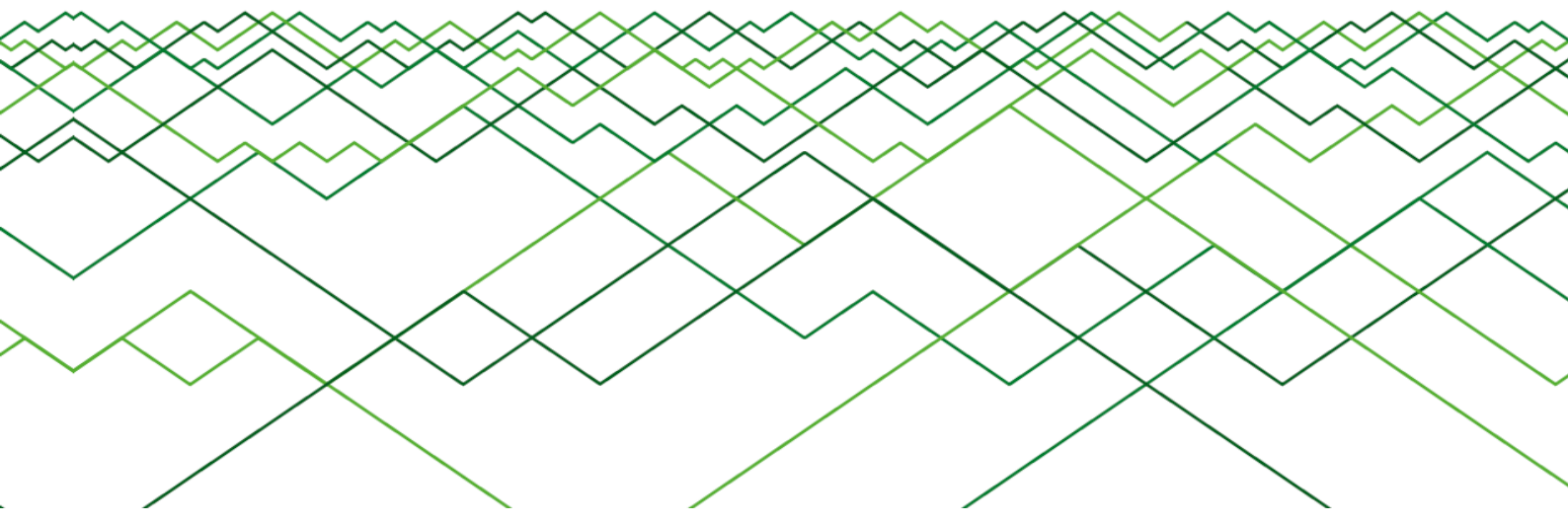
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аналитический Центр InfoWatch
www.infowatch.ru/analytics

Глобальное исследование утечек конфиденциальной информации в 2014 году



INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Оглавление

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Только цифры

- ✓ В 2014 году по всему миру обнародовано (в СМИ и иных источниках) и зарегистрировано Аналитическим центром InfoWatch **1395** случаев утечки конфиденциальной информации, что на **22%** превышает число утечек, зарегистрированных в 2013 году.
- ✓ Больше всего утечек информации связано с персональными данными – в **92%** случаев утекала именно эта информация. Более **767 млн** персональных данных были скомпрометированы из-за ошибок или намеренных действий внутренних нарушителей, вследствие внешних атак.
- ✓ В 2014 году зафиксировано **14** «мега-утечек». В результате каждой «утекло» более **10 млн** персональных данных. На «мега-утечки» пришлось **89%** всех скомпрометированных записей.
- ✓ Банки, наряду с интернет-сервисами, ретейлерами и медицинскими учреждениями, являются основным источником утечек персональных данных.
- ✓ В **55%** случаев виновными в утечке информации оказались сотрудники компаний. В **1%** случаев – высшие руководители организаций.
- ✓ Россия заняла второе место по числу известных утечек. В исследуемый период зарегистрировано **167** случаев утечки конфиденциальной информации из российских компаний и государственных организаций. Количество «российских» утечек по сравнению с 2013 годом выросло на **73%**.

Аннотация

Аналитический центр компании InfoWatch представляет отчет об исследовании утечек конфиденциальной информации в 2014 году. Авторы исследования попытались построить наиболее полную картину утечек информации в масштабе всего мира, выявить факторы, формирующие эту картину, показать, какими последствиями оборачиваются утечки данных для коммерческих компаний, государственных органов, граждан.

2014 год можно назвать годом «мега-утечек» персональных данных. Зафиксировано более 30 случаев, когда объем персональных данных, скомпрометированных в результате утечки, составил свыше 1 млн записей. Половина из этих утечек поистине гигантского масштаба – 10 млн записей и выше.

СМИ широко освещали атаки на инфраструктуру ретейлеров Home Depot, Michaels Stores, Neiman Marcus, Sally Beauty Holdings. Каждый раз речь шла о компрометации персональных данных, включая реквизиты пластиковых карт. Наряду с ретейлерами, от внешних атак серьезно пострадали банки, интернет-сервисы. В списке жертв злоумышленников Evernote, Experian, HSBC Turkey, JPMorgan Chase, Korea Credit Bureau, Google, Orange, Snapchat.

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.

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Методология

Исследование основывается на собственной базе данных, пополняемой специалистами Центра с 2004 года. В базу Аналитического центра InfoWatch включаются публичные сообщения[1] о случаях утечки[2] информации из коммерческих и некоммерческих (государственных, муниципальных) организаций вследствие злонамеренных или неосторожных действий[3] сотрудников, внешних нарушителей[4]. База утечек InfoWatch насчитывает несколько тысяч 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.

С 2014 года в базу добавляются утечки данных, произошедшие вследствие внешнего воздействия (таргетированная атака, фишинг, взлом веб-ресурса и пр.). Для корректного сравнения данных 2014 года с данными предыдущих периодов авторы провели коррекцию показателей 2013 года.

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 их 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% 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 выводы исследования и выявленные на выборке тренды репрезентативными для генеральной совокупности.

---

[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 потеря контроля над информацией вследствие 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. 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.

Для сохранения однородности выборки при составлении отраслевой карты мы целенаправленно вывели за рамки исследования утечки с несоразмерно большим (более 10 млн) количеством утекших персональных данных – «мега-утечки». При составлении отраслевой карты утечки с незначительным (менее 100) объемом «утекших» записей также удалены из выборки.

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

Общая статистика

В 2014 году Аналитическим центром InfoWatch зарегистрировано 1395[8] (3,8 в день, 116 в месяц) случаев утечки информации. В результате утечек скомпрометировано 767 млн персональных данных (записей ПДн), – номера социального страхования, реквизиты пластиковых карт, иная критически важная информация (см. Рисунок 1.

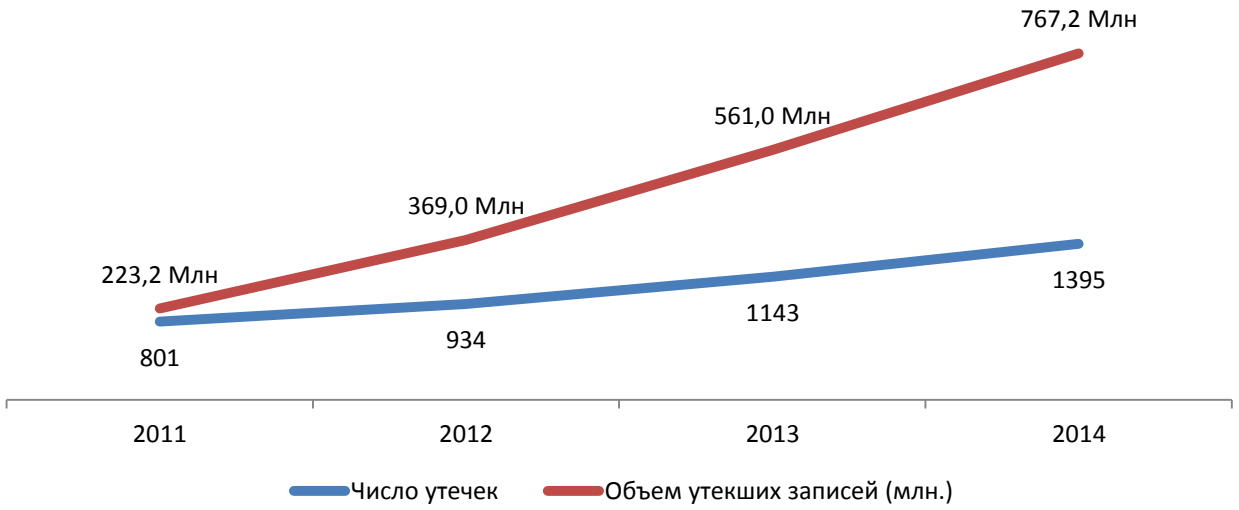
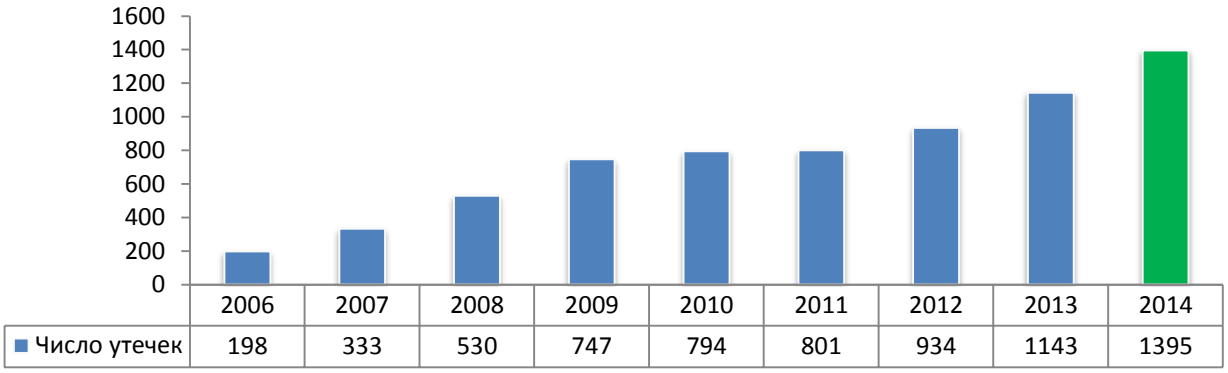


Рисунок 1. Число утечек информации и объем утекших записей ПДн, скомпрометированных в результате утечек. 2011 - 2014 гг.

Рост числа утечек информации в 2014 году продолжился (см. Рисунок 2).



	2006	2007	2008	2009	2010	2011	2012	2013	2014
Число утечек	198	333	530	747	794	801	934	1143	1395

Рисунок 2. Число зарегистрированных утечек информации, 2006 -2014 гг.

В исследуемый период динамика роста утечек осталась на уровне предыдущего года, составив 22% к числу утечек 2013 года. При этом прирост объема скомпрометированных персональных данных замедлился, составив 37% к

[8] 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.

предыдущему году. В результате одной утечки в среднем скомпрометировано 0,55 млн записей ПДн, - на 12% выше аналогичного показателя 2013 года (см. Рисунок 3).

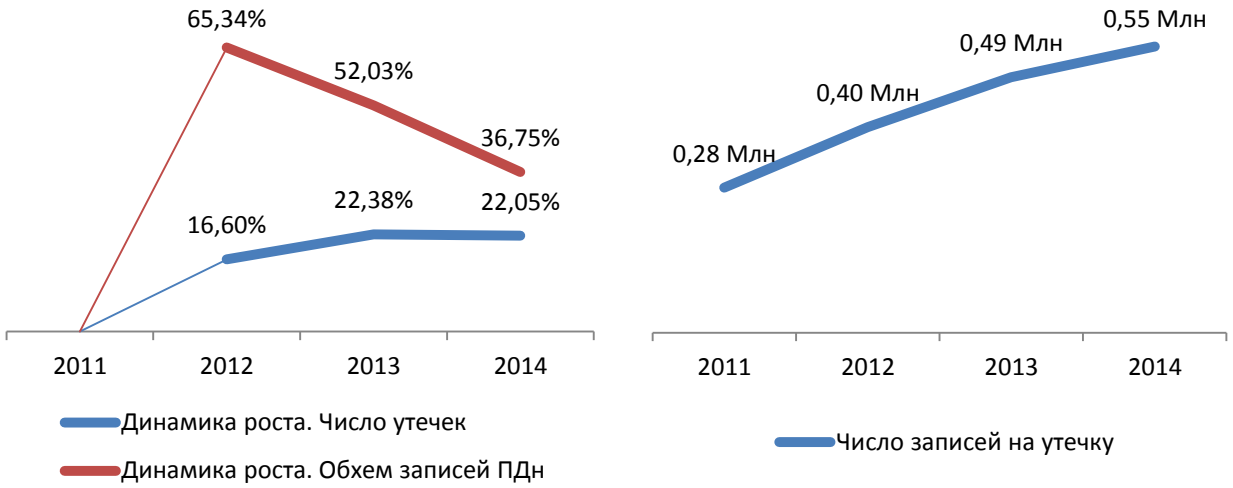


Рисунок 3. Динамика роста числа утечек, объема записей ПДн. Объем персональных данных, скомпрометированных в ходе одной утечки. 2011 -2014 гг.

Зарегистрировано 1016 (73%) утечек информации, причиной которых стал внутренний нарушитель. В 353 (25%) случаях утечка информации произошла из-за внешнего воздействия. В 2% случаев невозможно определить, откуда осуществлялась атака (см. Рисунок 4).

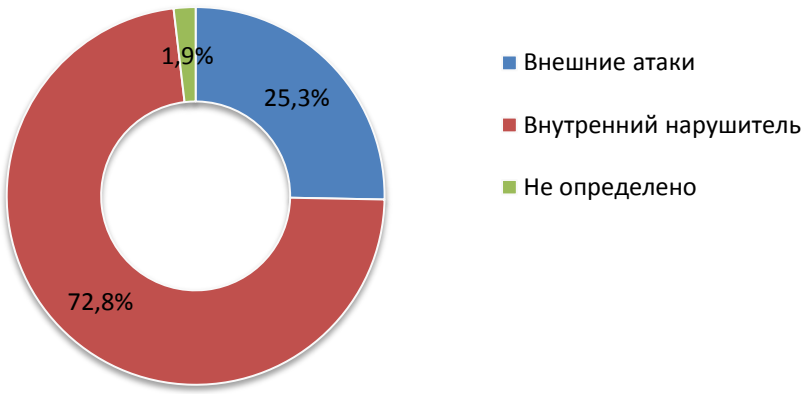


Рисунок 4. Распределение утечек по вектору воздействия, 2014 г.

В результате воздействия внутреннего нарушителя скомпрометировано 350 млн персональных данных (0,34 млн на утечку). Итогом внешнего воздействия стала компрометация 410 млн записей (1,16 млн на утечку).

В распределении по виновнику утечки[9] доля случаев, когда виновника не удалось определить, составила 13%. В 55% виновниками утечек информации были настоящие или бывшие сотрудники – 54% и 1% соответственно (см. Рисунок 5)[10].

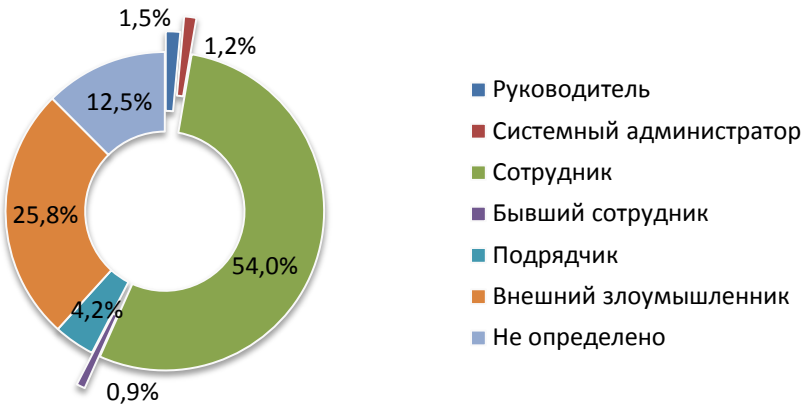


Рисунок 5. Распределение утечек по виновнику, 2014 г.

Велика доля утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к охраняемой информации (4%). Более чем в 1% случаев зафиксирована вина руководителей организаций (топ-менеджмент, главы отделов и департаментов); пользователей с расширенными правами доступа к информации (системных администраторов).

В 2014 году чуть менее половины утечек были случайными. По сравнению с 2013 годом, доля случайных утечек увеличилась на 10 п. п. Доля умышленных утечек, соответственно, уменьшилась (см. Рисунок 6).

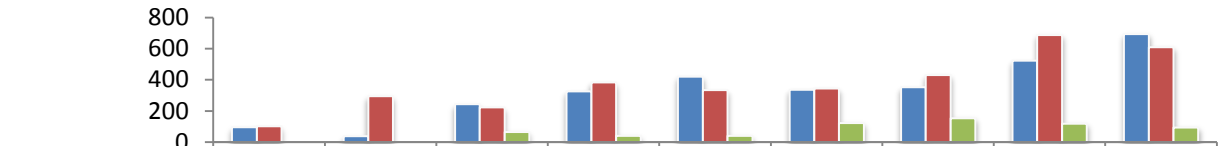
Рисунок 6. Распределение утечек по умыслу, 2013 - 2014 г.[11]

[9] Виновник утечки - лицо, неумышленно допустившее утечку информации, либо совершившее злонамеренные действия, следствием которых явилась компрометация охраняемой информации.

[10] Для данного распределения из выборки исключены утечки, где не установлено, откуда осуществлялась атака. Таким образом равное в числовом выражении количество утечек, которое пришлось на внешние атаки, распределилось как 25,3% (Рисунок 4) и 25,8% (Рисунок 6).

Перераспределение долей утечек по умыслу происходит вследствие того, с распространением средств защиты информации (в том числе DLP-решений) случайных утечек фиксируется все больше. Число злонамеренных утечек растет медленнее, чем случайных, поскольку их фиксация требует использования более дорогих средств противодействия утечкам данных.

Выявлено сокращение доли утечек, которые нельзя отнести к умышленным или случайным – неопределенные утечки, – с 9% в 2013 до 7% в 2014 году. Данный тренд сохраняется с 2012 года (см. Рисунок 7).



	2006	2007	2008	2009	2010	2011	2012	2013	2014
Случайные	96	38	242	325	420	336	352	522	693
Умышленные	102	295	223	382	334	344	430	687	609
Не определено	0	0	65	40	40	121	152	117	93

Рисунок 7. Динамика случайных и умышленных утечек, 2006 -2014 гг.

Исследователи связывают снижение доли неопределенных утечек с повышением общей грамотности среди специалистов по информационной безопасности, которые успешно определяют источник утечки, виновных, наличие умысла. В итоге сообщений об утечках, где неясен канал передачи информации, намерения нарушителя, становится все меньше.

Доля утечек персональных и платежных данных в распределении утечек по типу информации выросла на 7 п. п. к данным 2013 года, составив 92% (Рисунок 8).

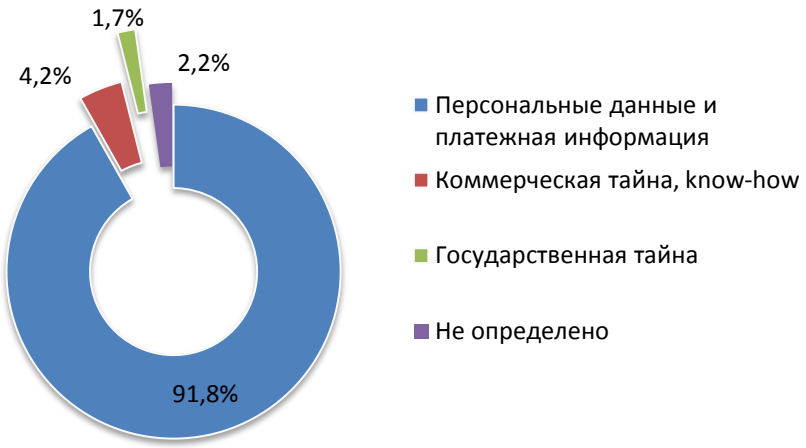


Рисунок 8. Распределение утечек по типам данных, 2014 г.

[11] Утечки информации, спровоцированные действиями внешнего нарушителя, авторы исследования по умолчанию относят к типу умышленных. Доля умышленных утечек в 2013 году скорректирована в большую сторону, с учетом доли утечек под воздействием внешнего нарушителя, зафиксированных в 2014 году.

На «мега-утечки» с объемом скомпрометированных данных свыше 10 млн записей ПДн пришлось 89% всех скомпрометированных записей. СМИ широко освещали атаку на инфраструктуру Target Corp. Не менее показательна внешняя атака на другого ретейлера - Home Depot, состоявшаяся в конце 2014 года:

> securitylab.ru: *Крупнейшая в мире компания по продаже стройматериалов и ремонтных приспособлений Home Depot заявила, что 53 миллиона адресов электронной почты клиентов сети магазинов были скомпрометированы. По предварительным подсчетам, убытки Home Depot вследствие взлома составили 56 млн долл. США. Хакерам удалось проникнуть в сеть Home Depot с помощью пароля, принадлежащего стороннему разработчику программного обеспечения. В результате манипуляций с правами доступа, под контролем злоумышленников оказались несколько сегментов сети компании. Хакеры внедрили в систему вредоносное ПО, с помощью которого и была похищена информация – электронные адреса и реквизиты пластиковых карт. Специалисты Home Depot отмечают уникальность вредоносного ПО, использованного для атаки на компанию. Антивирусы, развернутые в Home Depot, не смогли обнаружить подозрительную активность со стороны хакерских программ.*

В 2014 году огромное число утечек информации связано с использованием персональных данных в целях мошенничества – преступления, известные как «кража личности» (identity theft).

> Ведомости: *Имена, адреса, номера телефонов, адреса электронной почты около 83 млн владельцев домохозяйств и предприятий были украдены через систему JPMorgan Chase. Это одна из крупнейших краж персональных данных в истории. Атаке подверглись 76 млн частных счетов и 7 млн счетов, принадлежащих малым предприятиям.*

В распределении по характеру действий нарушителя (см. Рисунок 9) в 81% случаев зафиксирована «классическая» утечка – потеря контроля над информацией.

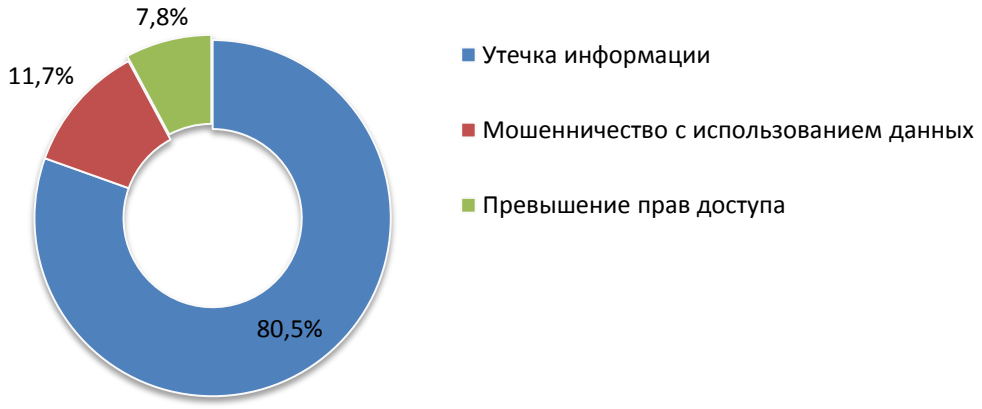


Рисунок 9. Распределение инцидентов по характеру, 2014 г.

8% зарегистрированных 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).

> databreaches.net: *Сотрудник одного из офисов испанского банка Santander в графстве Лестершир (Великобритания) оштрафован судом на 880 фунтов стерлингов. 29-летний Дэвингер Сингх (Dalvinder Singh) работал в отделе противодействия отмыванию денег и имел легитимный доступ к счетам клиентов банка. Он решил воспользоваться своими расширенными правами, чтобы выяснить, сколько зарабатывают его коллеги. По итогам инцидента любопытный сотрудник уволен. Представители банка рассказали, что незадолго до случившегося Сингх прошел тренинг о принципах работы с чувствительной информацией. Но это не помогло.*

В 12% случаев хищения информации отягощено ее неправомерным использованием с целью извлечения личной выгоды (как правило, финансовое мошенничество сотрудников кредитных учреждений – фрод).

> ***Вывод:***
>
> *Прирост объема скомпрометированных персональных данных происходит за счет «мега-утечек», прирост числа утечек спровоцирован в большей степени внешними атаками. Основные показатели, отражающие глобальную картину утечек данных – динамика роста утечек, доля персональных данных и коммерческой тайны, доля сотрудников в распределении по виновнику утечки – практически не изменяются год к году. Доля утечек неопределенной природы последовательно снижается.*

Каналы утечек

Изучение утечек в разрезе каналов, по которым уходит информация, имеет практическое значение. В зависимости от частоты утечек по тому или иному каналу, можно рекомендовать внедрение средств защиты в компании или в отрасли, определить, каким каналам следует уделить повышенное внимание.

В 2014 сократилась доля утечек через съемные носители (-0,4 п. п.), электронную почту (-0,5 п. п.), по голосовому и видеоканалам, через мгновенные сообщения (-3,9 п. п.). Доля утечек бумажных документов изменилась незначительно (+0,2 п. п.). На фоне других категорий заметно подросли утечки, связанные с кражей или потерей оборудования, в том числе пользовательского - ноутбуки, смартфоны (+4,5 п. п.).

В 18% случаев в сообщениях об утечке нет информации о канале. Доля таких случаев снизилась на 7,8 п. п. (см. Рисунок 10).

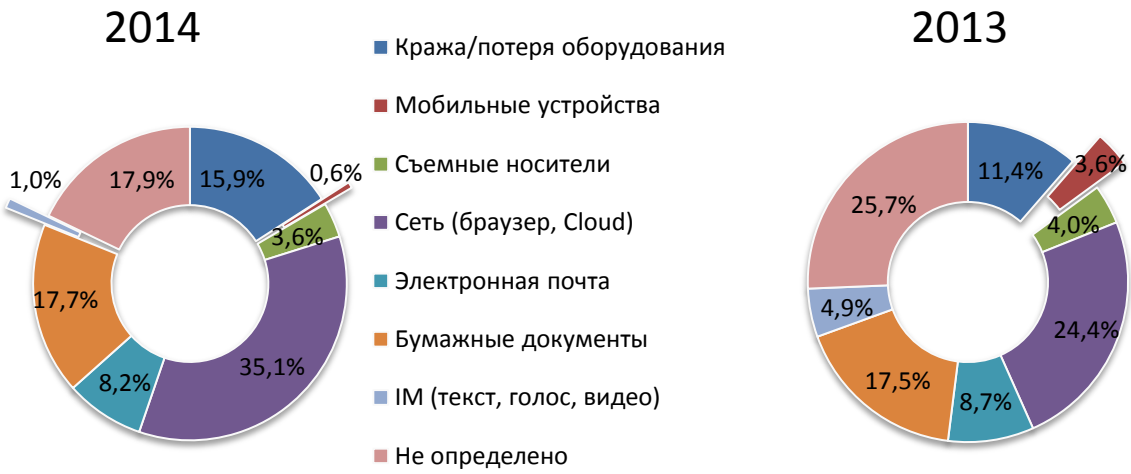


Рисунок 10. Распределение утечек по каналам, 2013 – 2014 гг.

Доля утечек через сеть составила 35% (+10,7 п. п.), что вполне объяснимо – именно через этот канал происходят утечки данных под воздействием внешних атак[12].

> *The Wall Street Journal: В результате хакерской атаки были скомпрометированы данные сотрудников, руководства и клиентов Почтовой службы США (USPS). В руках злоумышленников, возможно, оказались 800 тыс. записей, включая имена, адреса и номера социального страхования американцев. В числе пострадавших оказались действующие сотрудники и работники, ушедшие на пенсию. Атака затронула подразделения Почтовой службы, департамент инспектирования, департамент инспектирования.*

[12] В распределении по каналам учитываются утечки данных, спровоцированные внешним воздействием. Такие утечки происходят исключительно через сеть. Потому для данных 2013 года авторы скорректировали долю сетевого канала в сторону увеличения в пропорции, равной доле утечек 2014 года, спровоцированных внешним воздействием.

Утечки через мобильные устройства сократились (-3 п. п.). Малая доля утечек через мобильные устройства связана с низкой эффективностью существующих решений для защиты данных на смартфонах, планшетах. Однако, это не значит, что утечку через мобильные устройства нельзя отследить:

> *Triblive: Топ-менеджер PNC Bank Эйлин Дейли (Eileen Daly) фотографировала экран своего компьютера на личный мобильный телефон незадолго до того, как поменяла работу и ушла к конкурентам в Morgan Stanley. Система информационной безопасности банка не позволила Эйлин просто скопировать данные клиентов в электронном виде, поэтому ей пришлось фотографировать экран компьютера. По оценкам PNC Bank, ущерб от действий бывшего топ-менеджера составил 250 млн долл. Представители банка говорят как минимум о 15 крупных клиентах, которые ушли к конкуренту вслед за госпожой Дейли.*

Доли умышленных утечек через съемные носители, электронную почту, бумажные документы незначительны. Для сравнения: в 2013 году доля умышленных утечек через электронную почту составила 5,8%, в 2014 году по этому каналу мы наблюдали 1,2% умышленных утечек. Доли случайных и умышленных утечек с использованием мобильных устройств составили – 1% и 0,2% соответственно (см. Рисунок 11).

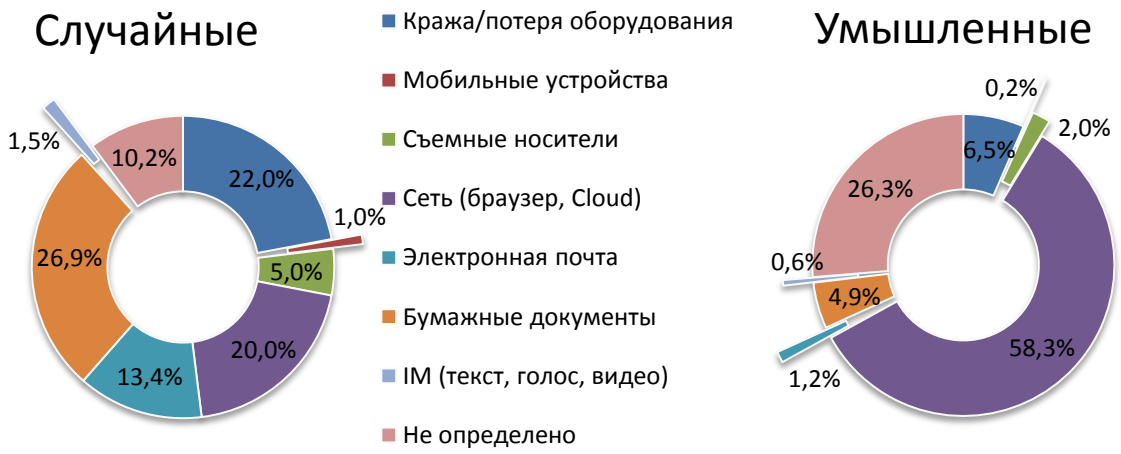


Рисунок 11. Распределение случайных и умышленных утечек, 2013 - 2014 гг.

Отметим, что доля утечек не всегда отражает размер опасности, связанный с конкретным каналом. Так, по каналу «электронная почта» регистрируется 13% всех случайных утечек и всего 1% из всех умышленных. Но очевидно, что достаточно одного случая утечки критически важной информации по электронной почте, чтобы компания столкнулась с многомиллионными финансовыми потерями.

> *Bloomberg: Канг Гао, бывшему аналитику фонда Two Sigma Investments LLC, предъявлены обвинения в краже конфиденциальной информации у работодателя. Аналитика арестовали еще в январе, после того, как он объявил о своем уходе из Two Sigma Investments. Представители Two Sigma*

сообщили, что Канг Гао использовал программу-декомпилятор для получения доступа к информации в скрытых модулях корпоративного ПО, а затем отправил эту информацию на свой личный электронный ящик. В компании признают, что распространение украденных данных нанесет непоправимый ущерб бизнесу.

Остается упомянуть еще один, довольно экзотический канал – утечки информации через текстовые и видеосервисы мгновенных сообщений. Данный канал представлен незначительными 1,5% на диаграмме случайных утечек и 0,6% на диаграмме злонамеренных. Однако само появление таких утечек – аргумент в пользу старой истины, что в информационной безопасности не бывает «мелочей» и неважных, «периферийных» каналов.

Известно, что DLP-системы успешнее всего проявляют себя в деле выявления и предотвращения случайных утечек информации. Все большее распространение решений класса DLP позволяет компаниям регистрировать случайные утечки, ранее остававшиеся незамеченными, и верно их классифицировать. С этим связано уменьшение доли случайных утечек по неопределенному каналу.

Впрочем, иногда даже для крупных утечек канал передачи данных остается неизвестным:

delfi.lv: Утечка информации в процессе продажи контролируемого латвийским государством коммерческого банка Citadele обошлась Латвии в 7 миллионов евро, пишет портал delfi.lv со ссылкой на министра экономики Вячеслава Домбровского. Министр отмечает, что в утечка данных и геополитические обстоятельства создали «помехи» конкуренции. Число потенциальных покупателей банка уменьшилось, некоторые инвесторы узнали об интересах конкурентов, заявил господин Домбровский. В итоге цена актива существенно упала.

Небольшие доли умышленных утечек через съемные носители, электронную почту, бумажные документы (особенно на фоне довольно существенных долей этих каналов в распределении неумышленных утечек) 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:

Существенное различие в распределении умышленных и случайных утечек по каналам говорит о растущей квалификации внутреннего нарушителя. Утечек данных по «традиционным» каналам фиксируется все меньше, так как злоумышленники их не используют, поскольку хорошо осведомлены о функциональных возможностях защитных решений.

Отраслевая карта

В 2014 году доля утечек из государственных и муниципальных учреждений в исследуемом периоде снизилась на 16 п. п., составив 16%, при этом на 13 п. п. подросла доля коммерческих компаний (см. Рисунок 12).

Рисунок 12. Распределение утечек по типу организации,2013 – 2014 гг.

Чаще всего утечки фиксировались в медицине (25%), реже всего в муниципальных учреждениях (2%). При этом по объему скомпрометированных записей пальму первенства удерживает банковская вертикаль – 41%, вдвое меньше данных утекло в высокотехнологичных компаниях – 17%, торговых компаниях – 15% (см. Рисунок 13).

Рисунок 13. Распределение числа утечек и объема скомпрометированных персональных данных по отраслям, 2013 - 2014 гг.

На данное распределение оказывают серьезное влияние «мега-утечки», где количество скомпрометированных записей превышает 10 млн. С другой стороны, из распределения не исключены «пустые» утечки (когда число скомпрометированных записей менее 100 либо неизвестно). Чтобы нивелировать влияние «пустых» и

«мега-утечек» на результат, авторы скорректировали выборку, оставив утечки с объемом скомпрометированных данных более 100 и менее 10 млн записей ПДн. Дальнейшие графики построены на скорректированных данных.

Распределение скомпрометированных записей в расчете на одну утечку в разрезе отрасли позволяет выделить отрасли, больше всего страдающие от утечек персональных данных (см. Рисунок 14).

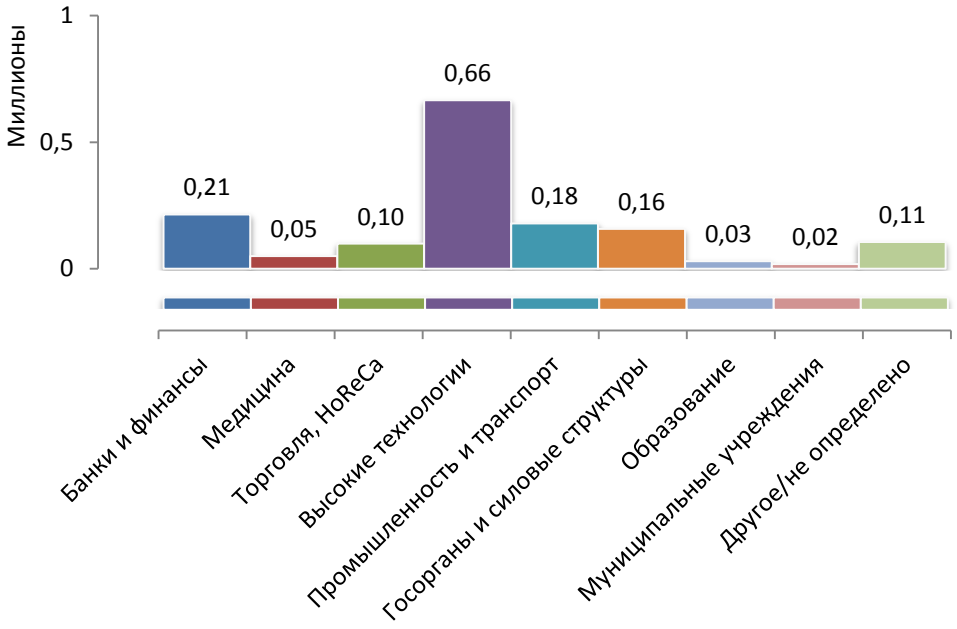


Рисунок 14. Объем скомпрометированных записей персональных данных на одну «непустую» утечку по отраслям. 2014 г., млн

Лидирующее положение по данному показателю заняла высокотехнологичная вертикаль (за счет интернет-сервисов), где на одну утечку пришлось 0,66 млн скомпрометированных персональных данных (в том числе финансовые данные сотрудников и клиентов).

> *The Irish Times: 500 тыс. евро потратил ирландский оператор программ лояльности Loyaltybuild на обновление системы информационной безопасности и ликвидацию последствий крупнейшей в истории Ирландии утечки, в ходе которой были скомпрометированы персональные данные 1,5 млн пользователей сервиса по всей Европе. Украдены не только имена или адреса клиентов, но и платежные данные, включая реквизиты кредитных карт и коды CSV, которые хранились в незашифрованном виде. На время следствия все операции Loyaltybuild были приостановлены. Компания смогла возобновить деятельность лишь спустя 3 месяца после происшествия.*

Банки, наряду с ретейлерами, также являются значимым «поставщиком» персональных данных на черный рынок.

Более объемно картину утечек иллюстрирует отраслевая карта. На диаграммах легко видеть, каков совокупный объем скомпрометированных персональных данных

в отрасли (размер пузырьков) с разбиением по размеру компании, каково число зафиксированных утечек (положение пузырьков по вертикали) см. Рисунок 15.

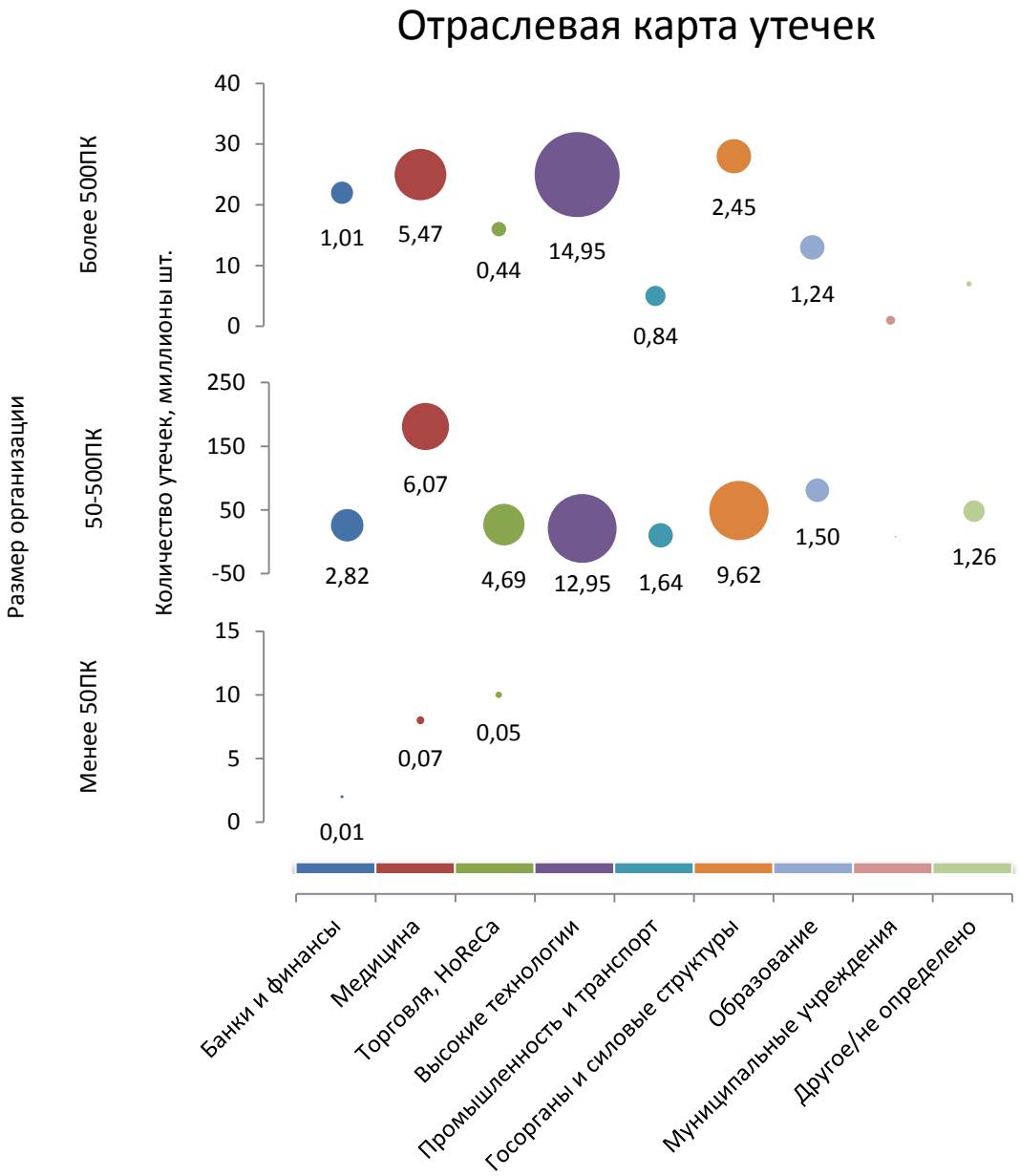


Рисунок 15. Отраслевая карта утечек персональных данных, млн.2014 г.

Отраслевая карта в исследуемом периоде получилась неоднородной. Наибольший объем скомпрометированных данных пришелся на высокотехнологичные компании (включая интернет-сервисы). Также со знаком минус отличились госорганы, медицина, торговля.

> *The Telegraph: Медицинские данные 47 миллионов пациентов медучреждений системы NHS проданы страховой компании. С помощью этих сведений страховая компания намерена «улучшить» свою систему выплат и премий,*

пересмотрев, в частности, риски по страхованию здоровья. Так на основе проданной информации выяснилось, что люди до 50 лет болеют чаще, чем страховщики предполагали ранее. Пока неизвестно, какие меры примут компетентные органы Британии к медикам и страховщикам.

57% утечек из средних компаний относятся к категории случайных. 36% - умышленные утечки. В крупных компаниях распределение иное. Здесь зафиксировано 36% случайных утечек, а более половины (52%) составляют утечки намеренные (см. Рисунок 16).

Рисунок 16. Распределение утечек ПДн по размеру организации 2014 г.

Общее количество утечек персональных данных в сегменте компаний среднего размера (до 500 ПК) существенно выше, чем в сегменте крупных компаний. На средние компании пришлось 71% всех утечек при доле крупных – 24%.

И это при том, что распределение по объему скомпрометированных персональных данных получилось совершенно другим – 45% записей ПДн скомпрометировано средними компаниями, 55% - крупными (см. Рисунок 17).

Рисунок 17. Распределение утечек по размеру организации 2014 г.

При более детальном рассмотрении получается, что на организации среднего размера приходится, в зависимости от отрасли, от 49% до 80% утечек данных.

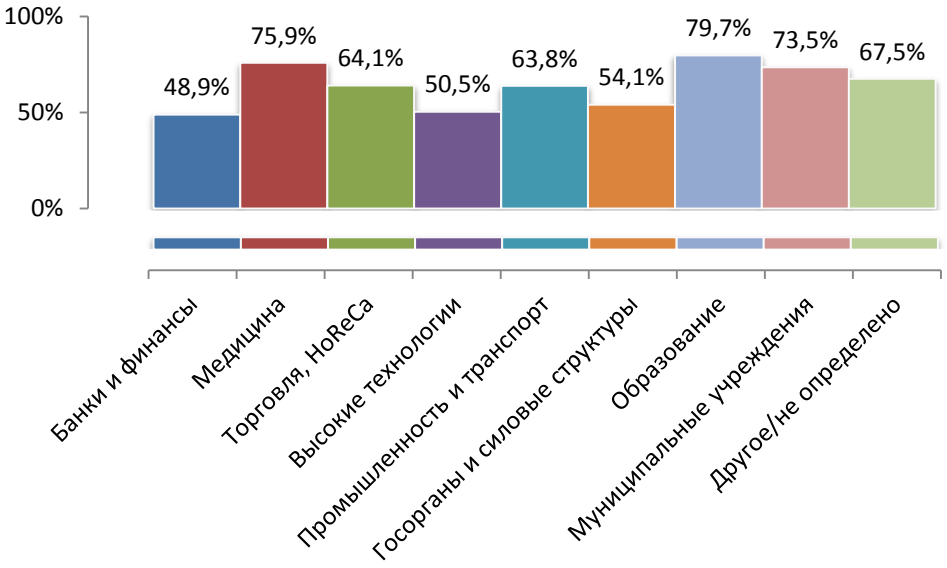


Рисунок 18. Доля утечек из средних компаний по отраслям. 2014 г.

Во многих вертикалях объем персональных данных, утекших из средних организаций, был не меньшим, чем объем данных, скомпрометированных крупными компаниями. В торговле и медицине из средних организаций «ушел» даже больший объем данных, чем из крупных компаний этих вертикалей.

Вывод:

Ситуация с защитой персональных данных в компаниях далека от идеальной. В большей степени это касается среднего бизнеса, где утечки данных происходят чаще, чем в крупных компаниях. Причем большая часть утечек в среднем бизнесе пришлась на случайные. В 2014 году компании среднего размера заняли главенствующее положение в ряду «поставщиков» конфиденциальной информации. В этом аспекте особенно «отличились» интернет-сервисы, образовательные и медицинские учреждения. Именно эти организации обладают наибольшим количеством персональных данных и не спешат их защищать, поскольку не несут прямых финансовых потерь.

Причина столь безрадостного положения небольших и средних компаний объясняется тем, что на рынке практически полностью отсутствуют эффективные и недорогие средства защиты информации, ориентированные на СМБ-сегмент.

Региональные особенности

В распределении утечек по регионам в 2014 году США традиционно вышли на первую строчку по числу утечек (906 или 65% от всех произошедших). Россия заняла уже привычное второе место (167 утечек), которое досталось нашей стране еще по итогам 2013 года. На третьем месте оказалась Великобритания (85 утечка).

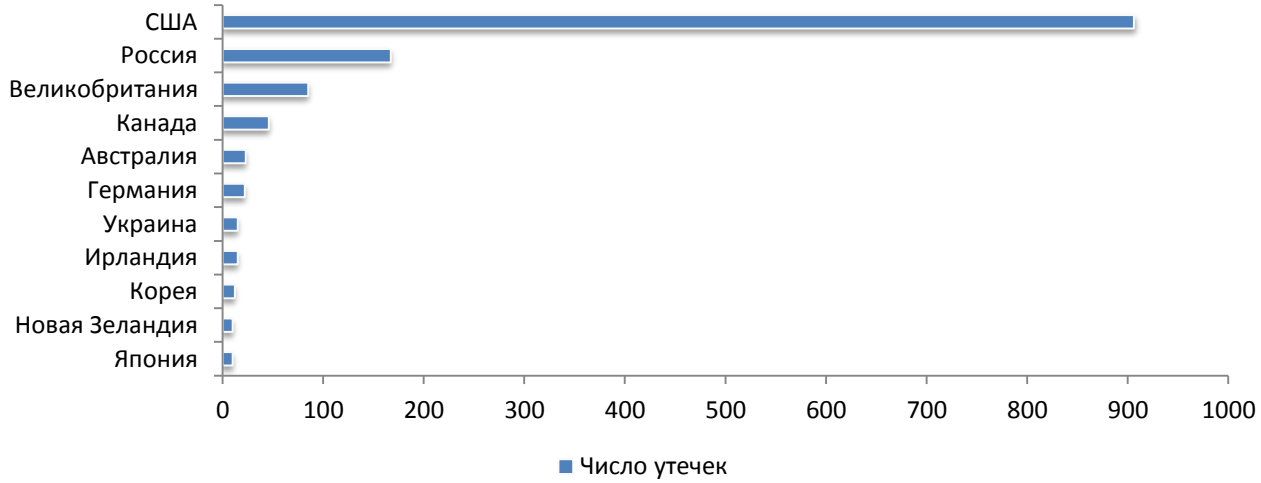


Рисунок 19. Распределение утечек по странам, 2014 г.

Получившееся распределение утечек обладает одной особенностью. На первые роли выходят страны, где государство, общество, СМИ уделяют теме защиты данных повышенное внимание. На данный момент это англосаксонские страны и Россия. ПО субъективным ощущениям, в других странах утекает ничуть не меньше данных, но информация об утечках не попадает в СМИ.

Современная глобальная картина утечек данных с незначительными изменениями характерна для всех стран, где оперируют информацией в электронном виде. Вот пример использования персональных данных в целях мошенничества в американском банке:

> *The Fresno Bee: Сотрудница налогового управления США (IRS) в городе Фресно (Калифорния) в течение двух лет занималась финансовыми махинациями с использованием персональных данных своих коллег. Виририана Эрнандес (Virirriana Hernandez) работала в налоговом ведомстве с 2006 года и по долгу службы имела доступ к данным сослуживцев. Воспользовавшись этими данными, Виририана, вместе с тремя сообщниками, похитила со счетов коллег более 1,2 млн долларов США. Мошеннице грозит более 30 лет тюрьмы и штраф в 250 тыс. долларов, если ее вина будет доказана в суде.*

Вот схожая ситуация в России:

> *oblvesti.ru: Сотрудница коммерческого банка в Волгограде предстанет перед судом по обвинению в крупном мошенничестве. Отдел «К» ГУ МВД и местное УФСБ установили, что 24-летняя жительница Волгограда,*

воспользовавшись служебным положением, передала подельникам персональные данные клиентов банка, в котором работала. С помощью этих данных мошенники переводили деньги со счетов клиентов. Впоследствии деньги обналичивались в банкоматах города Волгограда. В ходе обыска у сотрудницы банка и ее «друзей» изъяли более полумиллиона рублей наличными, 16 банковских карт, 10 сотовых телефонов, более 20 сим-карт различных сотовых операторов, компьютерную технику, а также восемь паспортов граждан РФ.

Существенные различия можно обнаружить лишь в подходах к проблеме утечки данных. В России к компрометации собственных данных граждане относятся более чем спокойно. А вот в тех же США нередки случаи, когда работники, чьи данные были скомпрометированы, предъявляли претензии к компании, допустившей утечку данных.

Pittsburg business times: *Два сотрудника госпиталя UPMC McKeesport в Питсбурге (США) подали в суд на своего работодателя за ненадлежащую защиту персональных данных. Истцы утверждают, что неизвестные хакеры взломали информационную систему госпиталя, получив доступ к финансовым данным сотрудников. После чего злоумышленники открыли на имя сотрудников несколько счетов в банках, оформили фальшивые требования по возврату налогов (income tax returns). Сотрудники, пострадавшие от действий мошенников, уверены, что их иску будет присвоен статус коллективного. Известно о 50 аналогичных случаях, когда данные работников госпиталя использовались злоумышленниками.*

И уж совсем непривычна для нашей страны, например, ситуация, когда за утечку данных топ-менеджеры крупных компаний лишаются должностей. В российских СМИ едва ли удастся найти такую историю, а в Южной Корее подобный случай зарегистрирован совсем недавно:

Cnews: *со ссылкой на The Wall Street Journal сообщает, что ответственность за недавнюю утечку данных из трех корейских организаций взяли на себя топ-менеджеры этих компаний. От утечки пострадали более 100 млн клиентов крупнейших игроков финансового рынка Кореи - KB Financial Group, NongHyup Financial Group и Lotte Group. В связи с инцидентом десятки топ-менеджеров банков подали в отставку. Об утечке стало известно в начале 2014 года, когда властям Кореи удалось арестовать сотрудника Korea Credit Bureau. Этот сотрудник привлекался для обслуживания оборудования трех пострадавших компаний (по другой версии был аудитором).*

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Выводы и прогнозы

2014 год ознаменовался рядом крупнейших утечек персональных и платежных данных. Атака на инфраструктуру сети магазинов Target была самой громкой, но не единственной. В результате 14 «мега-утечек» были скомпрометированы более 683 млн записей – 89% от всего объема утекших персональных данных. Зафиксировано более 30 случаев, когда объем персональных данных, скомпрометированных в результате утечки, составил свыше 1 млн записей.

Чуть ли не три четверти утечек персональных данных связаны с «кражей личности». Похищенная информация использовалась в мошеннических схемах. Преступники оформляли кредиты и налоговые вычеты на чужие данные.

От массированных атак пострадали банки, где сосредоточена информация о счетах физических лиц, реквизитах пластиковых карт и проч. - наиболее «ликвидные» данные. Параллельно шла настоящая охота за теми же типами данных вне банковских информационных систем. Например, с помощью вредоносных программ злоумышленники похищали платежные данные с терминалов оплаты сетевых ретейлеров. Атакам подверглись крупные интернет-сервисы, транспортные компании, государственные структуры.

Рост объемов утекших данных опережал рост числа утечек. Вырос объем скомпрометированных данных в расчете на одну утечку. Увеличилась доля утечек по вине внешнего злоумышленника. Иначе говоря, хакерских атак с целью извлечения персональных данных и иной ценной информации стало больше.

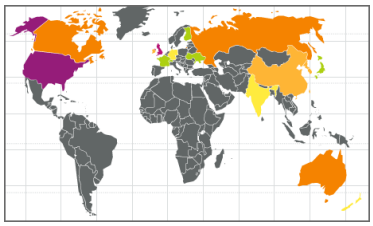
Не отставали и внутренние злоумышленники. 12% всех утечек данных сопряжено с неправомерным использованием информации, к которой сотрудник имел легитимный доступ. Как правило, в таких случаях речь шла о финансовом мошенничестве банковских работников. 8% утечек связаны с неправомерным доступом к данным. Внутренние нарушители практически не использовали такие каналы передачи информации, как мобильные устройства, съемные носители, электронную почту, бумажные документы. «Продвинутый» нарушитель осведомлен, что современные средства контроля позволяют успешно перехватывать передачу конфиденциальной информации по перечисленным каналам, и не рискует понапрасну.

Чем отвечали компании? Результаты исследования показывают, что даже с решением относительно простой задачи – обеспечить безопасность персональных данных – у многих в 2014 году возникли сложности. В большей степени это касается среднего бизнеса, где утечки данных происходили даже чаще, чем в крупных компаниях. Причем большая часть утечек пришлась на случайные. Компании среднего размера заняли главенствующее положение в ряду «поставщиков» конфиденциальной информации. В этом аспекте особенно «отличились» образовательные и медицинские учреждения.

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.



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

- Почтовая рассылка
- Facebook
- Вконтакте
- Twitter
- RSS

Аналитический Центр InfoWatch

www.infowatch.ru/analytics

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, а также потеря контроля над информацией вследствие внешней атаки.*

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.*

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».*