Утечки конфиденциальных данных коммерческих компаний и государственных организаций, произошедшие по вине или неосторожности внутреннего нарушителя. Сравнительное исследование. 2013-2017 гг.

# Оглавление

[Оглавление 2](#_Toc528251546)

[Только цифры 3](#_Toc528251547)

[Аннотация 4](#_Toc528251548)

[Методология 5](#_Toc528251549)

[Результаты исследования 7](#_Toc528251550)

[Заключение и выводы 19](#_Toc528251551)

[Мониторинг утечек на сайте InfoWatch 20](#_Toc528251552)

[Глоссарий 21](#_Toc528251553)

# Только цифры

* В 2017 году Аналитический центр InfoWatch зафиксировал **1228** утечек, случившихся в мире по вине или неосторожности внутренних нарушителей — сотрудников организаций, топ-менеджеров и иных привилегированных пользователей, подрядчиков.
* На утечки, случившиеся в результате умышленных или непредумышленных действий внутренних нарушителей, приходится 58% от общего числа утечек. В результате таких инцидентов скомпрометировано **4,7 млрд** записей, относящихся к типу персональных данных и финансовой информации.
* Объем данных, скомпрометированных по вине внутреннего нарушителя, показал **10-кратный рост** к показателям 2016 года. На одну утечку в среднем приходится 3,8 млн скомпрометированных записей.
* **95%** от совокупного объема персональных данных и финансовой информации были скомпрометированы в результате небрежности либо грубой неосторожности лиц, имеющих легитимный доступ к указанным данным.
* На долю непривилегированных сотрудников приходится **75-85%** всех внутренних утечек из организаций.
* Доля «квалифицированных» утечек в целом не превышает **25%** в период 2013-2017 года и демонстрирует тенденцию к снижению.

# Аннотация

До недавнего времени наблюдался лавинообразный рост случаев компрометации информации, спровоцированных внешним воздействием. Конечно, хакеры и раньше взламывали системы защиты, проникали в коммуникационные сети, но никогда прежде внешние утечки не имели столь разрушительных последствий.

В 2017 году по вине внешнего злоумышленника [было скомпрометировано](https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2017_year.pdf?rel=1) 6,6 млрд записей. Тема внешних атак и утечек информации ограниченного доступа вошла в повестку президентской избирательной кампании в США и во многом предопределила ее результаты — уровень, немыслимый еще несколько лет назад.

Утечки внутреннего характера[[1]](#footnote-2), т.е. случаи компрометации информации ограниченного доступа в результате умышленных или неосторожных действий сотрудников и подрядчиков коммерческих и некоммерческих организаций, органов государственной и муниципальной власти, отошли на второй план, в том числе для практикующих специалистов в области информационной безопасности.

Поддавшись влиянию «магии цифр», многие «безопасники» вспомнили о концепции защиты периметра от внешних угроз и бросились бороться с хакерами, забыв при этом, что сотрудник, даже если он обучен и дисциплинирован, совершает ошибки. И эти ошибки могут привести к последствиям не менее серьезным, чем атака самых изощренных киберпреступников.

В последние несколько лет на фоне массовой компрометации данных пользователей сформировался нелегальный рынок, где можно купить и продать большие объемы информации. У людей, имеющих доступ к чужим персональным данным, появилась реальная возможность заработать на этом деньги. В этот «бизнес» бросились фитнес-тренеры, медсестры, преподаватели школ и вузов, сотрудники полиции, все, чья работа предполагает использование сведений о гражданах, иных ликвидных типов данных. Массовые утечки информации по вине внутреннего нарушителя породили волну исков к организациям, чьи сотрудники или подрядчики допустили нарушение. Как следствие, значение внутренних утечек вновь возросло.

Аналитический центр группы компаний InfoWatch представляет второе сравнительное исследование внутренних утечек, произошедших в период с 2013 по 2017 год. В рамках данного исследования мы попытались отразить актуальную картину происшествий, связанных с внутренними утечками, обозначить тенденции и векторы возможного развития этого типа угроз.

Авторы уверены, что выводы исследования будут интересны практикующим специалистам в области информационной и экономической безопасности организаций, журналистам, собственникам бизнеса и высшему руководству компаний, оперирующих информацией ограниченного доступа, включая коммерческую, банковскую тайны, а также другими ценными информационными активами.

# Методология

Исследование проводится на основе собственной базы данных, пополняемой специалистами Аналитического центра InfoWatch с 2004 года. В базу попадают публичные сообщения[[2]](#footnote-3) о случаях утечки[[3]](#footnote-4) информации из коммерческих, некоммерческих (государственных, муниципальных) организаций, госорганов, которые произошли вследствие умышленных или неосторожных действий[[4]](#footnote-5) сотрудников и иных лиц[[5]](#footnote-6). База утечек InfoWatch насчитывает несколько тысяч зарегистрированных инцидентов.

В ходе наполнения базы каждая утечка классифицируется по ряду критериев, таких как размер организации[[6]](#footnote-7), сфера деятельности (отрасль), размер причинённого ущерба[[7]](#footnote-8), тип утечки (по умыслу), канал утечки[[8]](#footnote-9), типы утекших данных, вектор воздействия[[9]](#footnote-10).

Инциденты также классифицируются по характеру действий нарушителя. Наряду с «простыми» утечками авторы исследования выделяют «квалифицированные» утечки: когда сотрудник, имеющий легитимный доступ к данным, использует полученные сведения в целях мошенничества (манипуляции с платежными данными, инсайдерской информацией); когда сотрудник получает доступ к данным, которые не требуются ему для исполнения служебных обязанностей (превышение прав доступа).

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 тренды — репрезентативными для генеральной совокупности.

При формировании диаграмм по отдельным разрезам из выборки исключены утечки, классифицированные по основному критерию разреза как неопределенные[[10]](#footnote-11). Кроме того, все диаграммы в данном исследовании, если специально не оговорено иное, содержат сведения исключительно о внутренних утечках.

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

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

# Результаты исследования

В 2017 году Аналитический центр InfoWatch зафиксировал рекордные 1228 утечек конфиденциальной информации, случившихся по вине или по неосторожности внутренних нарушителей — топ-менеджеров и иных привилегированных пользователей, сотрудников организаций, подрядчиков (далее — внутренние утечки). При этом устойчивого объяснимого роста или снижения числа утечек, спровоцированных внутренним нарушителем, в исследуемом периоде (в частности, с 2014 года[[11]](#footnote-12)) не наблюдается (см. Рисунок 1).

Рисунок 1. Число внутренних утечек информации, 2004 -2017 гг.

Скорее, можно говорить о несистемных колебаниях числа внутренних утечек на фоне постоянного (на горизонте 3-5 лет) роста количества утечек данных в целом.

Доля внутренних утечек в распределении утечек по вектору воздействия[[12]](#footnote-13) три года подряд снижалась, затем в 2017 г. она немного выросла. Если в 2014 году на долю внутреннего нарушителя приходилось около 73% от всех утечек информации ограниченного доступа, то в 2017 году доля внутренних утечек составила менее 58% (см. Рисунок 2).

Рисунок 2. Число внутренних утечек информации и доля утечек этого типа от общего числа утечек, 2013 - 2017 гг.

Если в количественном выражении число внутренних утечек в 2017 году выросло по отношению к 2016 году на 40%, то в процентном выражении доля этих утечек за тот же период увеличилась лишь на 2%. Очевидно, подобное несоответствие вызвано опережающим ростом числа утечек под воздействием внешнего злоумышленника по отношению к динамике внутренних утечек.

Объем скомпрометированных данных в расчете на одну утечку («мощность» утечки) для внутренних инцидентов в 2017 году составляет 3,8 млн записей, для внешних — 8,2 млн записей.

В 2017 году мы зафиксировали стремительный рост «мощности» утечек — совокупного объема скомпрометированных данных, разделенного на общее число утечек. До этого в течение трех лет данный показатель оставался достаточно стабильным — на уровне 0,6 млн скомпрометированных записей на один инцидент. Если «мощность» внутренней утечки в 2017 году выросла в 6,8 раза (см. Рисунок 3), то средняя «мощность» утечек в целом за тот же период увеличилась в 4,2 раза.

Рисунок 3. Объем данных в расчете на одну утечку, совершенную внутренним злоумылшенником, млн записей, 2013 - 2017 гг.

Следует учитывать, что в 2017 году наблюдался взрывной рост объема скомпрометированных записей как в результате действий внутреннего нарушителя, так и под воздействием извне. Но если совокупный объем данных, скомпрометированных в результате внешних утечек, вырос в 2,6 раза, то объем данных, скомпрометированных по вине внутреннего нарушителя, показал почти десятикратный рост (см. Рисунок 4).

Рисунок 4. Объем данных, скомпрометированных в результате утечек, совершенных внутренними нарушителями, млн записей, 2013 - 2017 гг.

Приведенные цифры подтверждают, что

***утечки, случившиеся в результате внутренних нарушений, сегодня ничуть не менее разрушительны (в плане возможных негативных последствий для владельцев информации), чем утечки внешние.***

Ранее эта мысль подкреплялась лишь практикой, и мы отмечали, что внутренний нарушитель может быть даже более опасен, чем самый изощренный хакер, в силу осведомленности о правилах хранения и обработки информации ограниченного доступа в своей организации, хорошем представлении о ценности тех или иных конфиденциальных данных.

Теперь тезис о сравнимом разрушительном эффекте действий внутреннего нарушителя и внешнего злоумышленника подтвержден наглядно — в 2017 году в результате умышленных действий и неосторожности внутренних нарушителей скомпрометирован лишь вдвое меньший объем данных, чем объем, скомпрометированный вследствие активности внешнего злоумышленника. Ранее (в 2014-2016 годах) этот показатель для утечек внешнего и внутреннего типа отличался на порядок в пользу внешних.

При этом следует помнить, что в случае с внешними утечками мы всегда говорим об умышленной компрометации данных, то есть весь объем утекших данных приходится на злонамеренные утечки. Если же рассматривать утечки, произошедшие по вине внутреннего нарушителя, то здесь подавляющая часть (67-95% на горизонте 5 лет) объема скомпрометированных данных приходится на случайные утечки. То есть здесь речь идет об ошибках персонала при пересылке почты, неверной конфигурации баз данных, облачных хранилищ и прочих инцидентах.

[calgaryherald.com](http://calgaryherald.com/news/local-news/class-action-lawsuit-claims-city-leaked-personal-information-of-3700-employees): Утечка персональных данных более 3700 муниципальных служащих может дорого обойтись властям города Калгари. В коллективном иске пострадавшие требуют от работодателя компенсацию в размере 92,9 млн долл. США. Утечка произошла в июне 2017 г., когда один из сотрудников городского совета в ответ на просьбу своего коллеги из другого муниципалитета отправил письмо, содержащее медицинские сведения, номера местной системы социального страхования, адреса, даты рождения и данные о доходах жителей города.

Примечательно, что объем данных, скомпрометированных в результате случайных утечек внутреннего плана, увеличивается. При этом доля случайных утечек от всего числа внутренних нарушений год от года уменьшается (к примеру, если в 2015 году около 80% всех утечек, совершенных внутренним нарушителем, были случайными, то в 2017 году доля таких утечек не превышает 66% — см. Рисунок 5).

Рисунок 5. Число и объем скомпрометированных данных в процентах от совокупного числа утечек внутреннего характера и совокупного объема данных, пришедшихся на утечки внутреннего характера, 2013 - 2017 гг.

Представляется очевидным, что именно случайные внутренние утечки являются основным и наиболее разрушительным фактором, который обусловливает ежегодный рост объема скомпрометированных данных.

Поскольку сам объем вычисляется суммированием скомпрометированных записей (персональные данные владельцев и, как правило, персонифицированная платежная информация) можно утверждать, что:

***практически весь объем персональных данных, утекший в 2013-2017 годах по вине внутреннего нарушителя, был скомпрометирован в результате небрежности либо грубой неосторожности (ошибок, невнимательности, несоблюдения регламентов).***

На практике это означает, что внутренний нарушитель, действуя с умыслом, довольно нечасто покушается на персональные данные. Когда это все же происходит, объем похищенной информации, как правило, оказывается сравнительно небольшим — только действительно ликвидные сведения. Например, недобросовестного менеджера интересуют данные о клиентах банка, на которых можно оформить кредит, сведения о поставщиках и подрядчиках компании-работодателя, которые можно «забрать с собой» при переходе в конкурирующую организацию.

[khaleejtimes.com](https://www.khaleejtimes.com/news/crime/bank-employee-causes-client-to-lose-dh11-million): 28-летняя уроженка Индии работала руководителем отдела продаж в одном из банков ОАЭ. Пользуясь своим положением, она копировала из электронной системы данные о клиентах (имена, даты рождения, состояние счетов и номера банковских карт), а затем передавала полученную информацию своему земляку. От действий преступной группы пострадали более 2500 клиентов банка, злоумышленникам удалось похитить со счетов порядка $300 тыс.

## Доля персональных данных, скомпрометированных умышленно, снижается

Следует отметить две показательные закономерности: доля умышленных утечек персональных данных в 2013-2017 годах снижается, при этом неуклонно растет доля умышленных утечек других типов данных: информации, составляющей коммерческую и государственную тайну, а также секретов производства и ноу-хау (см. Рисунок 6).

Рисунок 6. Распределение утечек по умыслу и типу данных, 2013 – 2017 гг.

В количественном измерении умышленных утечек персональных данных не становится меньше — если в 2014 году мы зафиксировали 175 таких утечек, то в 2017 году их было 194. Тот же тезис относится к случайным утечкам, например, информации, составляющей государственную тайну, — их число также не уменьшается. Происходит перераспределение долей умышленных и случайных утечек, причем за счет двух факторов — это рост активности внутренних злоумышленников, нацеленных на конкретный тип данных, и увеличение возможностей систем защиты от утечек.

***Злоумышленники все больше интересуются наиболее ликвидными типами данных — за счет этого растет доля зафиксированных умышленных утечек информации, составляющей государственную и коммерческую тайну. При этом действия злоумышленников все чаще фиксируются системами защиты, становятся достоянием общественности и, в итоге, попадают в нашу статистику.***

Эти две тенденции неплохо иллюстрирует общее распределение внутренних утечек по типам данных (см. Рисунок 7). На диаграмме видно, что доля утечек персональных данных сокращается за счет роста утечек других типов данных, в основном информации, составляющей коммерческую тайну.

Рисунок 7. Распределение «внутренних» утечек по типу данных, 2013 – 2017 гг.

Вместе с тем, персональные данные остаются основным типом информации, который подвергается компрометации. Поэтому имеет смысл рассмотреть распределение утечек персональных данных применительно к отраслевому разрезу.

На диаграмме распределения случайных утечек персональных данных заметно, что число случайных утечек ПДн, приходящихся на учреждения медицины и образования, на протяжении 2014-2017 годов неуклонно снижалось (см. Рисунок 8).

Рисунок 8. Распределение случайных утечек ПДн по отраслям, 2013 – 2017 гг.

Медучреждения остаются при этом основным источником персональных данных и иных сведений о субъектах. Предположительно это связано с относительно высокой ликвидностью данных, обрабатываемых в медучреждениях, а также с недостаточно надежной защитой этих данных.

[sixthtone.com](http://www.sixthtone.com/news/1000988/millions-of-citizens-data-sold-online-in-hangzhou%2C-police-find): Полиция Восточного Китая арестовала 39 человек, подозреваемых в незаконном получении и продаже личной информации более 3,7 миллионов граждан. Члены группировки участвовали в сборе больших объемов информации в Центре контроля и профилактики заболеваний (округ Гуаньчжоу). Известно, что часть персональных данных относилась к детям, подлежащим вакцинации. За каждую запись покупатели платили по 10 центов.

Вместе с тем растет число зафиксированных случайных утечек в иных отраслях, в том числе в государственных и муниципальных органах, где направление информационной безопасности зачастую совершенствуется довольно медленно.

[standard.co.uk](https://www.standard.co.uk/news/london/islington-council-faces-huge-fine-after-massive-data-breach-hit-90000-people-a3613981.html): Совет округа Ислингтон, что на севере Лондона, признан виновным в нарушении защиты информации почти 90 тыс. человек. Чиновники не обеспечили безопасность транспортного приложения и теперь должны будут заплатить 56 тыс. фунтов. Транспортное приложение аккумулировало различную информацию, включая данные об автомобиле, имя и адрес водителя, а также медицинские и финансовые сведения. К этим данным мог получить доступ любой желающий, скорректировав адрес в строке браузера.

Вероятно, такое изменение связано не только с возросшим количеством утечек в сегментах, отличных от медицины и образования, но и с ростом уровня защищенности персональных данных в целом. Известно, что системы защиты от утечек (особенно в случае формализуемых и простых для распознавания типов данных, к которым относятся ПДн) сравнительно неплохо справляются со своей задачей. Поэтому нельзя исключать, что

***наблюдаемый во всех отраслевых сегментах количественный рост утечек ПДн может быть связан с повсеместным внедрением систем защиты.***

Косвенно такой вывод подтверждается тем, что и для умышленных утечек информации, составляющей коммерческую тайну и для ноу-хау, наблюдается сходная картина — если раньше умышленные утечки таких типов данных фиксировались лишь в отдельных отраслях, то в 2017 году умышленные утечки коммерческой тайны и ноу-хау зарегистрированы во всех исследуемых сегментах (см. Рисунок 9).

 Рисунок 9. Распределение умышленных утечек коммерческой тайны и ноу-хау по отраслям, 2013 – 2017 гг.

Таким образом, есть все основания полагать, что

***развитие и повсеместное внедрение систем защиты данных от утечек позволило выявить и вывести из тени те утечки, которые ранее происходили в отдельных отраслях, но не фиксировались.***

## Наиболее «проблемное» звено в безопасности данных — сотрудник компании

Статистика инцидентов в количественном выражении свидетельствует, что наиболее «проблемным» звеном в системе информационной безопасности является сотрудник компании. На долю этого нарушителя приходится 75-85% всех внутренних утечек (см. Рисунок 10).

Рисунок 10. Распределение «внутренних» утечек по виновнику, 2013 – 2017 гг.

Применительно к распределению внутренних утечек по виновнику наиболее актуальной на сегодня выглядит проблема так называемого «привилегированного пользователя» — сотрудника, чьи права доступа к информации, обрабатываемой в компании, практически не ограничены, при этом контроль действий такого сотрудника не организован либо осуществляется не в полном объеме. Как правило, к привилегированным пользователям относят топ-менеджмент компаний и организаций, системных администраторов и приравненных к ним сотрудников (в том числе офицеров безопасности).

В 2017 году на долю привилегированных пользователей пришлось 8,5% от всех умышленных внутренних утечек (см. Рисунок 11).

Рисунок 11. Доля умышленных утечек в разбивке по обычному и привилегированному пользователю, 2013 - 2017 гг.

С большой вероятностью, доля умышленных утечек, спровоцированных привилегированным пользователем, будет расти. Сообщения СМИ полны историй о нелегитимных действиях высших руководителей, причем не только в коммерческом секторе, но и в сфере государственного управления.

[straitstimes.com](http://www.straitstimes.com/singapore/courts-crime/lawyer-faces-fine-for-leaking-client-data-to-lover): В Сингапуре помощник руководителя юридической фирмы Райан Линь (Ryan Lin) предстал перед судом профессионального сообщества и был признан виновным в отправке посредством WhatsApp конфиденциальных данных женщине, с которой он состоял в любовной связи. По итогам разбирательства нарушитель оштрафован на $7 тыс.

Топ-менеджмент и иные лица с неограниченным доступом к информационным активам компаний намного чаще, чем рядовые сотрудники, допускают умышленные утечки. Так в 2017 году лишь каждая четвертая утечка, спровоцированная рядовым сотрудником, оказалась умышленной, в то время как утечки, спровоцированные привилегированными пользователями, носили умышленный характер в 38,5% случаев (см. Рисунок 12).

Рисунок 12. Доля умышленных утечек от общего числа утечек в распределении по обычному и привилегированному пользователю отдельно, 2013 - 2017 гг.

Определенные надежды связаны с тем, что доля умышленных утечек и для обычных сотрудников, и для привилегированных пользователей снижается.

Следует помнить, однако, что умышленные утечки отличает большая латентность (по сравнению со случайными утечками). Сообщения об умышленных утечках реже оказываются в центре внимания СМИ. Даже при наличии законодательно установленной обязанности сообщать о фактах утечек данных, не каждая компания готова «вынести сор из избы», то есть признать кражу коммерческих секретов и другой конфиденциальной информации внутренними злоумышленниками. Ведь такое признание означает, что сотрудники или руководство компании являются преступниками, а это чревато весьма разрушительными последствиями для репутации.

[mercurynews.com](https://www.mercurynews.com/2018/01/05/bay-area-life-insurance-agents-sentenced-in-identity-theft-scheme/): Трое сотрудников страховой компании American Income Life Insurance, используя персональные данные сотен человек, причинили ущерб работодателю и его клиентам на суму $2,8 млн. Преступное трио незаконно оформило сотни полисов по программам страхования жизни. Злоумышленники подавали заявки на получение премий и выводили деньги на фальшивые счета.

Наряду со снижением доли умышленных утечек, следует отметить и снижение доли так называемых «квалифицированных» утечек, т.е. таких инцидентов, когда компрометация информации неразрывно связана с ее использованием в личных целях (мошенничество с персональными данными, банковский фрод), либо сопряжена с нарушением правил, регламентирующих доступ к данным того или иного сотрудника, т.е. с превышением имеющихся прав доступа, нелегитимным доступом к информационному ресурсу.

Доля «квалифицированных» утечек в целом не превышала 25% в период 2013-2017 года и демонстрирует тенденцию к снижению. При этом доля утечек, сопряженных с использованием информации в личных целях (мошенничество) остается достаточно стабильной (см. Рисунок 13), при этом в 2017 г. более чем вдвое снизилась доля утечек, сопряженных с превышением прав доступа.

Рисунок 13. Доля внутренних «квалифицированных» утечек, 2013 - 2017 гг.

27,7% утечек от всех инцидентов, спровоцированных «привилегированными» пользователями, относятся к типу квалифицированных. Процент квалифицированных утечек для обычных пользователей меньше — лишь в 22,5% случаев утечка, спровоцированная обычным пользователем, была сопряжена с мошенничеством либо с превышением прав доступа (см. Рисунок 14).

Рисунок 14. Доля «квалифицированных» утечек от общего числа инцидентов в распределении по обычному и привилегированному пользователю, 2013 - 2017 гг.

## Наибольшая доля случайных внутренних утечек приходится на сетевой канал

Доля случайных утечек данных через сеть (в том числе из-за неверных настроек облачных хранилищ, неправомерного использования таких ресурсов, ошибок при публикации данных на сайтах компаний и ведомств) составляет от 20 до 47% в периоде 2013-2017 годов. Пиковое значение отмечено в 2016 году, далее имеется тенденция к снижению (см. Рисунок 15).

Рисунок 15. Распределение случайных утечек по каналам передачи информации, 2013 – 2017 гг.

Наряду с этим растет доля отличных от сетевого каналов, что свидетельствует в пользу высказанного ранее предположения, что с повышением уровеня защиты информации те утечки, которые не фиксировались ранее, стали попадать в поле зрения исследователей.

Несмотря на значительное снижение в 2016-2017 годы, по-прежнему высока доля утечек бумажной документации,

[newyork.cbslocal.com](https://www.infowatch.ru/analytics/leaks_monitoring/17707): Из автомобиля агента Секретной Службы США в Бруклине неизвестные похитили сумку, в которой, помимо прочего, был ноутбук, содержащий важную информацию. На устройстве хранились поэтажный план и протокол эвакуации Trump Tower, а также материалы расследования в связи с нарушениями, допущенными экс-госсекретарем Хиллари Клинтон при использовании электронной почты.

Снижается доля случайных утечек через съемные носители, вследствие потери или кражи оборудования.

По объективным причинам, распределение умышленных утечек по каналам не подчиняется строгой логике — зачастую встречаются совершенно экзотические случаи.

[cbsnews.com](https://www.cbsnews.com/news/alleged-nsa-leaker-told-fbi-she-stuffed-documents-in-her-pantyhose-feds-say/): Бывшая сотрудница Агентства национальной безопасности США (АНБ) Риэлити Виннер (Reality Winner) призналась, что спрятала в колготках конфиденциальные документы, чтобы вынести их из офиса и передать журналистам. Судебный процесс над Риэлити Виннер начался в марте 2018 г. За утечку государственных секретов ей грозит до 10 лет лишения свободы.

Вместе с тем для умышленных утечек необходимо учитывать ряд фактов. Во-первых, сетевой канал остается самым «популярным» у злоумышленников — свыше 10% утечек по этому каналу носят умышленный характер. Во-вторых, доля умышленных утечек по сетевому и остальным каналам снижается (см. Рисунок 16).

Рисунок 16. Доля умышленных внутренних утечек от общего числа внутренних утечек по каналу, 2013 – 2017 гг.

Предположительно, это означает, что злоумышленники, как и ранее, стремятся уйти из контролируемых каналов — прежде всего сетевого. Не секрет, что многие компании активно используют средства защиты данных для своевременного обнаружения подозрительной активности сотрудников. Также вполне естественно, что сведения о наличии такой системы в компании быстро распространяются среди сотрудников. Принципы и особенности работы систем защиты в целом понятны для рядовых сотрудников, не говоря уже о топ-менеджерах и технически подкованных специалистах.

***В итоге «грамотные» сотрудники, решившие украсть информацию у своего работодателя, просто не используют контролируемые каналы. Отсюда невысокая доля умышленных утечек по каналам в целом, практически нулевое число утечек через мобильные устройства, сервисы голосовых сообщений.***

[ehrintelligence.com](https://ehrintelligence.com/news/us-court-cuts-tcs-fine-from-940m-to-420m-in-epic-lawsuit): Крупнейшая индийская ИТ-компания Tata Consultancy Services (TCS) выплатит американской Epic Systems $420 млн. Epic Systems подала иск к Tata Consultancy Services в 2014 г., обвинив ее в краже технической документации программного решения для автоматизации медицинских организаций. Американская компания утверждала, что сотрудник TCS намеренно устроился консультантом в клинику Kaiser Permanente в Портленде, где проходило внедрение системы Epic EHR. Используя поддельную учетную запись, он получил доступ к порталу Epic UserWeb, созданному для поддержки инсталляции, интеграции и тестирования, и скачал более 6000 документов, содержащих конфиденциальную информацию о продукте.

# Заключение и выводы

На фоне бесконечного числа сообщений об утечках конфиденциальных данных в результате внешних атак на информационные системы неподготовленный читатель рискует впасть в заблуждение, недооценив значение утечек вследствие умысла или неосторожности внутреннего нарушителя. Между тем «внутренние» утечки никуда не исчезли. Простые сотрудники, руководители, системные администраторы, подрядчики и другие пользователи по-прежнему воруют информацию.

Картина современных «внутренних» утечек примерно такова: это компрометация огромных объемов данных вследствие ошибок легитимного пользователя или сбоев автоматизированных систем обработки. Сегодня случайная утечка – это прямая угроза бизнесу, поскольку утекает, как привило, критически важная информация — персональные и платежные данные, секреты производства, иные виды информации ограниченного доступа. Поэтому компания, обрабатывающая такие данные (по сути, любая компания), должна всерьез задуматься о распределении усилий между обеспечением защиты от внешних атак и от внутренних угроз (фактически ужесточая автоматизированный контроль действий собственных сотрудников).

Можно по-разному интерпретировать колебания числа внутренних утечек на протяжении исследуемого периода, но нельзя игнорировать тот факт, что внутренние утечки за последние несколько лет существенно добавили в «разрушительности». Компании обрабатывают все больший объем данных, ошибки и злонамеренные действия персонала и подрядчиков обходятся все дороже, причем не только в переносном смысле — компрометация заметного объема данных непременно приводит к крупным денежным штрафам и выплате компенсации пострадавшим.

Внутренние утечки сегодня ничуть не менее разрушительны (в плане возможных негативных последствий для владельцев информации), чем утечки внешние. Причем если основным и единственным драйвером внешних утечек остается умысел, то применительно к внутренним утечкам мы вынуждены говорить о случайной компрометации. То есть об ошибках сотрудников. Очевидно, что уберечься от ошибок, совершенных под влиянием человеческого фактора, бывает гораздо сложней, чем от действий пусть и злонамеренных, но осознанных, логичных и поддающихся прогнозированию.

Следует отметить два безусловно позитивных момента, выявленных в ходе исследования: во-первых, распределение утечек по каналам выравнивается, сеть остается доминирующим каналом компрометации данных, но не единственным. Это означает, что системы защиты наконец оказались способны эффективно контролировать перемещение информации по каналам, отличным от сетевого. Есть все основания полагать, что развитие и повсеместное внедрение DLP-систем позволило выявить и вывести из тени те утечки, которые ранее происходили в отдельных отраслях, но не фиксировались.

Во-вторых, можно говорить о постепенном снижении доли утечек, спровоцированных привилегированным пользователем. С вероятностью, это связано с постепенным «прорастанием» правил надлежащего обращения с информацией, повышением культуры информационной безопасности.

Безусловно, указанные позитивные тенденции требуют проверки и корректировки в тех случаях, когда мы говорим о действиях злонамеренных сотрудников. К сожалению, против этой категории нарушителей технические средства практически бессильны.

В целом, есть все основания полагать, что внутренние утечки сегодня не менее опасны, чем внешние. Это связано с увеличением объемов данных, обрабатываемых в компаниях, ростом числа каналов — способов передачи данных, а также повышением ликвидности самих данных. Но самое главное, что в ряду инцидентов ИБ, влекущих компрометацию данных, внутренние утечки остаются наиболее сложными. А значит, требуют особого внимания и от исследователей, и от практикующих специалистов в области обеспечения информационной безопасности.

# Мониторинг утечек на сайте InfoWatch

[На сайте Аналитического центра InfoWatch](http://www.infowatch.ru/analytics?utm_source=report&utm_medium=info&utm_campaign=analitics) 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](http://www.infowatch.ru/analytics/panels?utm_source=report&utm_medium=info&utm_campaign=analitics).

  

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

* [Почтовая рассылка](http://www.infowatch.ru/subscrybe)
* [Facebook](https://www.facebook.com/InfoWatch)
* [Twitter](https://twitter.com/InfoWatchNews)
* [RSS](http://www.infowatch.ru/taxonomy/term/3/feed)



Аналитический центр InfoWatch

[www.infowatch.ru/analytics](http://www.infowatch.ru/analytics?utm_source=report&utm_medium=info&utm_campaign=analitics)

# 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».*
1. Утечки, случившихся по вине или по неосторожности внутренних нарушителей — сотрудников организаций, топ-менеджеров и иных привилегированных пользователей, подрядчиков, имевших легитимный доступ (или возможность его получить) к информации, которая была скомпрометирована в результате утечки. [↑](#footnote-ref-2)
2. Сообщения об утечках данных, опубликованные официальными ведомствами, СМИ, авторами записей в блогах, интернет-форумах, иных открытых источниках. [↑](#footnote-ref-3)
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. [↑](#footnote-ref-4)
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. [↑](#footnote-ref-5)
5. Авторы классифицируют утечки по виновнику (источнику) инцидента. Наряду с внутренними нарушителями, в данную классификацию попадает внешний нарушитель. [↑](#footnote-ref-6)
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. [↑](#footnote-ref-7)
7. Данные об ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций в СМИ. [↑](#footnote-ref-8)
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. [↑](#footnote-ref-9)
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.). [↑](#footnote-ref-10)
10. 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. [↑](#footnote-ref-11)
11. До 2014 года методология исследования не предусматривала распределение утечек на «внешние» и «внутренние». [↑](#footnote-ref-12)
12. 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 закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.). [↑](#footnote-ref-13)