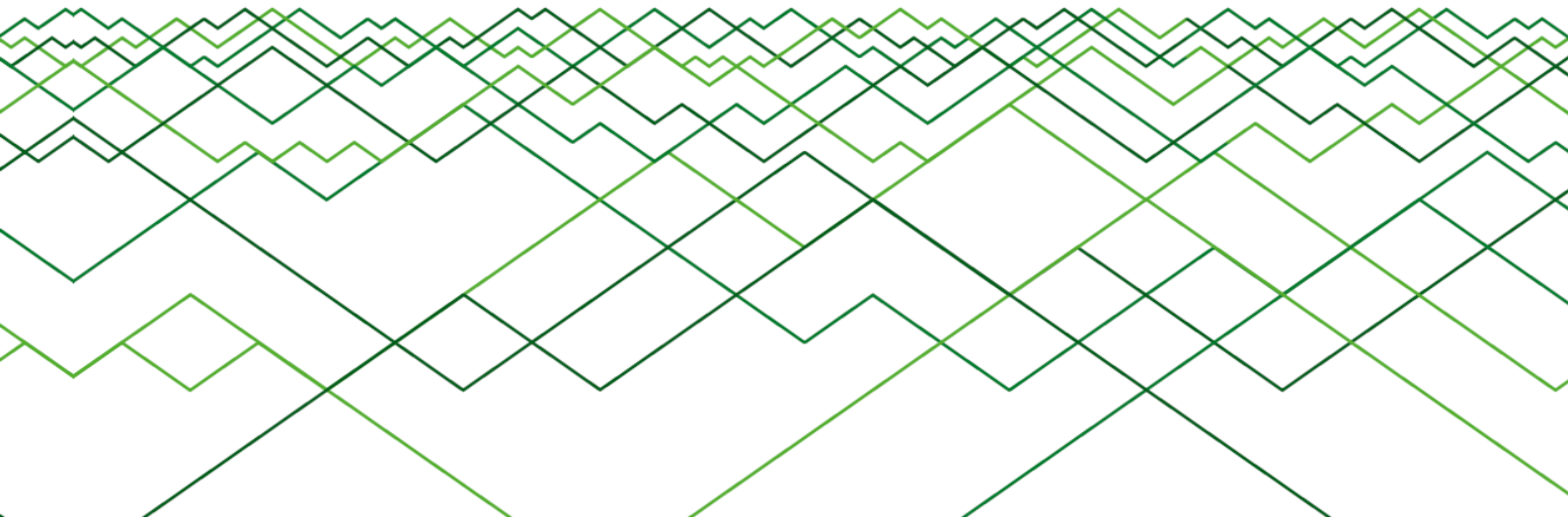
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аналитический центр InfoWatch
www.infowatch.ru/analytics

Глобальное исследование утечек конфиденциальной информации из компаний среднего и малого бизнеса в 2013 году



INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Оглавление

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Цифры и факты

- ✓ В 2013 году зарегистрировано **448** утечек конфиденциальной информации из небольших и средних компаний (менее 50 ПК и 50-500 ПК соответственно). На СМБ-сегмент пришлось чуть менее **40%** от общего количества утечек, зафиксированных по всему миру.
- ✓ В средних компаниях ущерб (в расчете на одну скомпрометированную запись) составляет **16** долл. США - на 2,5 долл. больше, чем в крупных организациях.
- ✓ Доля утечек персональных данных в сегменте СМБ составляет **95%** - на 12 п. п. выше, чем в крупном бизнесе.
- ✓ В небольших и средних компаниях **76%** утечек связаны с неправомерной деятельностью или ошибками собственных сотрудников организации. В крупных компаниях на долю сотрудников приходится лишь 45% утечек.
- ✓ Число скомпрометированных записей о клиентах и сотрудниках небольших и средних компаний превышает **129 млн**. Совокупный ущерб от утечек в сегменте СМБ - более **2 млрд.** долл.
- ✓ Основным каналом утечек остается **бумажная документация**.
- ✓ В России на долю небольших и средних компаний приходится **61%** всех утечек информации – на 21 п. п. больше, чем в целом по миру.
- ✓ Небольшие и средние компании чаще, чем крупные, страдают от утечек через съемные носители, сеть, электронную почту. То есть через каналы, которые можно контролировать с помощью технических средств защиты данных.

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аннотация

Аналитический центр компании InfoWatch представляет отчет об исследовании утечек конфиденциальной информации из небольших и средних компаний (далее - сегмент среднего и малого бизнеса, СМБ-компании), произошедших в 2013 году и обнародованных в СМИ, иных источниках. Предметное исследование утечек конфиденциальной информации на выборке утечек из небольших (до 50 ПК) и средних (50-500 ПК) компаний проводится впервые.

До недавнего времени считалось, что проблема утечек конфиденциальной информации не затрагивает малый и средний бизнес. Якобы, стоимость информационных активов в сегменте СМБ не столь высока, как в крупных компаниях, объем конфиденциальных данных (ноу-хау, иная интеллектуальная собственность) невелик, сами данные не влияют на создание конкурентного преимущества, а гипотетический ущерб от утечки данных минимален.

Однако результаты исследования показывают, что такое представление ошибочно. Вследствие халатного отношения организаций сегмента СМБ к обеспечению защиты информации страдают клиенты и сотрудники, чьи персональные данные попадают в руки мошенников. Это пагубно сказывается на бизнесе небольших и средних компаний, их репутации.

Авторы исследования уверены, что анализ утечек данных на глобальной выборке компаний СМБ дает ключ к пониманию ситуации в сегменте. Так выявление наиболее «популярных» каналов утечки информации позволяет небольшим компаниям, не распыляя силы, сосредоточить внимание на защите определенного участка, обеспечить контроль передачи данных по «проблемным» каналам. Статистика виновных в утечке помогает выделить «ненадежную» группу сотрудников, имеющих легитимный доступ к конфиденциальной информации. Применив к такой группе дополнительные меры контроля, несложно обезопасить компанию от возможных негативных последствий, вызванных злонамеренными действиями или ошибками этих сотрудников.

В рамках исследования авторы иллюстрируют ряд характерных для России региональных особенностей в плане безопасности конфиденциальной информации в СМБ. Несмотря на отсутствие принципиальных отличий в процессах развития сферы информационной безопасности в нашей стране и на Западе, в России есть несколько локальных особенностей, которые необходимо учесть и отечественным компаниям сегмента СМБ, и производителям средств защиты, чьи решения ориентированы на данный сегмент.

Отчет об исследовании адресован специалистам в области информационной безопасности, руководству небольших и средних компаний, представителям СМИ.

Методология

Исследование основывается на собственной базе данных, пополняемой специалистами Аналитического центра InfoWatch с 2004 года. В базу попадают

публичные сообщения[1] о случаях утечки[2] конфиденциальной информации[3] из коммерческих и некоммерческих (государственных, муниципальных) организаций по причине злонамеренных или неосторожных действий[4] сотрудников компаний, иных лиц. База утечек InfoWatch насчитывает несколько тысяч зарегистрированных инцидентов.

В ходе наполнения базы каждая утечка (если возможно и такая информация есть в сообщении об инциденте) классифицируется по ряду критериев: размер организации[5], сфера деятельности (отрасль), сумма ущерба[6], тип утечки (умысел)[7], канал утечки[8], типы утекших данных и пр.

Предметом данного исследования являются сообщения об утечках конфиденциальной информации из небольших и средних компаний (организации, где парк персональных компьютеров насчитывает менее 50 ПК и от 50 до 500 ПК соответственно).

Исследование охватывает не более 4-8%[9] случаев от предполагаемого совокупного количества утечек в сегменте. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества (категории) содержали достаточное или избыточное количество элементов (фактических случаев утечки). Такой подход к формированию поля исследования позволяет считать получившуюся выборку теоретической, а выводы исследования и выявленные на выборке тренды репрезентативными для генеральной совокупности.

Случаи нарушения конфиденциальности информации, произошедшие в результате внешних компьютерных атак, а равно иные инциденты ИБ (DDoS, фишинг, несанкционированный доступ к информации, саботаж сотрудников и пр.), не повлекшие утечек данных, в исследовании не рассматривались.

---

[1] Сообщения об утечках данных, опубликованные официальными ведомствами, СМИ, авторами записей в блогах, интернет-форумах, иных открытых источниках.

[2] Утечка информации (данных) - действие или бездействие лица, имеющего легитимный доступ к конфиденциальной информации, которое (действие) повлекло потерю контроля над информацией или нарушение конфиденциальности этой информации.

[3] 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 конфиденциальной информации мы включаем информацию, подпадающую под определение персональных данных.

[4] См. тип утечки по умыслу.

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

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

[7] 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.

[8] Под каналом утечки мы понимаем сценарий (действия 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.

[9] В ходе исследования мы столкнулись с явным свидетельством того, что уровень латентности (доля утечек, оставшихся неизвестными широкой публике) в мире серьезно снизился. Потому экспертная оценка процентной доли известных утечек по сравнению с утечками, оставшимися за рамками внимания данного исследования, повышена с 1-5% до 4-8%.

Результаты исследования

В 2013 году число скомпрометированных записей о клиентах и сотрудниках небольших и средних компаний превысило 129 млн. Совокупный ущерб от утечек составил более 2 млрд. долл.[10] (см. Рисунок 1).

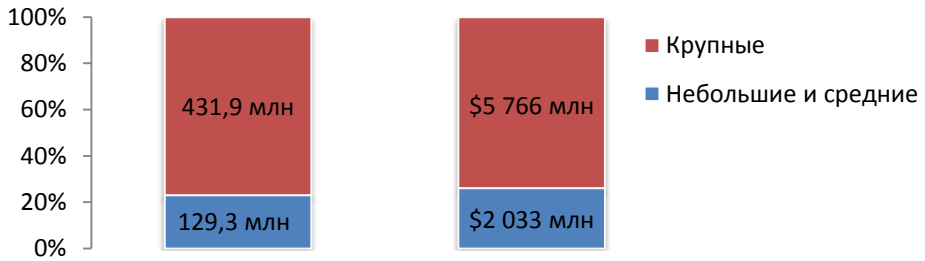


Рисунок 1. Утечки по числу записей и финансовому ущербу. СМБ и крупные. Доля.

Сегмент СМБ остается в тени крупных компаний и по числу утекших записей (на СМБ приходится чуть более 20% от всех скомпрометированных записей), и по сумме совокупного ущерба. Но есть ряд принципиальных особенностей картины утечек из небольших и средних компаний, которые необходимо отметить.

Ключевой факт: в средних компаниях ущерб (в расчете на одну утекшую запись) выше, чем в крупных организациях.

Если в крупных компаниях утечка одной записи о клиентах или сотрудниках (персональные данные, в том числе реквизиты пластиковых карт, номера соцстрахования и проч.) «стоит» 13,4 доллара, в среднем бизнесе ущерб от утечки (на одну запись) составляет 15,9 долл.[11] (см. Рисунок 2).

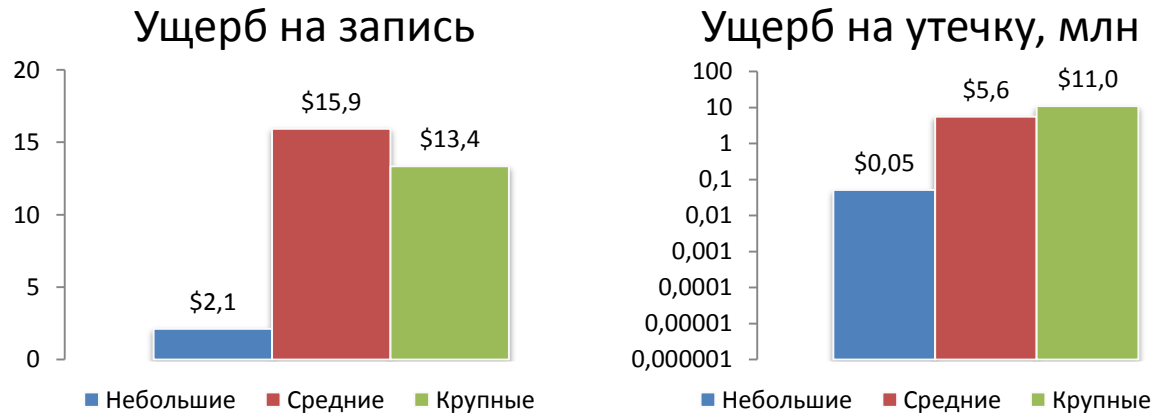


Рисунок 2. Ущерб от утечки в расчете на запись, на утечку. Долл. США.

[10] Здесь и в дальнейшем все оценки ущерба приведены в долларах США, если не указано иное.

[11] В данном случае речь идет не о стоимости единицы информации (записи), а о потерях компании, спровоцированных утечкой данных. Вероятно, больший ущерб в расчете на одну запись в средних компаниях (по сравнению с крупными) связан с характером утекающих данных – в средних компаниях чаще, чем в крупных, «уходит» критически важная информация (например, платежные данные).

Ущерб в расчете на одну утечку коррелирует с размером компаний. Крупные компании несут более существенные потери (в абсолютном выражении), чем средний и малый бизнес, поскольку суммы ущерба, зафиксированного в сообщениях СМИ, включают в себя не только недополученную прибыль, репутационные потери, но и снижение стоимости бренда, падение акций в случае утечки у публичных компаний.

Вывод:

Для малого и среднего бизнеса вопрос защиты информации от утечек сегодня столь же актуален, как и для крупного. Ущерб от утечки в расчете на скомпрометированную запись в среднем бизнесе даже выше, чем в крупных организациях.

Ключевой факт: на долю малых и средних компаний приходится 4 из 10 утечек конфиденциальной информации.

В 2013 году специалистами Аналитического центра InfoWatch зарегистрировано 448 случаев утечки конфиденциальной информации в небольших и средних компаниях. Это чуть менее 40%; от общего количества зафиксированных за год утечек[12], (см. Рисунок 3).

Рисунок 3. Распределение утечек по размеру компании. Количество, доли.

Утечки конфиденциальной информации из крупных компаний привлекают внимание СМИ по всему миру, активно освещаются на страницах периодических изданий и блогов, попадают в поле зрения аналитиков. Поэтому неудивительно преобладание крупных компаний в распределении утечек по размеру организации.

Но и на этом фоне процент утечек из средних компаний оказался неожиданно высоким - 31,8%. Еще 7,3% утечек пришлись на долю небольших организаций.

[12] В 2013 году Аналитическим центром InfoWatch зарегистрировано 1143 случая утечки конфиденциальной информации. См. Глобальное исследование утечек конфиденциальной информации в 2013 году. http://www.infowatch.ru/report2013

По мнению специалистов Аналитического центра InfoWatch, доля средних и малых компаний в распределении утечек будет расти. Журналистов и блогеров не удивишь утечками в Microsoft или Adobe. Все большую важность приобретает не громкое имя компании, допустившей утечку, а характер скомпрометированных данных, общественная опасность самого факта утечки, - в этом причина предполагаемого увеличения доли СМБ-компаний в картине утечек.

> *kp.ru 20-летняя сотрудница одного из банков в городе Михайлове, воспользовавшись персональными данными клиентов, оформила на них 13 потребительских кредитов на общую сумму более 250 млн рублей. Предприимчивой девушке грозит уголовное наказание за мошенничество в крупном размере.*

Кроме того, в соответствии с законодательством ряда стран, компании обязаны информировать общественность о нарушениях информационной безопасности. Особенно если речь идет о персональных данных клиентов или сотрудников. Компании все большее внимание уделяют защите собственной информации и данных своих клиентов. Внедряются системы для мониторинга трафика, предотвращения вторжений, защиты от утечек.

Естественно, что чем больше утечек регистрируется средствами защиты, тем больше сообщений об утечках публикуется в СМИ. Отсюда довольно значительная доля средних компаний в распределении утечек по размеру бизнеса. На практике, в настоящее время получают огласку такие факты компрометации данных, которые в иных условиях остались бы неизвестными широкой общественности.

> ***Вывод:***
>
> *Внедрение систем защиты от утечек в СМБ-компаниях началось. Но сегмент пока далек от насыщения. В ближайшие 2-3 года нас ждет количественный рост зарегистрированных утечек в СМБ – компании продолжат фиксировать нарушения, ранее остававшиеся незамеченными. Вырастет доля СМБ-компаний в распределении по размеру бизнеса. В горизонте 5 лет с насыщением сегмента средствами защиты можно ожидать стабилизации доли СМБ-компаний в картине утечек за счет роста общего уровня информационной безопасности в компаниях.*

Ключевой факт: доля утечек «неопределенной» природы в небольших и средних компаниях существенно выше, чем в целом в общемировой статистике.

По данным глобальной статистики утечек, в 2013 году на умышленные и случайные утечки пришлось 44,1% и 45,7% соответственно. В 10,2% невозможно установить, носит утечка злонамеренный или случайный характер. Причем доля таких утечек в 2013 году снизилась на 6,3 п. п. по сравнению с 2012 годом[13].

Распределение утечек по умыслу в средних и небольших компаниях выглядит несколько иначе. Обращает на себя внимание большая доля утечек

[13] См. Глобальное исследование утечек конфиденциальной информации в 2013 году. http://www.infowatch.ru/report2013.

«неопределенной» природы в среднем бизнесе - 23,1%, и в малых компаниях – 42,9% (см. Рисунок 4).

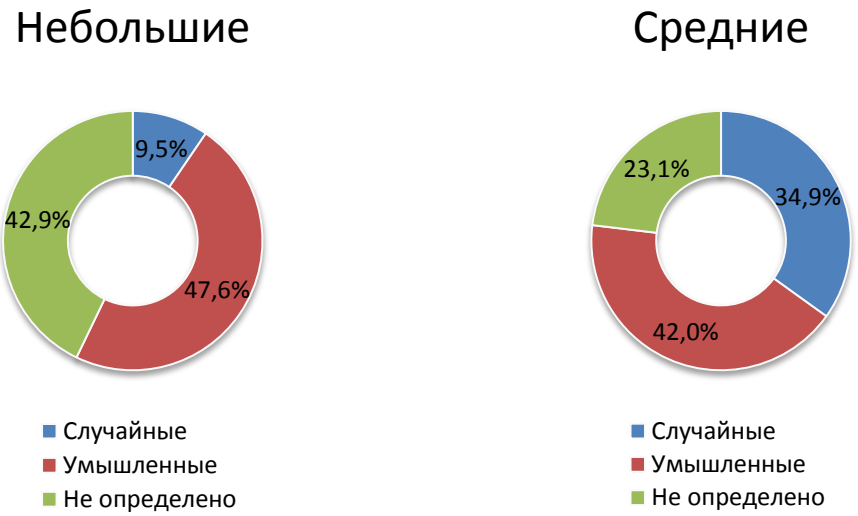


Рисунок 4. Распределение утечек по умыслу. Доли.

Как правило, информация о намерении сотрудника, допустившего утечку, имеется в официальном заявлении пострадавшей компании. В иных случаях представление о характере утечки (умышленном или случайном) с очевидностью следует из сообщения в СМИ. И лишь когда компании не обладают опытом или необходимыми средствами для контроля информации и определения виновника утечки, можно говорить о «неопределенном» характере утечки в распределении по умыслу.

Небольшая доля утечек «неопределенной» природы в глобальной статистике утечек, а равно ее последовательное сокращение год от года[14] свидетельствует о все большем распространении технических средств защиты от утечек. С помощью этих инструментов (как правило, системы класса DLP) компаниям удается легко установить виновного, канал передачи информации. В итоге утечка однозначно классифицируется как умышленная или случайная.

Из вышеприведенной диаграммы (см. Рисунок 4) очевидно, что о широком проникновении технических средств защиты от утечек в сегменте небольших компаний говорить пока не приходится. В компаниях среднего размера информация контролируется, но ответственным сотрудникам не всегда удается установить виновного даже в случае крупных утечек данных.

> *tcc.fl.edu Руководство колледжа в Таллахасси (США) объявило о компрометации персональных данных 3300 студентов. Сотрудники учебного заведения, отвечающие за безопасность данных, узнали об утечке от федеральных властей. Полиция обнаружила базу данных студентов*

[14] Падение доли утечек «неопределенного» характера в 2013 году составило 6,3% по отношению к 2012 году. См. Глобальное исследование утечек конфиденциальной информации в 2013 году. http://www.infowatch.ru/report2013

колледжа на компьютере мошенника, который зарабатывал деньги оформлением фальшивых требований о возврате налогов.

При этом доля умышленных утечек в средних (42,0%) и малых (47,6%) компаниях сопоставима с аналогичным показателем глобальной статистики – 44,1%[15].

Доля случайных утечек перераспределилась – 34,9% в средних и 9,5% в небольших организациях. Это не значит, что случайных утечек в СМБ-сегменте мало. Скорее, это показатель того, что случайные утечки есть, но компаниям не удается их отследить.

Распределение утечек по каналам также говорит в пользу невысокого уровня безопасности информации в сегменте СМБ. Небольшие и средние компании чаще, чем крупные, страдают от утечек через съемные носители, сеть, электронную почту (см. Рисунок 5). То есть через каналы, которые можно легко «перекрыть» и контролировать техническими средствами защиты данных.

Рисунок 5. Распределение по каналу утечки. Доли.[16]

Доля утечек из СМБ-компаний по «неопределенному» каналу также выше, чем в крупных организациях. Применительно к СМБ, мы часто знаем лишь о факте утечки, но нам не известно, как и по какой причине утечка произошла. Это еще один аргумент в пользу заключения о недостаточном уровне защиты данных в СМБ-компаниях.

Вывод:

Высокий процент утечек «неопределенного» типа в распределении по умыслу в сегменте СМБ однозначно говорит о «недовооруженности» СМБ-компаний средствами защиты информации. Налицо значительное отставание компаний сегмента СМБ от крупного бизнеса и в плане

[15] См. Глобальное исследование утечек конфиденциальной информации в 2013 году. http://www.infowatch.ru/report2013

[16] Подробнее о классификации по каналам утечки см. Глоссарий.

технических возможностей, и в плане общей зрелости, понимания, что и от кого следует защищать.

Ключевой факт: доля утечек персональных данных в небольших и средних компаниях выше, чем в крупном бизнесе.

С 2010 года на общемировой выборке наметился устойчивый тренд на снижение доли утечек персональных данных, и к 2013 году доля утечек этого типа составила лишь 85,1% (см. Рисунок 6)[17].

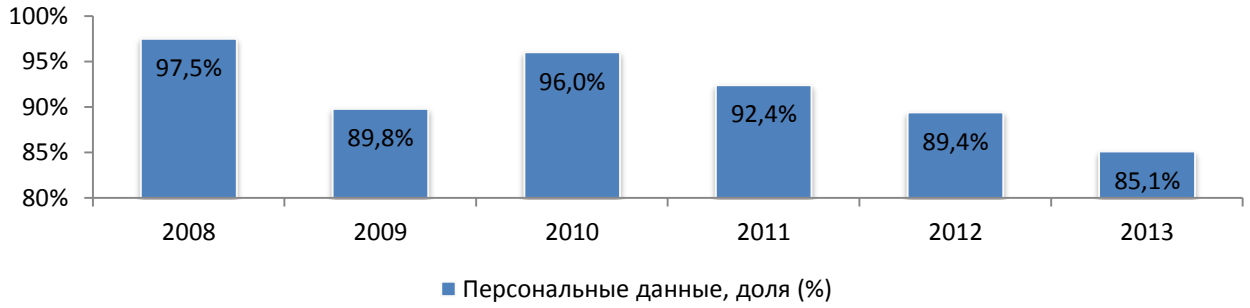


Рисунок 6. Доля утечек персональных данных по годам.

Аналитический центр InfoWatch связывает появление данного тренда с повышением внимания компаний и государственных органов к защите персональных данных клиентов и сотрудников. Компании, обрабатывающие персональные данные, всерьез озаботились внедрением технических средств защиты от утечек. Доля утечек ПДн начала снижаться.

Однако это не коснулось среднего и малого бизнеса. Доля утечек персональных данных в средних и малых компаниях составляет 95,0% (см. Рисунок 7), что на 11,6 п. п. превышает долю утечек персональных данных в крупном бизнесе (83,3%).

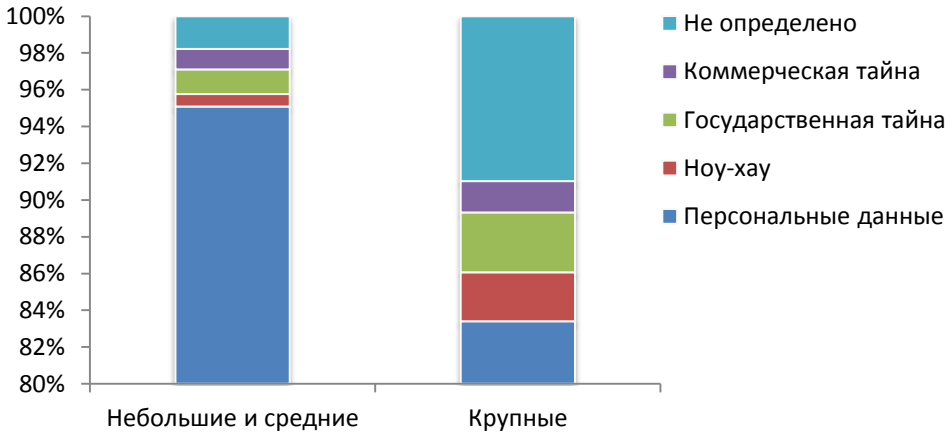


Рисунок 7. Распределение утечек по типу данных. Доли.

[17] См. Глобальное исследование утечек конфиденциальной информации в 2013 году. http://www.infowatch.ru/report2013

Как мы уже отмечали, источником информации об утечках персональных данных из небольших и средних компаний, как правило, являются СМИ, а не официальные сообщения пострадавших организаций. Это означает, что сами компании утечек данных практически не замечают, не способны их зафиксировать или предотвратить.

Факт утечки получает широкую огласку лишь в том случае, если утекшие данные всплывают на «черном рынке» в виде баз номеров социального страхования, реквизитов пластиковых карт. Второй вариант – обнародование подробностей утечки в ходе расследования уголовного дела в отношении, например, мошенников. Только тогда пострадавшая компания узнает, что данные ее пользователей или сотрудников скомпрометированы.

> *The Law Society Gazette Сервер с персональными данными 400 тыс. жертв и свидетелей преступлений был украден из здания суда города Солфорд (графство Манчестер), предположительно, сотрудником сервисной компании. Работники суда узнали о краже лишь тогда, когда полиция обнаружила похищенное оборудование – незадачливый вор попытался продать сервер через аукцион eBay.*

Выявление инцидентов «постфактум» — существенное отличие среднего и малого бизнеса от крупных компаний, где, благодаря средствам предотвращения утечек, удается своевременно перекрыть канал передачи информации, найти виновного. О таких утечках мы узнаем от самих компаний, так как законодательство многих стран обязывает эти организации обнародовать факт утечки и проинформировать пострадавших клиентов или сотрудников.

> *healthitsecurity.com Американская компания Joseph and Louise Gagnon выплатила 140 тыс. долларов в качестве компенсации за ненадлежащее обращение с медицинскими персональными данными. Сотрудники компании просто выбросили 67 тыс. файлов с записями о диагнозах пациентов.*

Своевременное обнаружение утечки персональных данных позволяет избежать масштабных финансовых потерь. При этом, однако, репутация компании в любом случае страдает.

> ***Вывод:***
>
> *В ряде стран к защите персональных данных предъявляются особые требования, вопрос регулируется на государственном уровне. Да и сам факт утечки данных клиентов или сотрудников не прибавляет компании популярности в глазах пострадавших. Однако доля утечек данных этого типа в СМБ драматически высока, что свидетельствует о низком уровне информационной безопасности в сегменте небольших и средних компаний. Малый и средний бизнес в большинстве не способен защитить даже персональные данные. Очевидно, что дело с обеспечением безопасности иных видов конфиденциальной информации обстоит еще хуже.*

Ключевой факт: сотрудники и руководители небольших и средних компаний «сливают» информацию чаще, чем их коллеги в крупном бизнесе.

В небольших и средних компаниях 75,8% утечек связаны с неправомерной деятельностью или ошибками собственных сотрудников организации. В крупном бизнесе на долю сотрудников приходится лишь 44,8% утечек (см. Рисунок 8).

Рисунок 8. Распределение по виновнику утечки. Доли.

Впрочем, тут вряд ли есть какое-то противоречие. Если посмотреть на картину утечек в крупных компаниях (правая диаграмма), легко увидеть перераспределение доли сотрудников в пользу доли контрагентов. Действительно, крупные компании чаще пользуются услугами подрядчиков, чем небольшие организации. Даже в том случае, когда речь идет о критически важных процессах – утилизация бумажных документов, сервис ИТ-инфраструктуры и проч. Естественно, время от времени системы защиты информации подрядчика дают сбой.

> *nbcdfw.com Сотрудник фирмы, предоставляющей банкам и страховым компаниям услуги по уничтожению конфиденциальных документов, состоял в преступной группе. Перед тем, как опустить банковские выписки и иные документы в шредер, он копировал их и передавал сообщникам. Число пострадавших измеряется тысячами, сумма ущерба превышает несколько миллионов долларов.*

В остальном распределение по виновнику утечек в крупных компаниях мало отличается от аналогичного распределения в малом и среднем бизнесе.

> ***Вывод:***
>
> *Существенных отличий в распределении по виновным в компаниях СМБ и крупном бизнесе нет, что говорит о принципиальной схожести психологии и действий нарушителя либо халатного сотрудника, допустившего утечку. Это означает, что и подходы к защите информации, контролю доступа к данным в СМБ не должны серьезно отличаться от подходов, принятых в крупных корпорациях.*

Ключевой факт: в России почти две трети утечек происходят из небольших и средних компаний.

Интересно сопоставить картину утечек из небольших и средних компаний в нашей стране с общемировой статистикой. Так если в целом по миру доля компаний сегмента СМБ составляет в общей картине утечек 39,2%, для России этот показатель равен 61,2% (см. Рисунок 9).

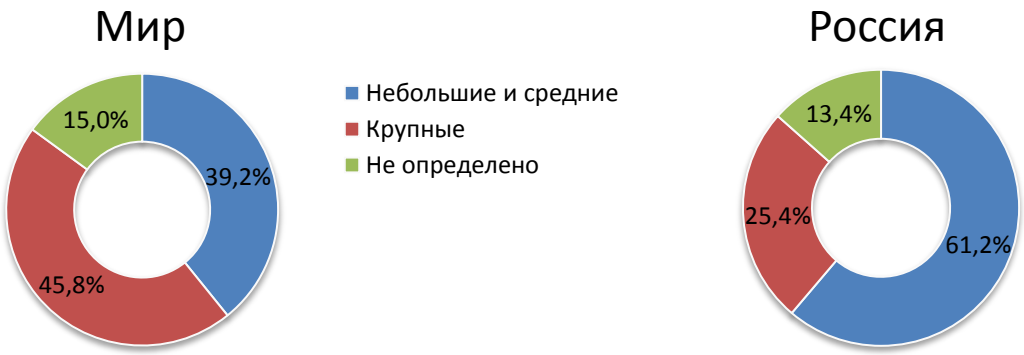


Рисунок 9. Распределение утечек по размеру компании. Доли. Мир, Россия.

Еще более примечательна ситуация с защитой персональных данных в нашей стране. В 2013 году на долю небольших операторов персональных данных пришлось до 66% всех утечек[18].

Интересно, что доля утечек с ущербом, свыше 10 тыс. руб., (на диаграмме крупный ущерб – см. Рисунок 10) в среднем бизнесе даже выше, чем в больших корпорациях.

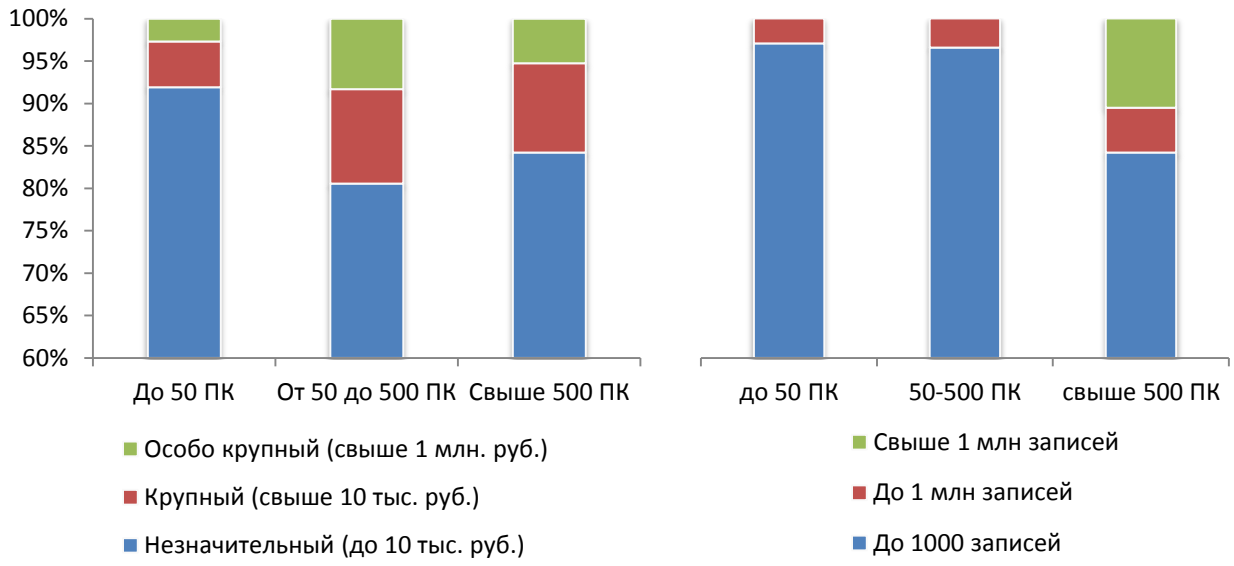


Рисунок 10. Картина утечек. Распределение по размеру компаний. Россия. Доли.

[18] Безопасность персональных данных в России в 2013 году. Статистика утечек. Отраслевые особенности. http://www.infowatch.ru/analytics/reports/5538

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 ущерб, который в ряде случаев более ощутим, чем в крупных компаниях. В таких отраслях, как торговля, туризм, где и представлены в основном небольшие организации, утечка базы данных клиентов, например, может привести к ущербу, сопоставимому с оборотом 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.

Заключение и выводы

Вопрос защиты информации для малого и среднего бизнеса сегодня не менее актуален, чем для крупного. Ущерб от утечек ноу-хау, коммерческой тайны, персональных данных сотрудников и клиентов компаний, зачастую, сопоставим с показателями оборота компании за несколько месяцев. Между тем, надежность защиты конфиденциальной информации в сегменте СМБ по-прежнему оставляет желать лучшего.

Высокий процент утечек «неопределенного» типа в распределении по умыслу в небольших и средних компаниях однозначно говорит о «недовооруженности» организаций в техническом плане. Службам информационной безопасности (в тех компаниях, где они есть) или ИТ-специалистам не хватает инструментов и знаний для своевременного обнаружения, предотвращения, расследования утечек. Налицо значительное отставание компаний сегмента СМБ от крупного бизнеса и в плане общей зрелости, понимания, что и от кого следует защищать. Возможно, одна из причин – недостаток финансирования направления информационной безопасности в средних и малых компаниях.

В ряде стран к защите персональных данных предъявляются особые требования, вопрос регулируется на государственном уровне. Но даже этот вид информации в средних и малых компаниях защищается плохо. Доля утечек персональных данных в общей картине утечек из СМБ-компаний драматически высока.

Небольшие компании остаются «слабым звеном» в плане защиты информации. Между тем в среднем бизнесе утечка зачастую приводит к более критичным последствиям – доля материальных потерь (относительно оборота) вследствие утечки в небольших компаниях даже выше, чем в сегменте крупных организаций.

Изменить ситуацию к лучшему можно лишь в случае появления простых и недорогих решений для защиты информации, ориентированных исключительно на СМБ-

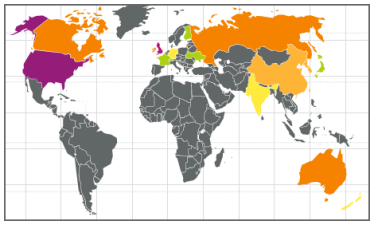
сегмент. Важно, чтобы такое решение работало точечно, по наиболее «популярным» каналам утечки и группам сотрудников, имеющих доступ к информации.

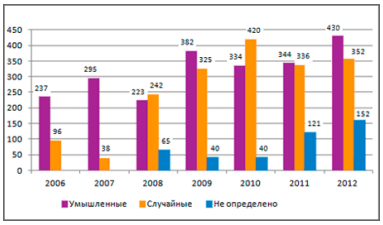
Не менее актуален вопрос просвещения персонала и руководителей средних и малых организаций. Пока, к сожалению, ни бизнес-руководство, ни технический персонал СМБ-компаний не видит связи между утечкой данных и убытками для бизнеса.

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 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.*

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.*