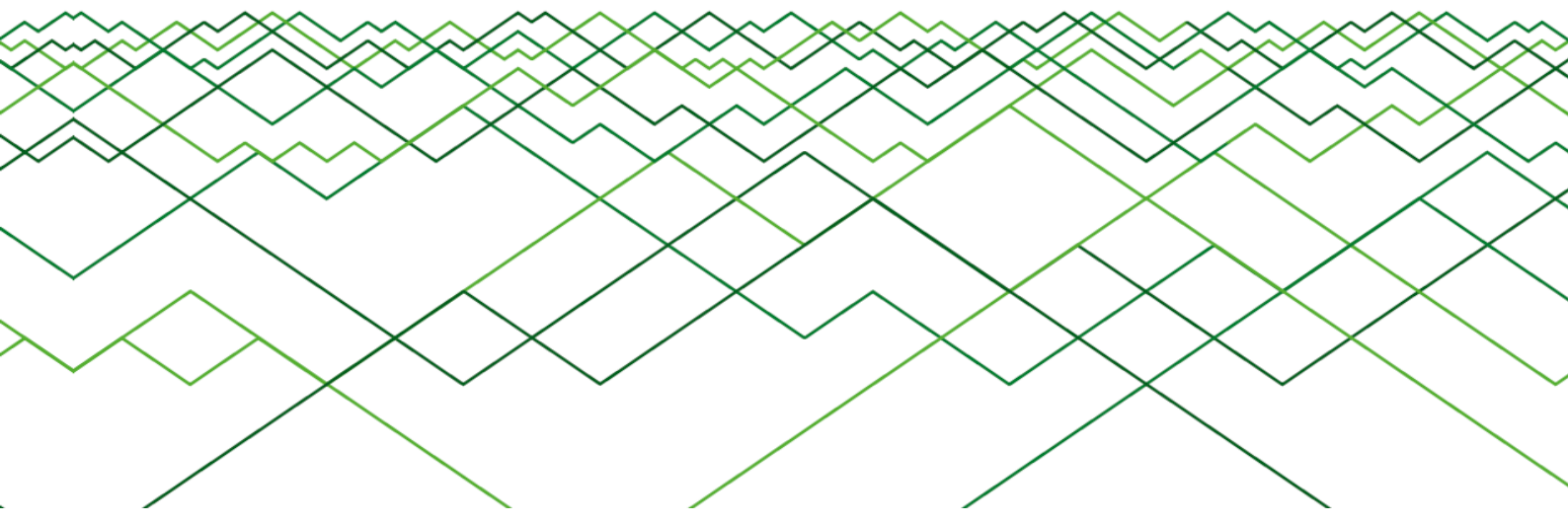
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аналитический Центр InfoWatch
www.infowatch.ru/analytics

Безопасность персональных данных в России в 2013 году. Статистика утечек. Отраслевые особенности.



INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Оглавление

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Только цифры

- ✓ В России за 2013 год в СМИ обнародовано **109** случаев утечки персональных данных, что **в 2,2 раза** выше аналогичного показателя 2012 года.
- ✓ В результате этих утечек скомпрометировано **3,1 млн записей**.
- ✓ На персональные данные пришелся **81%** от всех российских утечек.
- ✓ **49%** утечек персональных данных носили злоумышленный характер. В 48% утечку данных можно назвать случайной.
- ✓ **74%** случаев утечек персональных данных были связаны со злонамеренными или неосторожными действиями рядовых сотрудников. В **9%** вина за утечку лежит на руководителях (средний и высший уровень).
- ✓ **19%** утечек персональных данных пришлись на госорганы, **18%** на компании в сфере ЖКХ. Замкнули тройку «лидеров» финансово-кредитные организации с показателем **16%.**
- ✓ **Две трети** утечек произошло из небольших (менее 500 ПК) организаций.
- ✓ Основным каналом утечек ПДн по-прежнему остается **бумажная документация**.

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Аннотация

Аналитический Центр компании InfoWatch представляет отчет о степени защищенности[1] персональных данных[2] (далее ПДн) в России. **Впервые** в практике Аналитического Центра InfoWatch в качестве предмета исследования избраны случаи утечек[3] ПДн из коммерческих компаний, государственных и муниципальных органов (операторы ПДн[4]), обнародованные в СМИ[5] в истекшем 2013 году.

Также впервые авторы исследования **для некоторых примеров утечек указали размер финансового ущерба**, который понесли организации, пострадавшие от утечки ПДн. Расчет ущерба проведен по методологии компании InfoWatch.

Авторы исследования уверены, что анализ утечек ПДн в конкретном сегменте[6] дает **ключ к пониманию ситуации с безопасностью не только самих ПДн, но и других видов информации**[7] в стране, регионе, отрасли. Так именно на примере ПДн легко выявить каналы утечек[8], через которые информация «уходит» чаще всего, сделать выводы об активности государства и отраслевых регуляторов в вопросе информационной безопасности (далее ИБ) и пр.

В отчете о глобальном исследовании утечек конфиденциальных данных[9] мы назвали год 2012-й годом утечек из государственных органов. Выводы оказались справедливы и для России[10]. В силу различия объекта и предмета, сравнивать

---

[1] Степень защищенности – оценочный показатель того, насколько надежно защищены персональные данные. Формируется на основе экспертного мнения. Не выражается количественными показателями. В данном отчете авторы исследования оперируют терминами «низкая степень защищенности», «высокая степень защищенности», что отражает достаточный или недостаточный, по мнению авторов, уровень безопасности охраняемой информации.

[2] Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (п. 1 ст. 3 ФЗ 152 «О персональных данных»).

[3] Утечка конфиденциальной информации – инцидент информационной безопасности. 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.

[4] В данном исследовании иногда объединяются термином оператор ПДн/оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (п. 2 ст. 3 ФЗ 152 «О персональных данных»).

[5] А также в блогах, интернет-форумах, иных открытых источниках.

[6] Например, на множестве утечек из компаний определенной отрасли, размера и пр.

[7] Информация, доступ к которой ограничен федеральным(и) законом(нами).

[8] См. Методологию.

[9] Глобальное исследование утечек информации за 2012 год. http://www.infowatch.ru/sites/default/files/report/InfoWatch_global_data_leakage_report_2012.pdf

[10] Исследование утечек информации и конфиденциальных данных из компаний и госучреждений России 2012. http://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_rus_2012.pdf

цифры предыдущих исследований с результатами настоящего исследования год-в-год некорректно. Поэтому авторы ограничились сопоставлением наиболее общих трендов, выявленных в ходе этого и вышеназванных исследований.

Страницы СМИ пестрят сообщениями о случаях мошенничества с использованием чужих ПДн (похищенных копий паспортов, утекших записей из баз данных госорганов и коммерческих компаний). В 2013 году от утечек ПДн в России пострадали МВД РФ, Минобороны, Минобрнауки, Минфин Якутии, региональные отделения ФНС, ФМС и Пенсионного фонда, Сбербанк России, Альфа-Банк и Банк Хоум Кредит, «Мегафон», МТС, «Связной-логистика». На утечку ПДн ссылались адвокаты Алексея Навального, оспаривая в суде законность выборов мэра Москвы. В общем, в актуальности темы безопасности ПДн для нашей страны сегодня мало кто сомневается. А исследований степени защищенности персональных данных, мягко говоря, немного.

Отчет о данном исследовании снабжен примерами наиболее типичных или, наоборот, «выдающихся» утечек ПДн, а также комментарием ведущего эксперта InfoWatch по информационной безопасности Андрея Прозорова.

Методология

Исследование основывается на собственной базе данных, которая пополняется специалистами Центра с 2004 года. В базу InfoWatch включаются публичные сообщения о случаях утечки информации вследствие злонамеренных или неосторожных действий сотрудников. 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[11], сфера деятельности (отрасль), размер ущерба, тип утечки (умысел) [12], канал утечки[13], типы утекших данных[14] и пр. **Данные об ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций в СМИ**.

Исследование охватывает не более 1-2%[15] случаев от предполагаемого совокупного количества утечек ПДн, произошедших в российских компаниях[16]. Однако критерии

[11] 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.

[12] Мы разделяем утечки информации по признаку умысла (намерения) на умышленные (злонамеренные) и неумышленные (случайные) см. Глоссарий. Термины умышленные – злонамеренные и неумышленные – случайные (попарно) равнозначны и употребляются здесь как синонимы.

[13] 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.

[14] Предметом настоящего исследования являются исключительно сообщения об утечках персональных данных

[15] В ходе исследования мы столкнулись с явным свидетельством того, что уровень латентности (доля утечек, оставшихся неизвестными широкой публике) в России выше, чем по миру в целом (В

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 исследование на выборке 1-2% репрезентативным для генеральной совокупности**.

В данном исследовании **мы впервые приводим экспертную оценку величины ущерба вследствие утечки персональных данных**. Оценка основывается на собственной методологии компании InfoWatch. Размер ущерба рассчитывается с учетом следующих факторов: отрасль, размер организации (число сотрудников), состав и количество «утекшей» информации, объем и состав клиентской базы, показатель выручки на одного клиента. В модель оценки внесены следующие поправочные коэффициенты: коэффициент на уровень конкуренции (необходим для уточнения величины упущенной выгоды), коэффициенты на количество «утекших данных» (менее 1 тыс. записей, от 1 тыс. до 1 млн, более 1 млн).

В модели расчета ущерба рассматриваются три вида затрат, которые несут организации, в результате утечек: затраты на реагирование, устранение и расследование инцидентов, штрафы и другие санкции регуляторов (в том числе затраты на уведомление регуляторов), репутационные потери и упущенная выгода, выраженные в денежном эквиваленте за 1 год. Стоит отметить, что это не единственные возможные затраты организаций.

Случаи нарушения конфиденциальности информации, произошедшие в результате внешних компьютерных атак, а равно иные инциденты ИБ (DDoS, фишинг, и пр.), не относящиеся к утечкам, в данном исследовании не рассматриваются.

Качество и количество исходных данных (случаев утечки) позволяет подтвердить высокоуровневые гипотезы и обосновать с достаточной вероятностью выводы общего характера. Например, оценить степень защищенности персональных данных в масштабе страны или отрасли. Авторы далеки от намерения на имеющейся выборке строить прогнозы или выводить тренды для более частных разрезов – небольшие компании отрасли, операторы ПДн в регионах и пр.

Результаты исследования

За 2013 год специалистами Аналитического Центра InfoWatch зарегистрировано 109 случаев утечки ПДн из российских коммерческих компаний, государственных и муниципальных органов, что в 2,2 раза превышает число утечек ПДн в 2012 году. В результате утечек было скомпрометировано 3,1 млн записей.

мировой статистике преобладают утечки из американских компаний и госучреждений. И те, и другие обязаны раскрывать факты компрометации данных и информировать пострадавших). Потому экспертная оценка процентной доли известных утечек по сравнению с утечками, оставшимися за рамками внимания данного исследования, понижена с 1-5% до 1-2%.

[16] Компании, ведущие деятельность в Российской Федерации (в том числе иностранные компании и их представительства).

Ключевой факт: персональные данные являются самым массовым типом утекающей информации, однако в России доля таких утечек на 5% ниже, чем по миру в целом

Если в 2012 году на долю ПДн пришлось 65% от всех российских утечек, в 2013 этот показатель подрос до 81% (см. Рисунок 1).

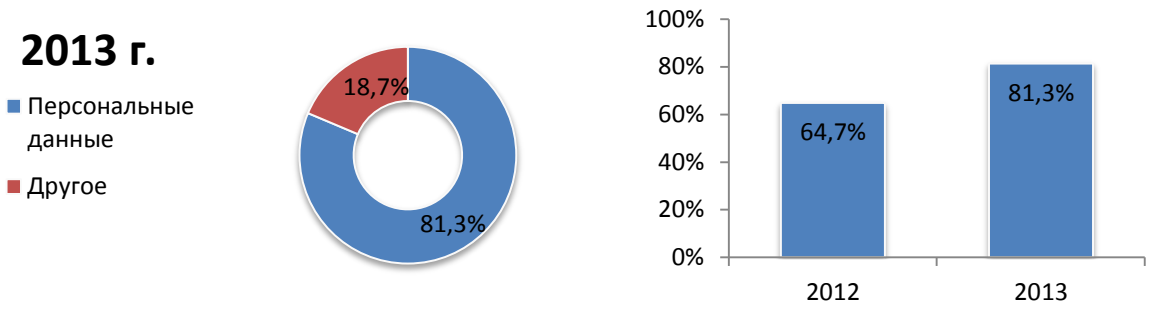


Рисунок 1. Доля персональных данных. Россия

Доля утечек ПДн в России ниже, чем в целом по миру. (По данным статистики, в мире этот показатель с 2008 года ни разу не опускался ниже отметки 86,2% - см. Рисунок 2).

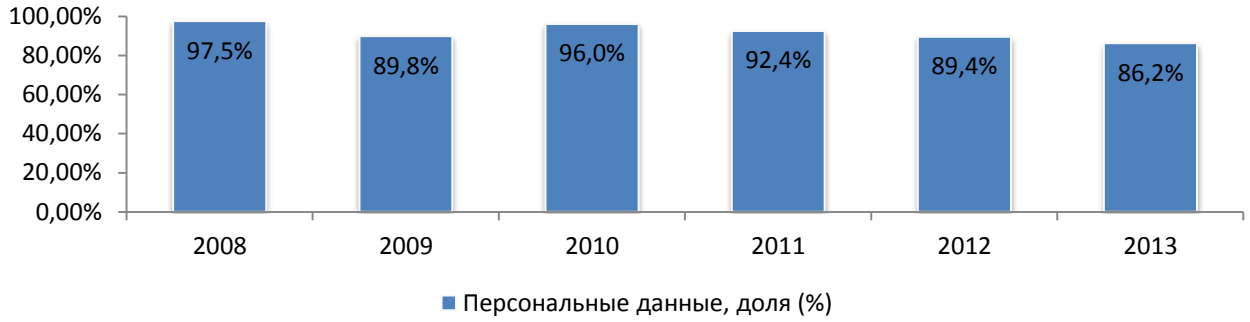


Рисунок 2. Доля утечек персональных данных по годам. Мир[17]

Отметим рост доли российских утечек ПДн в 2013 году (+16 п. п. к 2012 г.) на фоне падения доли ПДн в мировой картине (-4 п. п. к 2012 г.). Почему же динамика изменения доли утечек ПДн в России и в мире разнонаправленна?

Известно, что в глобальной статистике утечек на англосаксонские страны (США, Великобритания и др.) приходится до 78% от общемирового числа утечек данных[18]. Потому уместно, с определенной поправкой, рассматривать ситуацию в этих странах как некий глобальный ориентир. Итак, в этих странах (и по миру в целом) мы

[17] Возможно, данные по доле ПДн в 2013 г. будут скорректированы при создании глобального отчета.

[18] Законодательство этих стран предписывает компаниями и государственным организациям уведомлять пострадавших граждан об утечке их персональных данных. Как следствие, уровень сокрытия утечек ПДн довольно низок, большое количество утечек освещается в СМИ и иных открытых источниках.

наблюдаем устойчивое увеличение доли утечек ПДн с 2004 до 2010 года, после чего следует постепенное снижение (до 86%[19] в 2013 году).

Рост доли утечек ПДн в этих странах был связан с повышением внимания государства и отраслевых регуляторов к теме безопасности ПДн, и, как следствие, с увеличением числа публикаций конкретных случаев утечки ПДн в СМИ. Операторы ПДн под давлением общественности и закона всерьез озаботились внедрением технических средств защиты от утечек (класса DLP). Еще через пару лет проявился эффект – с 2010 года, помимо утечек ПДн, все чаще регистрируются утечки иных типов информации (коммерческой тайны, ноу-хау и пр.), а доля утечек ПДн закономерно снижается.

Рост доли утечек ПДн в «англосаксонском мире» свидетельствовал, таким образом, о все большем распространении технических решений для защиты от утечек и повышении степени защищенности персональных данных.

Означает ли увеличение доли утечек ПДн в российской картине (см. Рисунок 1), что и в нашей стране степень защищенности персональных данных также растет? С большой вероятностью, нет, и вот почему.

По аналогии с США, внимание государства к теме защиты персональных данных сказывается на увеличении сообщений об утечках персональных данных в российских СМИ и блогах. Как следствие, растет доля ПДн в распределении утечек по типам данных для России. Но есть существенное отличие – жесткость санкций (штрафы) к российским операторам, допустившим утечку, пока явно недостаточна. Кроме того, в нашей стране не работает «петля обратной связи» в цепочке государство – оператор – субъект ПДн.

В России утечка персданных не спровоцирует граждан, чьи данные утекли, отказаться от услуг страховой компании, оператора связи, госоргана, допустивших утечку, предъявить претензии государству. Граждане вообще вряд ли об этом узнают – в российском законодательстве, в отличие от США, пока нет нормы об обязательном информировании об утечке пострадавших граждан. А ведь именно такая норма (а вовсе не compliance), заставляет операторов ПДн в США обеспечивать безопасность персональных данных не на бумаге, а на деле. Иначе штрафы, многомиллионные коллективные иски, гражданские протесты.

Андрей Прозоров, ведущий эксперт InfoWatch по информационной безопасности: *«Важным фактором, который может повлиять на изменение количества инцидентов, связанных с утечкой информации, является повышение штрафов. Напомню, что в 2013 году повышения штрафов не произошло, но его мы ожидаем в 2014 году. Высока вероятность того, что, в дополнение к существующим штрафам за невыполнение требований по обработке и защите персональных данных, появятся новые. Скорее всего, операторам придется платить за каждый*

[19] Предположительно. Авторы исследования оперируют статистикой по утечкам в первом полугодии 2013 года и ориентировочными данными по второму полугодию 2013 года.

зафиксированный инцидент[20], возможно, появится норма, обязывающая операторов персональных данных уведомлять Роскомнадзор и других регуляторов обо всех произошедших инцидентах. Снижение темпов роста количества утечек ПДн в России в 2014 году возможно, только если произойдут все эти события. Такого рода регламенты и документы могут появиться под эгидой ФСТЭК России и/или ЦБ РФ».

Налицо две разнонаправленные тенденции. Регуляторы и государство способствуют популяризации темы защиты персональных данных – растет число сообщений об утечках ПДн в СМИ. Но реального сдвига, повышения степени защищенности ПДн не происходит. **Рост доли утечек ПДн в России пока не дает оснований говорить об улучшении ситуации с безопасностью персональных данных**.

Вывод:

Рост доли утечек ПДн в России объясняется возросшей популярностью этой темы в СМИ (как ответ на активность основных российских ньюсмейкеров в сфере ИБ – государства и регуляторов). Не следует (по аналогии с США) связывать выявленный рост доли утечек ПДн с повышением степени защищенности ПДн. Доля скрытых (латентных[21]) утечек, не ставших достоянием общественности, в России остается высокой – операторы ПДн склонны скрывать факты утечек.

Ключевой факт: подавляющее число утечек происходит через каналы, которые могут быть перекрыты техническими средствами

По данным российской статистики утечек ПДн, в 2013 году умышленные и случайные утечки распределились почти поровну – 49% и 48% соответственно (см. Рисунок 3).

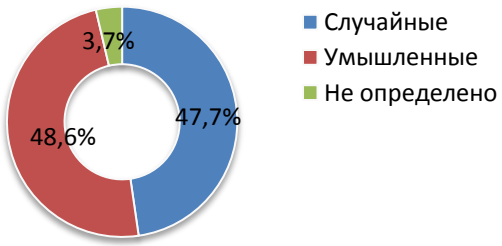


Рисунок 3. Распределение утечек персональных данных по умыслу

[20] Законопроект № 416052-6. «О внесении изменений в Федеральный закон "О персональных данных" и статью 28.3 Кодекса Российской Федерации об административных правонарушениях (в части уточнения порядка обработки персональных данных по поручению оператора, а также уточнения требований по обеспечению безопасности обрабатываемых персональных данных)» http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=416052-6&02

[21] Латентные утечки – факты утечки информации, скрытые от общественности по различным причинам. Латентность тем выше, чем выше процент скрытых утечек. Высокой латентностью утечек отличаются регионы, где практика информирования граждан, пострадавших в ходе утечек ПДн, законодательно не закреплена. Низкая латентность, наоборот, характерна для стран, где информирование пострадавших обязательно – Великобритания, США.

Примерно такое же распределение Аналитический центр InfoWatch регистрирует на данных общемировой статистики уже в течение 4-5 лет. Картина утечек персональных данных из российских компаний характеризуется низкой (менее 4%) долей случаев, когда намерения человека, допустившего утечку, остались неизвестными.

Принято считать, что низкий процент «неопределенных» утечек говорит о распространенности в стране или отрасли средств автоматического обнаружения и предотвращения утечек (DLP систем – с их помощью виновника утечки и его мотивы легко установить). **Для России, однако, такая логика не срабатывает**, и вот почему.

Во-первых, исследование выявило совсем небольшое число актуальных каналов утечки. Чаще всего это бумажные документы – выброшенные формы, медкарты, украденные ксерокопии паспортов.

> *procrf.ru: Прокуратура города Миасса Челябинской области провела проверку по обращению о незаконном распространении управляющей организацией персональных данных жильцов. В ходе проверки установлено, что ТСЖ «Привокзальный» разместило на информационных досках в подъездах многоквартирного дома копии судебного решения о взыскании с должников оплаты коммунальных услуг, в которых содержались персональные данные граждан (фамилия, имя, отчество, адрес проживания), не получив согласие на их распространение.*

На диаграммах (см. Рисунок 4) видна высокая доля утечек через бумажную документацию – чуть менее 42%.

> *km.ru: Конфиденциальные документы с личными данными клиентов зеленоградского «Сбербанка» оказались разбросаны возле здания кредитной организации в третьем микрорайоне города Зеленограда. Часть документов находилась возле мусорного контейнера, а часть — на газоне. Среди листов корреспондент портала обнаружил заявления на получение карт и банковское обслуживание, договоры на открытие счетов с именами клиентов, их адресами, телефонами, паспортными данными и суммами вкладов.*

На втором месте по «популярности» утечки через сеть (24% – интернет или локальная сеть[22]).

Во-вторых, не отличаются разнообразием и сценарии утечки. По «сетевому» каналу чаще всего осуществляется доступ к базе данных и последующее нелегитимное использование/копирование персональных данных клиентов, сотрудников – пример умышленной утечки. Типичная случайная утечка через этот канал – публикация в веб данных ограниченного доступа: списки учеников школ, граждан, записавшихся на прием в муниципальные органы и пр. [23]

[22] см. Глоссарий

[23] Напомним, что случайной утечкой мы считаем такое действие или бездействие, когда лицо, скомпрометировавшее информацию, не преследовало собственной выгоды.

Как экзотику, можно рассматривать зафиксированную утечку через голосовой канал – неправомерное раскрытие работником колл-центра сведений об абоненте другому абоненту.

Рисунок 4. Распределение утечек по каналам

Большинство исследованных сценариев утечек легко сводятся к трем-четырем типам, когда точно известно наличие умысла и канал. Поэтому **низкую долю утечек неопределенного типа** в распределении по умыслу правильнее объяснить не высоким уровнем проникновения технических средств защиты от утечек в нашей стране, а **сравнительно небольшим разнообразием самих утечек.**

В доказательство этой гипотезы приведем еще одно рассуждение – посмотрите на распределение каналов утечки персональных данных (все три диаграммы, см. Рисунок 4). Наиболее популярные каналы для общей картины и для случайных утечек давно и успешно контролируются техническими средствами защиты. Иначе говоря, если бы средства защиты от утечек были в достаточной мере популярны в России, утечек ПДн подобных тем, что мы фиксируем сейчас, просто не было бы.

Число утечек, где невозможно определить виновного, также невелико (~15% – см. Рисунок 5). Ответственность за утечки в основном лежит на конкретном сотруднике компании-жертвы.

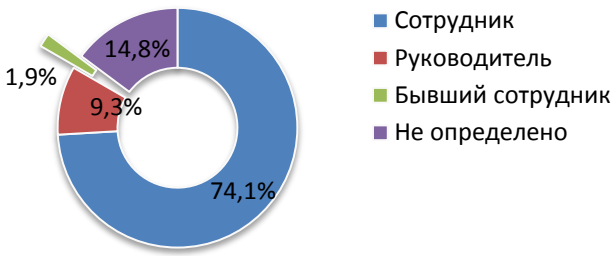


Рисунок 5. Распределение утечек по источнику (виновнику)

74% случаев утечек персональных данных связаны с намеренными или неосторожными действиями рядовых сотрудников. В 9% вина за утечку лежит на руководителях (средний и высший уровень)[24].

Отсюда вывод: низкий процент «неопределенных» по умыслу российских утечек ПДн не связан с распространенностью средств защиты (в том числе класса DLP). Скорее, причина в типичности самих утечек (сценарии, каналы).

Более того, **огромное количество случайных утечек по каналам, которые легко контролируются техническими решениями для защиты от утечек, говорит как раз о критически низком уровне проникновения технических средств защиты в российских компаниях. Иначе говоря, для защиты персональных данных технологии DLP в большинстве случаев просто не используются.**

Вывод:

Результаты исследования говорят о критически низком уровне использования средств защиты от утечек для обеспечения безопасности персональных данных в нашей стране. Это подтверждает существующее мнение, что большинство компаний занимаются «бумажной» безопасностью ПДн, выполняя требования регуляторов лишь формально. Реальной работы по повышению уровня безопасности персданных не ведется. Судя по характеру утечек – выброшенные документы, публикации баз данных в веб – можно говорить также о невысокой компетенции сотрудников, отвечающих за безопасность ПДн в России.

Ключевой факт: на долю государственных органов и организаций, занятых в сфере ЖКХ, приходится самый большой процент утечек персональных данных

В 2013 году 19% утечек персональных данных пришлись на государственные органы и силовые структуры, коммерческие и некоммерческие компании в сфере жилищно-коммунального хозяйства «отличились» почти в 18% случаев. Замкнули тройку «лидеров» финансово-кредитные организации с показателем 16% (см. Рисунок 6).

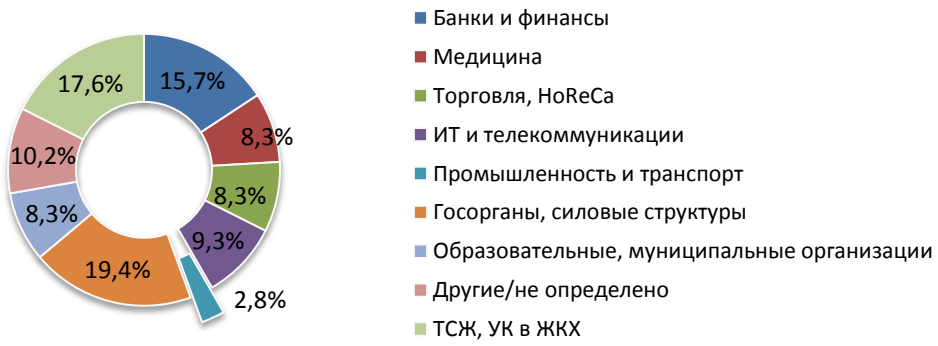


Рисунок 6. Утечки персональных данных из российских компаний

[24] Для большинства российских утечек ПДн легко определить виновного, наличие в его действиях злого умысла, понять, по какому каналу ушла информация. Виной тому – простота российских утечек, однообразность сценариев.

Каждая пятая утечка ПДн происходит из государственных органов. Наиболее типичным является ненамеренное раскрытие персональных данных граждан неопределенному кругу лиц. Как правило, госслужащие, нарушая требования законодательства о защите персональных данных, исходят из благих побуждений – например, удобство граждан. Однако в итоге стремление к удобству оборачивается несоблюдением законодательства:

> *kubantv.ru: В администрации Центрального района Новороссийска формировались списки граждан, записавшихся на личный приём к главе администрации, с отражением в них личных сведений. Каждую неделю эти списки размещались в приемной главы, куда имеется доступ для неопределенного круга лиц. За указанные нарушения глава администрации Центрального района оштрафован.*

Основным «поставщиком» утечек в категории «организации в сфере ЖКХ» выступают товарищества собственников жилья (ТСЖ), а также управляющие компании, эксплуатирующие и обслуживающие многоквартирные дома. Виной тому устоявшаяся практика публикации на подъездах домов информации о должниках (иногда включая точный адрес, телефон и паспортные данные) с целью воздействовать на граждан и добиться погашения долга. Число утечек персональных данных, произошедших по такому сценарию, измеряется десятками.

> *kp.ru: Жители Юго-Западного района г. Владимира в декабре получили квитки, оформленные в лучших советских традициях. В квитанции были указаны номера квартир должников. «Мы никак не нарушили закон. А прислать такие квитанции нас попросил советы многоквартирных домов, которые теперь есть в каждой многоэтажке», – объясняет Марина Трутнева, начальник юридического отдела ЖЭУ №4.*

Практически все утечки персональных данных из кредитных организаций и страховых компаний отягощены последующим неправомерным использованием этих сведений. Получив доступ к персональным данным, мошенники оформляют кредиты, изготавливают поддельные паспорта для того, чтобы вывести деньги со счетов клиентов:

> *ibryansk.ru: Сотрудница кредитно-кассового офиса «ОТП Банка» в Брянске незаконно оформила кредитные договоры, воспользовавшись доступом к персональным данным клиентов. От действий мошенницы пострадали 14 физических лиц, банк зафиксировал материальный ущерб на общую сумму 845 тысяч 579 рублей.*
>
> С учетом выручки банка за 2013 год[25], аналитики InfoWatch оценили ущерб банка (включая репутационные потери) в 104,7 тыс. руб.[26]

[25] Отчетность по РСБУ за 9 месяцев 2013 года. http://www.otpbank.ru/f/about/akcyy/ras_reporting/fin_report_2013_q3.pdf

[26] Методика расчета ущерба описана в Методологии.

Для полноты картины сравним случаи утечек персональных данных по признаку умысла из финансового сектора, государственных органов и организаций в сфере ЖКХ (см. Рисунок 7).

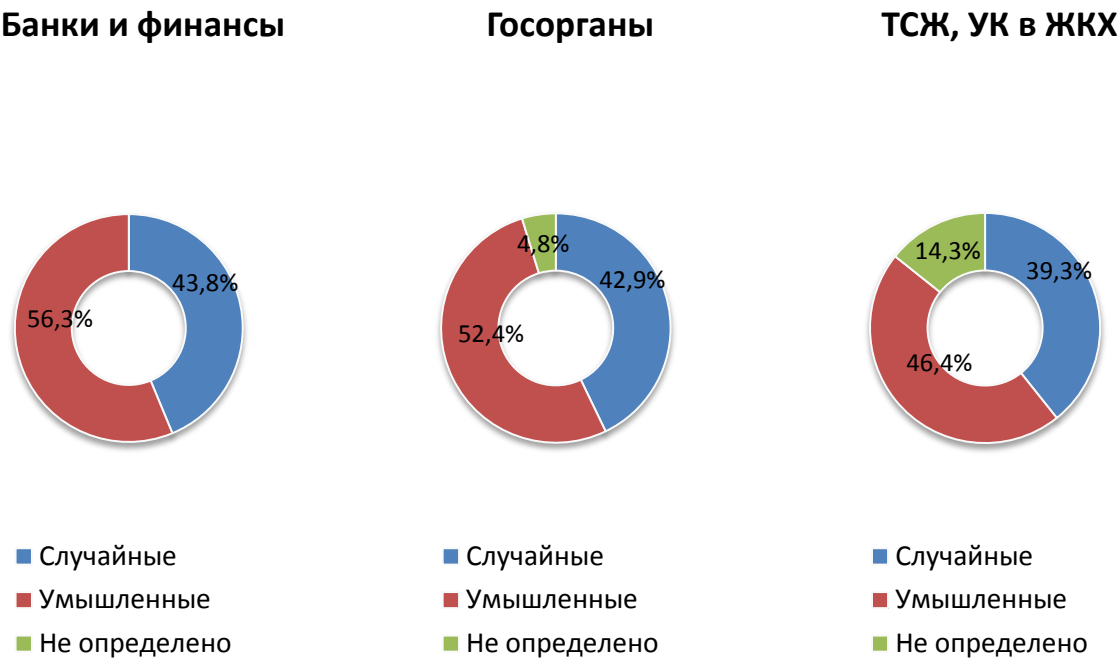


Рисунок 7. Распределение утечек по умыслу. Отраслевые особенности

Из практики исследований нам известны некоторые закономерности, связанные с распределением по этому признаку. Так высокий процент утечек «неопределенного» типа говорит о недостаточном использовании технических средств защиты (или их отсутствии – даже если факт утечки налицо, невозможно определить, умышленно или случайно «ушла» информация). Большая доля умышленных утечек говорит, скорее, о достаточном оснащении компаний отрасли техническими средствами защиты – информация утекает не случайно, но вследствие злонамеренных действий сотрудников или иных легитимных пользователей. Защититься от этого сценария в разы сложнее, чем от случайных утечек. Технических средств недостаточно – необходима тщательная проработка организационных мер внутри компании.

Как видим, наиболее слабо в техническом отношении выглядят компании в сфере ЖКХ (ТСЖ, управляющие компании). Чуть лучше обстоят дела в государственных организациях – здесь не так высок процент утечек «неопределенной» природы. Следовательно, средства защиты от утечек в госорганах пусть и ограниченно, но применяются. Распределение по умыслу в финансовом сегменте говорит о довольно высоком уровне оснащенности средствами защиты от утечек информации – более 50% приходится на «злоумышленные» утечки. При этом утечки «неопределенного» типа отсутствуют.

Вывод:

Персональные данные в банках и финансовых организациях обладают самой высокой (по сравнению с другими отраслями) «ликвидностью». Поэтому,

несмотря на высокий уровень информационной безопасности, утечки ПДн из финансового сектора останутся во главе списков самых крупных и «громких». Персданные в финорганизациях, очевидно, будут и дальше привлекать злоумышленников. В случае с муниципальными органами и некоммерческими организациями (ТСЖ, УК в ЖКХ), в отличие от финансового сектора, уместно, к сожалению, говорить о недостаточной защищенности персональных данных как основной причине утечек. В этих организациях отсутствуют не только технические средства защиты, но и понимание сути проблемы – зачем и что требуется защищать.

Ключевой факт: две трети утечек персональных данных происходит из малых и средних компаний

На долю небольших операторов ПДн (до 500 ПК) приходится 66% всех утечек.

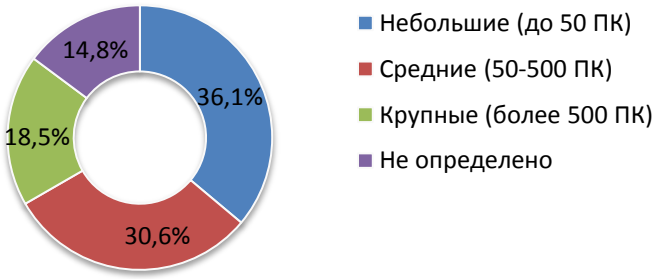


Рисунок 8. Распределение утечек по размеру операторов ПДн

Причем совсем не обязательно, что число записей или прямой ущерб от утечек в небольших организациях будет также небольшим. В ряде случаев, когда утекали базы данных с числом записей 5 тыс. и выше, а ущерб составлял более 10 тыс. руб., речь шла именно о малых и средних организациях. Отметим, что для среднего бизнеса последствия от утечек крупных массивов ПДн весьма критичны – это серьезный репутационный и финансовый ущерб, который в ряде случаев более ощутим, чем в компаниях крупных.

bk55.ru: Мэрия Омска и УФНС России по Омской области подвели промежуточные итоги так называемого «проекта по информированию граждан о задолженности по имущественным налогам физических лиц». В органы местного самоуправления были переданы сведения о задолженности по имущественным налогам на 120 тысяч жителей всех округов Омска.

Интересно, что доля утечек с ущербом, свыше 10 тыс. руб., (на диаграмме крупный ущерб – см. Рисунок 9) в среднем бизнесе даже выше, чем в больших корпорациях. В ряде отраслей (торговля, туризм), где и представлены в основном небольшие организации, утечка базы данных клиента, например, может привести к убыткам, сопоставимым с оборотом компании за несколько месяцев.

Впрочем, невысокую долю утечек из крупных компаний (свыше 500 ПК), отягощенную крупным ущербом (таких утечек чуть менее 17% см. Рисунок 9), можно объяснить и

тем, что крупные компании лучше скрывают факты «больших» утечек данных, а в средних утечки более «заметны».

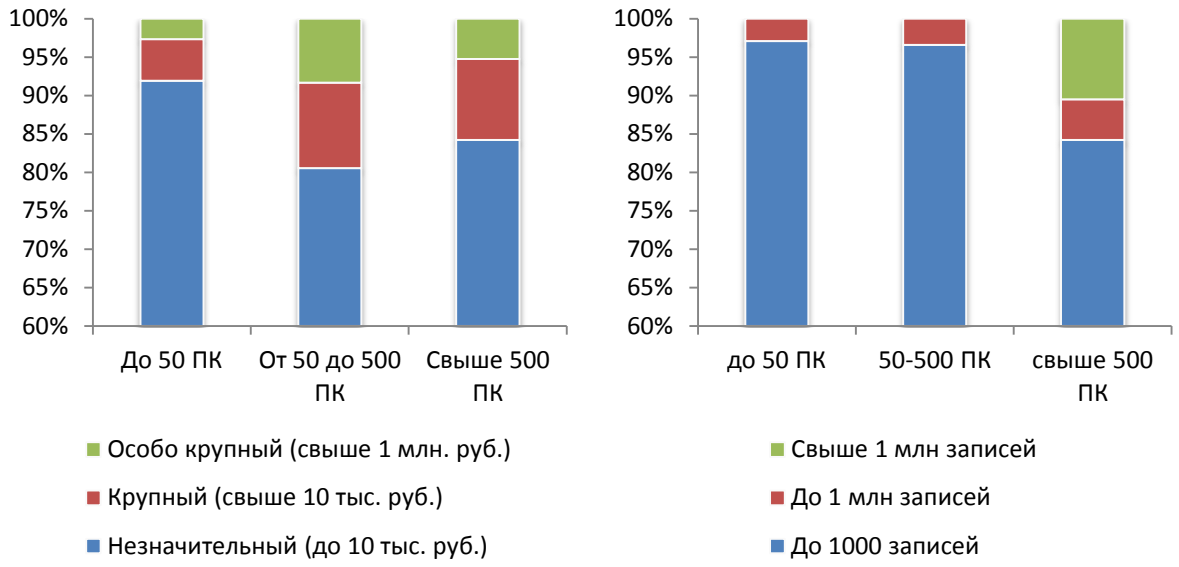


Рисунок 9. Картина утечек. Распределение по размеру компаний

В завершении темы ущерба отметим, что число скомпрометированных записей указано только в 23% исследованных сообщений, прямой ущерб зафиксирован в 13% случаев. Это говорит, во-первых, о нежелании организаций, допустивших утечку, делиться даже примерной информацией об ущербе. Во-вторых, в большинстве случаев персональные данные сотрудников, клиентов, контрагентов просто не рассматриваются службой информационной безопасности (и бизнес-подразделениями) как ценный актив, то есть не имеют ценности для самой компании.

Вывод:

Небольшие компании остаются «слабым звеном» в плане защиты персональных данных. Между тем в среднем бизнесе утечка ПДн приводит к более критичным последствиям – доля крупных материальных потерь вследствие утечки в небольших компаниях даже выше, чем в сегменте крупных организаций. Следует констатировать серьезные недостатки систем защиты персональных данных в небольших организациях, а часто полное отсутствие каких-либо усилий в деле обеспечения безопасности ПДн.

Ключевой факт: количество утечек ПДн коррелирует с количеством новостных сообщений в СМИ по теме защиты персональных данных

Поскольку исследование Аналитического Центра InfoWatch основывается на информации из открытых источников, вряд ли следует удивляться выявленной

взаимосвязи количества новостных публикаций по теме защиты персональных данных и числа известных утечек персональных данных (см. Рисунок 10) [27].

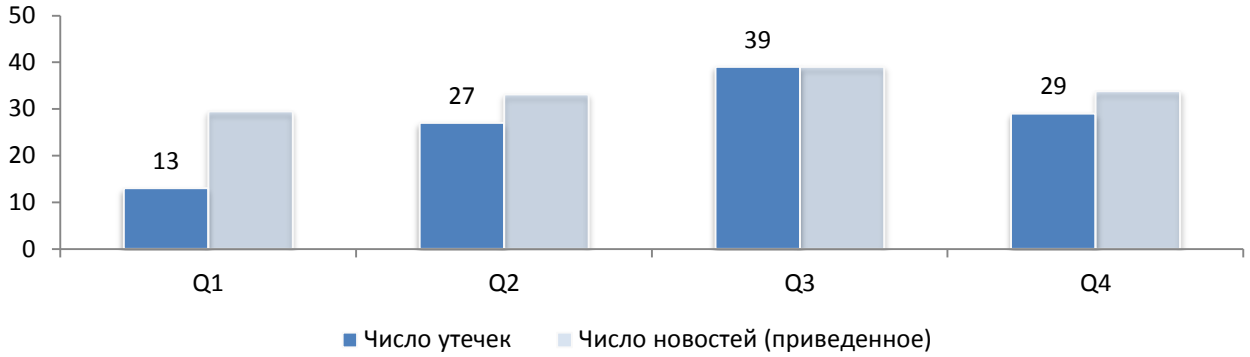


Рисунок 10. Утечки информации по кварталам

Авторы исследования отмечали выше, что любое информационное сообщение законодателей и регуляторов на тему защиты ПДн порождает волну публикаций в СМИ – тема более чем популярна. Информационный фон в СМИ, в свою очередь, подталкивает к действиям законодателей и регуляторов (создание новых нормативно-правовых актов, предложение поправок в действующие законы).

Но, если проанализировать сообщения об утечках ПДн (то, что является предметом данного исследования), мы обнаружим довольно поверхностную подачу материала (в отличие от новостных сообщений об утечках ПДн в США, например). Новости о российских утечках не содержат конкретики. Не уточняется, сколько записей скомпрометировано, какой ущерб субъектам и оператору персональных данных нанесен.

Для всех заинтересованных сторон (регуляторы, операторы, субъекты) важнее сам факт утечки, чем реальный ущерб. В СМИ сплошь и рядом говорится о том, что утечка ПДн – это плохо, и совершенно не говорится, почему, каковы последствия этой утечки для оператора ПДн. В итоге операторы рассматривают лишь один вариант негативного развития событий – штраф за несоблюдение требований законодательства.

Субъекты (то есть граждане) также не осведомлены о возможных последствиях и не стремятся защищать свои интересы.

Регуляторы же, судя по всему, текущим состоянием дел вполне довольны. Так, судя по сообщениям СМИ, за два месяца сотрудники «Роскомнадзора» выявили лишь **один** факт незаконной продажи электронной базы данных граждан. Правда, общее число скомпрометированных записей только по данному факту утечки **составляет 2 млн**:

[27] Информация о количестве информационных сообщений за квартал по теме персональных данных получена путем подсчета среднего числа новостей в поисковых сервисах Яндекс и Google. Для наглядности количество информационных сообщений приведено к максимальному количеству утечек (на диаграмме представлены абсолютные цифры утечек и относительные данные по новостным публикациям).

> *Открытые системы: В сентябре-октябре 2013 года территориальными органами Роскомнадзора было проверено более 200 мест розничных продаж в 75 субъектах России с целью выявления фактов незаконной продажи электронных баз персональных данных граждан. Был зафиксирован только один такой случай. Анализ показал, что диск с базой данных содержит телефонные справочники с фамилиями, инициалами, номерами телефонов и адресами, базы абонентов крупнейших операторов связи, базы со сведениями об административных правонарушениях, уголовных преступлениях и судимостях (**общее число записей около 2 млн**), базу владельцев автотранспортных средств.*

Между тем, помимо штрафа за нарушение требований законодательства о защите ПДн, операторы несут в ряде случаев вполне ощутимые материальные потери. Недополученная прибыль вследствие ухода клиентов к конкурентам, похитившим базу данных – показательный, но далеко не единственный сценарий. Приведем пример, где экспертами InfoWatch дана оценка материального ущерба вследствие утечки ПДн:

> *Известия: В июле 2013 года произошла утечка базы данных клиентов международной страховой компании «Цюрих». Злоумышленники похитили полные данные более чем на 1 млн клиентов, заключивших за последние 1,5 года договоры страхования. В СК «Цюрих» размер возможного ущерба не комментируют.*
>
> Учитывая рост бизнеса компании[28] и выручку российского подразделения за 2012 год[29], эксперты InfoWatch оценивают ущерб от данного инцидента (включая репутационные потери и недополученную прибыль) в **2-2,5 млрд. руб.**, в том числе **4,4 млн руб.** - затраты на расследование и ликвидацию последствий инцидента.[30]

Субъекты ПДн – т.е. граждане – страдают еще больше. Не проходит недели, чтобы в СМИ не появилось сообщение об очередном оформлении кредитов на украденные паспортные данные, раскрытии сведений о судимостях, болезнях, финансовом положении, небрежном хранение медицинских данных детей.

> ***Вывод:***
>
> *«Популярность» в СМИ темы утечек ПДн совершенно не сказывается на повышении степени защищенности ПДн в России. Операторы не видят угрозы в возможных штрафах со стороны регуляторов, не осознают, что утечка ПДн – это ощутимый материальный ущерб в виде упущенной выгоды и репутационных потерь.*

[28] http://www.zurich.com/internet/main/SiteCollectionDocuments/financial-reports/half-year-report-2013-en.pdf

[29] ООО СК «Цюрих» Форма №2-страховщик по ОКУД http://zurich.ru/upload/accounting/form2ooo.pdf
ЗАО «Цюрих надежное страхование» Форма №2-страховщик по ОКУД http://zurich.ru/upload/accounting/zao-form2.pdf

[30] Методика расчета ущерба описана в Методологии.

Изменить ситуацию к лучшему можно лишь в том случае, если операторы начнут отвечать за утечки персональных данных рублем и репутацией. Только тогда у российских коммерческих компаний и государственных (муниципальных) органов появляется мотивация обеспечить безопасность ПДн на должном уровне. Для первых стимулом будут возможные финансовые потери, для вторых – публичные претензии общественности на фоне фактического неисполнения государством своих обязанностей по защите персональных данных граждан.

Заключение и выводы

Авторы исследования с сожалением вынуждены констатировать критически низкую степень защищенности персональных данных в России. Связано это с комплексом взаимовлияющих факторов, в том числе:

- ✓ Позиция законодателей и регуляторов, требующих от операторов персональных данных соблюдения требований по защите ПДн лишь «на бумаге». Операторы выполняют предписания закона и регуляторов, зачастую, формально, а факты утечек персональных данных просто замалчивают.
- ✓ Мизерные суммы штрафов за нарушение требований по защите ПДн никак не мотивируют операторов повышать защищенность персональных данных. Низкая активность регуляторов в плане проведения плановых и внеплановых проверок исправлению ситуации не способствует.
- ✓ Субъекты персональных данных, в интересах которых, по идее, принимался закон о защите ПДн, остались за скобками применения 152-ФЗ. Даже в перспективе инициатив законодателей речь не идет о том, чтобы обязать операторов персональных данных публиковать факты утечки ПДн и информировать об этом пострадавших граждан.

В распределении по источнику утечки (отраслевой принадлежности операторов персональных данных) большинство утечек пришлось на организации, находящиеся на разных полюсах с позиции зрелости ИБ: банки (и страховые компании, которые мы относим к данному сегменту) - наиболее «продвинутая» отрасль, и государственные органы, где с информационной безопасностью традиционно не все благополучно. Огромное количество утечек персданных в компаниях сферы ЖКХ вынудило авторов исследования выделить эти организации в отдельную категорию.

При этом с банками ситуация более-менее ясна – причина большого количества утечек кроется в ликвидности данных. Конкурент, «уведя» базу данных банка или страховой компании, легко конвертирует ее в дополнительную прибыль, переманив клиентов лучшим предложением.

С госорганами и компаниями из сферы ЖКХ все сложнее. С вероятностью, можно говорить об отсутствии технических мер защиты персональных данных. С еще большей вероятностью – об отсутствии понимания сути проблемы – что и зачем нужно защищать – у сотрудников и руководства компаний.

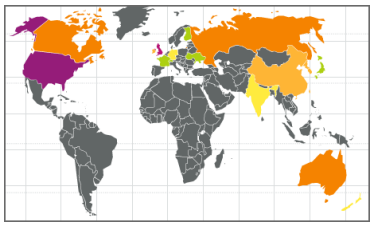
Отметим, что более двух третей утечек ПДн приходится на небольшие организации. Причем доля утечек с ущербом более 10 тыс. руб. в среднем бизнесе (компании от 50 до 500 ПК) даже выше, чем в крупном.

Изменить ситуацию к лучшему можно лишь в том случае, если операторы начнут отвечать за утечки персональных данных рублем и репутацией. Только тогда у российских коммерческих компаний и государственных (муниципальных) органов появляется реальный стимул обеспечивать безопасность ПДн на должном уровне.

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.*

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».*