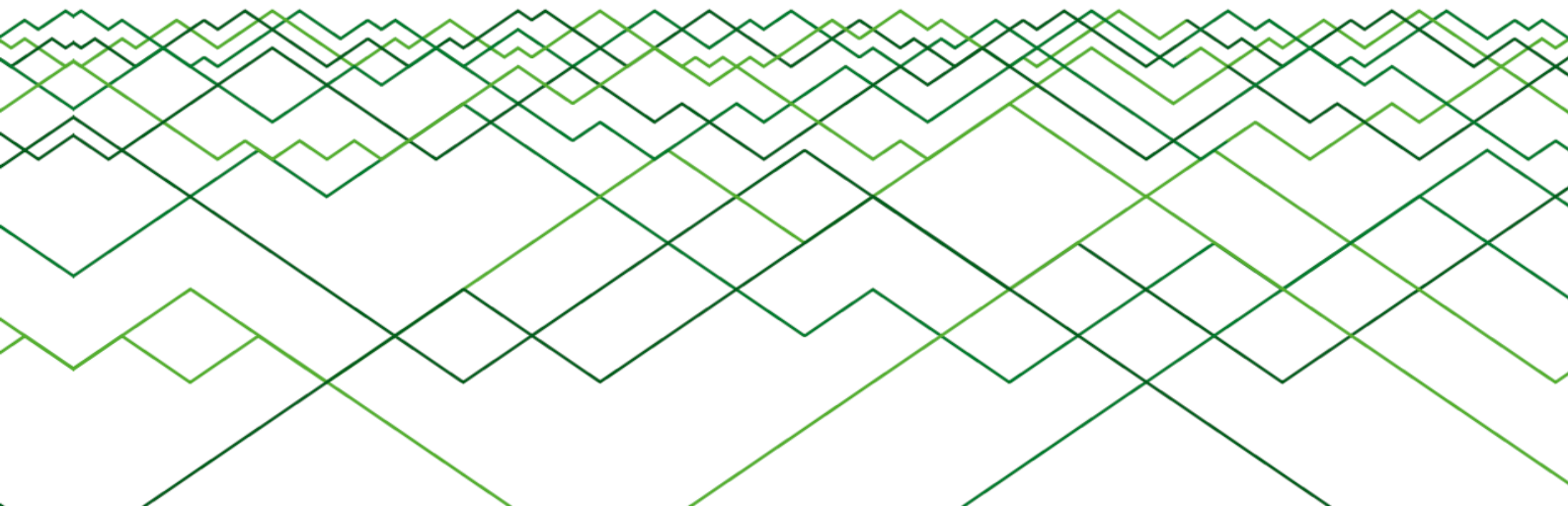
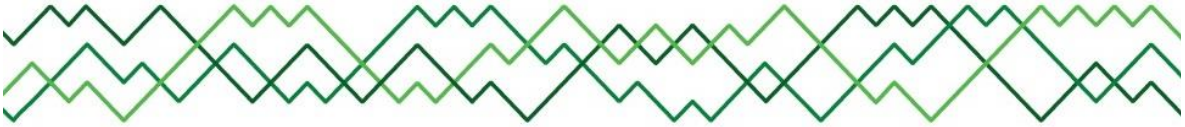
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Аналитический центр InfoWatch
www.infowatch.ru/analytics

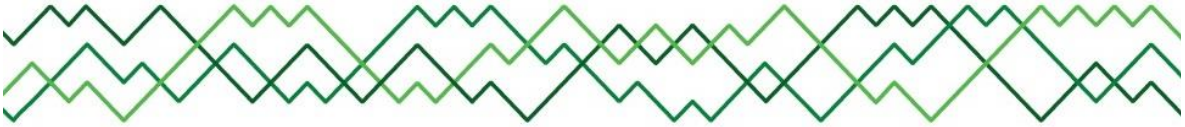
Исследование утечек информации в компаниях сектора «Высокие технологии» в 2016 году





INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

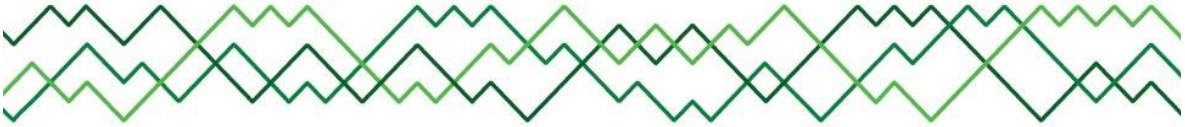
Оглавление



INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Только цифры

- ✓ В 2016 году Аналитическим центром InfoWatch во всем мире зарегистрирован **231** случай утечки конфиденциальной информации из компаний сегмента «Высокие технологии», что на **27%** превышает количество утечек, зарегистрированных в данной отрасли в 2015 году.
- ✓ Объем скомпрометированных записей в сегменте вырос более чем в **8 раз.**
- ✓ Доля утечек информации из высокотехнологичных компаний составила **14,9%** в общем распределении утечек. При этом на эти же компании пришлось **73%** скомпрометированных во всем мире записей.
- ✓ **90,9%** утечек в рассматриваемом сегменте были связаны с компрометацией персональных данных и платежной информации.
- ✓ В 2016 году в отрасли была зафиксирована **31** «мега-утечка», в результате каждой из которых «утекло» не менее **10 млн** единиц персональных данных. Совокупно на «мега-утечки» пришлось **96,6%** всех скомпрометированных записей.



Аннотация

Аналитический центр компании InfoWatch представляет отчет об исследовании утечек конфиденциальной информации в сегменте «Высокие технологии» (производители программного и аппаратного обеспечения, операторы связи, интернет-провайдеры, поисковые системы, социальные сети, ИТ-сервисы).

По итогам 2016 года мы зафиксировали взрывной рост объема утекших данных в рассматриваемой отрасли. В результате на высокотехнологичные компании пришлось почти три четверти всей скомпрометированной в мире информации.

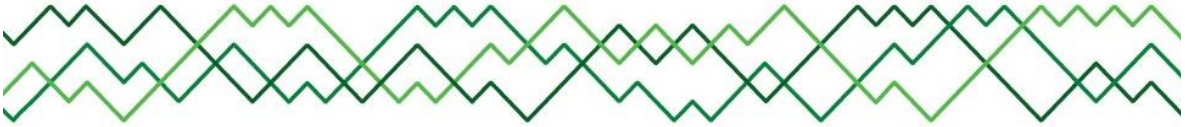
2016 год стал периодом атак на социальные сети и интернет-сервисы. В результате внешнего воздействия похищены данные сотен миллионов пользователей таких ресурсов, как Facebook, Foursquare, GitHub, iCloud, LinkedIn, MySpace, Snapchat, Telegram, Tumblr, Twitter, Yahoo. Кроме того, хакеры с успехом для себя атаковали все крупнейшие почтовые сервисы – Google (Gmail), Mail.ru, Microsoft (Hotmail), Yahoo. Досталось и телекоммуникационным компаниям. Злоумышленники похищали данные клиентов Deutsche Telekom, Three UK, Verizon и других операторов.

Львиная доля информации из высокотехнологичных компаний утекла в результате неправомерных действий внешних злоумышленников. Однако влияние внутреннего фактора не следует недооценивать. Например, в июне 2016 года сотрудник чешского подразделения T-Mobile похитил данные 1,5 млн клиентов с целью продажи. Случай с T-Mobile – это напоминание о том, что преступников интересует любые данные, которые легко конвертируются в денежные средства.

Не имея адекватных средств защиты от инсайдеров, компания рискует потерять очень многое. Для высокотехнологичных компаний информация, в том числе клиентская, - это ключевой актив. Поэтому любая утечка оказывается весьма чувствительной для бизнеса. По данным исследования Ponemon Institute и IBM, средний ущерб телекоммуникационных и ИТ-компаний составляет, соответственно, $150 и $165 в расчете на одну потерянную или украденную запись, что выше среднего показателя по всем отраслям. Таким образом, любая массовая утечка в сегменте «Высокие технологии» почти наверняка означает многомиллионный ущерб, не считая негативного влияния на репутацию – актив, который можно скрупулезно собирать долгие годы, а растерять за один день.

О масштабах косвенных финансовых потерь от компрометации данных можно судить на примере Yahoo, владельцы которой недополучили $350 млн из-за появившейся на рынке информации о массовых утечках в компании.

Авторы исследования считают, что его результаты будут полезны различным категориям читателей: практикующим специалистам в области информационной и экономической безопасности; собственникам и руководителям компаний, чья деятельность предполагает взаимодействие с информацией ограниченного доступа (коммерческая, банковская, налоговая тайна), иными ценными информационными активами; журналистам и аналитикам в области ИБ; всем, кто интересуется темой защиты информации и предотвращения утечек конфиденциальных данных.



Методология

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

База утечек InfoWatch насчитывает несколько тысяч инцидентов. В ходе наполнения базы каждая утечка (если возможно и такая информация есть в сообщении об утечке) классифицируется по ряду критериев: размер организации[5] , сфера деятельности (отрасль), размер ущерба[6], тип утечки (по умыслу), канал утечки[7] , типы утекших данных.

Исследование охватывает не более 1%[8] случаев от предполагаемого совокупного количества утечек. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества (категории) содержали достаточное или избыточное число элементов (фактических случаев утечки). Такой подход к формированию поля исследования позволяет считать получившуюся выборку достаточной для выявления и прогнозирования закономерностей на всей совокупности утечек.

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

---

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

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

[3] Утечки данных разделяются на умышленные (злонамеренные) и неумышленные (случайные) в зависимости от наличия или отсутствия умысла у лица, которое спровоцировало утечку данных. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы.

[4] В данном исследовании авторы представляют картину утечек в разрезе виновных лиц. Наряду с внутренними нарушителями, в данную классификацию попадает внешний нарушитель.

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

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

[7] Под каналом утечки мы понимаем такой сценарий (действия (или бездействие) пользователя корпоративной информационной системы, направленные на оборудование или программные сервисы), в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. Классификация каналов утечек приведена в глоссарии.

[8] С вероятностью, для России доля зафиксированных утечек от общего числа утечек, случившихся в нашей стране, значительно (на несколько порядков) меньше 1%.

INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Результаты исследования

В 2016 году Аналитическим центром InfoWatch был зарегистрирован 231 случай утечки конфиденциальной информации из компаний, принадлежащих к отраслевой группе «Высокие технологии» (см. Рисунок 1). В результате утечек было скомпрометировано более 2,29 млрд записей персональных данных (записей ПДн), — почтовые и электронные адреса, номера социального страхования, реквизиты платежных карт и иная критически важная информация.

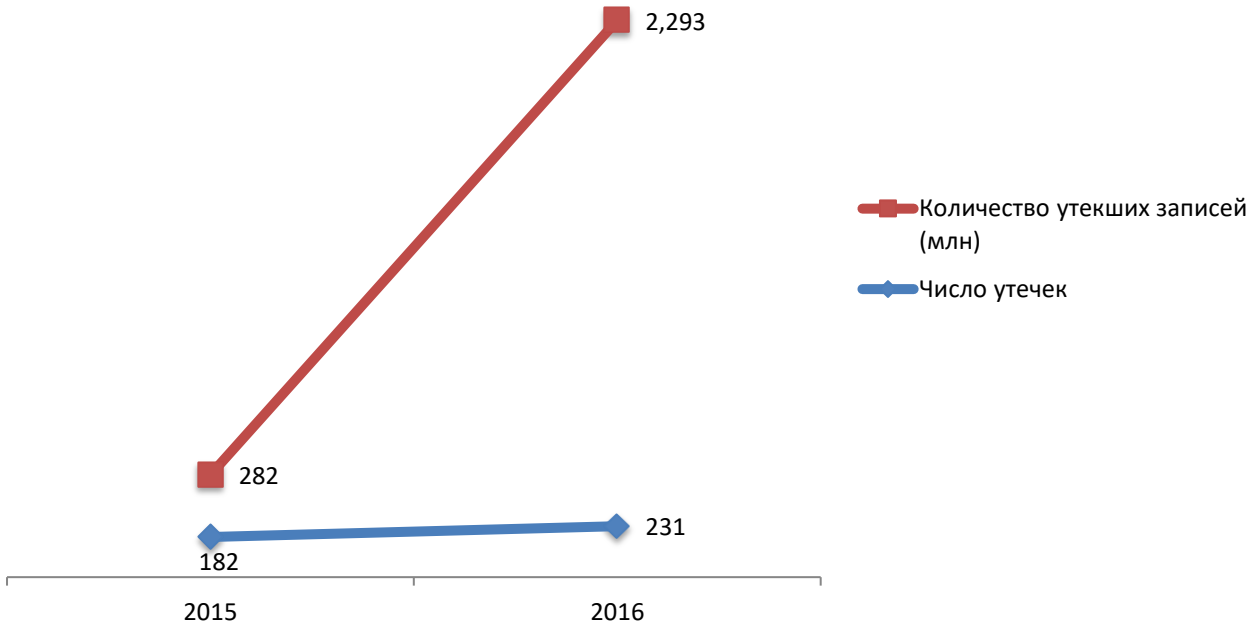


Рисунок 1. Число утечек информации и объем персональных данных, скомпрометированных в высокотехнологичных компаниях, 2015-2016 гг.

По сравнению с 2015 годом число утечек увеличилось на 26,9%, при этом объем скомпрометированных записей вырос на 713%. Доля высокотехнологичного сегмента в общем распределении инцидентов за год выросла с 12,1% до 14,9% (Рисунок 2).

С точки зрения потерь информации наиболее масштабными инцидентами в 2016 году были хакерские атаки на социальные сети и интернет-сервисы. Злоумышленники не преминули нанести удары по компаниям с огромными базами клиентской информации, отыскав слабые места в системах безопасности.

> *Ars Technica: Сайт знакомств для взрослых AdultFriendFinder.com был взломан, скомпрометированы аккаунты более 400 млн человек. Взломанная база включает адреса электронной почты, последние IP-адреса для входа на сайт, а также пароли.*

Рисунок 2. Распределение долей утечек, 2015-2016 гг.

В 2015 году на долю высокотехнологичных компаний пришлось 29% от совокупного объема скомпрометированных записей, а уже в 2016 году этот показатель составил 73% (Рисунок 3). Высокотехнологичные компании стали драйвером роста объема скомпрометированной информации во всем мире.

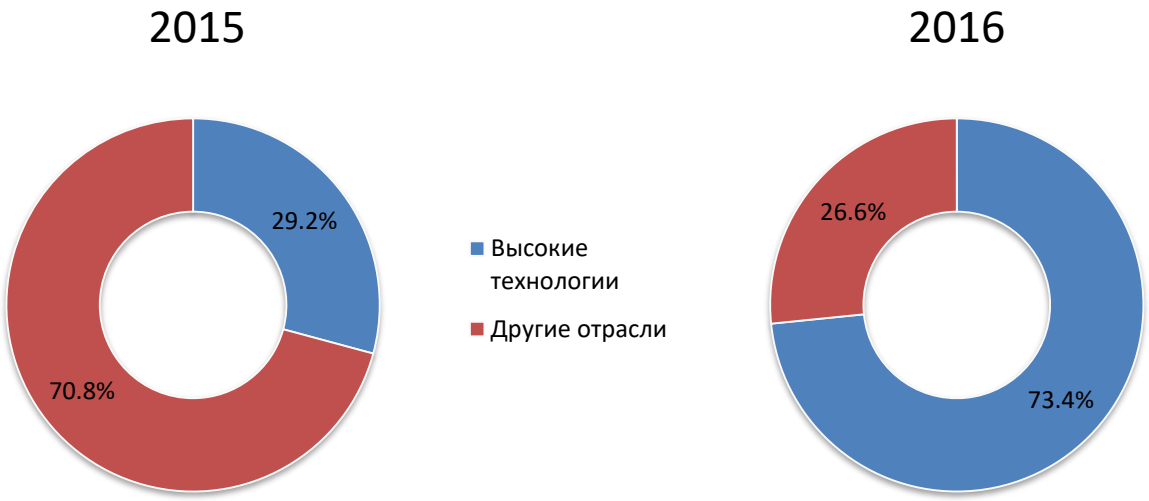


Рисунок 3. Доли скомпрометированных записей, 2015-2016 гг.

Взрывной рост объема утекшей информации на фоне относительно небольшого увеличения числа утечек свидетельствует о повышенном внимании злоумышленников, прежде всего организованных преступных групп, к обладателям обширных баз данных. Ценность информации в цифровую эпоху постоянно возрастает, а крупные клиентоориентированные ИТ-компании и операторы связи – это кладезь персональных данных.

Оценивая последствия утечек, можно отметить, что средний инцидент в ИТ и телекоме «потяжелел» в 6,4 раза и составил почти 10 млн записей (Рисунок 4). «Мощность» утечки по другим отраслям в среднем выросла только в 1,2 раза.

В исследуемом отраслевом сегменте за 2016 год зафиксирована 31 «мега-утечка» (более 10 миллионов скомпрометированных записей на инцидент — по классификации InfoWatch). На долю таких случаев пришлось 96,6% всех скомпрометированных в отрасли записей. Годом ранее среди высокотехнологичных компаний было зафиксировано девять «мега-утечек» с общей долей утекшей информации 81,8%.

Таким образом, именно масштабные инциденты в ИТ- и телекоммуникационных компаниях внесли решающий вклад в общий рост количества скомпрометированных данных во всем мире.

> *Daily Mail: Хакер Peace выставил на продажу в «даркнете» учетные данные 200 млн аккаунтов Yahoo. Данная информация включает имена и даты рождения пользователей, а также резервные адреса электронной почты. Изучение представленных образцов подтверждает, что многие аккаунты являются действующими. За весь «комплект» злоумышленник хочет сумму в биткойнах, эквивалентную $1860.*

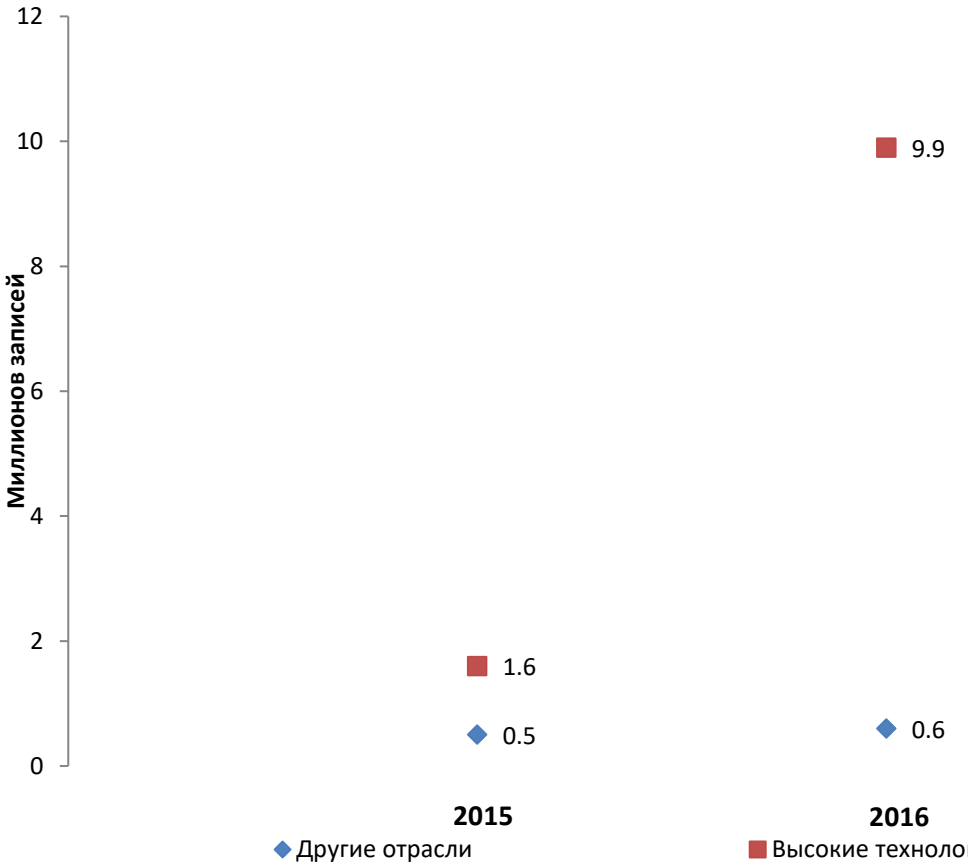


Рисунок 4. Величина средней утечки в ИТ и совокупности других отраслей, 2015-2016 гг.

«Работу» хакерам облегчают как компании, использующие ненадлежащие средства защиты, так и сами пользователи, не соблюдающие элементарные правила «информационной гигиены» и сопровождающие свои логины смехотворно простыми паролями.

> *vc.ru: В результате хакерской атаки на музыкальный сервис Last.fm были похищены более 43,5 млн логинов и паролей. Пароли пользователей были защищены с помощью алгоритма MD5, который легко взломать. Самым популярным паролем в LeakedSource назвали «123456». В топ-5 также вошли пароли «password» (92,6 тысячи), «lastfm» (66,8 тысячи), «123456789» (63,9 тысячи) и qwerty (46,2 тысячи).*

В 2016 году подавляющая доля утечек в рассматриваемой отрасли пришлась на персональные данные — 87% (Рисунок 5). Доли платежных данных и коммерческой тайны перераспределились главным образом из-за резкого роста утечек ПДн.

Рисунок 5. Распределение утечек по типу информации, 2015-2016 гг.

Всплеск числа инцидентов, в которых основным объектом выступают персональные данные, подтверждает высокую ликвидность этого типа информации на черном рынке. Причем охотятся за ней как внешние злоумышленники, так и внутренние нарушители. Обострение проблемы утечек ПДн говорит о недостаточном уровне защиты информации со стороны многих высокотехнологичных компаний.

Персональные данные — лакомый объект для злоумышленников в цифровую эпоху. Эта информация обладает высокой ликвидностью на черном рынке, так как легко монетизируется. Личные данные востребованы не только рекламными агентами и поставщиками различных услуг, они все чаще используются для совершения финансовых преступлений и «кражи личности» — получения материальной выгоды за счет использования информации других людей.

> *SecurityLab.ru: Бизнес-подразделение компании Verizon стало жертвой утечки данных. По сведениям независимого ИБ-исследователя Брайана Кребса, в руки злоумышленников попала информация 1,5 млн клиентов Verizon*

Enterprise Solutions. Данные пользователей выставлены на продажу на одном из подпольных киберфорумов по цене $100 тыс.

Если в 2015 году преобладали утечки, связанные с активностями внутренних нарушителей, то в 2016 году большинство инцидентов произошло в результате умышленных действий внешних сил (Рисунок 6). В общем распределении других отраслей соотношение внешних и внутренних нарушений за год практически не изменилось — по вине внутренних злоумышленников по-прежнему происходит примерно 2/3 утечек.

Мы ожидаем, что влияние внешних нарушителей в ИТ- и телекоммуникационных компаниях будет только расти в ближайшие годы. Насколько эффективным будет противоядие деструктивным силам — зависит от скорости принятия решений по совершенствованию средств информационной безопасности, от своевременного выделения бюджетов на внедрение решений, актуальных существующим угрозам.

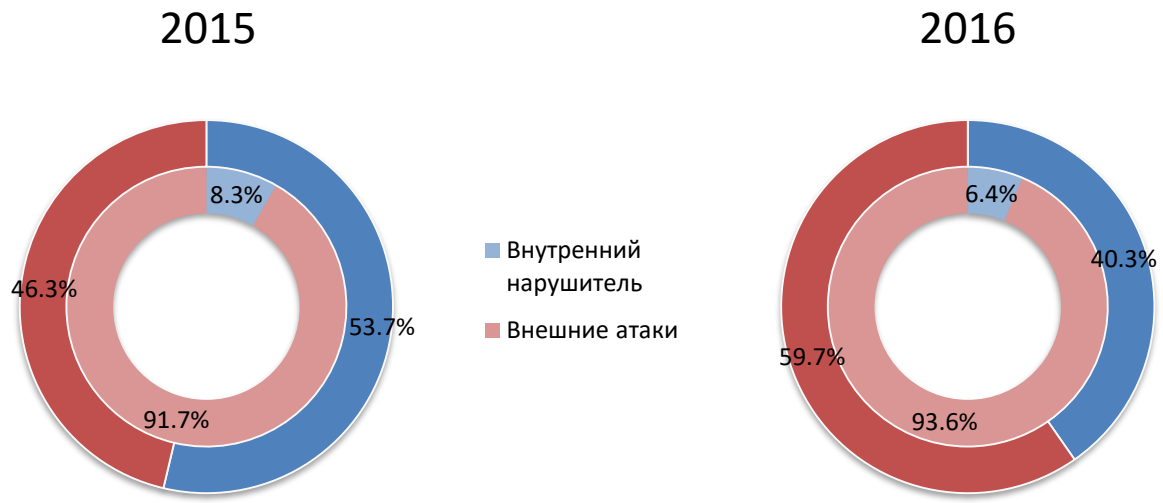


Рисунок 6. Распределение по вектору воздействия, 2015-2016 гг. Внешний круг — число утечек, внутренний круг – объем скомпрометированных записей.

В 2016 году произошла компрометация сотен миллионов аккаунтов крупнейших почтовых служб. Учитывая то, что многие пользователи используют одинаковые учетные данные для регистрации на разных сервисах, в том числе финансовых, последствия инцидента могли быть еще более масштабными. Элементарные и одинаковые пароли — это всегда отложенная угроза, пренебрежение правилами защиты информации влечет самые непредсказуемые последствия — неприятные инциденты могут случиться в любое время.

Reuters: Украдены 272,3 млн учетных записей электронной почты. Аккаунты в основном принадлежат пользователям самого популярного в России почтового сервиса Mail.ru, в меньшей степени инцидент затронул пользователей сервисов Google, Yahoo и Microsoft.

Более 93% данных из высокотехнологичных компаний утекает в результате атак внешних злоумышленников. Если взглянуть на общую картину по другим отраслям, то

там доли утечек под воздействием внутреннего нарушителя и внешнего злоумышленника составили, соответственно, 46% и 54%.

Кибератаки — это бич для любого бизнеса. Представленные данные подтверждают, что для представителей ИТ- и телекома, обладающих большими массивами данных, действия хакеров несут чрезвычайно разрушительные последствия.

В секторе «Высокие технологии» в 2016 году объем данных, скомпрометированных умышленно, рос опережающими темпами по сравнению с непреднамеренными случаями. При этом в совокупности других отраслей отмечена противоположная картина — значительно чаще информация стала утекать в результате случайных действий (сотрудник ошибочно отправил базу данных третьим лицам, системный администратор неверно настроил сервер и т.д.).

> *HackRead: В мессенджере Telegram появился чат-бот, который по запросу выдавал информацию о более чем 20 млн абонентов IranCell, второго по величине оператора мобильной связи в Иране. Вписав номер телефона, можно было узнать имя и фамилию абонента, а также его почтовый индекс, город и другую информацию. Чат-бот был заблокирован через 20 часов.*

Рост доли внутренних утечек умышленного характера в высокотехнологичном сегменте — тревожный симптом, который может свидетельствовать о том, что в компании намеренно проникают люди, целью которых является добыча ПДн и другой востребованной на черном рынке информации (Рисунок). Находящегося внутри периметра нарушителя очень сложно вычислить без DLP-систем, поэтому компании, не обладающие современными средствами противодействия таким злоумышленникам, очень сильно рискуют.

> *Times of India: Сотрудник ИТ-компании Daffodil Software был уличен в хищении коммерческой информации и продаже ее конкурентам. Даже после увольнения он продолжал использовать полученные данные для личной выгоды.*

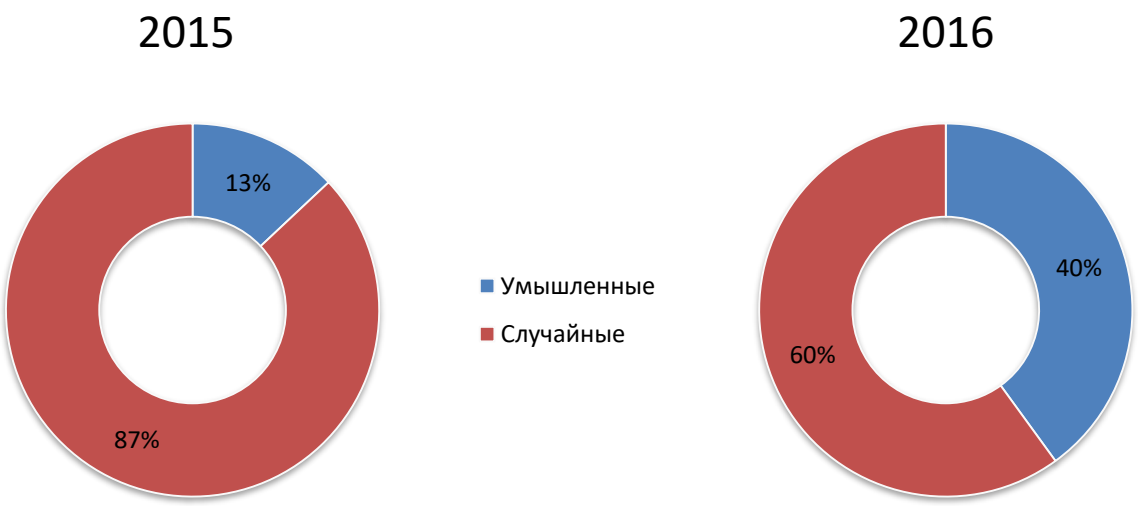


Рисунок 7. Распределение внутренних утечек по характеру умысла, 2015-2016 гг.

По итогам 2016 г. более 73% внутренних случаев компрометации данных в ИТ-отрасли приходятся на преднамеренные и случайные утечки (Рисунок), 12% инцидентов сопряжены с мошенническими действиями, а 14,5% классифицированы как нарушения, связанные с несанкционированным доступом к информации (превышение прав доступа, манипуляция с информацией, которая не требуется сотруднику для выполнения служебных обязанностей).

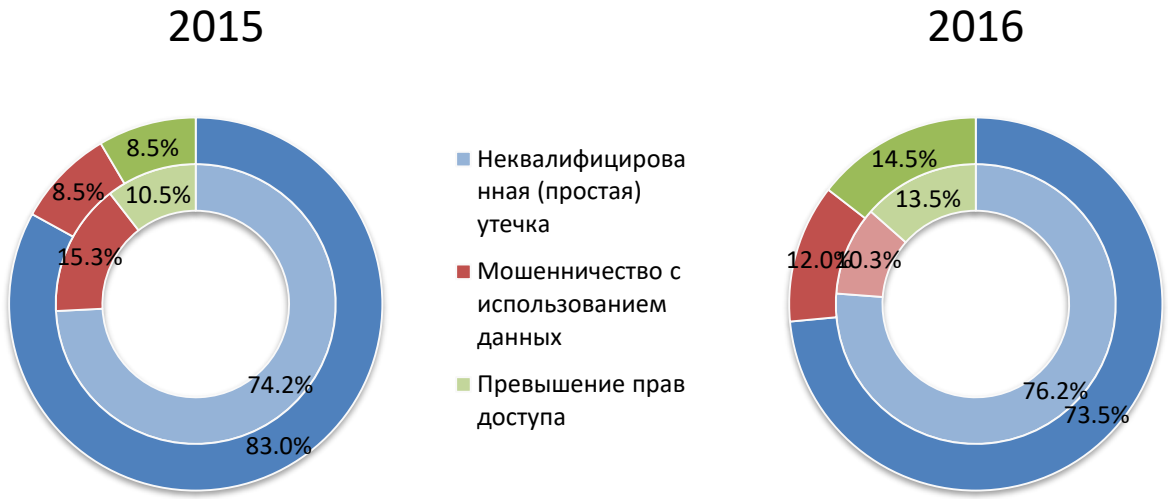


Рисунок 8. Доли инцидентов по характеру, 2015-2016 гг. Внешний круг – высокотехнологичные компании, внутренний круг — предприятия из других отраслей.

Таким образом, среди компаний, работающих в области высоких технологий, за год выросла доля так называемых «квалифицированных утечек» — случаев, когда сотрудники намеренно используют свое привилегированное положение для кражи информации или нелегитимно получают доступ к базам данных.

> *The Times of India: Полиция Чатуранги в Индии арестовал троих должностных лиц, которые подозреваются в краже данных и жизненно важной корпоративной информации молодой ИТ-компании Technovate Consultancy Services. Они собирались инвестировать в стартап, но вместо этого взломали сервер компании. Используя полученную информацию злоумышленники стали предлагать клиентам собственные продукты.*

Существенный рост доли умышленных утечек, совершенных сотрудниками и допущенными в пределы периметра подрядчиками, наряду с возросшим деструктивным влиянием привилегированных пользователей, говорят о том, что имеющегося арсенала средств борьбы с внутренними нарушителями уже явно недостаточно для высокотехнологичных компаний.

Сама специфика ИТ-, телеком-, интернет-компаний предполагает, что в них работают много технически подкованных специалистов. Соответственно, здесь гораздо выше риск несанкционированного извлечения данных из корпоративных информационных

систем, а значит, требуются более продвинутые решения для противодействия внутренним нарушителям.

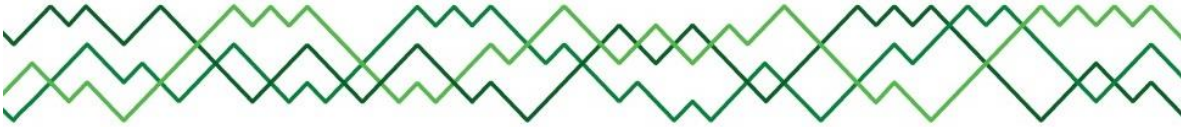
В высокотехнологичном сегменте, как и в общем распределении других вертикалей, доля инцидентов, сопряженных с компрометацией персональных данных, значительно выросла и составила около 87% (*Рисунок*).

Рисунок 9. Распределение утечек по основным типам данных, 2015-2016 гг. Внешний — высокотехнологичные компании, внутренний круг — предприятия из других отраслей.

Вместе с тем, в общем «пироге» произошло существенное снижение долей утечек платежной информации и коммерческих секретов.

> SecurityLab.ru: *Крупнейший оператор сотовой связи в Великобритании Three UK сообщил о несанкционированном проникновении в базу данных клиентов, которые могли получить новые телефоны по программе обмена. Предположительно, в результате хакерской атаки могли быть украдены персональные данные порядка 6 млн клиентов, сообщает The Daily Mail.*
>
> *Согласно заявлению представителей компании, скомпрометированная информация включает имена, номера телефонов, адреса и даты рождения. Получить доступ к данным о платежах, банковских счетах или номерах кредитных карт хакерам не удалось. По сведениям Three UK, злоумышленники смогли проникнуть в клиентскую базу данных при помощи логина и пароля одного из сотрудников компании.*

События 2016 г. демонстрируют резко возросший интерес злоумышленников к личной информации. В цифровую эпоху, по мере развития электронных услуг и удобных способов монетизации, этот вид данных становится все более ликвидным товаром. Судя по всему, компании отрасли «Высокие технологии» пока не могут найти эффективное средство для противодействия охотникам за персональными данными.



Заключение и выводы

Хакеры проводят «большую охоту» за ликвидной информацией высокотехнологичного сегмента, и под прицелом может оказаться любая компания. Если в 2015 г. злоумышленники часто атаковали телекоммуникационное направление, то в 2016 г. основной мишенью стали компании, работающие в Интернете: социальные сети, сайты знакомств, поисковые системы, веб-сервисы. Высокотехнологичные компании обладают огромными массивами информации, в том числе очень чувствительной для клиентов и бизнеса. Поэтому именно рассматриваемая отрасль наиболее привлекательна для злоумышленников. Динамика роста объема утекших данных в ИТ-компаниях в 2016 г. задавала тон в увеличении количества скомпрометированной информации во всем мире.

Увеличение числа атак на ИТ-сервисы напрямую связано с возросшей ценностью корпоративных и клиентских данных. Особую тревогу вызывает резкий рост объемов скомпрометированных персональных данных. Таким образом, сильный удар получает не только сама компания, допустившая утечку, но и ее клиенты: в лучшем случае личная информация может войти в базы операторов спам-рассылок, а в худшем, и это с каждым годом все более вероятно, может быть использована мошенниками, в том числе с целью совершения «кражи личности», то есть извлечения выгоды с использованием идентификаторов другого человека.

Агрегируя большие объемы пользовательских данных, игроки ИТ-рынка охотно используют технологии анализа структурированной и неструктурированной информации – Big Data и другие средства, технологический уровень и функционал которых в последнее время существенно вырос. Но по мере увеличения объемов генерируемой, обрабатываемой и хранимой информации повышаются риски внешних атак на корпоративные ресурсы. Одновременно с этим растет влияние внутренних нарушителей, а значит, ИТ-компаниям требуются не только эффективные средства защиты от хакеров, но и современные многофункциональные системы предотвращения утечек информации (DLP). А в связи с опережающим ростом числа квалифицированных инцидентов, то есть утечек, сопряженных с мошенническими действиями и превышением прав доступа, необходимо задуматься о включении в арсенал бизнеса решений для поведенческого анализа пользователей.

Судя по всему, высокотехнологичный сегмент, продвинутый в технологическом плане, пока не смог обеспечить соответствующий вызовам времени уровень информационной безопасности. ИТ-сфера как локомотив «цифровой экономики» может резко снизить эффективность своей работы, рискует оказаться наиболее проблемным элементом новой экономической системы.

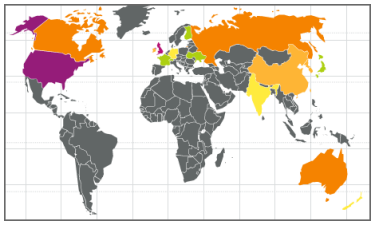
Информация как высоколиквидный актив требует многоуровневых систем защиты. В условиях комплексного характера угроз неразумно полагаться исключительно на технологии (средства ИБ) и не заботиться о повышении культуры обращения с конфиденциальной информацией среди сотрудников.

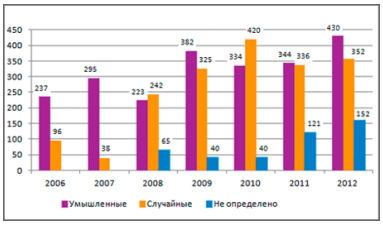
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Мониторинг утечек на сайте InfoWatch

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

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



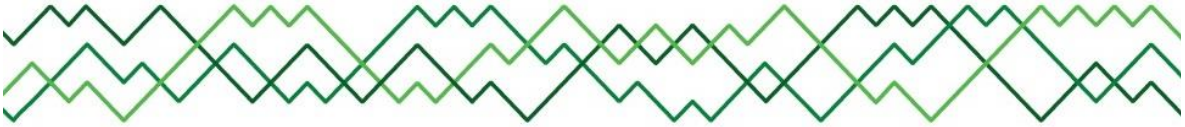


Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Twitter
- RSS

Аналитический центр InfoWatch

www.infowatch.ru/analytics



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».*