренных или неосторожных действий (бездействия)[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, и пр.

С 2014 года в базу добавляются утечки данных, произошедшие вследствие внешнего воздействия[8] (таргетированная атака, фишинг, взлом веб-ресурса и пр.). В связи с этим к списку критериев утечки добавлен вектор воздействия[9].

Также с 2014 года инциденты классифицируются по характеру действий нарушителя. Авторы исследования наряду с утечками (компрометацией данных с потерей контроля над информацией) выделяют утечки данных, когда сотрудник, имеющий легитимный доступ, 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).

---

[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] Авторы провели коррекцию статистических показателей, выведенных на основе данных 2013 года и ранее для получения аккуратного сравнения этих данных с данными 2014 года и позднее, когда утечки данных под влиянием внешнего воздействия не учитывались

[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.)

Исследование охватывает не более 1% случаев от предполагаемого совокупного количества утечек. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества (категории) содержали достаточное или избыточное количество элементов (фактических случаев утечки). Такой подход к формированию поля исследования позволяет считать получившуюся выборку достаточной для выявления и прогнозирования закономерностей на всей совокупности утечек.

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.

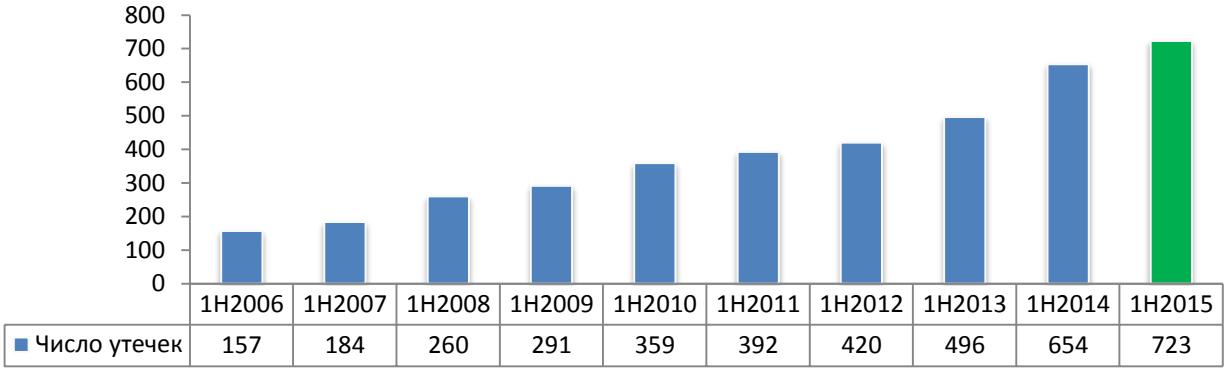
Использование ограниченной выборки для построения диаграмм специально оговаривается. В иных случаях авторы оперируют полной выборкой (без исключения отдельных утечек).

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

Данные в тексте отчета (количественные и процентные) округлены (за некоторым исключением) до целых значений. В диаграммах – до десятых.

Общая статистика

За I полугодие 2015 года Аналитическим центром InfoWatch зарегистрировано 723 случая утечки конфиденциальной информации (см. Рисунок 1). Это на 10% больше, чем за аналогичный период 2014 года (654 утечки). В пределах исследуемого периода рост утечек замедлился на 22 процентных пункта (п. п.) по сравнению с показателями I полугодия 2014 года (тогда рост к 2013 году составил 32%).



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

Рисунок 1. Число зарегистрированных утечек информации, ½ 2006 – ½ 2015 гг.

Зарегистрирована 471 (65%) утечка информации, причиной которой стал внутренний нарушитель. В 233 (32%) случаях утечка информации произошла из-за внешнего воздействия. Для некоторых случаев (2,6%) установить вектор воздействия (направление атаки) оказалось невозможно (см. Рисунок 2).

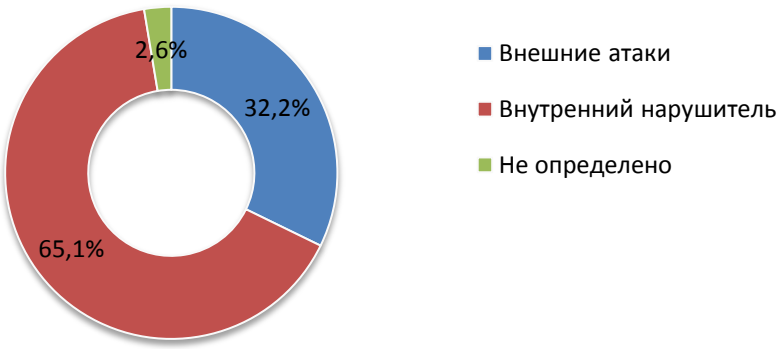


Рисунок 2. Распределение утечек по вектору воздействия, ½ 2015 г.

Доля утечек под воздействием внешних атак оказалась на 9 п. п. выше аналогичного показателя за I полугодие 2014 года (тогда на долю утечек под воздействием внешних атак пришлось 22% утечек).

На одну утечку в среднем приходится 0,36 млн скомпрометированных записей о персональных данных. Общий объем скомпрометированных персональных данных за исследуемый период составил 262 млн записей.

В результате внешнего воздействия скомпрометировано 230 млн персональных данных (0,98 млн на утечку). Итогом воздействия внутреннего нарушителя стала компрометация 30 млн записей (0,06 млн на утечку).

Внешние атаки спровоцировали 7 из 8 зафиксированных «мега-утечек»[10]. На «мега-утечки» приходится 218 млн записей о персональных данных, скомпрометированных в результате утечек в I полугодии 2015 года (83% от общего числа).

Доля утечек под воздействием внешнего злоумышленника выросла на 9 п. п. и составила 32%. Доля случаев, когда виновника не удалось определить, по сравнению с показателем I полугодия 2014 года снизилась на 2 п. п. и составила 6%. (см. Рисунок 3).

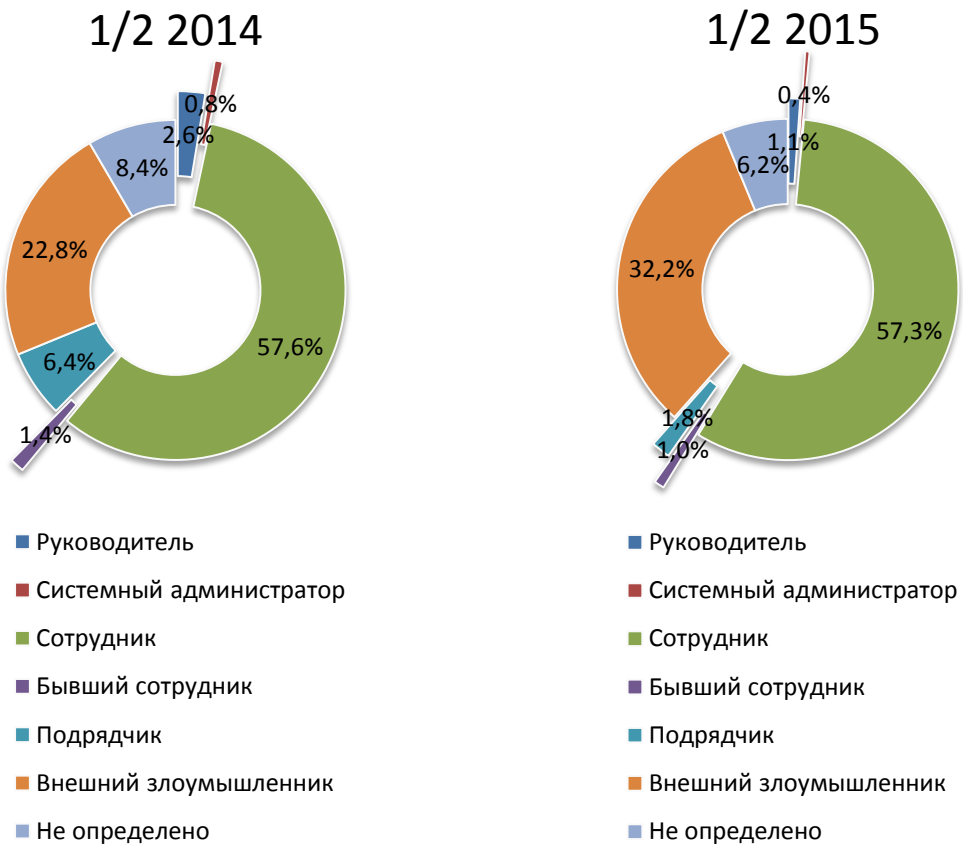


Рисунок 3. Распределение утечек по источнику (виновнику), ½ 2014 – ½ 2015 г.

В 58% случаев виновниками утечек информации были настоящие или бывшие сотрудники - 57% и 1% соответственно (изменение к предыдущему периоду незначительно). Более чем в 1% случаев (-1 п. п. к данным 2014 года) зафиксирована вина руководителей организаций (топ-менеджмент, главы отделов и департаментов). Доля утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к охраняемой информации, упала на 5 п. п., составив 2%.

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

Доля утечек персональных и платежных данных[11] осталась на уровне 2014 года – 90%. Незначительно (+1 п. п.) подросли утечки информации, составляющей государственную и коммерческую тайну. Доли таких утечек - 3% и 5% соответственно (Рисунок 4).

Рисунок 4. Распределение утечек по типам данных, ½ 2014 – ½ 2015 г.

Как и год назад, мы наблюдали огромное число утечек информации, связанных с использованием персональных данных в целях мошенничества – преступления, известные как «кража личности» (identity theft). Внутренние и внешние злоумышленники пытаются любым способом получить доступ к базам с персональными данными клиентов и сотрудников компаний, используют эти данные при проведении мошеннических финансовых операций. Например, при оформлении электронных требований на возврат налогов.

> *nola.com: Бывший глава программ лечения от наркозависимости в штате Луизина предстанет перед судом по обвинению в краже личности и злоупотреблении служебным положением. Шанта Барнс (Shanta Barnes) выписывал рецепты на оксикодон (опиоид, обезболивающий препарат). Однако пациенты, на чье имя выписывался препарат, его не получали. Господин Барнс продавал лекарства через систему распространителей.*

[11] 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».

При этом он умудрялся получать компенсацию за выписанные и купленные препараты.

Впрочем, по сравнению с аналогичным периодом 2014 года, в 2015-м году доля утечек данных, сопряженных с последующим использованием скомпрометированной информации в целях мошенничества (как правило, банковский фрод) снизилась и составила 11%. (см. Рисунок 5).

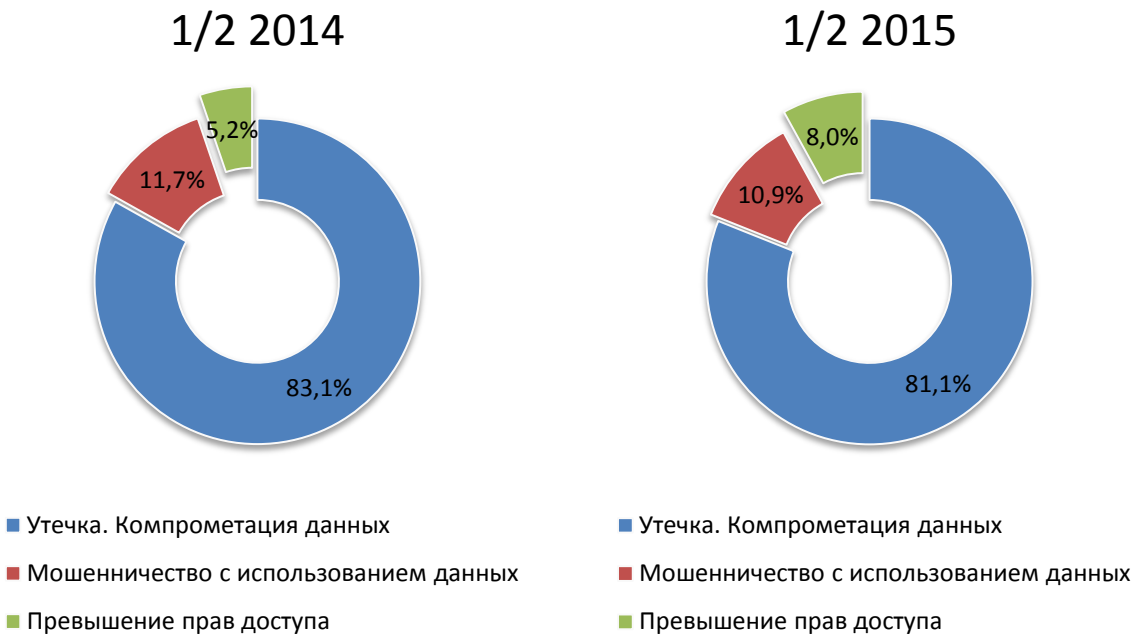


Рисунок 5. Распределение утечек по характеру, ½ 2014 – ½ 2015 г.

Доля утечек данных, сопряженных с неправомерным доступом к информации (злоупотребление правами доступа, внутренний шпионаж), составила 8%.

nj.com: Капитан полиции города Ньюарк (Нью-Джерси, США) арестован по обвинению в незаконном доступе к информации. Шестидесятилетний Антонио Буно вместе с бывшим сотрудником полиции Дино Д'Элиа в ходе расследования мошенничества со страховками получили доступ к базе данных неназванной организации. Информацию из этой базы предприимчивые полицейские продавали по 100 долларов за запись.

81% инцидентов, сопряженных с потерей контроля над информацией, относится к типу «классических» утечек, не отягощенных «особой» ролью нарушителя – нет превышения прав доступа, нет использования в целях мошенничества. На диаграмме мы их обозначили как утечки, приведшие к компрометации данных[12].

actualpolitics.ru: Личные данные тысяч пользователей онлайн-аптек 2U проданы без их ведома. Владельцы сервисов передавали адреса и имена

[12] 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.

клиентов различным медицинским компаниям, кредитным брокерам. По информации издания, помимо персональных данных, оказались скомпрометированы сведения о финансовом состоянии тысяч британцев, воспользовавшихся сервисами по продаже лекарств.

Распределение случайных и умышленных утечек в I полугодии 2015 года и за аналогичный период 2014 года представлено ниже. Отметим снижение доли утечек неопределенной природы (до 2,4%) и перераспределение умышленных и случайных утечек в сторону повышения (+9 п. п.) доли случайных (см. Рисунок 6).

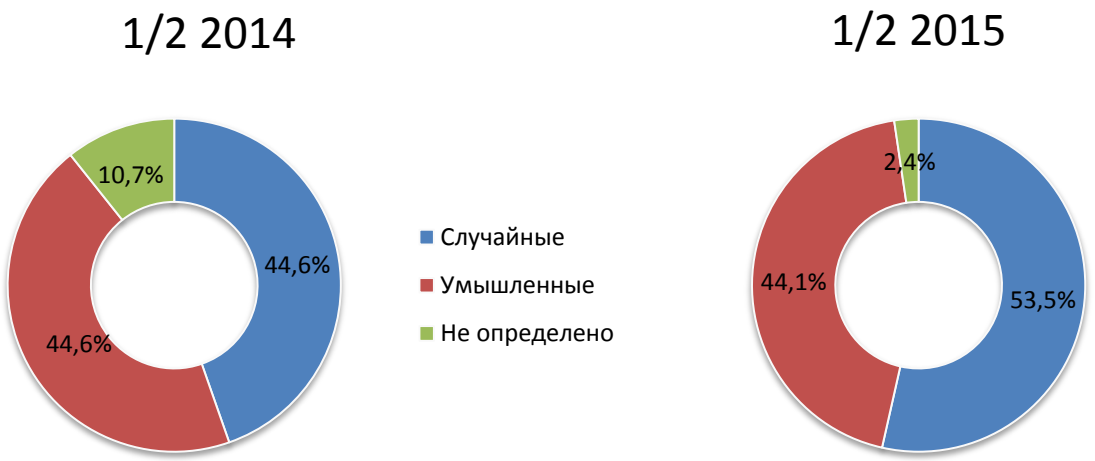


Рисунок 6. Соотношение случайных и умышленных утечек, ½ 2014 – ½ 2015 гг.

Данные за I полугодие 2015 года подтверждают вывод авторов исследования, сделанный годом ранее: картина утечек стабилизируется. Существенными изменениями в картине утечек год к году можно считать увеличение доли утечек данных под воздействием внешних атак (+9 п. п.) и, соответствующее увеличение доли внешнего злоумышленника в распределении по критерию «виновник утечки».

Вывод:

Утечки данных по вине внутреннего нарушителя (случайные и намеренные) медленно, но неуклонно превращаются в обыденное явление. Количество таких утечек год от года растет, но их доля в распределении по вектору воздействия[13] неуклонно снижается, темпы роста уже не столь впечатляющие, как несколько лет назад.

Показательно, что широко распространенные средства контроля и ограничения доступа (как альтернатива DLP-системам в плане защиты информации), судя по всему, не оказывают системного

[13] 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.)

влияния на текущую картину утечек данных. Доля утечек вследствие злоупотребления (превышения) правами доступа растет.

На первый план выходят утечки данных, произошедшие вследствие внешних атак. Именно внешние атаки на сегодня являются основным фактором, который оказывает решающее воздействие на формирование картины утечек данных. С внешними атаками связано подавляющее большинство крупнейших и самых заметных инцидентов.

Каналы утечек

В I полугодии 2015 года авторы исследования выявили две разнонаправленные тенденции на каналах, которые можно контролировать с помощью технических средств защиты. Сокращается доля утечек по каналам «потеря оборудования» (-3 п. п.), «электронная почта» (-4 п. п.), «бумажные документы» (-4 п. п.). Доли утечек через съемные носители, через мобильные устройства, текстовые и видеосообщения остались на уровне I полугодия 2014 года (см. Рисунок 7).

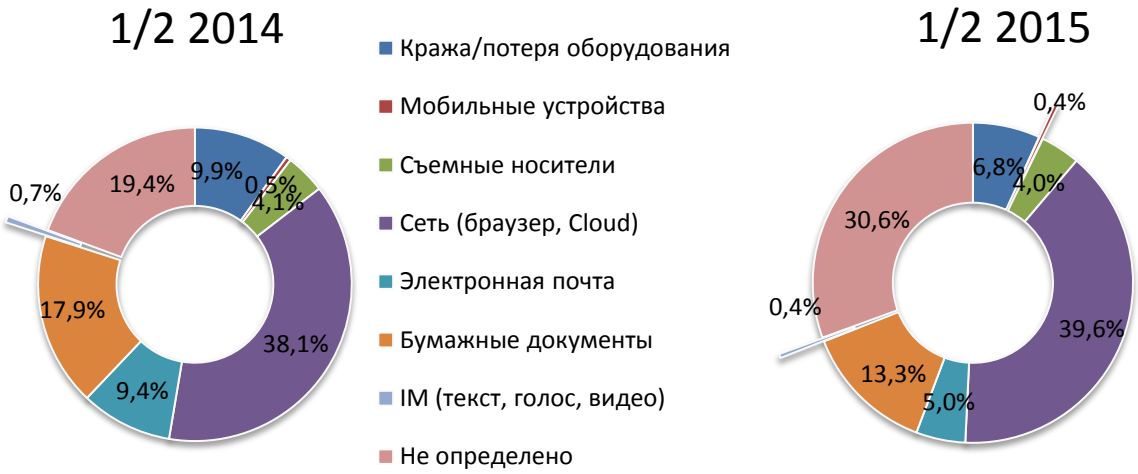


Рисунок 7. Распределение утечек по каналам, ½ 2014 – ½ 2015 гг.

С другой стороны, выросла доля «сетевого» канала (+1 п. п.). Наблюдался во многом неожиданный рост числа случаев, когда невозможно точно определить, по какому каналу «ушла» информация. Доля таких утечек (категория «не определено») составила 31%, рост к данным 2014 года – 10 п. п.

Доля утечек не всегда отражает размер опасности, связанный с конкретным каналом. Так по каналу «мобильные устройства» регистрируется 0,4% утечек. Но очевидно, что достаточно одного случая утечки критически важной информации по данному каналу, чтобы у организации возникли серьезные проблемы.

The Washington Post: Три жительницы Хьюстона предстанут перед судом по обвинению в мошенничестве с использованием чужих персональных данных.

По данным издания, небольшой «бизнес» мошенниц существовал с 2010 года. Подозреваемые работали на государственный департамент США и имели доступ к именам, номерам социального страхования, иной персональной информации американцев, благодаря чему оформляли кредиты на чужие данные для покупки электроники, включая устройства iPhone, iPad. Для кражи информации ограниченного доступа мошенницы использовали собственные смартфоны. Журналисты издания усматривают прямую связь между случаем в Хьюстоне и запретом на пользование мобильным телефоном на работе, который ввело паспортное бюро (The Passport Agency) в отношении своих сотрудников.

Доли умышленных утечек на каналах «кража/потеря оборудования», через мобильные устройства, съемные носители, электронную почту, бумажные документы, текстовые и видеосообщения год от года все более незначительны. Распределение умышленных утечек по каналам не отличается однородностью. В основном информация уходит через сеть (Рисунок 8).

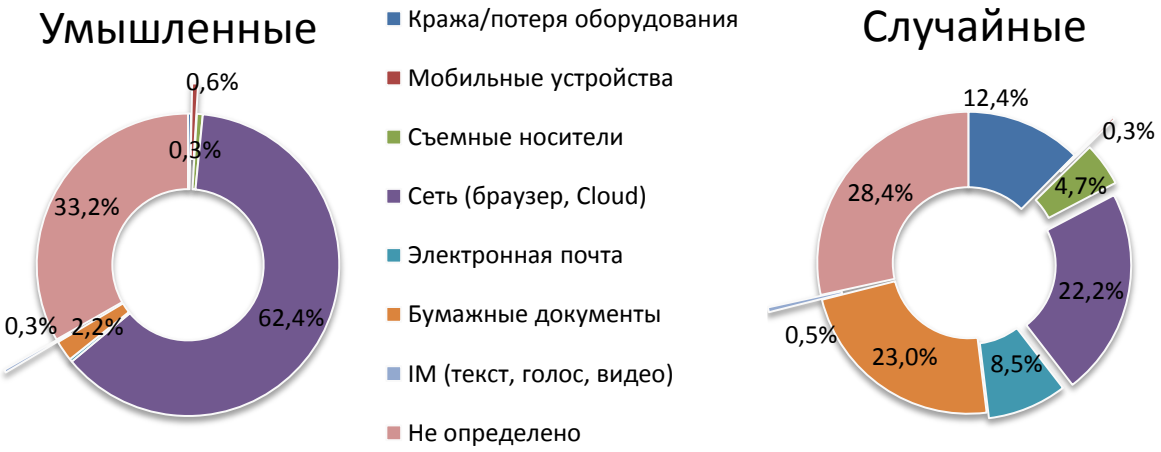


Рисунок 8. Распределение утечек по каналам, ½ 2015 г.

Случайные утечки распределились более однородно. По сравнению с умышленными, заметны доли утечек через съемные носители - 5%, сеть - 22%, электронную почту - 9%, бумажные документы - 23%.

1obl.ru: Письма, адресованные налогоплательщикам, оказались на помойке. 146 писем предназначались жителям Миасса и содержали конфиденциальные данные о каждом из адресатов. В пластиковом пакете с корреспонденцией Налоговой службы, помимо писем нашли свиную голову. Налоговая служба пообещала перепечатать письма и доставить их миасцам.

Доля случайных утечек с неустановленным каналом ожидаемо меньше, чем доля умышленных утечек той же категории.

Остается упомянуть еще два канала: утечки информации через мобильные устройства и сервисы мгновенных сообщений. Первый канал представлен незначительными 0,6% на диаграмме злонамеренных утечек и 0,3% на диаграмме

случайных. Второй – 0,3% и 0,5% соответственно. Само появление таких утечек, впрочем – аргумент в пользу старой истины, что в информационной безопасности не бывает «мелочей» и неважных, «периферийных» каналов.

В целом, как мы упоминали, на первый план и по количеству утечек, и по объему скомпрометированных данных выходит сетевой канал. 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). Совсем иная история – внешние злоумышленники. В погоне за персональными данными пользователей и иными «ликвидными»[14] видами информации хакеры проявляют завидную изобретательность и упорство.

> *BGN News: Государственная служба аудита (The Presidency's State Audit Institution) сообщила, что медицинские персональные данные 14 миллионов жителей Турции были украдены. Похищенная информация использовалась злоумышленниками для приобретения лекарств. Причем заплатить за эти лекарства пришлось владельцам украденных персональных данных. В расчете на каждую украденную запись, ущерб составил 13 турецких лир (5,6 долл. США). В общей сложности граждане потеряли чуть более 80 млн долларов США.*

Неудивительно, что большая часть (62%) утечек персональных данных (конкретно – платежной информации) приходится на сетевой канал (см. Рисунок 9).

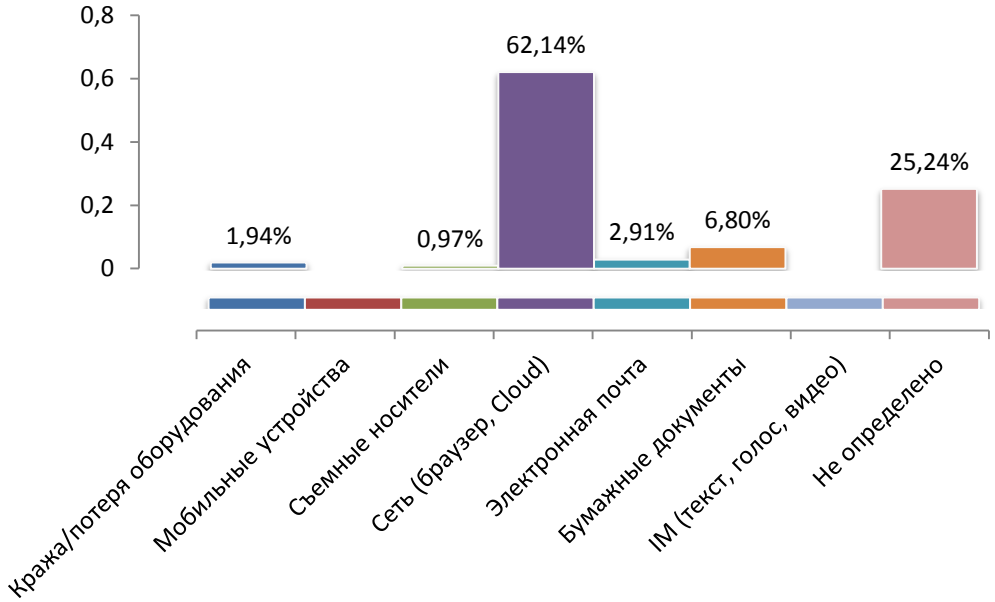


Рисунок 9. Утечки платежных данных, распределение по каналам, ½ 2015 г.

[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.

Про сетевой канал и «мега-утечки» данных под воздействием внешнего злоумышленника мы уже говорили. Приведем лишь один пример:

> *The Wall Street Journal: Неизвестные злоумышленники взломали компьютерную сеть американской Anthem. Компания занимается медицинским страхованием, является одним из крупнейших страховщиков в США. Хакеры получили доступ к персональным данным 80 млн клиентов и сотрудников организации. По данным издания, скомпрометированы имена, даты рождения, адреса и номера социального страхования американцев. Хакеры не добрались до номеров счетов, кредитных карт, медицинской информации.*

Небольшие доли умышленных утечек через съемные носители, электронную почту, 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 перечисленным каналам, и не рискует понапрасну.

Изучение утечек в разрезе каналов, по которым уходит информация, имеет 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. По причине всё большего распространения смартфонов, мы полагаем, что этот канал утечек также является одним из важнейших. Однако средства контроля смартфонов, по сути, отсутствуют сегодня на рынке. Очевидно, с этим связана низкая доля утечек, зафиксированных по этому каналу.

> ***Вывод:***
>
> ***Явно наметилось доминирование сетевого канала в рейтинге наиболее «проблемных». Бесконечно появляющиеся веб-сервисы, протоколы передачи данных, усложнение бизнес-процессов в организациях – все это, в конечном счете, приводит к тому, что организационные и технические меры, применяемые для контроля передачи информации по сети, устаревают чуть ли быстрее, чем удается их задействовать.***
>
> ***Растет «квалификация» внутреннего нарушителя – злонамеренный инсайдер не использует в своей неправомерной «деятельности» электронную почту, сервисы мгновенных сообщений, съемные носители. Об этом говорит огромная разница между распределениями (диаграммами) умышленных и случайных утечек. Растет «профессионализм» злоумышленников (в том числе внутренних). Инсайдер уверен, что почта, бумажная документация, мессенджеры (и им подобные каналы) контролируются, и потому находит иные способы для «слива» информации.***

Отраслевая карта

В I половине 2015 года доля утечек из государственных организаций снизилась на 12 п. п. и составила 17%. До 75% выросла доля утечек из коммерческих компаний (см. Рисунок 10).

Рисунок 10. Распределение утечек по типу организации, ½ 2014 – ½ 2015 гг.

Если рассматривать компании по отраслям, то чаще всего утечки фиксировались в медицине (24%), реже всего в муниципальных учреждениях (>1%). По объему скомпрометированных записей пальму первенства делят медицина и государственные учреждения – 36% и 32% соответственно (см. Рисунок 11).

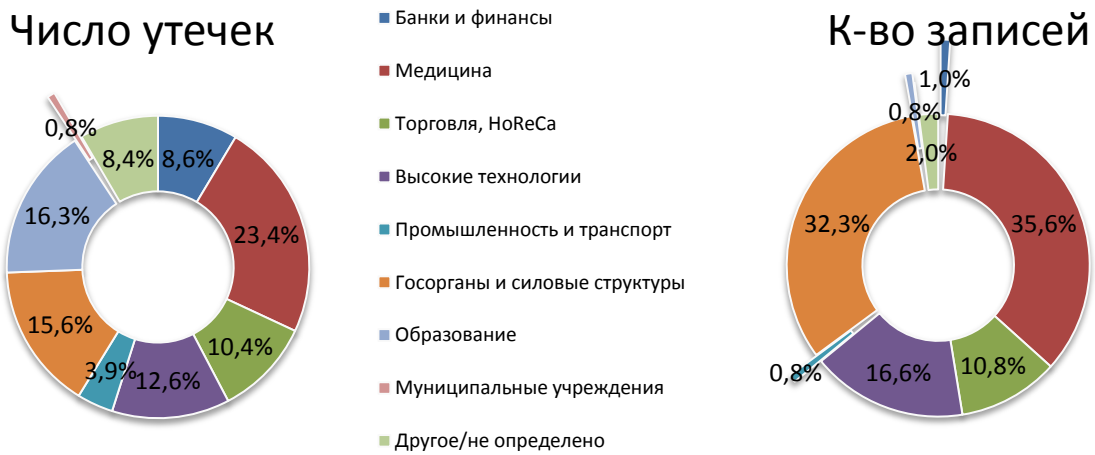


Рисунок 11. Распределение числа утечек и объема скомпрометированных персональных данных по отраслям, ½ 2015 гг.

Вдвое меньше данных утекло в высокотехнологичной вертикали – 17%, торговых компаниях – 11%. Объем данных, «утекших» из информационных систем банков, промышленных предприятий, образовательных и муниципальных учреждений, в общем-то, незначителен.

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:

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

Если сделать выборку утечек одного типа информации (в нашем случае мы отобрали утечки персональных данных), то отраслевое распределение умышленных утечек даст нам ответ на вопрос, какие сегменты наиболее «привлекательны» для злоумышленника (и наиболее уязвимы).

В I полугодии 2015 года таковыми следует признать торговые, транспортные и высокотехнологичные компании. В этих отраслях более половины утечек, сопровождавшихся компрометацией персональных данных, носили умышленный характер (см. Рисунок 13).

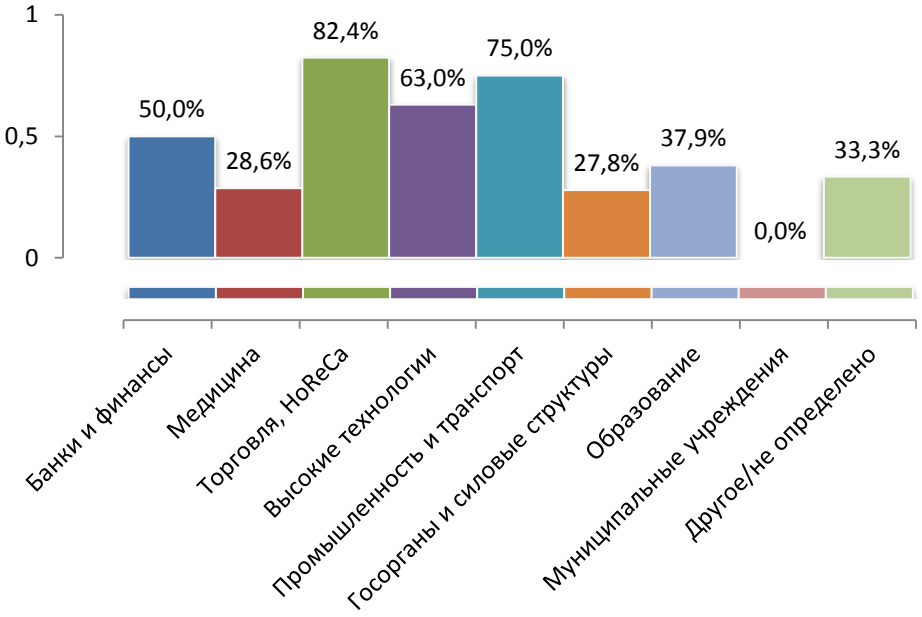


Рисунок 12. Доля умышленных утечек ПДн от общего количества утечек ПДн по отраслям, ½ 2015 г.

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

Банки и финансовые учреждения оказались на четвертой позиции. Умышленный характер носили ровно 50% утечек, в ходе которых персональные данные и платежная информация оказались в руках злоумышленников.

Казалось бы, банки являются наиболее привлекательной мишенью. Однако злоумышленники просчитывают возможные риски, последствия, вероятность успеха атаки. Бытует мнение, что уровень защиты информации в банковской системе высок. Поэтому злоумышленнику в погоне за теми же платежными данными проще «увести» информацию из торговых компаний (атака на платежные терминалы и приложения), турагентств и гостиниц, крупных интернет-сервисов. Что на деле и происходит.

Как мы уже упоминали, реальный или возможный ущерб от утечки мало зависит от отрасли, канала передачи данных, иных обстоятельств инцидента. Вот пример одной из крупнейших утечек в госорганах – сегменте, который, судя по приведенной диаграмме, сложно признать привлекательным для злоумышленников:

> welivesecurity.com: *Данные 100 тыс. американцев скомпрометированы в результате атаки на налоговое управление США (IRS). Украденных данных достаточно для проведения мошеннических операций на сумму 50 млн долларов США, например, в виде налоговых возвратов, считают эксперты.*

Показатели внешних атак (соотношение числа утечек, произошедших в результате действий внешних злоумышленников, к общему числу «результативных»[16] утечек) подтверждают уже озвученное — высокотехнологичные, торговые, транспортные компании намного чаще (в процентном отношении), чем компании других отраслей, страдают от действий внешних злоумышленников (см. Рисунок 13).

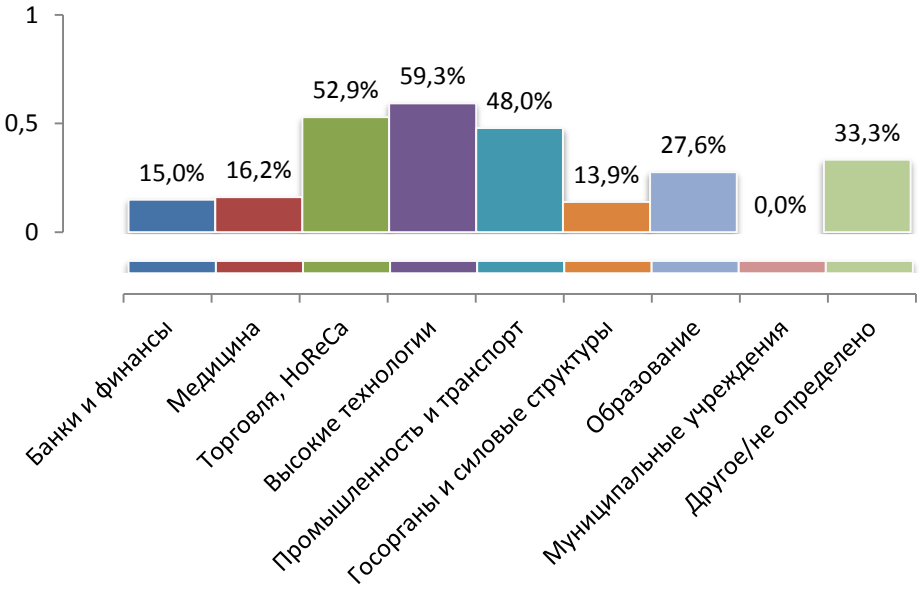


Рисунок 13. Доля умышленных утечек ПДн под воздействием внешнего злоумышленника от общего числа утечек ПДн по отраслям, ½ 2015 г.

[16] Утечки, в ходе которых хотя бы одна запись о персональных данных оказалась скомпрометирована.

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 «пузырьков» показывает совокупное число скомпрометированных записей, их положение по вертикали – число утечек в отрасли[17] (см. Рисунок 14).

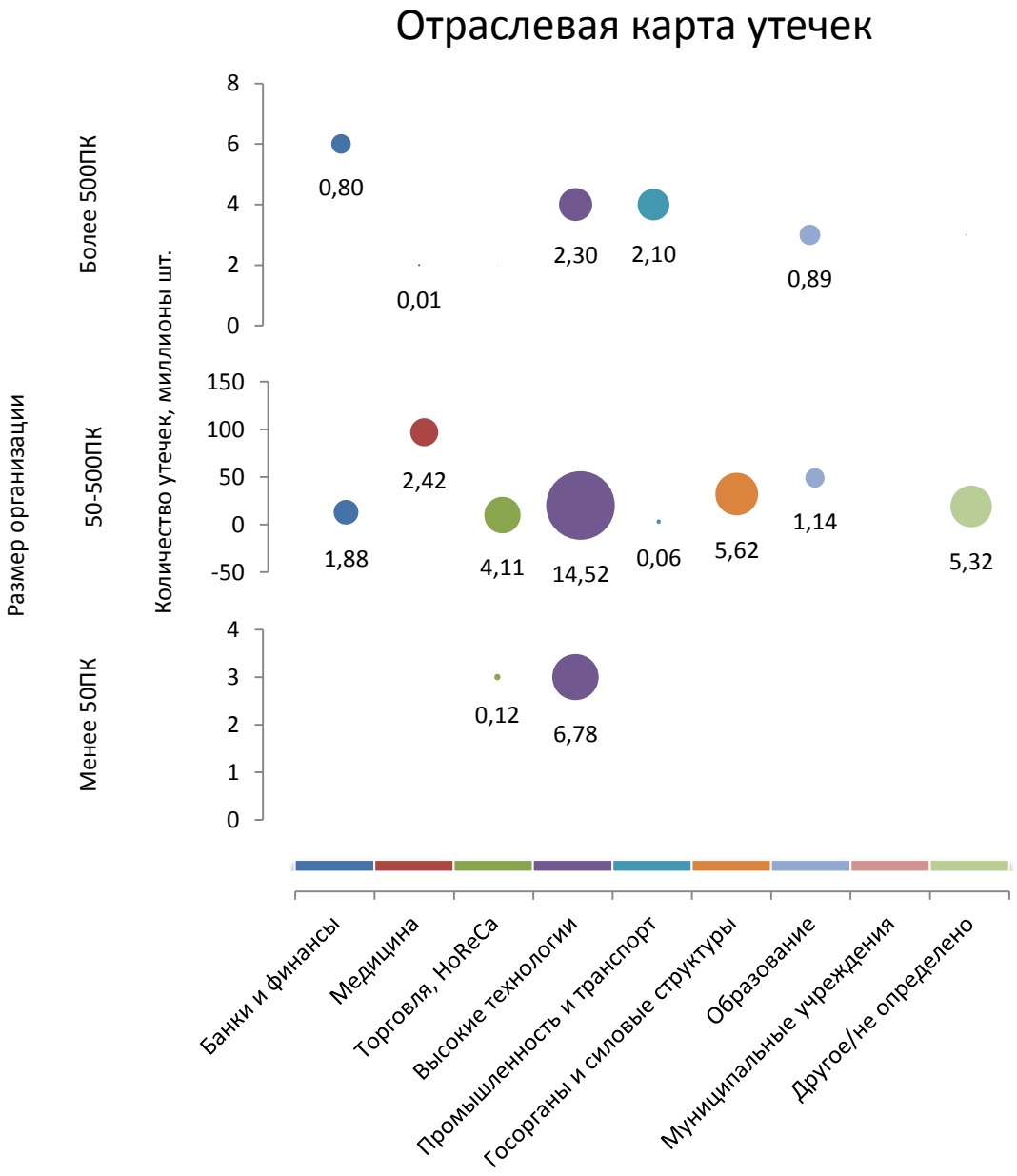


Рисунок 14. Отраслевая карта утечек персональных данных, млн, ½ 2015 г.

[17] 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 высокотехнологичные компании (включая интернет-сервисы). Со знаком минус «отличились» госорганы, торговые компании, медицина.

> macworld.com.au: *Мошенники «заработали» более 700 тыс. долларов на чужих персональных данных. Группа из пяти злоумышленников похитила данные 200 американцев. Преступники оформили на имена пострадавших подарочные сертификаты Apple и приобрели цифровую технику. За добычу персональных данных в группе отвечала 27-летняя сотрудница стоматологической клиники Энни Вонг (Annie Vuong).*

За I полугодие 2015 года утечек персональных данных в сегменте компаний среднего размера (до 500 ПК) зафиксировано в разы больше, чем в сегменте крупных компаний. На средние компании пришлось 86% утечек при доле крупных – 9% (см. Рисунок 15).

Рисунок 15. Распределение утечек по размеру организации ½ 2015 г.

За весь период наблюдений мы впервые столкнулись с ситуацией, когда объем данных, скомпрометированных компаниями среднего размера, в несколько раз превысил объем данных, скомпрометированных крупными компаниями. Следует признать, впрочем, что в некоторых вертикалях (торговля, медицина), такая ситуация наблюдалась еще год-два назад. Современные средства защиты от утечек слишком дороги для среднего бизнеса, что выливается в огромные объемы скомпрометированных данных – записи о сотрудниках, клиентах и пр.

Вывод:

Наиболее «привлекательными» для злоумышленников и, как следствие, уязвимыми отраслями оказались: сегмент высоких технологий, торговля, транспорт. 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 2015 года США традиционно заняли первую позицию по количеству утечек (430 или 59% от всех произошедших). Россия оказалась на уже привычном втором месте (59 утечек), которое досталось нашей стране еще по итогам I полугодия 2013 года. На третьем месте — Канада (39 утечек).

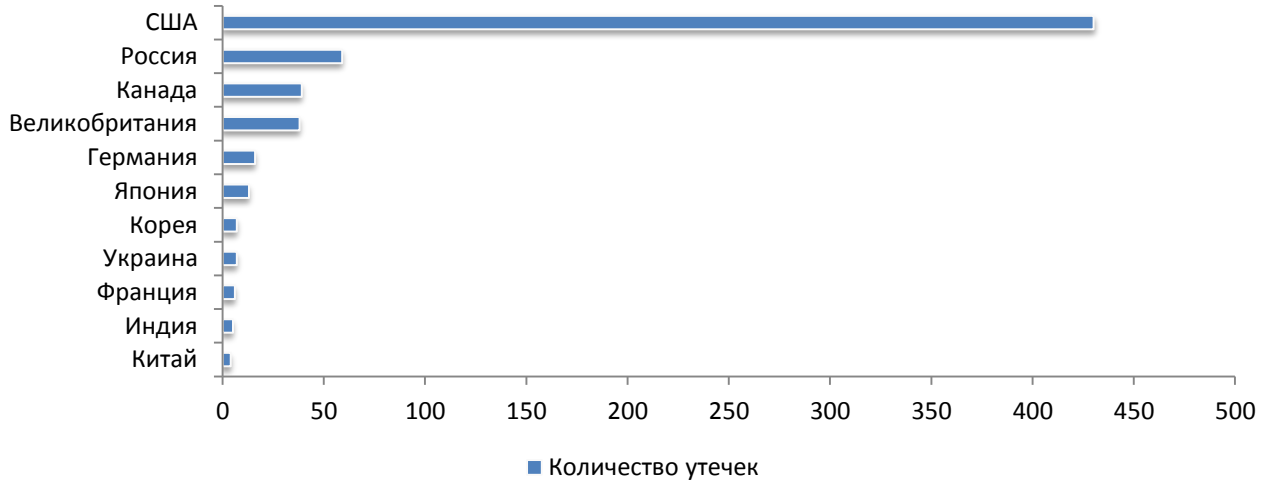


Рисунок 16. Распределение утечек по странам, ½ 2015 г.

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, в вопросах восприятия утечек данных, в оценке последствий, возможного ущерба, опасности утечек. Для примера, утечка данных в Великобритании:

> *scmagazineuk.com: В 2011 году в распоряжении полиции оказался DVD-диск, на котором было записано интервью жертвы сексуального насилия. Это свидетельство неопровержимо указывало на виновность одного из подозреваемых. Однако диск был утерян спустя два месяца после записи интервью. Управление полиции Южного Уэльса заплатит 160 тыс. фунтов стерлингов в виде штрафа за потерю цифровых доказательств.*

Утечка данных в России:

> *РБК: Персональные данные российских сенаторов опубликованы в интернете. Аппарат Совета Федерации в сентябре 2014 года разместил на официальном портале государственных закупок реквизиты паспортов 164 из 170 членов верхней палаты парламента. Однако сенаторы не считают произошедшее «серьезным преступлением». Николай Власенко, представляющий в СовФеде Калининградскую область, сомневается, что может наступить ответственность за публикацию паспортных данных сенаторов. Сам он не придает этому большого значения. «Плохо, конечно,*

> *что опубликовали. Но в наш информационный век это секрет Полишинеля», — цитирует сенатора РБК.*

В России сложно представить, что пострадавшие от утечек персональных данных обратятся в суд с коллективным иском о возмещении ущерба. Между тем это обычная практика для тех же США. Иногда размер компенсации в расчете на одного пострадавшего невелик.

> *securitylab.ru: 800 тысяч американских пользователей LinkedIn, чьи данные были скомпрометированы в результате хакерской атаки на сервис, получат по одному доллару США в виде компенсации. Атака на LinkedIn произошла в 2012 году. В результате инцидента в открытом доступе оказались более 6 млн хешей паролей к аккаунтам социального сервиса. Владельцы аккаунтов подали коллективный иск, оценив ущерб в 5 млн долларов США. Они обвинили LinkedIn в том, что компания не смогла защитить персональных данных пользователей ресурса.*

Но наличие этой возможности, факт выплаты крупной суммы, очевидно, стимулирует компании предпринимать значимые усилия в деле защиты персональных данных своих клиентов.

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Заключение и выводы

В 2014 году мы объявили о наступлении эры «мега-утечек»[18]. За истекшие полгода ситуация ухудшилась – зафиксировано 22 утечки, в ходе которых объем скомпрометированных персональных данных превысил 1 млн записей. Из них 8 «мега-утечек» – 10 млн записей и выше. (Напомним — за весь 2014 год зафиксировано 30 утечек с объемом записей свыше 1 млн).

Внешние атаки с целью хищения данных, платежной информации превратились в основной фактор, формирующий картину утечек. В результате воздействия внешнего злоумышленника скомпрометировано 230 млн записей о персональных данных – 87% от общего объема «утекших» персональных данных. Наметившаяся тенденция, скорее всего, сохранится. Уже сейчас до трети утечек данных происходит вследствие внешних атак, хотя в I полугодии 2014 года мы фиксировали лишь 22% утечек по причине внешнего воздействия.

С ростом осведомленности нарушителей о применении технических средств контроля каналов передачи информации, меняется распределение утечек по каналам. 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.

Влиянием двух факторов – рост числа и эффективности внешних атак и повышение «квалификации» внутреннего злоумышленника, - можно объяснить растущую год от года долю утечек информации через сеть. «Сетевой» канал приобретает особое положение – наиболее проблемного для служб информационной безопасности и создателей средств защиты.

Вопрос защиты ПДн от утечек для среднего бизнеса сегодня даже более актуален, чем для крупного. В организациях среднего размера зафиксировано в разы больше утечек, чем в крупных компаниях. Совокупный объем скомпрометированных записей в средних компаниях впервые за годы наблюдения превысил объем скомпрометированных записей в крупных компаниях.

Исходя из результатов исследования, наиболее уязвимыми следует считать сегмент высоких технологий, торговые и транспортные компании. Наибольший объем скомпрометированных данных (без учета «мега-утечек») пришелся на интернет-сервисы.

К сожалению, сообщения об утечках в большинстве не содержат сведений о том, какой ущерб понесла организация (или физическое лицо – субъект персональных данных) вследствие утечки информации. Исключения сравнительно редки:

> *РБК: Утечка квартальной отчетности Twitter спровоцировала падение акций компании. Финансовые результаты Twitter раньше других*

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

опубликованы службой финансовой разведки Selerity (в твиттер-аккаунте). Оборот сервиса микроблогов оказался меньше ожидаемого – $436 млн против $456 млн. После чего и началось падение Twitter. К закрытию торгов акции Twitter подешевели на 18%. Это самое значительное падение акций сервиса микроблогов с октября 2014 года.

Впрочем, даже при отсутствии систематизированных сведений об ущербе, невозможно игнорировать очевидное: утечек данных без последствий не бывает.

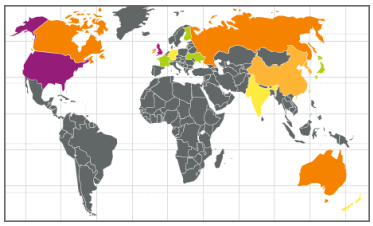
Глобальная картина и факторы, влияющие на распределение утечек по категориям, практически не изменяются с 2008 года. Уместно говорить о стабилизации роста утечек и их распределений, в том числе из-за довольно широкого распространения средств защиты от утечек и контроля информации. Исключение – фактор внешних (в том числе целенаправленных) атак, против которых действенного средства пока не найдено.

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

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®
BECAUSE YOUR DATA IS YOUR BUSINESS

Глоссарий

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

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

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

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

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.)*

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

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