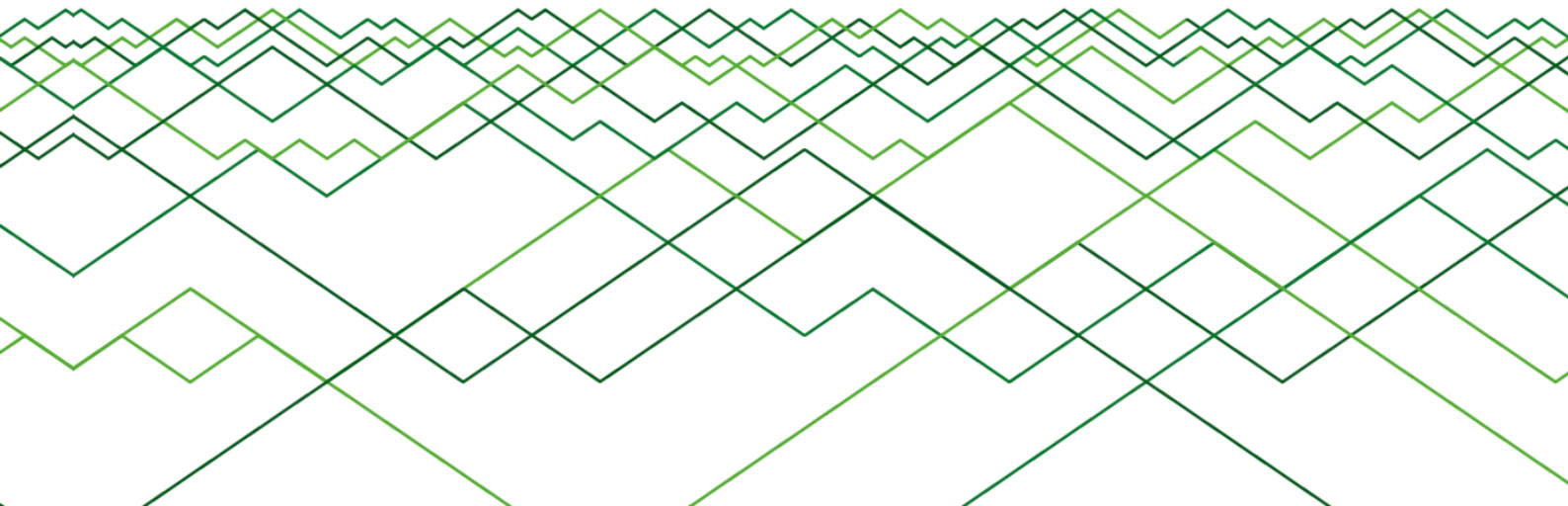
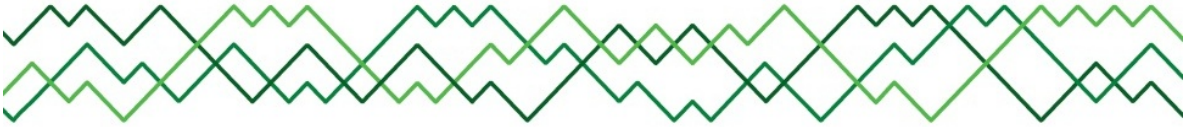
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Аналитический центр InfoWatch
www.infowatch.ru/analytics

Глобальное исследование утечек конфиденциальной информации в 2015 году



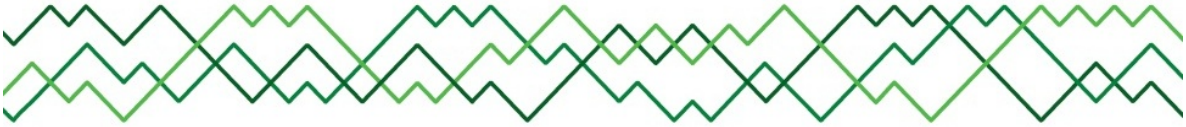


Оглавление

INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Только цифры

- ✓ В 2015 году в мире обнародовано (в СМИ и иных источниках) и зарегистрировано Аналитическим центром InfoWatch **1505** случаев утечки конфиденциальной информации, что на **7,8%** превышает количество утечек, зарегистрированных за 2014 год.
- ✓ Внешние атаки стали причиной **32%** утечек данных. Доля утечек вследствие внешних атак выросла на 7,2 п. п. по сравнению с аналогичным показателем 2014 года.
- ✓ **90,8%** утечек связаны с компрометацией персональных данных. За исследуемый период скомпрометированы более **965,9 млн** записей, в том платежная информация.
- ✓ За 2015 год зафиксировано **21** «мега-утечка». В результате каждой «утекло» более **10 млн** персональных данных. На «мега-утечки» пришлось **84,3%** всех скомпрометированных записей.
- ✓ В **51,2%** случаев виновными в утечке информации оказались сотрудники компаний. В **1,1%** случаев – высшие руководители организаций.
- ✓ Транспортные компании, наряду с интернет-сервисами, ретейлерами, образовательными и медицинскими учреждениями, являются основным источником утечек персональных данных.
- ✓ Россия заняла второе место по числу известных утечек. В исследуемый период зарегистрировано **118** случаев утечки конфиденциальной информации из российских компаний и государственных организаций. Число «российских» утечек по сравнению с данными 2014 года сократилось на **28,1%**.



Аннотация

Аналитический центр компании InfoWatch представляет отчет об исследовании утечек конфиденциальной информации в 2015 году.

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: 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.

Не обошла беда правительственные учреждения стран, 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.

Впрочем, «громкие» инциденты — это лишь верхушка «айсберга». В 2015 году чаще всего мы фиксировали утечки данных, произошедшие по вине или по неосторожности рядового персонала медицинских и финансовых учреждений:

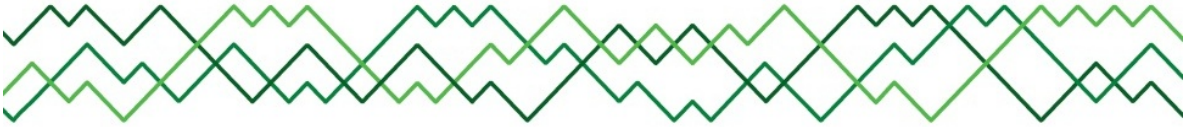
> *The Washington Post: Три жительницы Хьюстона предстанут перед судом по обвинению в мошенничестве с использованием чужих персональных данных. По данным издания, небольшой «бизнес» мошенниц существовал с 2010 года. Подозреваемые работали на государственный департамент США и имели доступ к именам, номерам социального страхования, иной персональной информации американцев, благодаря чему оформляли кредиты на чужие данные для покупки электроники, включая устройства iPhone, iPad.*

Еще один типичный сценарий – внешняя атака с целью хищения агрегированных персональных данных:

> *securitylab.ru: Неизвестные злоумышленники вторглись в сеть страховой компании Excellus BlueCross BlueShield и получили доступ к персональным данным ее клиентов. От взлома пострадали более 10 млн человек. Хакеры получили доступ к номерам социального страхования, платежным данным, адресам, датам рождения клиентов Excellus. Компания заявила, что атака началась более 2 лет назад.*

Анализ утечек данных больше похож на статистику больших данных, чем на скрупулезное исследование отдельных случаев. Важно, какой канал наиболее уязвим в настоящее время и почему, какую отрасль злоумышленники считают наиболее привлекательной, что опаснее – внешняя атака или действия злонамеренного инсайдера. На эти и многие другие вопросы и призвано ответить настоящее исследование.

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.



INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

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, и пр.

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 исследуемые множества (категории) содержали достаточное или избыточное количество элементов (фактических случаев утечки). Такой подход к формированию поля исследования позволяет считать получившуюся выборку теоретической, а

---

[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.

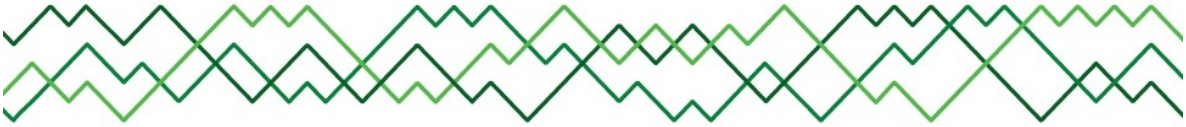
[5] Аналитики Центра InfoWatch классифицируют организации по размеру в зависимости от известного либо предполагаемого парка персональных компьютеров (ПК). Небольшие компании – до 50 ПК, средние - от 50 до 500 ПК, крупные – свыше 500 ПК.

[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%.



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.

Случаи нарушения конфиденциальности информации (обнаруженные уязвимости), иные инциденты ИБ (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.

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

В 2015 году Аналитическим центром InfoWatch зарегистрировано 1505[10] случаев утечки конфиденциальной информации (см. Рисунок 1). В результате утечек скомпрометировано 965,9 млн персональных данных (записей ПДн), - номера социального страхования, реквизиты пластиковых карт, иная критически важная информация.

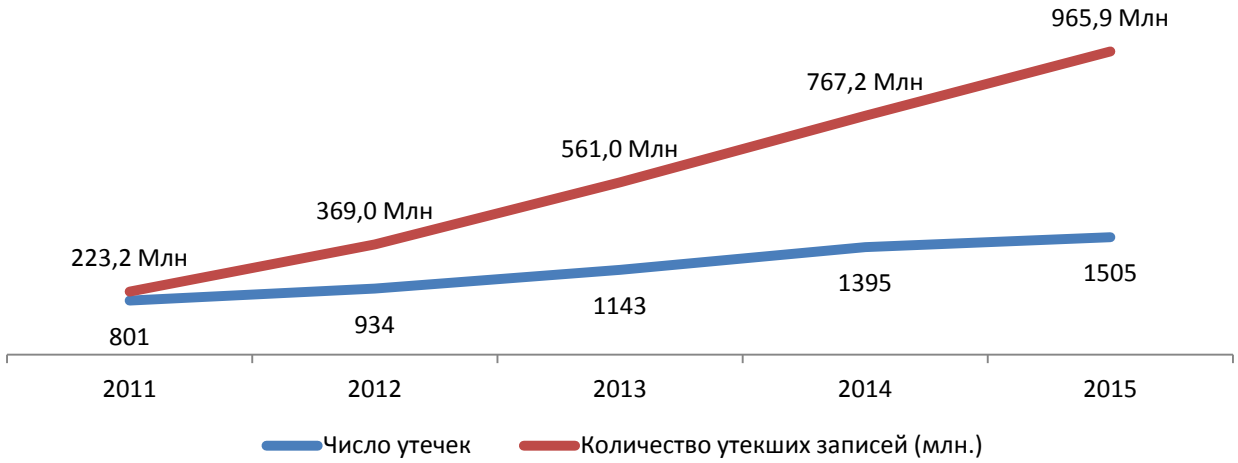


Рисунок 1. Число утечек информации и объем персональных данных, скомпрометированных в результате утечек. 2011 - 2015 гг.

Количественный рост утечек информации в 2015 году продолжился (см. Рисунок 2).

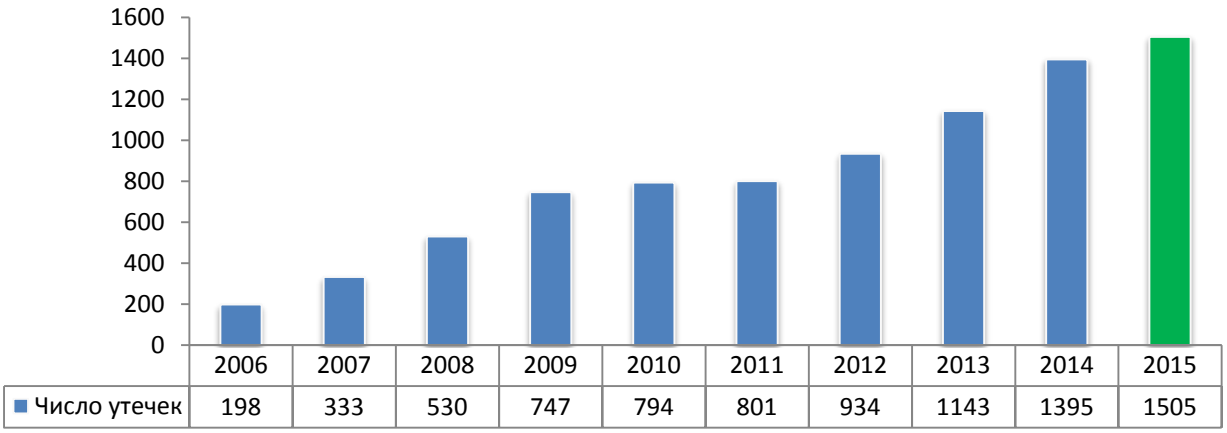


Рисунок 2. Число зарегистрированных утечек информации, 2006 -2015 гг.

Наблюдается замедление темпов роста числа утечек. Если в 2014 этот показатель составил 22%, то в 2015 году рост утечек по отношению к 2014 году остановился на

[10] С 2014 года Аналитический центр InfoWatch наряду с утечками, причиной которых стали внутренние нарушители, регистрирует утечки информации, причиной которых стали внешние воздействия – целевые атаки и проч., повлекшие компрометацию данных.

уровне 7,8%. Также замедлился прирост объема скомпрометированных персональных данных, составив в 2015 году 25,9% (см. Рисунок 3).

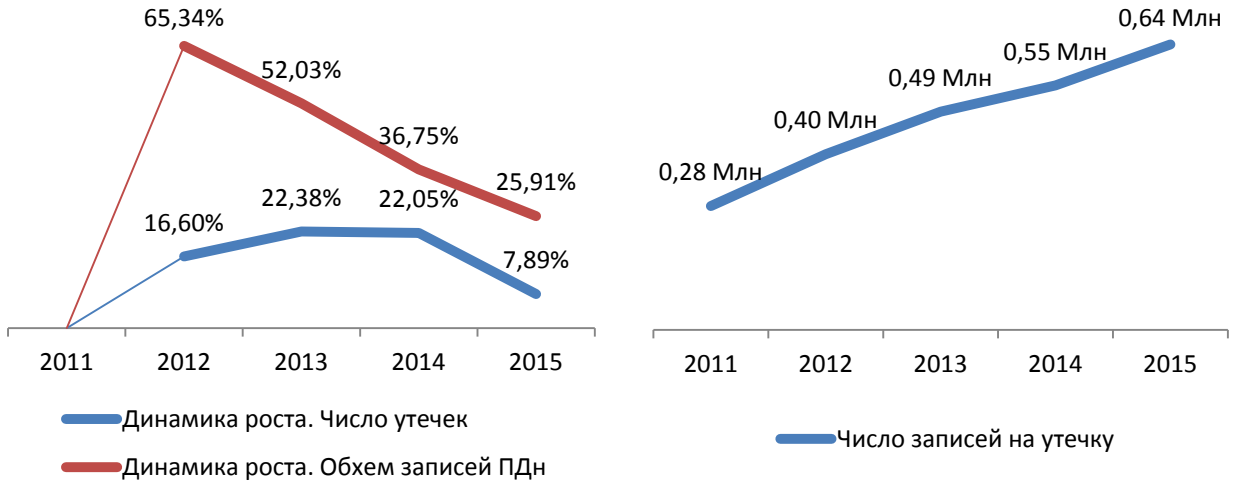


Рисунок 3. Динамика роста числа утечек, объема записей ПДн. Объем персональных данных, скомпрометированных в ходе одной утечки. 2011 -2015 гг.

В результате одной утечки в среднем скомпрометировано 0,64 млн записей ПДн, - на 16% выше аналогичного показателя 2014 года.

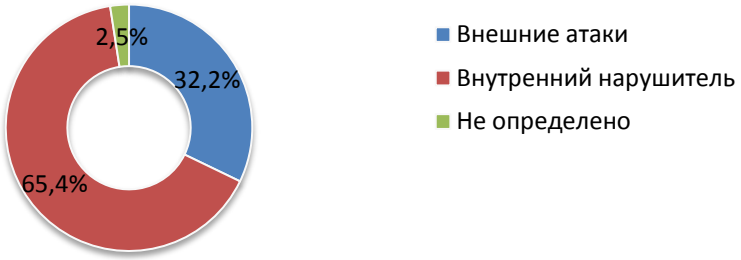


Рисунок 4. Распределение утечек по вектору воздействия, 2015 г.

Зарегистрировано 484 (32,2%) утечки информации, причиной которых стал внешний злоумышленник. В 984 (65,4%) случаях утечка информации произошла по вине или неосторошности внутреннего нарушителя.

Доля утечек под воздействием внешних атак оказалась на 7,2 п. п. выше аналогичного показателя 2014 года (тогда года на долю утечек под воздействием внешних атак пришлось 25% утечек). По вине внешнего злоумышленника скомпрометировано 610,8 млн записей ПДн или 63,2% от совокупного объема скомпрометированных записей. Внешние атаки спровоцировали 15 из 21 зафиксированных «мега-утечек»[11].

[11] «Мега-утечки» - утечки информации, в ходе которых скомпрометированы свыше 10 млн записей персональных данных. На «мега-утечки» приходится 814,5 млн записей, скомпрометированных в результате утечек в 2015 году (84,3% от совокупного объема скомпрометированных данных).

> *Ведомости: В результате кибератаки на Кадровое управление правительства США (U.S. Office of Personnel Management – OPM) пострадали от 18 до 22 млн служащих. Персональные данные настоящих и бывших сотрудников управления оказались скомпрометированы. В результате инцидента в руки злоумышленников попали отпечатки пальцев 5,6 млн сотрудников американских госучреждений.*

Утечки данных под воздействием внешних атак отличаются большим объемом скомпрометированных данных. В среднем, на одну «внешнюю» утечку приходится 1,26 млн скомпрометированных ПДн. Для сравнения - в результате одной утечки данных по вине или неосторожности внутреннего нарушителя скомпрометировано в среднем 0,34 млн ПДн. Впрочем, это не означает, что утечки, случившиеся в результате недозволенных действий внутреннего нарушителя менее разрушительны, чем утечки, произошедшие в результате внешнего воздействия.

> *РБК: Утечка квартальной отчетности Twitter спровоцировала падение акций компании. Финансовые результаты Twitter раньше других 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%. Цена акций составила $42,27, капитализация компании – $27,6 млрд. Это самое значительное падение акций сервиса микроблогов с октября 2014 года.*

В 2015 году в 51,2% случаев виновниками утечек информации были настоящие или бывшие сотрудники – 48,9% и 2,3% соответственно (доля сотрудников снизилась на 4 п. п. к данным 2014 года, доля бывших сотрудников выросла на 1,4 п. п.). Более чем в 1% случаев зафиксирована вина руководителей организаций (топ-менеджмент, главы отделов и департаментов). Доля утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к охраняемой информации, выросла на 3,5 п. п., составив 7,6% (см. Рисунок 5).

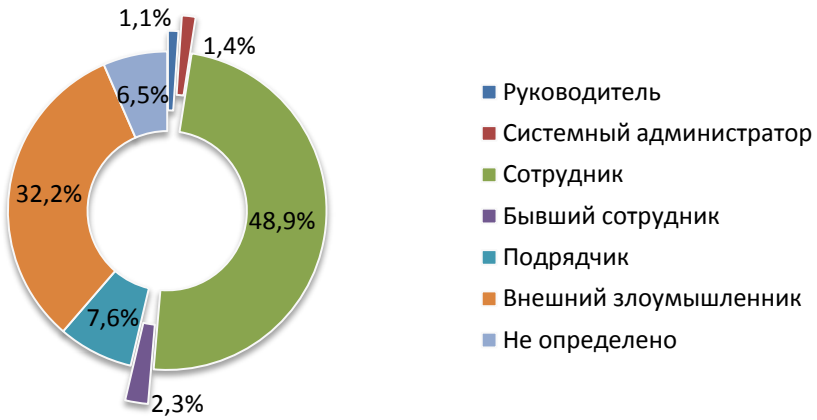


Рисунок 5. Распределение утечек по источнику (виновнику), 2015 г.

Доля утечек персональных и платежных данных в распределении утечек по типу информации осталась на уровне прежних лет, составив 90,8%. Незначительно (менее

1 п. п.) подросли утечки информации, составляющей государственную тайну (см. Рисунок 6).

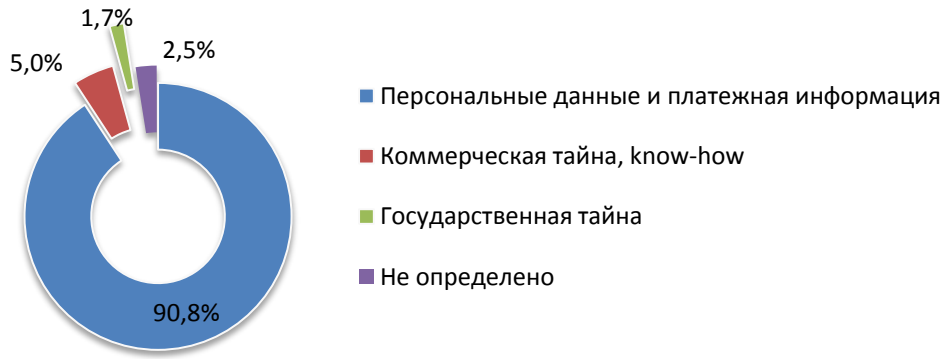


Рисунок 6. Распределение утечек по типам данных, 2015 г.

В 2015 году доля утечек данных, сопряженных с последующим использованием скомпрометированной информации в целях мошенничества (как правило, банковский фрод) снизилась на 1,4 п. п. и составила 10,3%.

Рисунок 7. Распределение инцидентов по характеру, 2015 г.

7,7 % инцидентов классифицированы как нарушения, сопряженные с получением несанкционированного доступа к информации (превышение прав доступа, манипуляции с информацией, которая не нужна сотруднику для исполнения служебных обязанностей).

Вывод:

Наиболее важным трендом на глобальной выборке следует считать рост доли утечек под воздействием внешнего злоумышленника. Чуть менее 2/3 от совокупного объема персональных данных, скомпрометированных в 2015 году, «утекли» в результате внешней атаки. Самые заметные инциденты 2015 года связаны с неправомерной деятельностью хакеров, проникновением в инфраструктуру компаний, извлечением агрегированной информации о сотрудниках и клиентах.

Каналы утечек

В 2015 году сократилась доля утечек по таким каналам, как «потеря оборудования» (на 8,3 п. п.), «электронная почта» (на 1,2 п. п.), «бумажные документы» (на 3,7 п. п.). Доли утечек через съемные носители, мобильные устройства текстовые и видеосообщения остались на уровне 2014 года. Доля «сетевого» канала выросла на 10,5 п. п. (см. Рисунок 7).

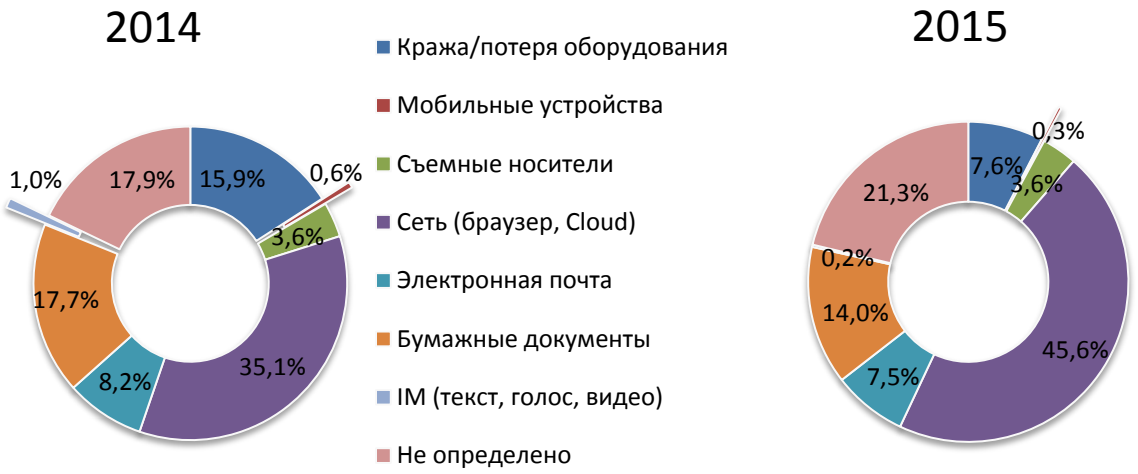


Рисунок 8. Распределение утечек по каналам, 2014 – 2015 гг.

Наблюдался во многом неожиданный рост случаев, когда невозможно точно определить, по какому каналу «ушла» информация. Доля таких утечек (категория «не определено») составила 21,3%, рост к данным 2014 года – 3,4 п. п.

Случайные утечки распределились однородно. Заметны доли утечек через съемные носители – 5,5%, сеть – 27,4%, электронную почту – 12,1%, бумажные документы – 21,9%. Соотношение случайных утечек год к году сравнительно стабильно. В сравнении с 2014 годом немного подросли доли утечек по сетевому каналу (+5,2 п. п.), по электронной почте (+3,6 п. п.).

Существует во многом ошибочное мнение, что случайные утечки менее опасны для компаний, чем злонамеренные. Практика показывает, что масштаб последствий зависит, скорее, не от типа утечки, наличия умысла в действиях (бездействии) конкретного лица, но от характера информации, которая утекает в результате инцидента. Последствия от случайной утечки особо охраняемой информации могут быть весьма разрушительными.

> *РИА Новости: Сотрудник кенийской авиакомпании рассекретил информацию о визите Барака Обамы. В письме, адресованном коллегам, нарушитель уведомил о датах и времени закрытия аэропортов Кении в связи с визитом президента США. В результате утечки точное время прилета борта номер один в Найроби (Кения) стало известно неограниченному кругу лиц, что нарушает стандарты безопасности, принятые Белым домом.*

Однородное распределение случайных утечек свидетельствует о достаточно высоком уровне проникновения средств защиты от утечек, благодаря чему и удается эти самые утечки зафиксировать.

В случае с умышленными утечками складывается принципиально иная ситуация - распределение явно не однородно. 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. Фактически весь объем умышленных утечек сводится к утечкам одного типа – по сетевому каналу (см. Рисунок 9).

Рисунок 9. Распределение случайных и умышленных утечек, 2015 гг.

Сетевой канал следует признать наиболее критичным как для случайных, так и в случае умышленных утечек. «Сетевые» утечки характеризует высокий уровень критичности данных, огромные объемы скомпрометированной информации.

> *ZDnet: Персональные данные 191 млн американских избирателей обнаружены в сети. Среди скомпрометированных данных фамилии и имена граждан, почтовые адреса, даты рождения, личные номера избирателей и история участия в выборах с 2000 года. Утечка данных произошла из-за неправильной настройки базы данных, где хранилась информация об избирателях. В базе собрана информация обо всех жителях США, которые ходили на выборы хотя бы один раз за последние 15 лет. Неназванная маркетинговая фирма оценила стоимость утекшей информации в 270 тыс. долл.*

В результате внешней атаки компании несут огромные финансовые потери. Одна утечка данных способна кардинально изменить будущее бизнеса, негативно повлиять на стратегию организации.

> *Reuters: Хакерская атака на сайт знакомств Ashley Madison, скорее всего, не позволит его создателям выйти на IPO. Владелец ресурса компания Avid Dating Life Inc (ADL) планировала выручить от размещения на лондонской бирже до 200 млн долларов США. В результате взлома сайта в сети оказались данные 37 млн человек.*

В 45,5% инцидентов наиболее ликвидные данные[12] – платежная информация, в том числе номера счетов, данные баланса, реквизиты платежных карт, - утекали через сеть (см. Рисунок 10).

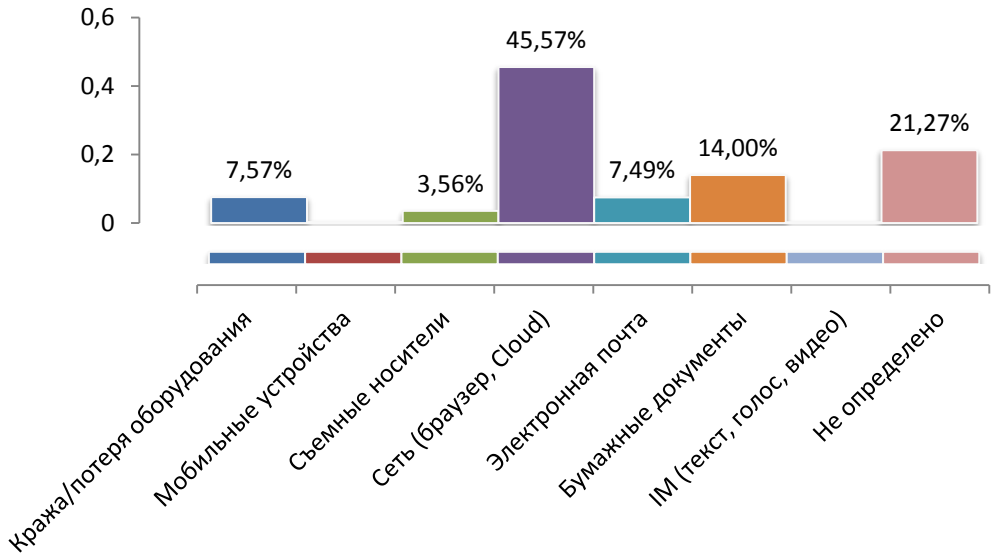


Рисунок 10. Утечки платежных данных, распределение по каналам, 2015 г.

Небольшие доли умышленных утечек через мобильные устройства, 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.

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 распространении информации по сети, публикациях данных в вебе и пр.

С другой стороны, злоумышленники все реже используют заведомо контролируемые каналы передачи информации – электронную почту, сервисы мгновенных сообщений. В этом смысле сеть – единственный канал злонамеренного инсайдера, который удается хоть как-то контролировать.

[12] 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.

Отраслевая карта

По сравнению с данными 2014 года, распределение утечек по типу организации не претерпело существенных изменений (см. Рисунок 11).

Рисунок 11. Распределение утечек по типу организации, 2014 - 2015 гг.

Чаще всего утечки фиксировались в медицине (20,2%), реже всего в муниципальных учреждениях (<2%). По объему скомпрометированных записей пальма первенства безраздельно принадлежит компаниям высокотехнологичного сегмента (речь идет о крупных интернет-сервисах, торговых онлайн-площадках и пр.). На долю этих компаний приходится почти треть (29,2%) от всего объема скомпрометированных данных. Заметна доля образовательных учреждений – 20,2% (см. Рисунок 12).

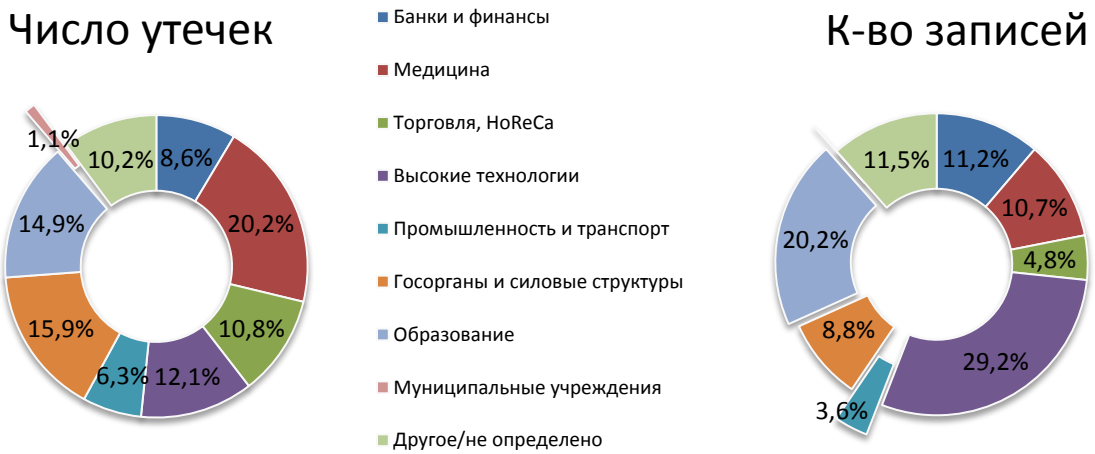


Рисунок 12. Распределение числа утечек и объема скомпрометированных персональных данных по отраслям, 2015 г.

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

«Привлекательность» отрасли прямо обусловлена «ликвидностью» данных, которые обрабатывают компании данного сегмента[13]. 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 выборка утечек персональных данных), то отраслевое распределение умышленных утечек даст нам ответ на вопрос, какие сегменты наиболее «привлекательны» для злоумышленника (и наиболее уязвимы).

В 2015 году наиболее «привлекательными» следует признать торговые, транспортные и высокотехнологичные компании (в том числе операторов связи). В этих отраслях более половины утечек, сопровождавшихся компрометацией персональных данных, носили умышленный характер.

> *T-mobile: Глава мобильного оператора Джон Леджер заявил, что хакеры получили доступ к данным 15 млн клиентов компании, включая имена, адреса, даты рождения, номера социального страхования. Утечка произошла на стороне партнера T-mobile – кредитного бюро Experian. По заказу оператора, Experian проводит оценку кредитной истории и финансового положения американцев, которые заключают договор с T-mobile.*

К этой тройке вплотную примыкает банковский сегмент, страхование, где на долю умышленных утечек персональных данных приходится 51,3% (см. Рисунок 13).

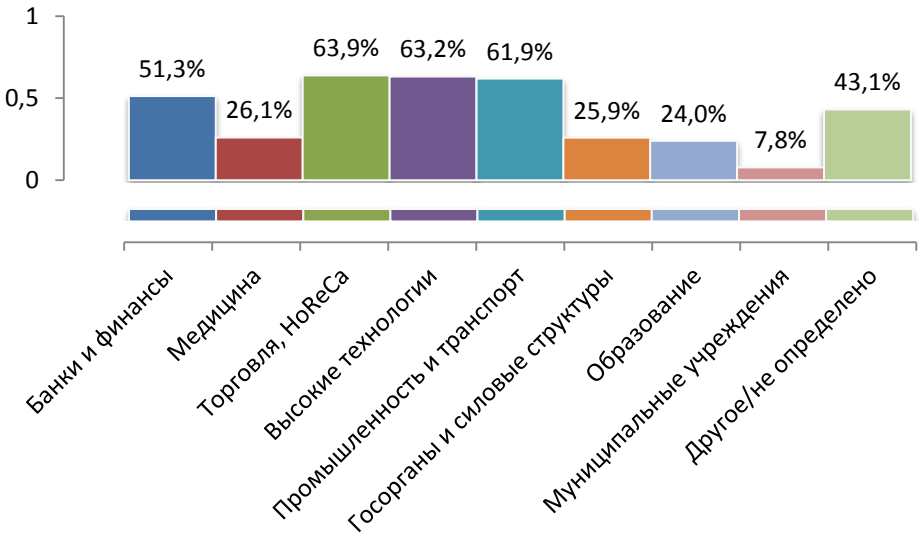


Рисунок 13. Доля умышленных утечек ПДн от общего количества утечек ПДн по отраслям, 2015 г.

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

Предыдущая диаграмма говорит о «привлекательности» отдельных отраслей в целом. 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).

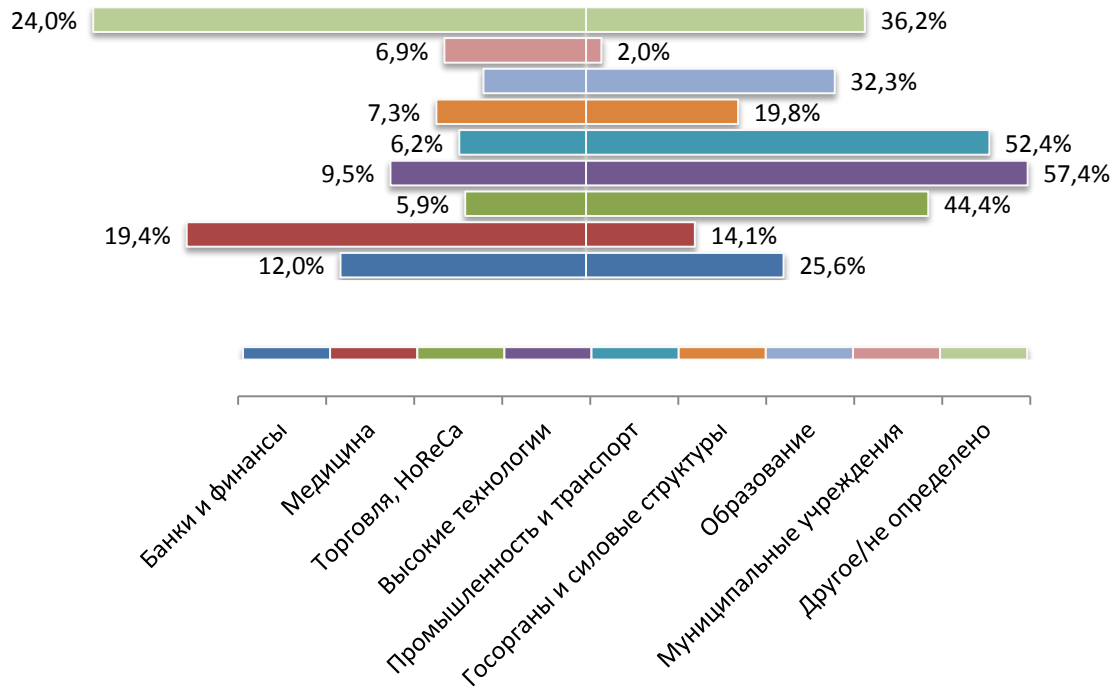


Рисунок 14. Доля умышленных утечек ПДн под воздействием внешнего (слева) и внутреннего (справа) злоумышленника от общего числа утечек ПДн по отраслям, 2015 г.

Как видно из диаграммы, высокотехнологичные компании, наряду с торговлей и транспортом, чаще всего становились жертвой внешних атак, направленных на хищение данных. Доля ПДн, украденных внутренними злоумышленниками, в этих отраслях незначительна. С другой стороны, чаще всего от злонамеренных действий внутреннего нарушителя страдали медучреждения и банки.

Одна из основных причин – чрезвычайно низкий уровень культуры обращения с информацией ограниченного доступа и высокая ликвидность данных, с которыми работает персонал медицинских и финансовых учреждений.

> *un-sentinel.com: Полиция города Бока-Ратон (Флорида, США) арестовала сотрудницу госпиталя Бетесда города Бойтон Бич по подозрению в крупном мошенничестве. 24-летняя Элексис Теддис (Elexes Thaddies) пользовалась персональными данными коллег, совершая крупные покупки в магазине Nordstrom. Сумма мошенничества составила 20 тыс. долларов США.*

Более объемно картину утечек иллюстрирует отраслевая карта. Размер «пузырьков» показывает совокупный объем скомпрометированных записей – млн ПДн (по всем компаниям сегмента), положение «пузырьков» по вертикали отражает число утечек в

отрасли[14]. В зависимости от размера пострадавшей компании, карта разбита на три диаграммы – небольшие, средние, крупные организации (см. Рисунок 15).

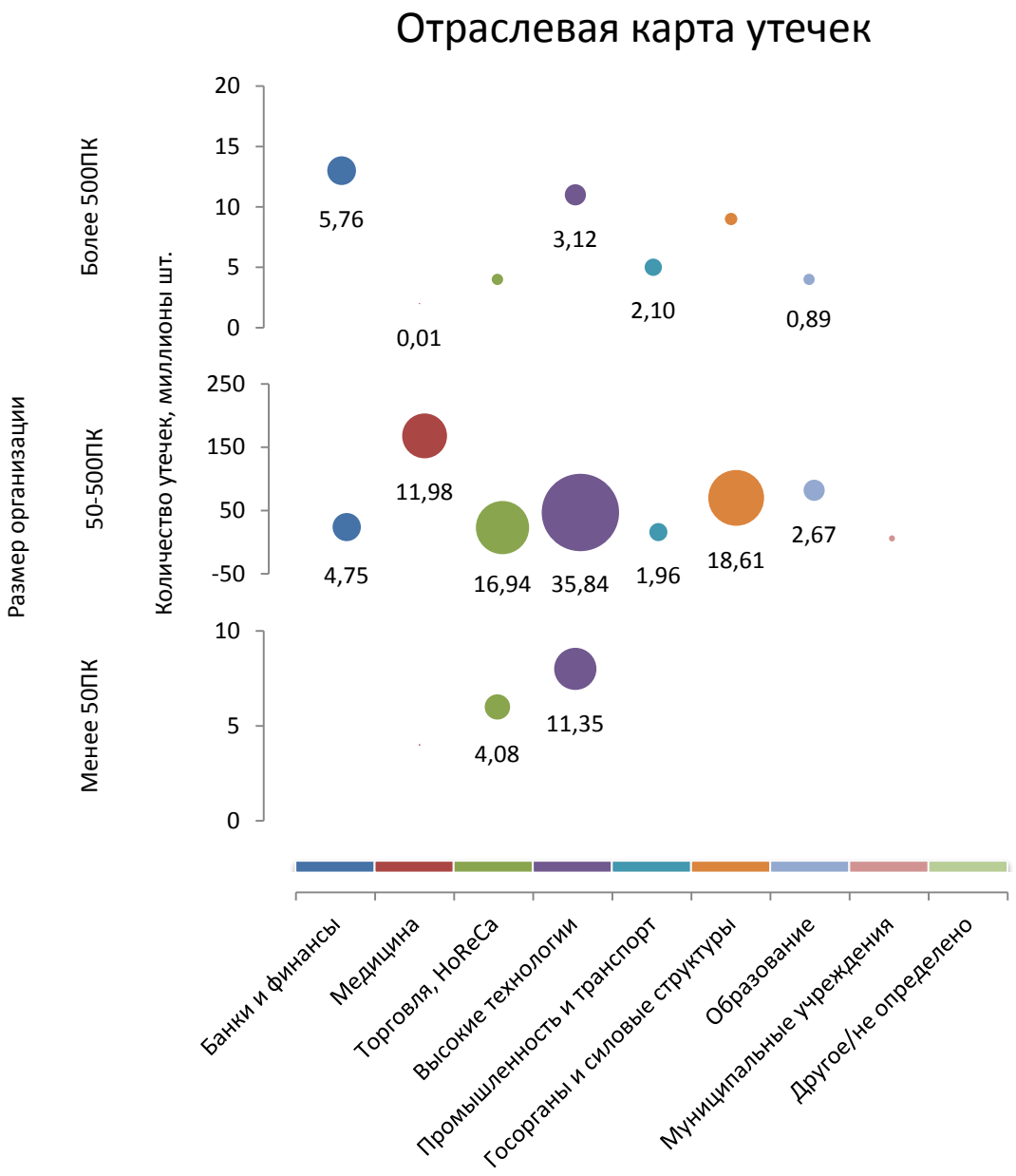


Рисунок 15. Отраслевая карта утечек персональных данных, 2015 г.

В 2015 году утечек персональных данных в сегменте компаний среднего размера (до 500 ПК) зафиксировано в разы больше, чем в сегменте крупных компаний. На средние компании пришлось 85,6% всех утечек при доле крупных – 5,2%. Распределение по объему скомпрометированных персональных данных повторяет

[14] 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.

эту картину – 85% записей персональных данных скомпрометировано средними компаниями, 6,3% - крупными (см. Рисунок 16).

Рисунок 16. Распределение утечек по размеру организации 2015 г.

В 2015 году 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.

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 высокотехнологичные компании и организации в сфере образования. Данные торговых, транспортных, высокотехнологичных компаний чаще всего атакуют извне. В банках, страховании, медицине компрометация ПДн связана, как правило, с действиями внутренних злоумышленников. Средний бизнес подвержен утечкам персональных данных в большей степени, чем крупные компании.

Региональные особенности

В распределении утечек по регионам в 2015 году США традиционно заняли первую позицию по количеству утечек (859 или 57% от всех произошедших). Россия оказалась на уже привычном втором месте (118 утечек), опередив Великобританию всего на 6 инцидентов.

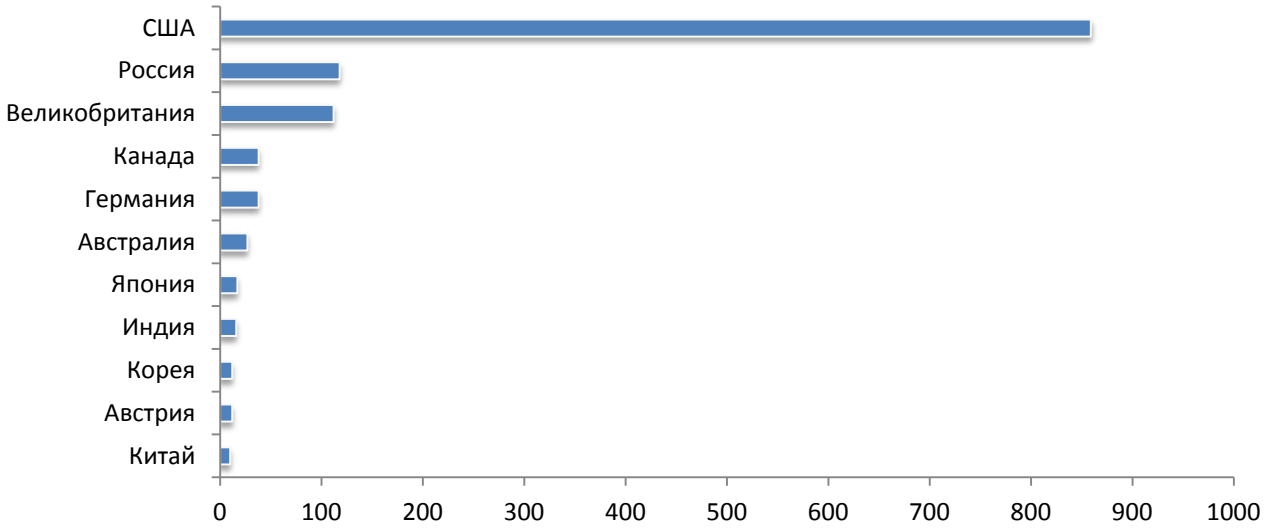


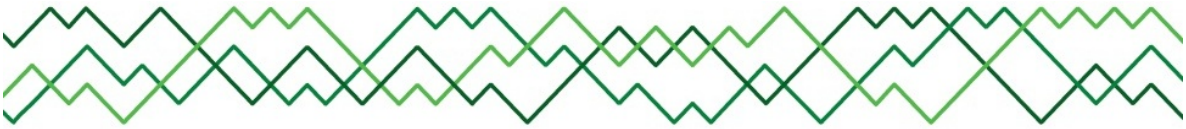
Рисунок 17. Распределение утечек по странам, 2015 г.

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.

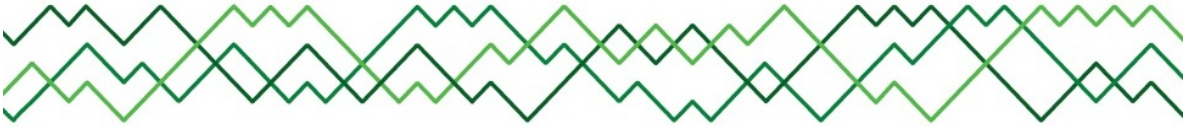
Долгое время мы отмечали определенную инертность российского бизнеса и граждан в вопросе защиты информации. В этом году отечественные компании продемонстрировали готовность защищать свои данные не только административным путем, но и в судебном порядке.

> *РИА Новости: Бывший сотрудник «Яндекса» получил условный срок за кражу исходного кода и алгоритмов Яндекс.Поиска. По данным следствия, злоумышленник скопировал с сервера компании программу «Аркадия», которая содержала код и исходные алгоритмы поисковика. В Яндексе утверждают, что стоимость похищенных данных составляет несколько миллиардов рублей. Потеря исходного кода могла обернуться для поисковика «годами судебных разбирательств, серьезными репутационными издержками и падением капитализации», поскольку поисковик – «основной сервис компании», - пишет Ъ.*

Информация об утечках все чаще появляется не только в отечественных СМИ, но и в прессе таких стран, как Индонезия, Вьетнам, Индия.



infowatch.ru: Заместитель министра и сотрудник министерства финансов Индии арестованы по подозрению в краже конфиденциальной информации. По версии следствия, чиновники передали группе лиц секретные сведения относительно инвестиционных планов иностранных корпораций в Индии. Посредником выступил консультант одной из компаний в г. Мумбаи. Сами документы передавались по электронной почте либо курьерской доставкой. В ходе обысков, проведенных ЦБР в Мумбаи и Дели, в офисе консультанта найдены 60 млн Шри-Ланкийских рупий наличными (около 500 тыс. долларов США). Также найдены копии конфиденциальных документов.



Заключение и выводы

В 2014 году мы объявили о наступлении эры «мега-утечек»[15]. За истекший год ситуация ухудшилась – зафиксировано 55 утечек, в ходе которых объем скомпрометированных персональных данных превысил 1 млн записей. Из них 21 «мега-утечка» – 10 млн записей и более.

Наиболее весомый вклад в увеличение объема скомпрометированных данных принадлежит внешним атакам. В результате воздействия внешнего злоумышленника скомпрометировано чуть менее 1 млрд записей о персональных данных. Наметившаяся тенденция, скорее всего, сохранится. Уже сейчас на долю внешних атак приходится до двух третей от совокупного объема скомпрометированных ПДн.

Самые заметные инциденты 2015 года связаны с неправомерной деятельностью хакеров, проникновением в инфраструктуру компаний, извлечением агрегированной информации о сотрудниках и клиентах.

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.

Следует уже сейчас серьезно задуматься о смене подходов к защите информации. Применение методов поведенческого анализа в сочетании с фокусированием на контроле конкретных, наиболее критичных каналах коммуникации – прежде всего сеть — способно дать дополнительный синергетический эффект, повысив в целом уровень защиты данных.

Самыми «привлекательными» для злоумышленников и, как следствие, уязвимыми отраслями оказались сегмент высоких технологий, торговля, транспорт. Наибольший объем скомпрометированных данных (без учета «мега-утечек») пришелся на высокотехнологичные компании и организации в сфере образования. Данные торговых, транспортных, высокотехнологичных компаний чаще всего атакуют извне. В банках, страховании, медицине компрометация ПДн связана, как правило, с действиями внутренних злоумышленников. 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. Пока, к сожалению, подобные оценки актуальны лишь для стран англо-саксонского мира.

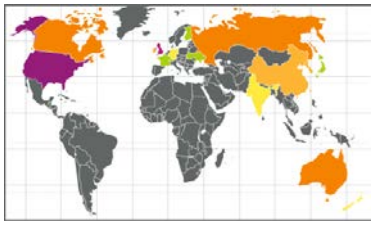
[15] Под «мега-утечками» авторы исследования понимают утечки данных, в результате которых объем скомпрометированных данных составил 10 млн записей и выше.

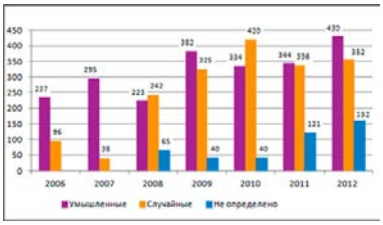
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

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.



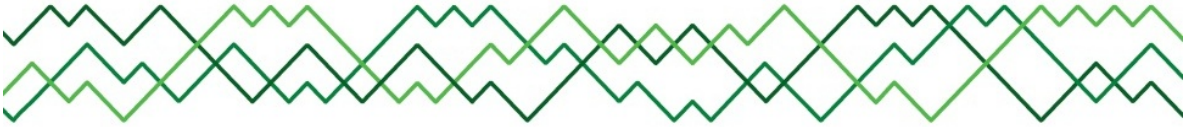


Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- 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».*