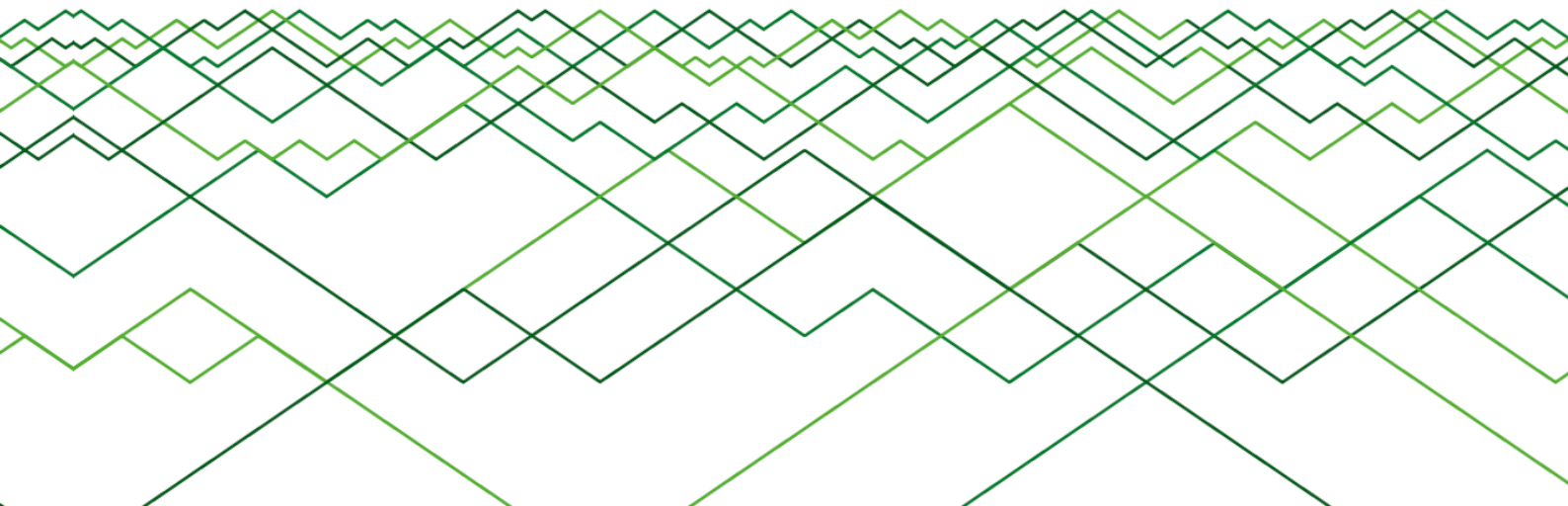
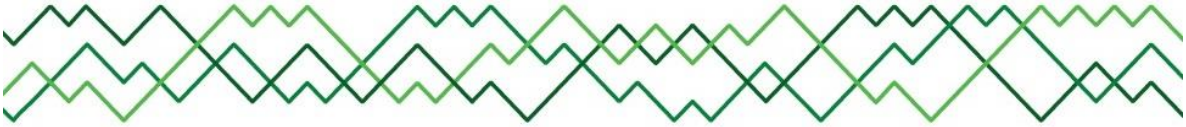
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Аналитический центр InfoWatch
www.infowatch.ru/analytics

Утечки данных. Россия. 2016 год

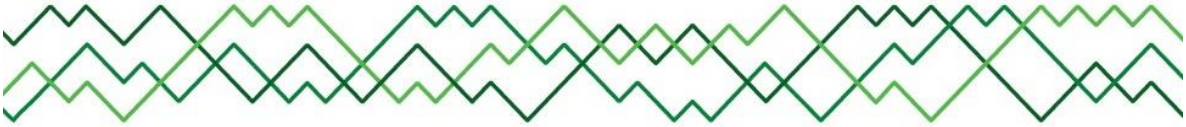




INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Оглавление

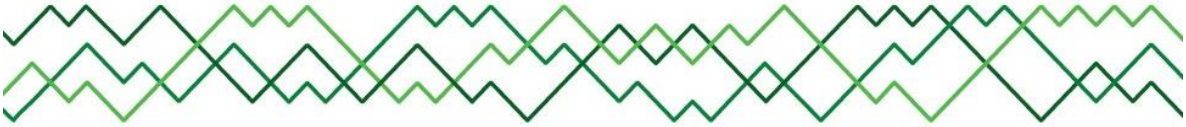
Оглавление 2
Только цифры 3
Аннотация 4
Методология 5
Результаты исследования 7
Коммерческая тайна утекает чаще, платежные данные реже, чем в мире 8
«Квалифицированные» утечки — признак низкого уровня культуры информационной безопасности в стране 9
Почти 2/3 утечек связаны с ошибками или злонамеренными действиями сотрудников 11
Внутренний злоумышленник со временем становится опаснее 13
По числу утечек в Росси лидируют госорганы, высокотехнологичные компании, образовательные учреждения и банки 15
Заключение и выводы 19
Мониторинг утечек на сайте InfoWatch 22
Глоссарий 23



INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Только цифры

- ✓ В 2016 году в СМИ обнародовано **213** случая утечки информации из российских компаний и государственных органов, что составляет 14% от числа утечек данных по всему миру.
- ✓ Чаще всего в России утекают персональные данные и платежная информация. На эти типы данных приходится **80%** утечек, случившихся в 2016 году.
- ✓ В **68%** случаев виновными в утечке информации оказались сотрудники компаний. В **8%** случаев — руководство организаций.
- ✓ В 2016 году в России наибольшие доли утечек пришлись на сетевой канал и бумажную документацию — **64%** и **26%** соответственно.



Аннотация

Аналитический центр компании InfoWatch представляет отчет об исследовании инцидентов[1], связанных с компрометацией информации ограниченного доступа, зафиксированных в российских коммерческих и некоммерческих компаниях, государственных органах и организациях в 2016 году и обнародованных в СМИ, блогах, социальных сетях.

Мы неоднократно подчеркивали, что картина утечек данных из российских организаций стремительно приближается к общемировой. Это связано со схожестью объектов защиты (типов используемых данных), ростом ценности информации и увеличением числа каналов передачи данных.

Случаи мошенничества с чужими персональными данными по вине сотрудников банков, страховых компаний, салонов сотовой связи, даже госслужащих происходят чуть ли не ежедневно. Такие правонарушения уже стали нормой для «продвинутых» в плане информационной безопасности стран (например, США, Великобритания). Теперь «кража личности» — обыденное преступление и для России.

> *irksib.ru: В течение двух лет шестеро подозреваемых похищали с банковских счетов инвалидов Тулюшкинского психоневрологического интерната их пенсии. Двое жителей села Тулюшка Куйтунского района Иркутской области с участием трех бывших и одного действующего сотрудника банка оформили на инвалидов банковские карты, которые прикрепили к социальным счетам пострадавших. Поступившие пенсии подозреваемые снимали с карт в иркутских банкоматах. Персональные данные инвалидов для оформления банковских карт организаторам группы передали сотрудники психоневрологического интерната. В общей сложности им удалось похитить около 6 млн рублей.*

С другой стороны, сообщения об утечках данных в нашей стране не сопровождаются таким же широким общественным резонансом, как, например, в США, где скандалы, связанные с утечками, стали непременным атрибутом политической жизни. Эта особенность обусловливает специфическую подачу сообщений об утечках в российских СМИ, когда акцент смещается в сторону привлекательных для читателя, но второстепенных деталей (сведения о владельце пострадавшей компании, истории клиентов, потерявших данные). Более важная информация (механизм утечки, оценки реального ущерба, вопросы компенсации) практически не раскрывается.

Невысокий интерес к утечкам данных в России связан с особенностями менталитета, нейтральным отношением общества к темам защиты тайны частной жизни и безопасности интеллектуальной собственности. Впрочем, особенно крупные или социально значимые утечки все же получаются достаточно «громкими» и в России.

В 2016 году СМИ писали об утечке полного сезона сериала Первого канала, о персональных данных дошкольников и школьников, обнаруженных в открытом доступе на сайтах образовательных учреждений, о «ритуальном бизнесе»

[1] Определения понятий, использованных в данном отчете об исследовании, приведены в разделе «Методология» и в Глоссарии. Значение общепринятых понятий, употребляемых в узком смысле, оговаривается особо.

сотрудников полиции и медучреждений, которые работали информаторами похоронных контор. В центре масштабных скандалов периодически оказывались политические партии, органы судебной власти, силовые структуры.

Отсутствие принципиальных отличий между российской и мировой картинами утечек, сходство факторов, формирующих эти картины, оставляет открытым вопрос о наличии и значении национальной специфики. Региональная специфика (если она есть) заключается в небольшом отставании России в плане утилитарного использования данных в цифровом виде и в вопросе защиты этих данных. Поэтому рискнем предположить, что в создавшихся условиях необходимо отказаться от слепого копирования опыта зарубежных стран, так называемой «догоняющей модели». Зарубежный опыт следует всесторонне изучить, но выработать свой путь, сфокусироваться на поиске и популяризации наиболее эффективных подходов к обеспечению корпоративной информационной безопасности.

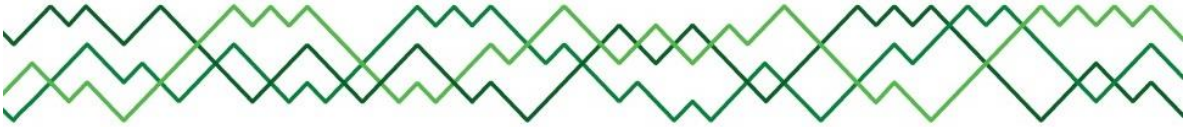
В этом смысле настоящее исследование представляет собой ценный источник первичной информации для представителей государственных структур, владельцев компаний, руководителей и сотрудников служб ИБ, которые пытаются найти оптимальный способ построения систем защиты информации, используя необходимый минимум финансовых вложений.

Методология

Исследование проводится на основе собственной базы данных, пополняемой специалистами Аналитического центра InfoWatch с 2004 года. В базу попадают публичные сообщения[2] о случаях утечки[3] информации из коммерческих, некоммерческих (государственных, муниципальных) организаций, госорганов, которые произошли вследствие умышленных или неосторожных действий[4] сотрудников и иных лиц[5]. База утечек InfoWatch насчитывает несколько тысяч зарегистрированных инцидентов.

В ходе наполнения базы каждая утечка классифицируется по ряду критериев, таких как размер организации[6], сфера деятельности (отрасль), размер причинённого

[2] Сообщения об утечках данных, опубликованные официальными ведомствами, СМИ, авторами записей в блогах, интернет-форумах, иных открытых источниках.
[3] Утечка информации (данных) – утрата контроля над информацией (данными) в результате внешнего воздействия (атаки) а также действий лица, имеющего легитимный доступ к информации или действий лица, получившего неправомерный доступ к такой информации.
[4] Утечки данных разделяются на умышленные (злонамеренные) и неумышленные (случайные) в зависимости от наличия вины в действиях лица, которые привели к утечке данных. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы.
[5] Авторы классифицируют утечки по виновнику (источнику) инцидента. Наряду с внутренними нарушителями, в данную классификацию попадает внешний нарушитель.
[6] 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.



ущерба[7], тип утечки (по умыслу), канал утечки[8], типы утекших данных, вектор воздействия[9].

Инциденты также классифицируются по характеру действий нарушителя. Наряду с «простыми» утечками авторы исследования выделяют «квалифицированные» — случаи, когда деструктивное поведение сотрудников выражается в использовании легитимного доступа к данным в мошеннических целях (манипуляции с платежными данными, инсайдерской информацией); случаи превышения прав доступа, когда сотрудник знакомится, копирует, передает данные, к которым не должен иметь доступа по роду службы или работы.

По оценке авторов, исследование охватывает не более 1% случаев предполагаемого совокупного количества утечек из-за высокого уровня латентности инцидентов, связанных с компрометацией информации. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества (совокупности категорий) содержали достаточное или избыточное количество элементов — фактических случаев утечки. Такой подход к формированию поля исследования позволяет считать полученную выборку теоретической, а выводы исследования и выявленные с учетом данной выборки закономерности — репрезентативными для генеральной совокупности.

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

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

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

---

[7] Данные об ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций в СМИ.

[8] Под каналом утечки мы понимаем такой сценарий (совокупность действий пользователя корпоративной информационной системы, направленных на оборудование или программные сервисы), в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. Каналы утечек определяются только для таких утечек, которые спровоцированы действиями внутреннего нарушителя.

[9] Вектор воздействия – признак действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников, направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации информации, и действия внутренних злоумышленников, атакующих системы защиты изнутри (нелегитимный доступ к ресурсам, неправомерные действия с инсайдерской информацией и проч.).

Результаты исследования

В 2016 году Аналитический центр InfoWatch зарегистрировал 213 случая утечки информации ограниченного доступа из коммерческих и некоммерческих компаний, государственных органов и организаций, работающих в России (Рисунок 1). В результате этих утечек было скомпрометировано 128 млн записей о персональных данных (в том числе финансовые данные — реквизиты пластиковых карт, данные банковских счетов), иная критически важная информация.

Рисунок 1. Число зафиксированных утечек, Россия – мир, 2006-2016 гг.

По сравнению с данными 2015 года, число утечек увеличилось на 89%, объем скомпрометированных данных вырос более чем в 100 раз[10].

Как и в прошлом году, в мировом «рейтинге» стран, пострадавших от утечек, Россия заняла второе место — сразу вслед за США (Рисунок 2).

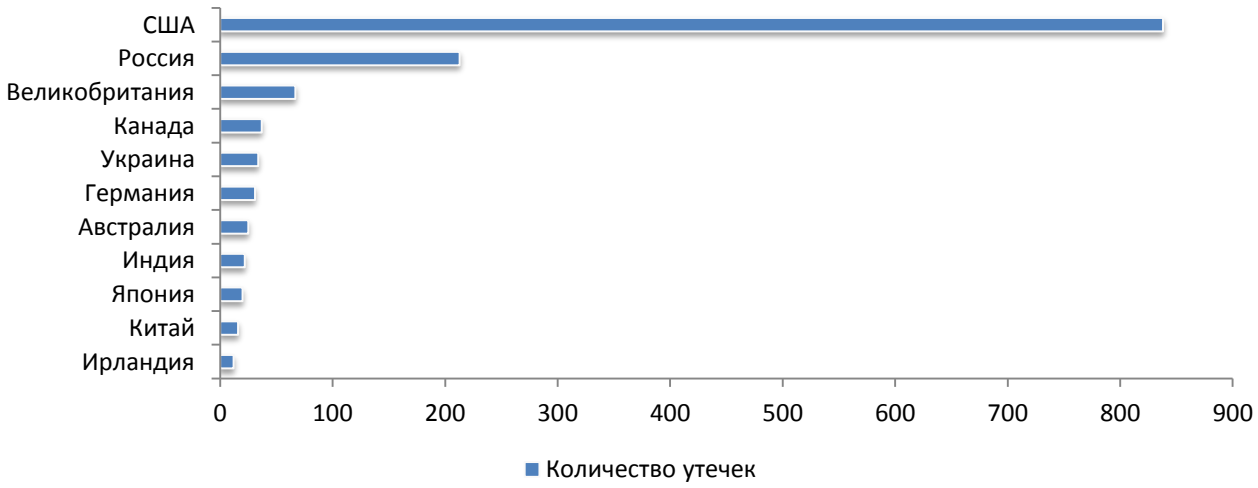


Рисунок 2. Распределение утечек по странам, 2016 г.

[10] Основной вклад в увеличение объема скомпрометированных данных пришелся на связанные между собой утечки информации из компаний Mail.Ru Group. В 2016 году зафиксировано 4 случая общим объемом 127,8 млн записей о персональных данных. Представитель Mail.ru настаивал, что украденные данные не относятся к «живым» аккаунтам.

В общемировом распределении доля «российских» утечек от общего числа составила 14%. Объем скомпрометированных персональных данных, который пришелся на российские компании и государственные органы и организации, не превысил 4% от совокупного объема ПДн, скомпрометированных по всему миру.

Российская картина утечек, в целом, соответствует мировой. Все закономерности, выявленные на глобальной выборке в 2016 году, справедливы и для нашей страны. Это означает, что угрозы, с которыми сталкивается мировое сообщество уже сейчас, можно и нужно принимать в расчет при выработке национальных подходов к защите информации. Причем как в масштабах страны, так и применительно к обеспечению информационной безопасности в конкретной отрасли, организации.

Вместе с тем, сравнивая распределения утечек в мире и России по отдельным критериям, можно отметить ряд особенностей, которые характеризуют своеобразие российской картины утечек информации, отражают специфику отечественной цифровой реальности.

Коммерческая тайна утекает чаще, платежные данные реже, чем в мире

Распределение утечек по типам данных свидетельствует о значительно меньшем количестве случаев компрометации платежных данных в России по сравнению с мировой картиной. При этом доля утечек информации, составляющей коммерческую тайну, из российских организаций более чем вдвое выше аналогичного мирового показателя (Рисунок 3).

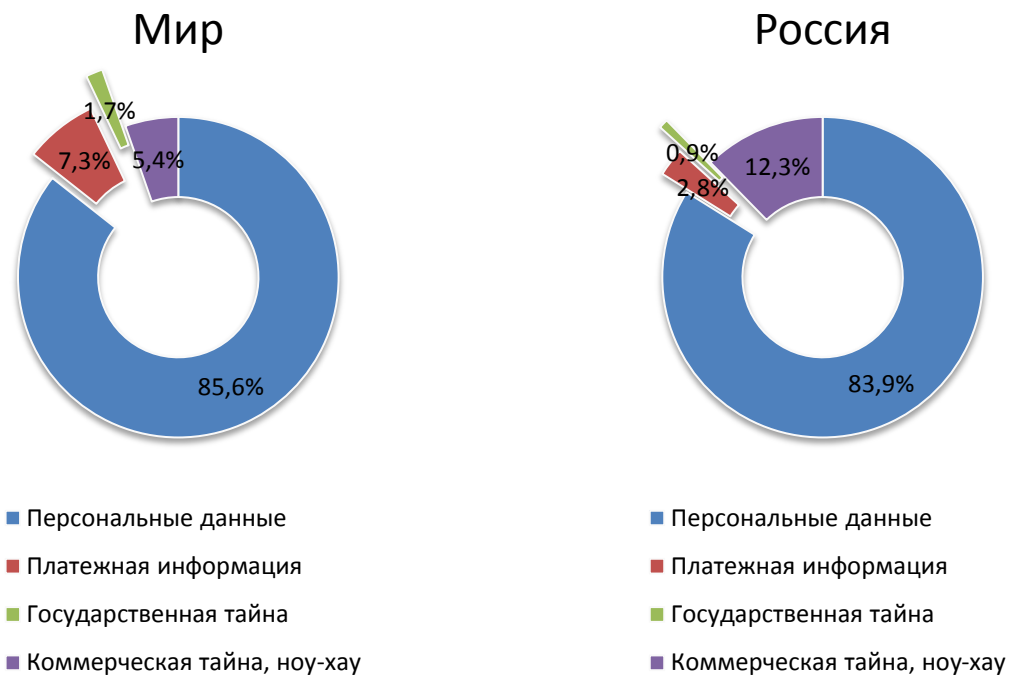


Рисунок 3. Распределение утечек по типам данных, Россия – мир, 2016 г.

Причины такого странового отклонения от глобальной картины кроются в свойственной российской сфере ИБ неоднородности проникновения систем защиты в

различные отрасли. Хозяйствующие субъекты, чья деятельность предполагает обработку платежной информации, традиционно считаются лидерами в плане использования решений для обеспечения информационной безопасности. Сказать то же самое о промышленных компаниях, где ценным активом является именно коммерческая тайна, пока не получается. Последние в итоге чаще страдают от утечек информации ограниченного доступа.

> interfax-russia.ru: *Двое жителей Ставрополя за деньги передали конкурентам сведения, составляющие коммерческую тайну компании. Преступников интересовали особенности производства искусственных сапфиров АО «Монокристалл». Предприятию был причинен ущерб на сумму не менее 14 млн рублей.*

Кроме того, обеспечить безопасность платежной (финансовой) информации несравнимо проще, чем сведений, составляющих коммерческую тайну. Во-первых, платежные данные легко поддаются формализации — 16 цифр номера кредитной карты, 20 цифр счета, шаблоны платежных поручений, установленная законом или практикой структура финансовых документов,— все это позволяет обеспечить безопасность финансовых данных, обрабатываемых организациями, с помощью автоматизированных систем сравнительно небольшими усилиями.

«Закрыть» проблему безопасности коммерческой тайны столь легко не получится — такие сведения, как правило, формализации не поддаются. В большинстве случаев компании просто не знают, какую ценность имеет та или иная информация, где именно она хранится, и потому ориентируются на примерный перечень объектов защиты. Лишь свершившийся факт утечки данных зачастую дает ответ на вопрос, сколько же на самом деле стоит тот или иной информационный актив и чем именно он ценен.

> samara.aif.ru: *В одной из гостиниц Самары сотрудники УФСБ задержали жителей Чапаевска, которые планировали продать конкурентам секреты ООО «Промперфоратор». Похищенные бывшей сотрудницей компании сведения, составляющие коммерческую тайну, были записаны на флэшку объемом 32 гигабайта. За нее «продавцы» просили два миллиона рублей.*

«Квалифицированные» утечки — признак низкого уровня культуры информационной безопасности в стране

Для России характерна более высокая по сравнению с остальным миром доля так называемых «квалифицированных» утечек данных. То есть таких случаев, когда злоумышленник осознанно использует украденную им информацию для достижения личной выгоды (мошенничество с данными, банковский фрод), или получает доступ к информации, заведомо не нужной ему для выполнения трудовой функции (превышение прав доступа).

> province.ru: *Сотрудница одного из банков Владимирской области, имея доступ к персональным данным вкладчиков, внутренней информации банка и электронной цифровой подписи, оформляла дебетовые карты и распоряжалась денежными средствами клиентов банка. По результатам проверки в отношении 27-летней сотрудницы возбуждено уголовное дело по*

подозрению в мошенничестве. По версии следствия, злоумышленнице удалось похитить 400 тыс. рублей.

Приведенный случай далеко не единичный. Так в феврале 2016 года СМИ сообщили об аналогичном мошенничестве — сумма ущерба составила более 1 млн рублей. В августе 2016 года была опубликована новость о поимке преступника, которому удалось мошенническим путем присвоить 1,6 млн рублей.

Большое число «квалифицированных» утечек в России можно объяснить сравнительно низким уровнем культуры информационной безопасности. Сотрудники организаций, ежедневно имеющие дело с чувствительной информацией, периодически «забывают», что результат их труда является служебным произведением и, по общему правилу, принадлежит работодателю. Отсюда многочисленные случаи продажи баз данных, содержащих сведения о клиентах и контрагентах организации-работодателя.

gazeta.ru: Управляющий директор группы активных продаж одного из столичных банков обвиняется в покушении на незаконное получение и разглашение сведений, составляющих банковскую тайну. По версии ГУ МВД, он перенес на электронный носитель базы данных банка, в которых содержалась информация о физических и юридических лицах для последующей продажи. В момент сделки злоумышленник был задержан.

Другой аспект этой проблемы проявляется в том, что рядовые сотрудники организаций, агрегирующих чувствительную информацию, зачастую без всяких сомнений используют свое служебное положение в личных целях. Так сотрудники операторов связи и сотовых ретейлеров часто злоупотребляют доступом к сведениям о соединениях абонентов, балансе лицевого счета. Мотивы могут быть разные — от досужего интереса до банальной корысти.

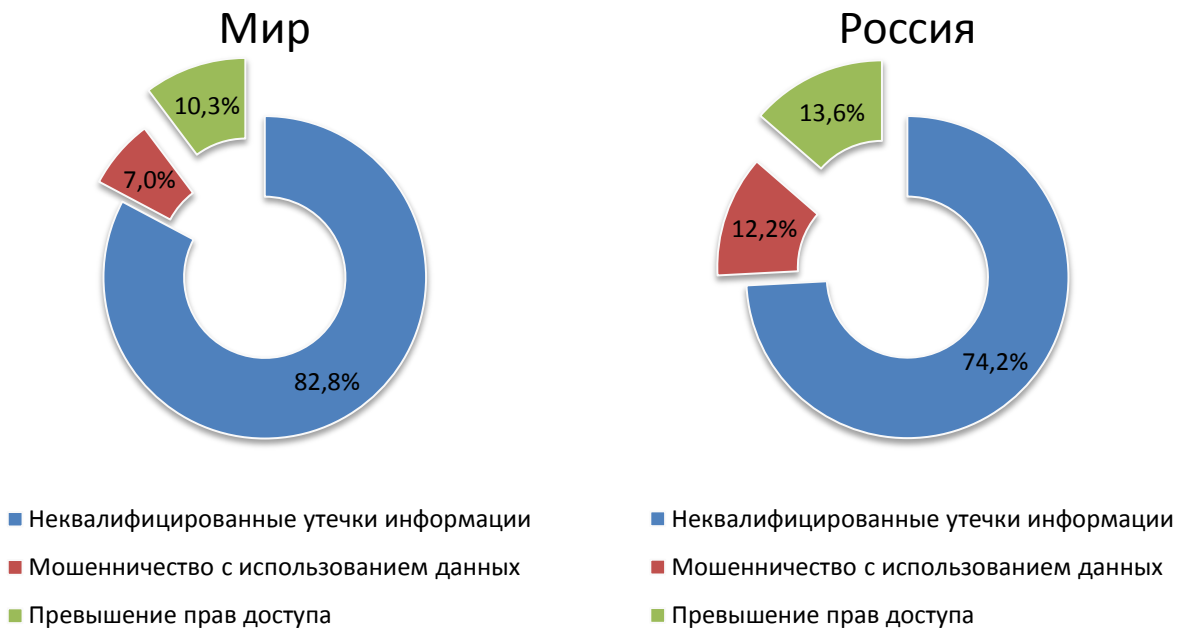


Рисунок 4. Распределение утечек по типу инцидентов, Россия – мир, 2016 г.

То же касается сотрудников аппарата органов публичной власти, работников налоговых инспекций, различных проверяющих организаций.

> *bryanskreview.ru: Сотрудница одной из сельских администраций Комаричского района оказалась на скамье подсудимых за разглашение информации о банковских счетах и недвижимости своей начальницы. Чиновница разместила на сайте администрации района данные о доходах своей начальницы и ее супруга, указав адреса принадлежащего им имущества, а также суммы денежных средств, хранящихся на счетах супружеской пары.*

Почти 2/3 утечек произошли по вине сотрудников

Доля утечек данных по вине сотрудников компаний год от года сокращается. Основным фактором в этом процессе выступает растущее число (и, соответственно, доля) утечек в результате внешнего воздействия — атак на инфраструктуру организаций, в результате которых происходит потеря контроля над информацией.

В 2015 году в России на долю непривилегированных пользователей — сотрудников организаций — пришлось 84% утечек, в 2016 году — уже 65%. По миру аналогичный показатель равен 52% и 34% соответственно.

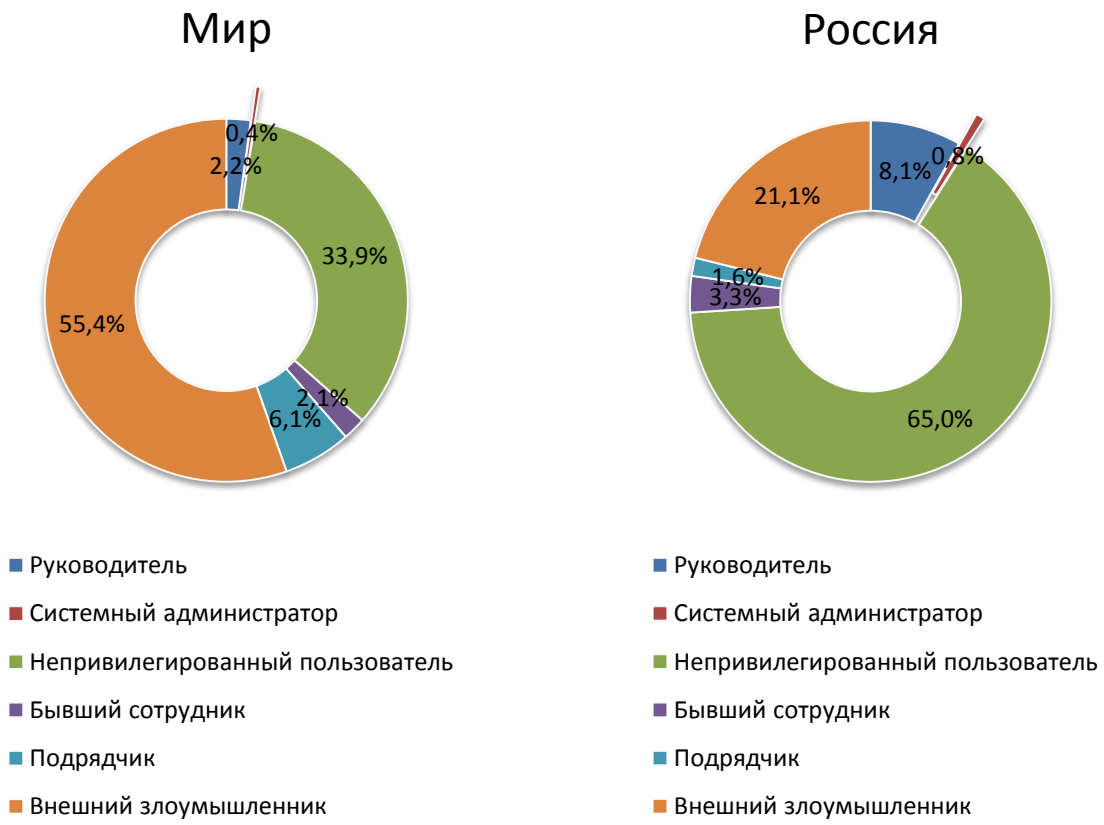


Рисунок 5. Распределение утечек по виновнику, Россия – мир, 2016 г.

Для России характерна более высокая доля утечек по вине руководства организаций — 8% по сравнению с 2% в мире. Утечек по вине подрядчиков и контрагентов в нашей стране происходило меньше, чем на глобальной выборке.

Сравнительно небольшая доля утечек по вине внешнего злоумышленника не должна вводить в заблуждение. Действительно, из данных статистики следует, что основной проблемой для российской информационной безопасности остается внутренний нарушитель. Однако увеличение объемов данных, обрабатываемых организациями, повышение стоимости этих данных с неизбежностью ведет к росту количества внешних атак на ИТ-инфраструктуру предприятий. Речь идет не только и не столько о «продвинутых» хакерах, работающих «по заказу», сколько о массовых взломах с целью получения доступа к информации организаций, представляющей ценность.

> vdvbezheck.ru: *Клиенты сети магазинов «Fix Price» стали жертвой взлома базы данных бонусных карт лояльности компании. Покупатели копили бонусы, а мошенники их обналичивали. Кроме того в сеть утекла личная информация участников акции, такая как адрес электронной почты, номер телефона, дата рождения, ФИО и адрес. С учетом слабой системы защиты предприятия, существует предположение, что взлом мог быть совершен школьниками.*

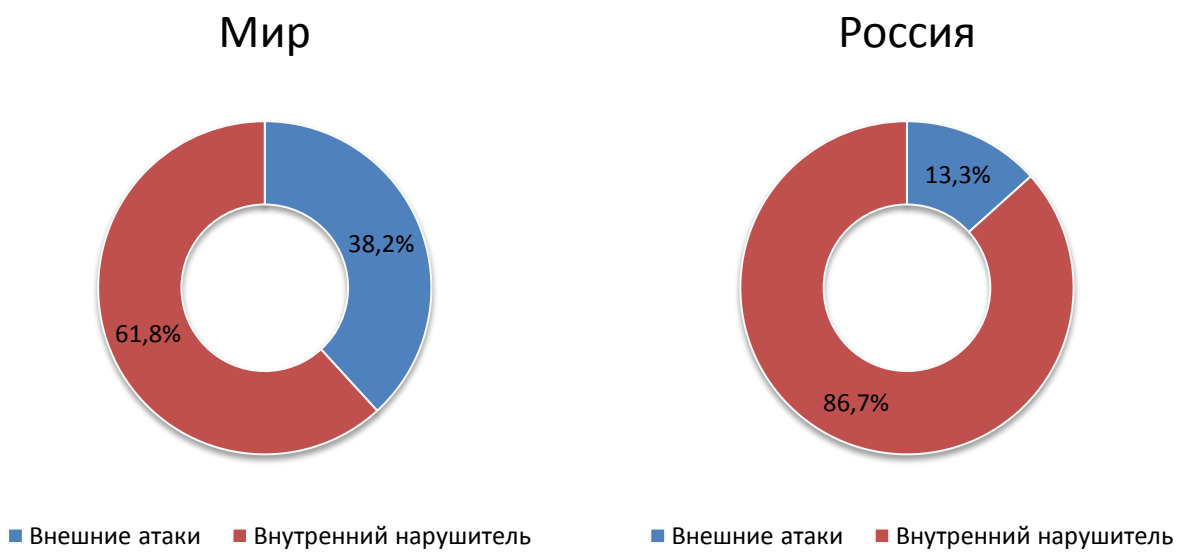


Рисунок 6. Распределение утечек по вектору воздействия, Россия – мир, 2016 г.

Приходится с сожалением констатировать, что выявленная диспропорция — в частности, характерная для России большая по сравнению с мировой выборкой доля сотрудников и руководителей, виновных в утечке информации,— скорее всего, сохранится. Оснований утверждать обратное немного, поскольку существенного снижения указанной доли невозможно добиться одним лишь внедрением технических средств защиты. Нужна серьезная работа по повышению культуры обращения с информацией ограниченного доступа. А это всегда длительный процесс.

> time56.ru: *Жительница поселка Тюльган, работая старшим продавцом в салоне связи, имела доступ к персональным данным клиентов оператора*

сотовой связи. Чтобы получить сведения о телефонных переговорах одного из клиентов, женщина сменила учетные данные абонентского номера, которые принадлежали потерпевшей, и заменила персональные данные на собственные. Злоумышленница неоднократно получала детализацию абонентских соединений потерпевшей.

В цифровую эпоху увеличивается стоимость данных и их ликвидность. Как следствие, повышается риск неправомерных действий сотрудников организаций, имеющих доступ к высоколиквидным данным.

procrf.ru: Главным специалистом администрации Нюксенского района подготовлена и направлена юридическому лицу справка о составе семьи, проживающей в селе Нюксеница. В нарушение требований закона указанные персональные данные переданы третьему лицу.

Как правило, организации сосредоточены на обеспечении безопасности объектов защиты — самих документов, информации. При этом упускают из вида субъекта, не занимаются сегментированием сотрудников по объему необходимых прав на доступ к данным, забывают об аудите и управлении выданными правами. Следствие — многочисленные случаи умышленных утечек данных по вине сотрудников.

kaluga-poisk.ru: Несмотря на судимость, 25-летняя калужанка работала экспертом прямых продаж в одном из банков Калуги. На своем рабочем месте она «пробила» по базе персональные данные клиента и без его ведома оформила на его имя целевой потребительский кредит для покупки меховых изделий в сумме около 130 тысяч рублей. Получив разрешение, девушка купила себе норковую шубу, меховые шапку и жилетку.

Внутренний злоумышленник со временем становится опаснее

В 2016 году в России наибольшие доли утечек пришлись на сетевой канал и бумажную документацию — 64% и 26% соответственно (Рисунок 7).

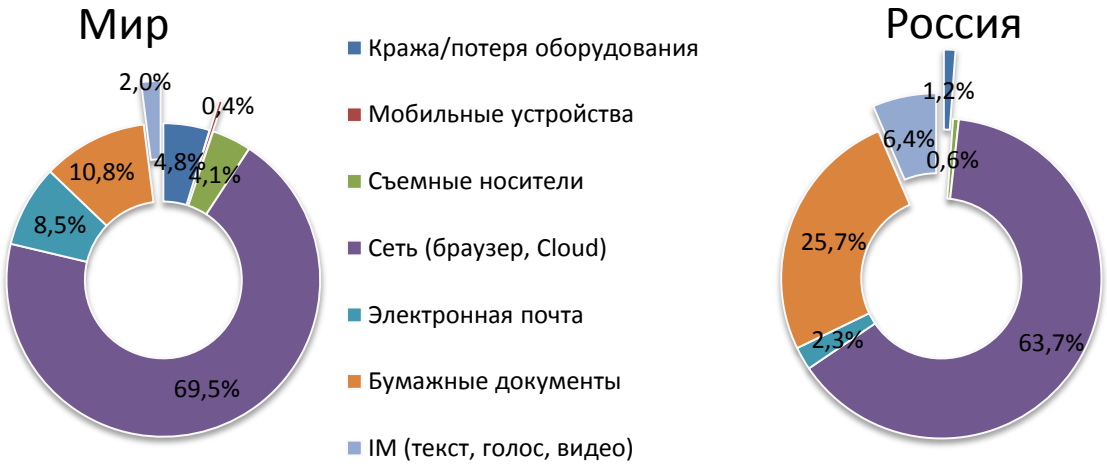


Рисунок 7. Распределение утечек по каналам, Россия – мир, 2016 г.

Незначительны доли утечек, связанных с использованием электронной почты — около 2%, потерей или кражей оборудования (ПК, ноутбуки, серверы) — около 1%, утечек через съемные носители информации — менее 1%.

В исследовании 2014 года мы обращали внимание на специфичность каналов утечки информации, указывая, в частности, что практически все утечки данных, зафиксированные по каналу «съемные носители» были совершены умышленно. То есть сотрудник намеренно попытался похитить данные компании с использованием внешнего носителя данных, но был пойман. Тогда мы предположили, что среднестатистический российский злоумышленник в области компрометации данных не сильно заботится о том, чтобы его не поймали в силу убежденности в том, что службы информационной безопасности никогда не обнаружат сам факт утечки.

За два года ситуация серьезно изменилась. В 2016 году количество утечек по таким каналам, как «съемные носители», «потеря и кража оборудования» исчислялось единичными случаями. Злоумышленники, зная о том, что их действия контролируются, просто не используют указанные каналы. Либо, что более вероятно, злонамеренные утечки ценной информации из организаций по этим каналам происходят, однако нарушителям удается обойти системы защиты.

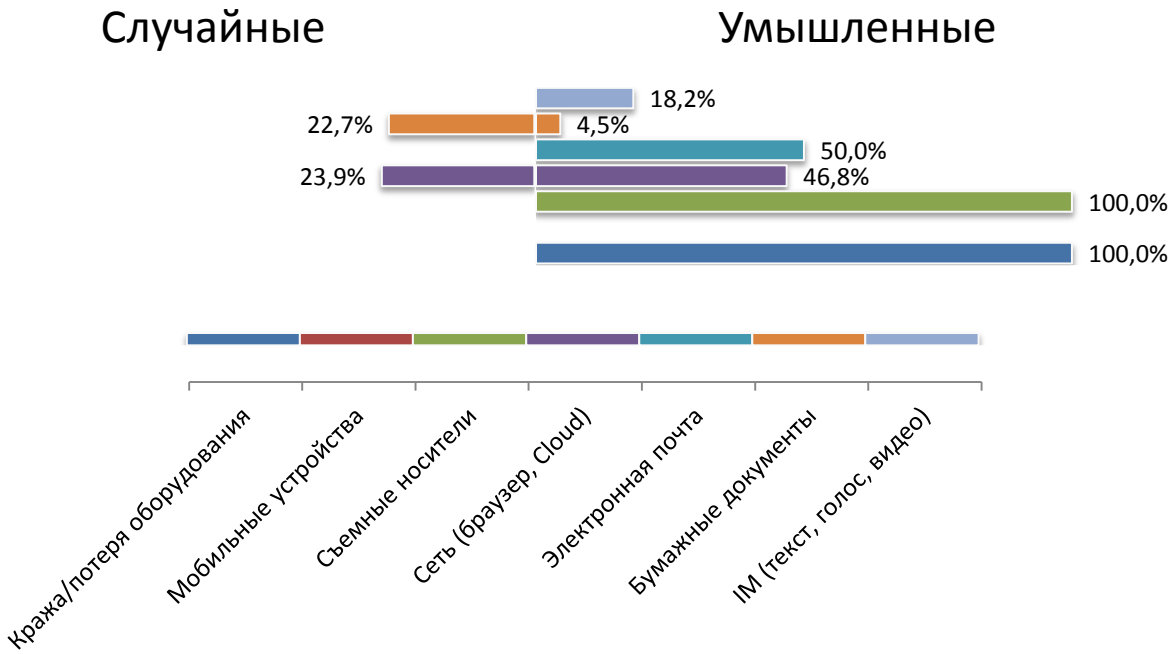


Рисунок 8. Доля случайных и умышленных утечек по каналам, 2016 г.

По-прежнему наиболее типичными для нашей страны являются сценарии утечек, которые предполагают использование бумажных носителей информации. Например, коммерческие организации вывешивают на подъездах жилых многоквартирных домов списки должников с полным перечнем персональных данных.

> *interfax-russia.ru: Мировой суд Губкина Белгородской области оштрафовал «Лето Банк» за разглашение персональных данных клиентки, задолжавшей*

по кредиту. Местная жительница обратилась в прокуратуру, когда обнаружила в подъезде объявления со своими фотографией, ФИО, адресом, номерами телефонов, а также рекламой об оказании ею платных услуг интимного характера. Компрометирующие женщину листовки с указанием ее персональных данных были расклеены представителями «Лето Банка».

О банках и страховых компаниях, органах власти, выбрасывающих копии паспортов граждан на ближайшие к офису свалки, даже говорить не приходится — слишком обыденными стали такие истории.

currenttime.tv: Архив судебных приставов Хакасии с полным набором данных по должникам (указаны фамилия, имя, отчество, ИНН, индивидуальный номер в системе пенсионного страхования) оказался на городской свалке.

По числу утечек данных в Росси лидируют госорганы, высокотехнологичные компании, образовательные учреждения и банки

Российское отраслевое распределение утечек серьезно отличается от мирового.

Рисунок 9. Отраслевое распределение утечек, Россия – мир, 2016 г.

В мире более 25% утечек информации происходит из медицинских учреждений, в России доля таких утечек составляет 7%. Обращает на себя внимание высокая (в сравнении с общемировой) доля утечек, которые пришлись на банки и финансовые организации (12%). Также высоки (в сравнению с мировыми показателями) доли образовательных учреждений (14%), госорганов и силовых структур (22%).

> ura.ru: *Сканы паспортов и миграционных карт граждан КНДР, расписки в получении «черного нала» и внутренняя документация строительной фирмы обнаружил житель Екатеринбурга в кустах около здания УФМС. Среди бумаг — документация об аукционе на ремонт здания института ФСБ на Сибирском тракте, детальный план одного из торговых центров Екатеринбурга.*

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

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

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

Показателем «привлекательности» можно считать число умышленных утечек в конкретной отрасли. Отраслевое распределение умышленных утечек данных одного типа даст нам ответ на вопрос, какие сегменты наиболее «привлекательны» для злоумышленника и, следовательно, наиболее уязвимы (Рисунок 10).

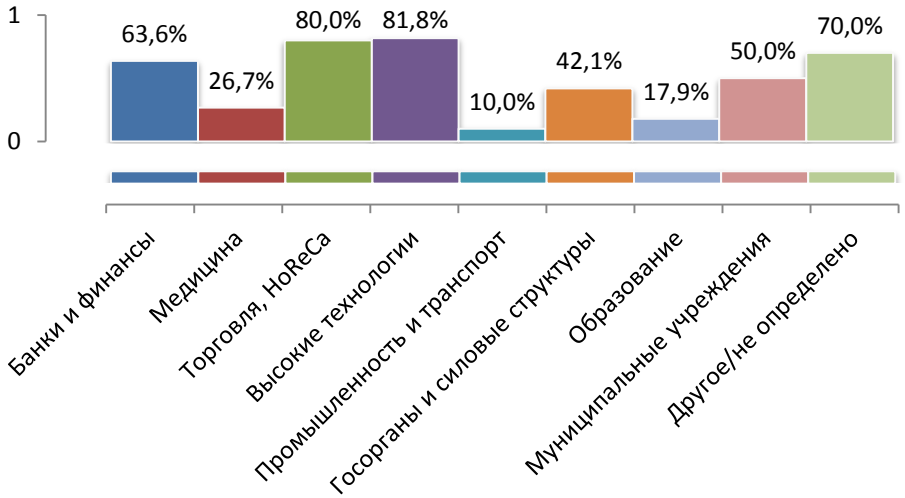


Рисунок 10. Доля утечек ПДн и финансовых данных по отраслям, Россия, 2016 г.

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

В 2016 году наиболее «привлекательными» для похитителей данных в России оказались торговые и высокотехнологичные компании, к которым добавились финансовые учреждения. В этих отраслях более половины утечек, сопровождавшихся компрометацией персональных данных, носили умышленный характер.

> *theins.ru: журналисты обнаружили базу данных «кредитных историй» клиентов и должников крупнейших банков России, с указанием ФИО, адресов, телефонов и места работы (службы). В базе оказались и персональные данные сотрудников засекреченных подразделений ФСБ. Среди «засвеченных» клиентов — высокопоставленные чиновники, депутаты и более 100 тысяч действующих или бывших сотрудников силовых структур. Общий объем базы составляет 20 млн записей.*

Если перестроить уже приведенное распределение по вектору атаки, то мы получим наглядное представление о «привлекательности» конкретной отрасли для внешнего и внутреннего злоумышленников (Рисунок 11).

Как видно из диаграммы, высокотехнологичные компании, наряду с торговыми организациями, чаще всего становились жертвами внешних атак, направленных на хищение данных. С другой стороны, от злонамеренных действий внутреннего нарушителя чаще всего страдали банки, торговые компании и муниципальные учреждения. Одна из основных причин — чрезвычайно высокая ликвидность данных, с которыми работает персонал компаний перечисленных отраслей.

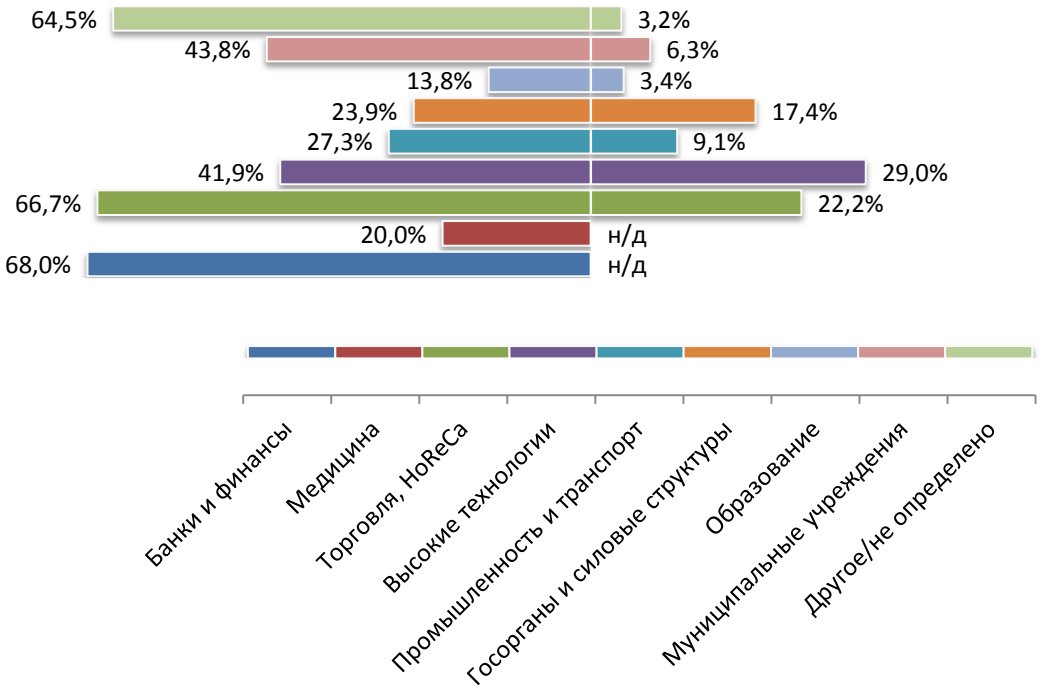


Рисунок 11. Доля умышленных утечек ПДн под воздействием внутреннего (слева) и внешнего (справа) злоумышленника от общего числа утечек ПДн по отраслям, 2016 г.

Отметим также, что российская картина утечек показывает большее, в сравнении с общемировым, число утечек, которые пришлись на небольшие организации (менее 50 ПК) – 11% к 5% по миру (см. Рисунок 12). С другой стороны, в мире на этот сегмент приходится 0,6% от всего объема скомпрометированных данных. В России этот показатель составляет менее 0,01%.

Небольшой объем скомпрометированных данных в российских организациях до 50 ПК может быть связан с тем, что эти компании крайне редко используют современные технологии для работы с агрегированными данными. Нет единых баз данных (у каждого сотрудника своя база), автоматизированных инструментов для удаленной совместной работы (облачные CRM). Получается, что технологическое отставание от западных коллег по рынку (где использование инструментов совместной работы в порядке вещей даже в небольших организациях) снижает риск утечки больших объемов данных.

При этом статистика свидетельствует, что каждая десятая утечка данных произошла из компаний, работающих в сегменте малого бизнеса. Недофинансирование, низкий уровень культуры обращения с информацией ограниченного доступа, недостаточный контроль персонала, отсутствие специально выделенного сотрудника, ответственного за безопасность информации — с такими проблемами в области ИБ сталкивается сегодня малый бизнес в России.

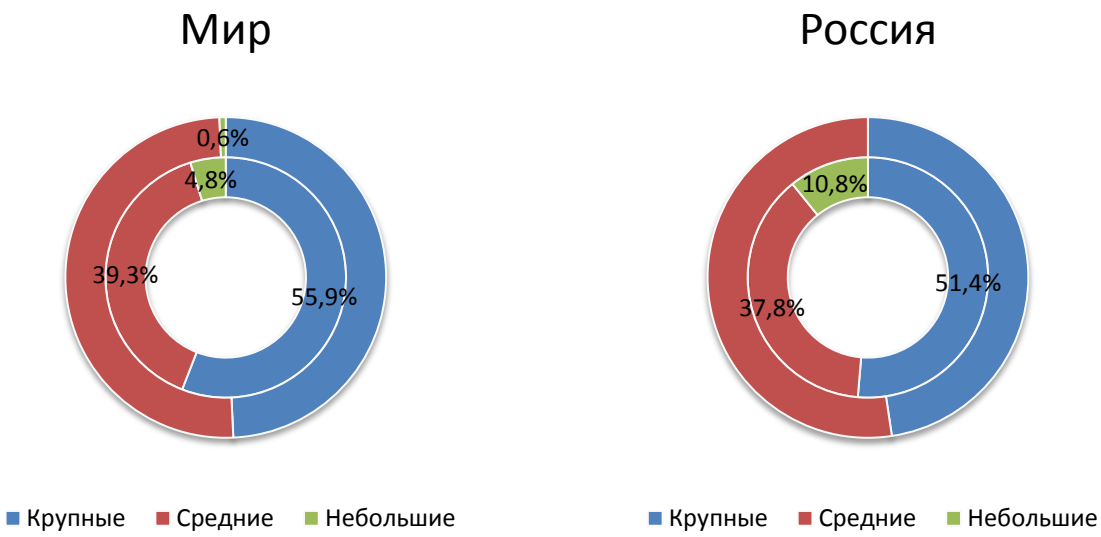


Рисунок 12. Распределение количества утечек (внутренний круг) и объема скомпрометированных ПДн (внешний) по размеру организаций, Россия – мир, 2016 г.

Средние и малые организации выступают основным источником утечек информации в России — на этот сегмент приходится до двух третей всех зафиксированных инцидентов. Более того, в случае с утечками отдельных типов информации (например, баз данных со сведениями о клиентах и партнерах, персональных и финансовых данных), средний и малый бизнес можно назвать главным «поставщиком» коммерчески значимой скомпрометированной информации.

> *izvestia29.ru: Как установили сотрудники полиции, перед покупкой очередной партии продукции, агент одного из постоянных покупателей попросил у менеджера предоставить ему сведения о наценке, которую делает его фирма при продаже продукции, то есть сообщить сведения, составляющие коммерческую тайну. Боясь, что в случае отказа сделка может не состояться, а, значит, уменьшится размер причитающейся ему от продажи премии, менеджер переслал клиенту по электронной почте один из внутренних документов компании.*

К сожалению, в большинстве небольших организаций утечки данных просто не расцениваются как действительно серьезный инцидент в области информационной безопасности. Например, образовательные учреждения с пугающей частотой публикуют на своих сайта списки выпускников, учеников, их родителей, включая сведения, относящиеся к персональным данным. Складывается ощущение, что администрация школ и вузов просто далеко не всегда отдает себе отчет в том, что своими действиями нарушает действующее законодательство. То же относится к различным управляющим компаниям, службам ЖКХ, и прочим организациям, связанным с обеспечением интересов населения при решении вопросов местного самоуправления и коммунального благоустройства.

> *zlatoust74.ru: На сайте Управления жилищно-коммунального хозяйства Златоустовского городского округа в реестре маршрутов внутримуниципальной маршрутной сети были указаны места жительства 12 индивидуальных предпринимателей, занимающихся пассажирскими перевозками. Однако закон не требует размещения таких сведений в реестре.*

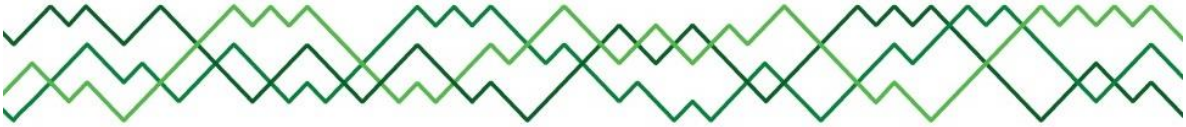
Отдельно стоит упомянуть принципиально большую (в сравнении с мировой) долю утечек данных, которые приходятся в России на государственные (и муниципальные) органы и организации — 29% (в мире — 18%).

> *rg.ru: В кировском районе Перми, недалеко от отдела полиции, прохожие нашли документы с персональными данными жителей города. В документах были указаны имена, фамилии, адреса, даты рождения, телефоны, сведения о наличии судимости, фотографии и прочие сведения.*

Заключение и выводы

Мы являемся свидетелями уникального процесса, когда данные в электронном виде превращаются в актив с известной, определенной ценностью. Утрата контроля над таким активом для организации или гражданина всегда приводит к финансовым потерям. Причем речь идет не только о сложной для расчета и взыскания категории причиненного морального вреда, но и о прямом материальном ущербе.

Наша страна глубоко интегрирована в глобальные процессы информатизации бизнеса, государства и общества. Отсюда все преимущества и проблемы, которые влечет за собой такая интеграция. С одной стороны, возникают все новые варианты сценариев взаимодействия пользователей с информацией. Повышение уровня удобства работы положительно сказывается на росте производительности труда. «Цифровизация» госуслуг, межведомственный документооборот оставляют все



меньше места для чиновничьего произвола. С другой стороны, с ростом ценности информации повышается вероятность утечки данных. Фактически, мы переступили незримую черту, за которой утечка информации из организации превратилась в рядовое явление. Ни одна система защиты не способна со 100% гарантией справиться с разнообразием каналов передачи данных, способов использования информации.

К сожалению, общество не успевает за развитием технологий. Старые процессы и подходы не всегда вписываются в новую реальность. И в мире, и в России проблему безопасности данных пытаются решать за счет применения технических средств защиты, но уже сейчас очевидно, что надеяться только на технологии нельзя. Не информация, а человек должен стать точкой приложения основных усилий, направленных на обеспечение информационной безопасности.

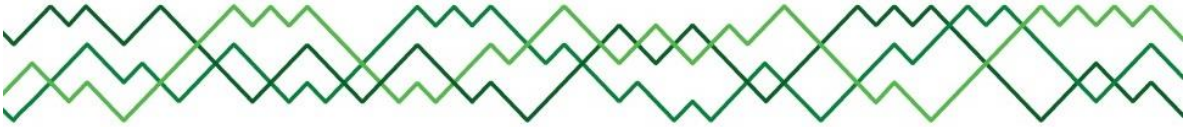
Российская картина утечек свидетельствует о том, что речь не может идти о ликвидации утечек данных как таковых, можно говорить лишь об управлении рисками утечек данных и связанными с этими рисками информационной безопасности организаций. И технические средства в этом смысле — необходимы, но уже недостаточны.

Так с помощью одних лишь технологий можно контролировать то, что поддается формализации — например, обработку платежной информации, персональных данных. Однако контроль и предотвращение утечек сведений, составляющих коммерческую тайну, весьма непросто осуществить без активного применения организационных мер, обучения персонала «информационной гигиене», изменения отношения к проблеме информационной безопасности у самих сотрудников, которые зачастую могут даже не задумываться о противоправности собственных действий, скачивая при увольнении всю корпоративную информацию, до которой могут дотянуться.

Внутренний нарушитель сегодня представляет наибольшую опасность для организаций-владельцев информации ограниченного доступа. При этом опыт западных стран показывает, что рано или поздно эта ситуация будет меняться. Уже сейчас доля утечек вследствие внешних атак в России составляет 13%, и этот показатель неизбежно вырастет. Причины просты — ценность агрегированных данных повышается, системы защиты от внешних взломов не успевают за совершенствованием инструментов проникновения. Нельзя забывать и про ошибки, число которых, с увеличением обрабатываемых объемов данных, будет также расти. С большой вероятностью, уже в течение следующих двух-трех лет нас ожидает стремительный рост объема данных, скомпрометированных в результате внешних атак.

Показанная выше картина диктует наиболее простой и очевидный путь развития, предполагающий совмещение двух моделей обеспечения информационной безопасности. То есть контроль информации (объектов защиты) и сотрудников, которые осуществляют к ней доступ. В широком смысле — анализ пользовательского поведения.

Второй немаловажный аспект — сегментирование и фокусирование. Очевидно, что защищать все и от всех одинаково хорошо уже не получится. Необходимо



сосредоточиться на наиболее ценных активах (а для этого определить их ценность и расположение), наиболее «проблемных» каналах передачи, наиболее подверженных риску компрометации данных сотрудниках.

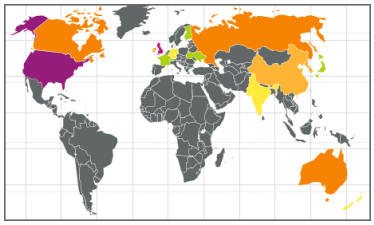
Третий аспект — анализ и систематизация лучших практик в пределах отрасли. Отраслевая специфика не проявляется на уровне контроля объектов защиты (данные могут иметь более-менее похожую структуру и ценность вне зависимости от отрасли), но на уровне управления информационной безопасностью (анализ рисков, связь ИБ и экономической безопасности) прослеживается довольно отчетливо. Степень заинтересованности нарушителей также привязана к отраслевым особенностям компании-жертвы. Например, банки и интернет-сервисы, агрегирующие наиболее ликвидную информацию, чаще всего становятся целью внешнего злоумышленника, и это вряд ли кого-то удивляет.

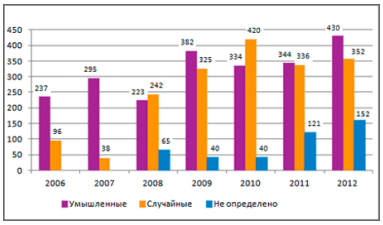
С учетом выявленных и обозначенных особенностей российской картины утечек, известных факторов, формирующих эту картину, вызовов, стоящих перед отраслью информационной безопасности, наиболее приемлемым подходом следует признать создание и использование таких систем защиты, которые позволяют контролировать конкретные типы информации ограниченного доступа (базы данных, финансовые документы, информацию, составляющую коммерческую тайну), проводить «глубокий» мониторинг «проблемных» каналов передачи информации (исходящий интернет-трафик, бумажные документы, передачу данных на съемные устройства). Кроме того, необходимо акцентировать внимание на всестороннем применении анализа поведения сотрудников в жесткой привязке к их роли в компании, объему прав доступа к информации. В идеальном случае такая защита дополняется решением для противодействия внешним атакам на информационные системы организации.

Мониторинг утечек на сайте InfoWatch

На сайте Аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

Кроме того на сайте представлены статистические данные по утечкам информации за прошедшие годы, оформленные в виде динамических графиков.



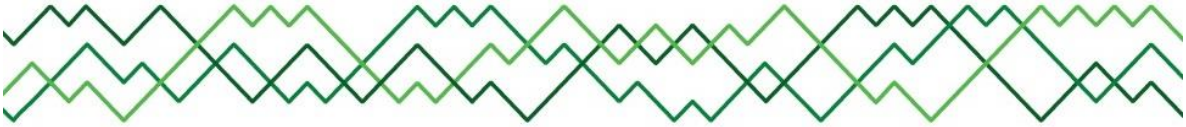


Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Twitter
- RSS

Аналитический центр InfoWatch

www.infowatch.ru/analytics



INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Глоссарий

Инциденты информационной безопасности — *в данном исследовании к этой категории авторы относят случаи компрометации информации ограниченного доступа вследствие утечек данных и/или деструктивных действий сотрудников компании.*

Утечка данных — *под утечкой мы понимаем утрату контроля над информацией (данными) в результате внешнего воздействия (атаки) а также действий лица, имеющего легитимный доступ к информации или действий лица, получившего неправомерный доступ к такой информации.*

Деструктивные действия сотрудников — *действия сотрудников, повлекшие компрометацию информации ограниченного доступа: использование информации ограниченного доступа в личных целях, сопряженное с мошенничеством; нелегитимный доступ к информации (превышение прав доступа).*

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

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

К неумышленным относятся утечки информации, когда пользователь не предполагал наступления возможных негативных последствий своих действий и не преследовал личной выгоды. При этом неважно, имели ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы.

Вектор воздействия — *критерий классификации в отношении действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников – (Внешние атаки), направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации информации, и действия внутренних злоумышленников – (Внутренний нарушитель), атакующих системы защиты изнутри (нелегитимный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.)*

Канал передачи данных — *сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. На данный момент мы различаем 8 самостоятельных каналов:*

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