Утечки данных организаций по вине или неосторожности внутреннего нарушителя. Сравнительное исследование. 2013-2019 гг.

Оглавление

Только цифры

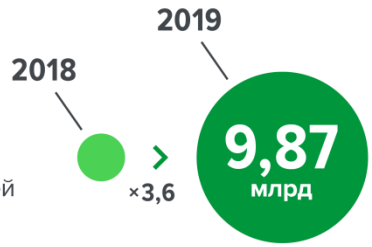
В **2019** году Экспертно-аналитический центр InfoWatch зафиксировал по всему миру **1348 утечек данных** по вине или по неосторожности внутренних нарушителей

В **2018** году по всему миру было зафиксировано **1393** утечки

На внутренние утечки приходится **53,7%** от общего числа утечек

В результате внутренних утечек по всему миру скомпрометировано **9,87 млрд записей,** относящихся к типу пользовательских данных

В **2018** году на внутренние утечки пришлось **61,5%** утечек, в результате которых было скомпрометировано **>2,76 млрд** записей



На одну внутреннюю утечку в среднем приходится **7,3 млн** скомпрометированных записей пользовательских данных

В **2018** году аналогичный показатель составил **1,9 млн**

98% от совокупного объёма персональных данных и финансовой информации были скомпрометированы в результате небрежности либо грубой неосторожности лиц, имеющих **легитимный доступ** к указанным данным

Доля аналогичных утечек в **2018** году составила **94%**

На долю **сотрудников** приходится **81,5%** всех внутренних утечек из организаций. В **2018** году на долю сотрудников пришлось **83,1%**

Сокращения

ИБ	Информационная безопасность
ИС	Информационная система
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение

Аннотация

Экспертно-аналитический центр группы компаний InfoWatch представляет третье сравнительное исследование утечек информации, произошедших по вине или неосторожности персонала (включая руководство) коммерческих компаний, государственных органов и организаций. Рассматриваемый период - с 2013 по 2019 год. Утечки по вине или неосторожности сотрудников, в отличие от утечек информации под воздействием извне, авторы настоящего исследования предлагают условно именовать внутренними утечками. Сотрудников, чьи действия (бездействие) спровоцировали утечку данных из указанных компаний и организаций, авторы предлагают называть внутренними нарушителями.

Кроме этого, к числу внутренних нарушителей в рамках настоящего исследования также относятся лица из числа персонала подрядных организаций, осуществляющих обработку информации ограниченного доступа по заданию коммерческой компании или госоргана (госорганизаций) и допустивших утечку такой информации (в период действия контракта).

Для группы внутренних нарушителей (в отличие от внешних нарушителей (злоумышленников — хакеров) определяющим признаком является наличие правомерного (легитимного, санкционированного) доступа к информации, необходимость знать и соблюдать правила обработки информации ограниченного доступа, юридическая связь (трудовой договор, соглашение на оказание услуг) с компанией, обрабатывающей информацию ограниченного доступа (то есть договорные отношения с владельцем или оператором информации).

В рамках данного исследования авторы поставили перед собой задачу отразить актуальную картину происшествий, связанных с внутренними утечками, обозначить тенденции и векторы возможного развития этого типа угроз.

Исследование дополняет линейку аналитических продуктов компании, прежде всего, ежегодные исследования глобальной картины утечек, расширяет представление о развитии феномена внутренних утечек в динамике.

Авторы уверены, что выводы настоящего исследования будут интересны 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.

Методика

Исследование проводится на основе собственной базы данных, пополняемой специалистами экспертно-аналитического центра InfoWatch с 2004 года. В базу попадают публичные сообщения[1] о случаях утечки информации из коммерческих, некоммерческих (государственных, муниципальных) организаций, госорганов, которые произошли вследствие умышленных или неосторожных действий[2] сотрудников и иных лиц[3].

В настоящий момент количество записей в базе превышает 18 000.

В ходе наполнения базы каждая утечка классифицируется по ряду критериев, таких как сфера деятельности (отрасль), размер причинённого ущерба[4], тип утечки (по умыслу), канал утечки[5], типы утекших данных, вектор воздействия[6].

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

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

Инциденты безопасности, не повлекшие утечки данных, а также инциденты – утечки из неизвестных источников (от неизвестного оператора и/или владельца информации) в данную выборку не включены.

---

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

[2] 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. См. Глоссарий.

[3] Авторы классифицируют утечки по виновнику (источнику) инцидента. См. Глоссарий.

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

[5] 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.

[6] 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.).

При формировании диаграмм по отдельным разрезам из выборки исключены утечки, классифицированные по основному критерию разреза как неопределенные[7].

Исследования Экспертно-аналитического центра InfoWatch в основном ориентированы на работу с сообщениями об утечках данных на английском и русском языке, также используется некоторое количество арабских и немецких источников. Во многом, с этим связана большая доля информации о российских утечках, сообщений об утечках из американских и европейских компаний. При этом мониторинг сообщений об утечках проводится без каких-либо ограничений по странам.

Авторы полагают, что региональные особенности, безусловно присущие определенным группам стран, на большой выборке данных нивелируются. Поэтому, с учетом указанных выше ограничений, неравномерная представленность различных стран и страновых групп в базе исходных сообщений об утечках, по мнению авторов исследования, заметно не отражается на итоговых результатах и выводах.

[7] 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.

Результаты исследования

В 2019 году Экспертно-аналитический центр InfoWatch по всему миру зафиксировал 1348 утечек, случившиеся по вине или по неосторожности внутренних нарушителей. На графике заметно, что очевидного тренда, описывающего динамику утечек указанного типа (внутренних утечек), на горизонте 2004-2019 гг. не наблюдается (Рисунок 1).

Рисунок 1. Число внутренних утечек информации, 2004 -2019 гг.

Так рост числа внутренних утечек, отмечавшийся в 2017-2018 годах, в 2019 году сменился небольшим снижением (на 3,3%).

Более показательно снижение доли внутренних утечек от общего числа утечек — как видно на диаграмме, если в 2018 году этот показатель составлял 61,6%, то в 2019 году доля внутренних утечек составила 53,7%. При этом уже четыре года подряд доля внутренних утечек от общего числа утечек остается в диапазоне 53-61%, т.е. все эти годы более половины всех утечек, зафиксированных в мире, происходят не по причине воздействия внешних хакеров, а из-за ошибок или умышленных действий сотрудников (в широком смысле, включая руководство) владельцев и операторов информации (Рисунок 2).

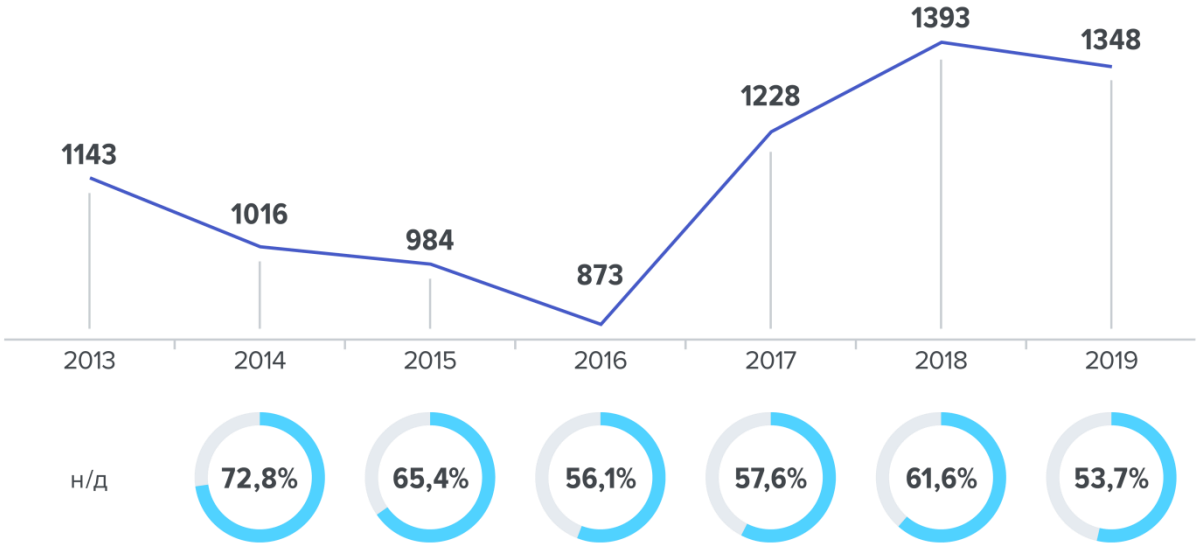


Рисунок 2. Число внутренних утечек информации и доля утечек этого типа от общего числа утечек, 2013 - 2019 гг.

Совокупный объем данных, скомпрометированных в результате внутренних утечек, в 2019 году составил 9,87 млрд записей. Впервые за все время наблюдений объем записей, скомпрометированных в результате внутренних утечек, превысил аналогичный показатель для утечек внешних (в 2019 году в результате внешних утечек скомпрометировано 4,7 млрд записей). В динамике также видно, что первый заметный пик объема скомпрометированных данных применительно к внутренним утечкам наблюдался в 2017 году – тогда объем скомпрометированных записей вырос почти в 10 раз. Пик 2019 года динамически более скромный – по сравнению с данными 2018 года объем скомпрометированных записей вырос «всего лишь» в 3,6 раза (см. Рисунок 3).

Рисунок 3. Объем данных, скомпрометированных в результате «внутренних» утечек, млн записей, 2013 - 2019 гг.

До недавнего времени среди исследователей было распространено мнение, что наиболее опасными для организаций, обрабатывающих информацию ограниченного доступа, являются действия внешних злоумышленников — хакерские атаки. Представленные цифры свидетельствуют о противоположном — «внутренние» утечки фактически выходят на первый план (по крайней мере в том, что касается объема скомпрометированных персональных данных и платежной информации).

Справедливости ради, напомним, что впервые проблема внутренних утечек была серьезно поставлена еще на заре появления технологий контроля интернет-трафика (электронная почта, web), когда выяснилось, насколько высоки угрозы со стороны сотрудников при работе с информацией. Сегодняшнее пристальное внимание к проблеме внутренних утечек как представляется, тесно связано с вопросами недостаточной лояльности персонала, нарушений элементарных правил обработки информации ограниченного доступа со стороны рядовых сотрудников и руководства компаний. Феномен внутренних утечек получил новое прочтение — по объему скомпрометированных данных внутренние утечки не только сравнялись, но и вдвое превзошли внешние утечки.

Очевидная опасность внутренних утечек заставила серьезно пересмотреть подходы к защите информации (прежде всего персональных данных и платежной информации, далее — пользовательских данных) по всему миру. Как следствие, в 2017-2018 годах мы наблюдали ужесточение регуляторной политики в области защиты персональных данных сразу в нескольких регионах — США, страны Европы, — т. е. в государствах, являющихся основными «поставщиками» утечек персональных данных в мировом распределении.

В результате уже в 2018 году фиксировалось падение объема скомпрометированных записей как по утечкам в целом (двукратное), так и по внутренним утечкам (более, чем в два раза). В 2019 году внутренние утечки «отыграли позиции», показав уникальную

способность приспосабливаться к жестким правилам игры (усилению мер по обеспечению безопасности информации), с одной стороны, и подтвердив гипотезу о том, что репрессивные меры административного плана не всегда эффективны.

Мир пришел к ситуации, когда одновременно растут суммы и штрафов, накладываемых государством за утечки данных, и объем скомпрометированных данных.

> *healthitsecurity.com: Американская сеть клиник Sentara наказана за неточное и несвоевременное оповещение регулятора об утечке информации пациентов. В качестве штрафа медики выплатят $2,175 млн. Sentara отправила по неверным адресам 577 писем с персональными данными пациентов. В общей сложности отправления с платежными документами насчитывали более 16 тыс. адресатов. В почтовых рассылках были такие данные, как имена пациентов, сведения об учетных записях и даты оказания услуг.*

Объем скомпрометированных данных в расчете на одну утечку (средняя «мощность» утечки) для внутренних утечек в 2019 году составляет 7,3 млн записей (см. Рисунок 4).

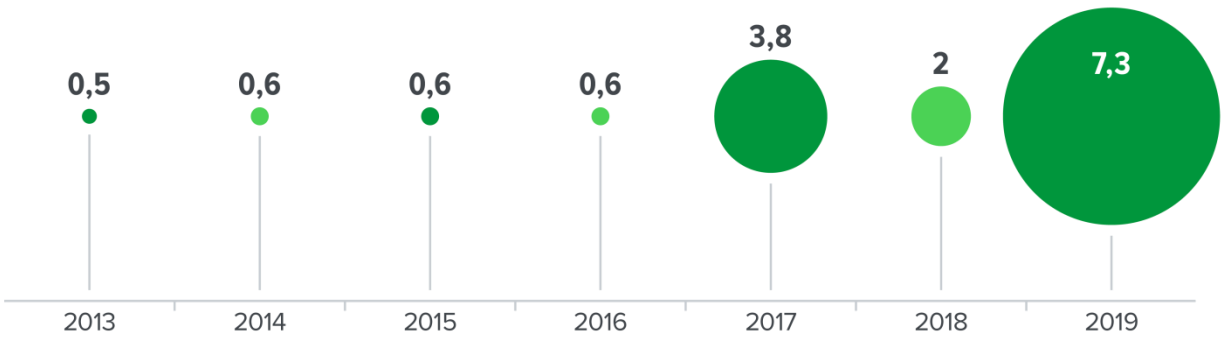


Рисунок 4. Объем данных в расчете на одну утечку, млн записей, 2013 - 2019 гг.

Следует учитывать, что показатель объема скомпрометированных данных фиксирует лишь общее число скомпрометированных записей, относящихся к персональным данным и платежной информации. Указанные типы данных характеризует высокая способность к формализации. Имена и фамилии людей, индивидуальные идентификационные номера (налоговые, медицинские), реквизиты пластиковых карт и иная информация такого рода легко поддается машинной обработке, пользовательские данные без особенных проблем выявляются в потоке других данных. Это означает, что утечки пользовательских данных должны чаще выявляться средствами контроля защищенности (средствами обнаружения и предотвращения утечек).

На практике мы видим обратную картину — растет общий объем записей, скомпрометированных в результате внутренних утечек, растет «мощность» утечек. С учетом отмеченного выше , можно предположить, что компании, обрабатывающие

пользовательские данные, либо не используют, либо не эффективно (некорректно настраивают, не обучают персонал)

Кроме того, допустима и вторая причина —огромный объем скомпрометированных данных является следствием стремления компаний максимально использовать возможности коллективной работы с данными для «обогащения» этих данных. Как пример, работа с маркетинговыми агентствами для собирания сведений о предпочтениях своих клиентов требует предоставления доступа к собственной базе данных. Как правило, сотрудники маркетингового агентства не контролируются службой безопасности компании-владельца базы клиентов. Затем кто-то в длинной цепочке партнеров и агентов намеренно использует предоставленный доступ в личных интересах. В результате владелец данных теряет над ними контроль, происходит утечка информации.

Еще чаще стремление обеспечить максимальное удобство в работе с некими общими информационными ресурсами оборачивается банальной человеческой ошибкой — администратор организовал доступ в базу данных извне и не защитил его (иногда даже просто паролем), владелец внешнего ресурса по ошибке не проверил, индексируется ли база поисковиками и пр. В 2019 году 58,1% случаев компрометации данных в компаниях и госорганах носили случайный характер. На случайные утечки пришлось 98,1% от общего объема пользовательских данных, скомпрометированных в результате внутренних утечек (см. Рисунок 5).

Рисунок 5. Число, объем скомпрометированных данных от совокупного числа внутренних утечек и совокупного объема данных, пришедшихся на внутренние утечки. 2013 - 2019 гг.

Злонамеренный нарушитель редко покушается на пользовательские данные. И в том случае, когда это все же происходит, объем похищенной информации будет

сравнительно небольшим — только действительно ликвидные сведения. Например, это данные о поставщиках и подрядчиках компании-работодателя, которые можно «забрать с собой» при переходе в конкурирующую организацию. Объем записей, скомпрометированных в результате умышленных действий внутреннего нарушителя, просто несопоставим с объемом данных, скомпрометированных в результате ошибок (Рисунок 6).

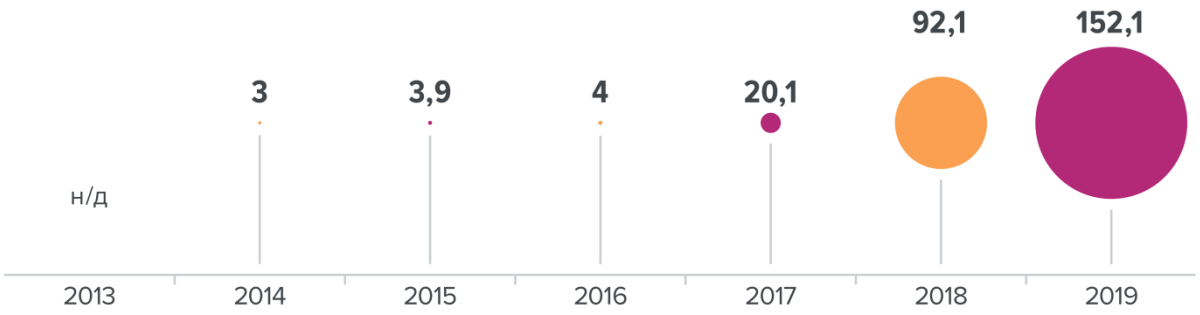


Рисунок 6. Объем данных, скомпрометированных в результате умышленных утечек, млн записей, 2013 - 2019 гг.

По-настоящему злонамеренного нарушителя интересует только действительно ценные сведения — коммерческая тайна компании.

> *law.com: Суд присяжных распорядился признать компанию Charles River Analytics (CRA) виновной по делу о хищении коммерческой информации у компании LBI. Ответчику предстоит выплатить истцу почти $840 тыс. В центре расследования находились бывшие сотрудники LBI Джаред Спаркс (Jared Sparks) и Джей Уильямс (Jay Williams). Прокуратура предъявила им обвинения в том, что они украли коммерческие секреты бывшего работодателя в интересах Charles River Analytics. Так, установлено, что Спаркс загрузил тысячи конфиденциальных файлов LBI в свой личный аккаунт на облачном файловом хостинге Dropbox. В этих документах были бухгалтерские сведения и инженерная документация. Вскоре после того, как Спаркс присоединился к CRA, он скачал из облака украденные файлы.*

Статистика показывает, что внутренние утечки информации, составляющей коммерческую тайну, в 2019 году прочно занимают второе место после безусловного лидера — внутренних утечек персональных данных (см. Рисунок 7).

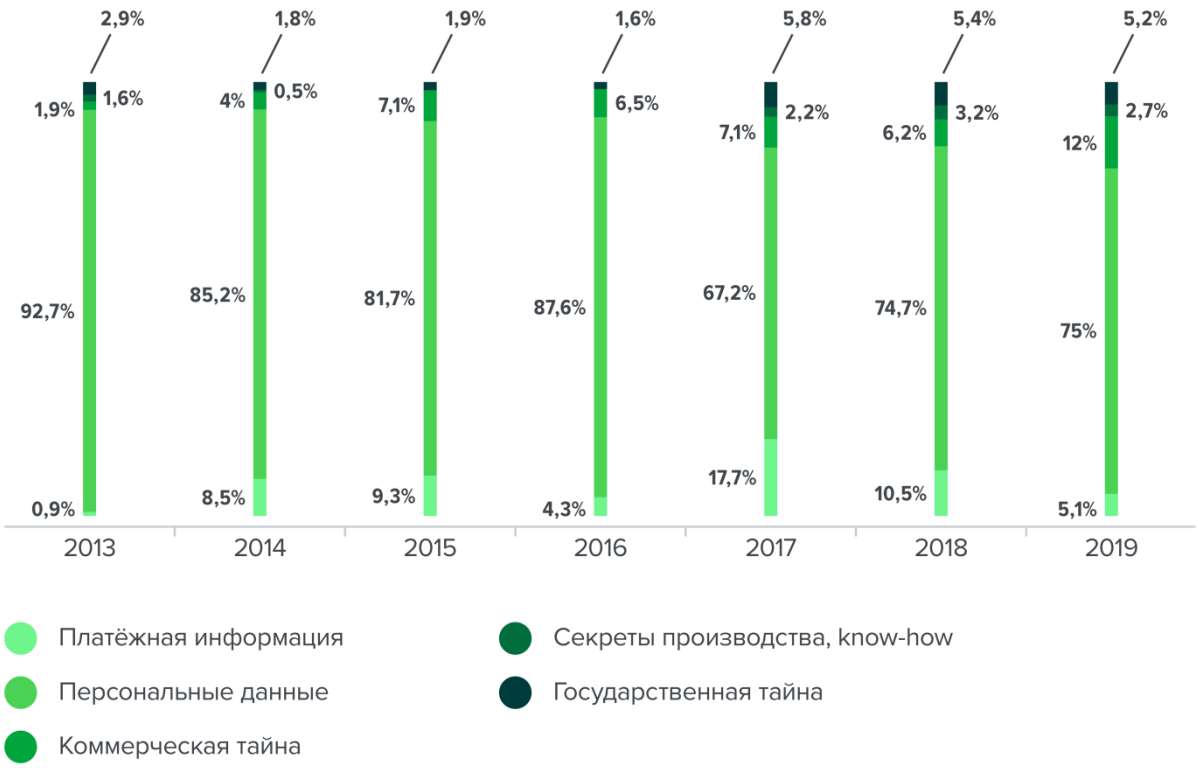


Рисунок 7. Распределение «внутренних» утечек по типу данных, 2013 – 2019 гг.

При этом следует учитывать, что утечки информации, составляющей коммерческую тайну, в 80% случаев носят умышленный характер. Утечки персональных данных, наоборот, большей частью случайны.

> *phonearena.com Исследователи компании vpnMentor обнаружили в Сети незащищенную базу с пользовательскими данными сервисов обмена текстовыми сообщениями. Специалисты считают, что эта утечка могла затронуть более 100 млн человек. База данных общим объемом 604 ГБ насчитывает порядка миллиарда различных записей. Хранилище принадлежит американскому сервис-провайдеру TrueDialog, который специализируется на разработке корпоративных решений для передачи SMS. База на платформе Microsoft Azure размещена в облаке Oracle Marketing Cloud.*

Распределение внутренних утечек по типу данных со всей очевидностью демонстрирует, особенность двух групп типов данных — группы пользовательских данных (персональные данные и платежная информация) и группы, куда вошли остальные типы данных. На гистограмме видно, что в случае с пользовательскими данными более половины утечек происходит случайно. В случае с иными типами данных большая часть утечек происходит вследствие умышленных действий (Рисунок 8).

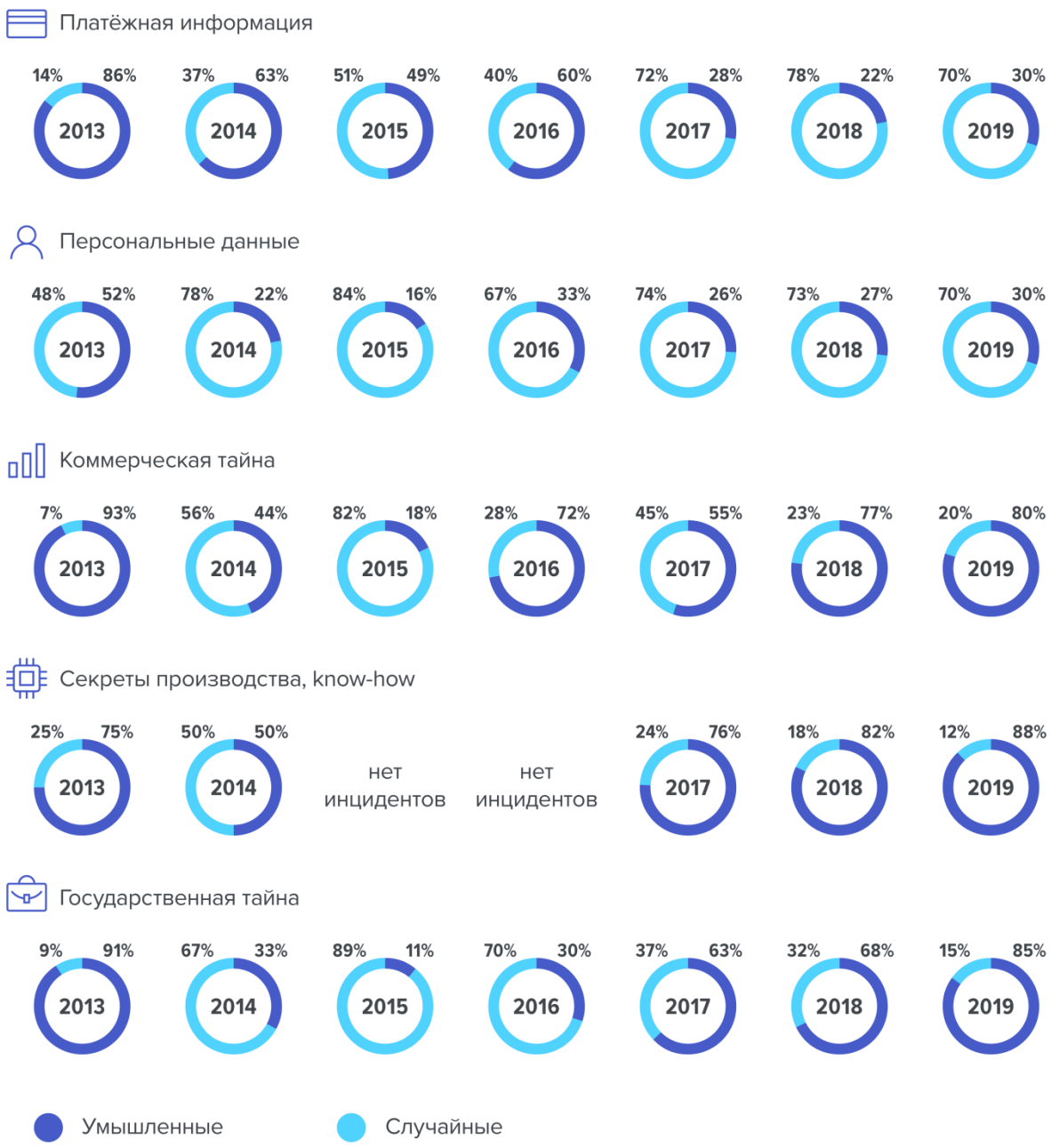


Рисунок 8. Распределение утечек по умыслу и типу данных, 2013 – 2019 гг.

Таким образом, можно сделать вывод, что данные нельзя без учета их специфики (типов). Данная диаграмма показывает, что такая специфика есть. По сути, это означает, что системы защиты должны уметь корректно распознавать защищаемую информацию, оперативно информировать о выявленных инцидентах.

Указанная «специализация» типов данных позволяет объяснить, почему с усилением регулирования в области защиты информации, с ростом возможностей технических средств защиты проблема утечек коммерческой тайны, секретов производства не становится менее острой.

Авторы исследования полагают, что умышленные утечки в принципе менее восприимчивы к применению технических средств защиты. Внутренний злоумышленник, «нацелившись» на кражу коммерческих секретов работодателя, как правило, неплохо осведомлен о том, где хранится интересующая его информация, как и кем контролируются каналы передачи данных. В итоге утечка коммерческих секретов либо вовсе не фиксируется, либо обнаруживается пострадавшей компанией уже постфактум. Чтобы система могла реагировать на подобные «сложные утечки», ее необходимо правильно настраивать и учить персонал работе с ней.

> *bloomberg.com: Компания Cisco Systems подала в суд на бывших сотрудников — ведущих инженеров и менеджера по продажам. В иске утверждается, что они скопировали тысячи конфиденциальных документов и перешли с этой информацией на сторону конкурентов. Согласно исковому заявлению, в феврале компанию Cisco покинул Уилсон Чанг (Wilson Chung), один из ее главных инженеров. Перед уходом он загрузил более 3000 внутренних файлов с коммерческой информацией, включая данные о вкладе компании в развитие технологии связи пятого поколения (5G) и соответствующие проектные спецификации для создания прототипа новейшей системы видеоконференций. Кроме того, поддавшись на уговоры Уилсона Чанга, другой сотрудник стал фотографировать на свой iPhone конфиденциальные документы. Он также скопировал различные данные и электронную переписку.*

Отметим, что умышленные утечки информации, составляющей коммерческую тайну, фиксируются во всех отраслях экономики. Безусловным лидером здесь выступают ИТ, телекоммуникационные и промышленные компании (Рисунок 9).

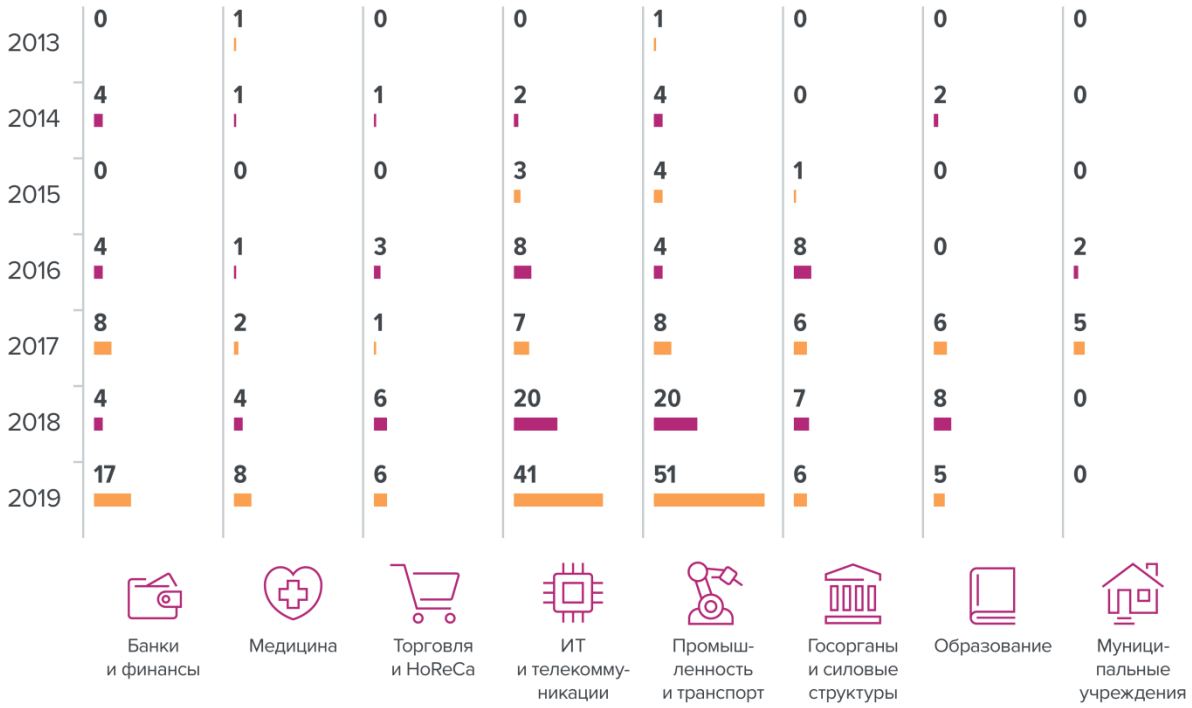


Рисунок 9. Распределение умышленных утечек коммерческой тайны и ноу-хау по отраслям, 2013 – 2019 гг.

Впрочем, умышленные утечки коммерческой тайны — совершенно неспецифический тип утечек в том смысле, что применительно к таким утечкам невозможно говорить об отраслевой специфике. Очевидно, что любая коммерчески значимая информация ценна в той степени, в какой на нее есть спрос. Поэтому, несмотря на то, что лидерами по утечкам коммерческих секретов и ноу-хау являются промышленные компании и сфера ИТ, угрозам утечек информации, составляющей коммерческую тайну, в равной степени подвержены все высококонкурентные отрасли экономики .

> *fiercepharma.com: В Австралии биофармацевтическая компания CSL подала в суд иск против своего бывшего исполнительного директора Джозефа Чао (Joseph Chiao). Истцы утверждают, что топ-менеджер ушел к конкурентам, прихватив с собой множество конфиденциальных файлов. По данным истцов, Чао начал вести переговоры с Pharming в апреле 2019 года, а к сентябрю конкуренты предложили ему работу. Чао покинул CSL 23 сентября, но накануне отправил на свой личный аккаунт электронной почты различную конфиденциальную информацию, включая данные, составляющие коммерческую тайну. Кроме того, Джозеф Чао скопировал информацию на свой USB-накопитель.*

Не менее интересно распределение случайных (неумышленных) утечек персональных данных. Легко заметить, что здесь лидерами выступают медицинские организации и компании сегмента ИТ-телеком (Рисунок 10).

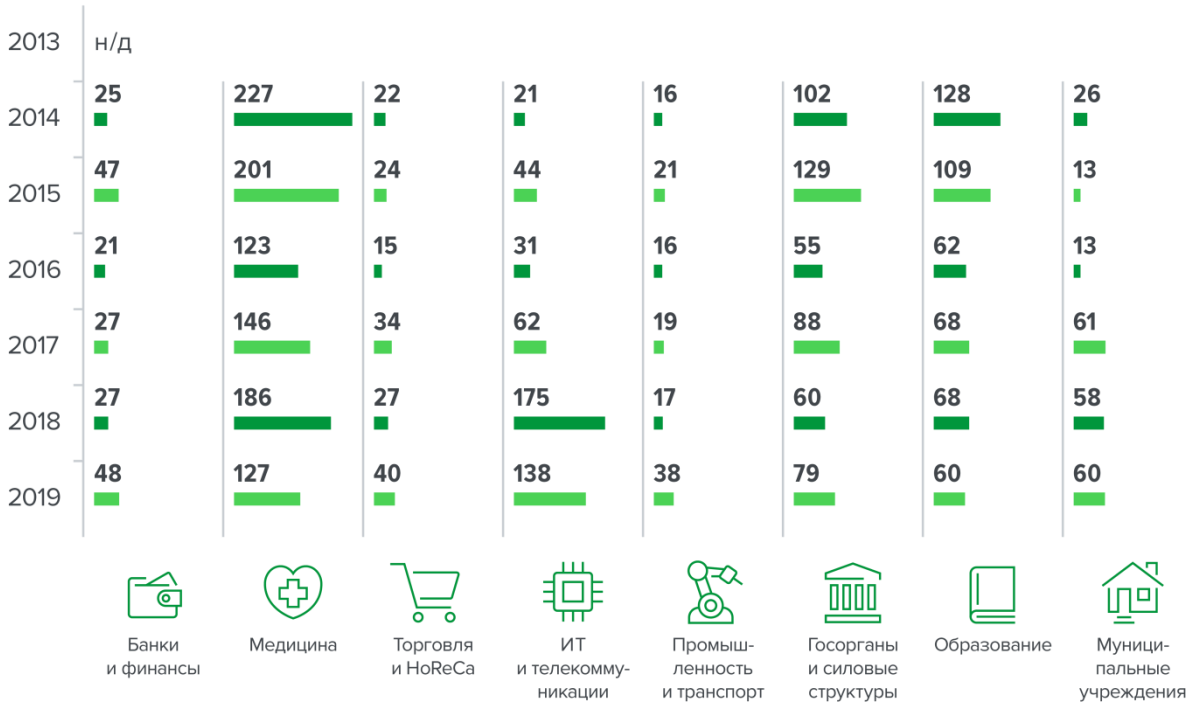


Рисунок 10. Распределение случайных утечек ПДн по отраслям, 2013 – 2019 гг.

Количество утечек, зафиксированных в медицинских учреждениях, стабильно растет с 2016 года, что, как ни странно, следует признать обнадеживающим фактом. На фоне очевидно высокой латентности утечек именно в медицине, с учетом предположительно невысокого (по сравнению с отраслями — лидерами) уровня защиты информации, характерного для медучреждений, рост числа зафиксированных утечек может свидетельствовать о том, что системы защиты информации (в том числе контроля) в медицине наконец-то заработали должным образом, вследствие чего те утечки, которые ранее не фиксировались, теперь удалось вывести из тени.

В количественном выражении наиболее «проблемным» звеном в системе информационной безопасности является сотрудник компании. На его долю приходится 81,5% всех внутренних утечек (Рисунок 11).

Рисунок 11. Распределение «внутренних» утечек по виновнику, 2013 – 2019 гг.

В 2019 году обращает на себя внимание высокая доля утечек по вине подрядчика — на долю утечек этого типа приходится 9,1% всех утечек.

> *nytimes.com: Неизвестные выложили в Сеть данные 15 млн банковских карт. Утечка затронула клиентов трех крупнейших банков Ирана – Mellat, Tejarat и Sarmayeh. Министр информации и связи Ирана Мохаммад Джавад Азари Джахроми (Mohammad Javad Azari Jahromi) назвал виновником утечки недовольного подрядчика, который имел доступ к данным и решил слить их в Сеть с целью вымогательства.*

Применительно к распределению внутренних утечек по виновнику наиболее актуальной на протяжении последних лет 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 2019 году на долю привилегированных пользователей пришлось 12% от всех умышленных внутренних утечек (Рисунок 12).

Рисунок 12. Доля умышленных утечек в разбивке по обычному и привилегированному пользователю. 2013 - 2019 гг.

Сообщения СМИ полны историй о нелегитимных действиях высших руководителей.

> *justice.gov: Бывший ИТ-специалист одной из клиник Нью-Йорка признал себя виновным в компрометации десятков учетных записей своих коллег и краже конфиденциальных данных пациентов. По данным Министерства юстиции США, ему грозит до 10 лет тюремного заключения. По данным американской прокуратуры, одержимый нездоровым любопытством, Ричард Лириано не только вторгался в частную жизнь коллег, но и взламывал компьютеры с защищенной медицинской информацией и персональными данными пациентов. Утечка этой информации стоила клинике больших финансовых потерь – всего на ликвидацию последствий инцидентов было потрачено порядка $350 тыс.*

Заметим, что утечки по вине привилегированных пользователей, как правило, носят умышленный характер. В 2019 году 81,5% утечек, спровоцированных топ-менеджментом, были умышленными. Применительно к рядовым сотрудникам на умышленные утечки приходится лишь 35,7% инцидентов (Рисунок 13).

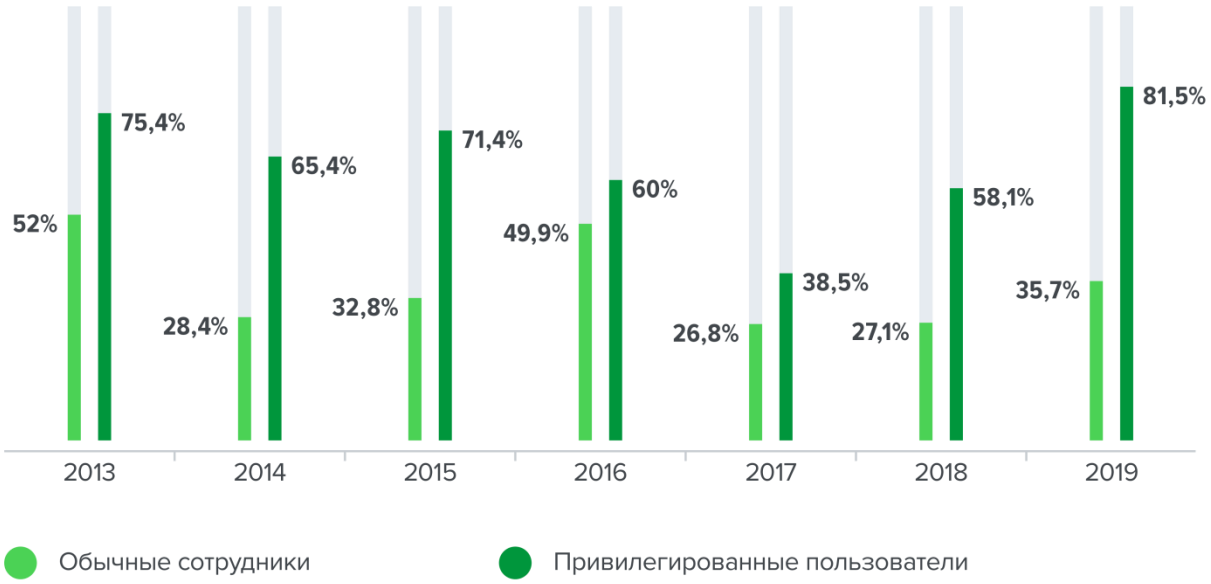


Рисунок 13. Доля умышленных утечек от общего числа утечек в распределении по обычному и привилегированному пользователю, 2013 - 2019 гг.

Выше мы отмечали, что умышленные утечки отличает б***о***льшая 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 утечки данных, не каждая компания готова признать умышленную утечку, опасаясь репутационных потерь.

В 2019 году снизилась доля 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 (Рисунок 14).

Рисунок 14. Доля внутренних «квалифицированных» утечек,. 2013 - 2019 гг.

К числу «квалифицированных» утечек можно отнести случаи умышленного саботажа сотрудников, порчи или уничтожения данных работодателя по мотивам мести, обиды, допущенной, по мнению нарушителей, несправедливости. Но такие утечки пока сравнительно редки. Основная часть «квалифицированных» утечек связана с использованием скомпрометированной информации в целях личного обогащения и превышением прав доступа.

> *blog.trendmicro.com: Японская компания Trend Micro — один из крупнейших мировых производителей ПО для кибербезопасности, сообщила, что ликвидировала серьезную инсайдерскую угрозу. Обнаружен сотрудник, продавший на сторону крупную базу клиентских данных. В ходе расследования выяснилось, что злонамеренный сотрудник обошел внутренние системы защиты и получил доступ к базе данных службы клиентской поддержки. В базе хранилась такая информация, как имена клиентов, адреса электронной почты, номера заявок в службу техподдержки, а в некоторых случаях и номера телефонов. По оценкам компании, всего утекла информация 68 тыс. клиентов. Внутреннее расследование показало, что инсайдер продал украденную информацию злоумышленнику за пределами компании — его имя пока неизвестно.*

Каждая третья утечка по вине привилегированного пользователя является «квалифицированной», сопряжена с мошенничеством либо с превышением прав доступа (Рисунок 15).

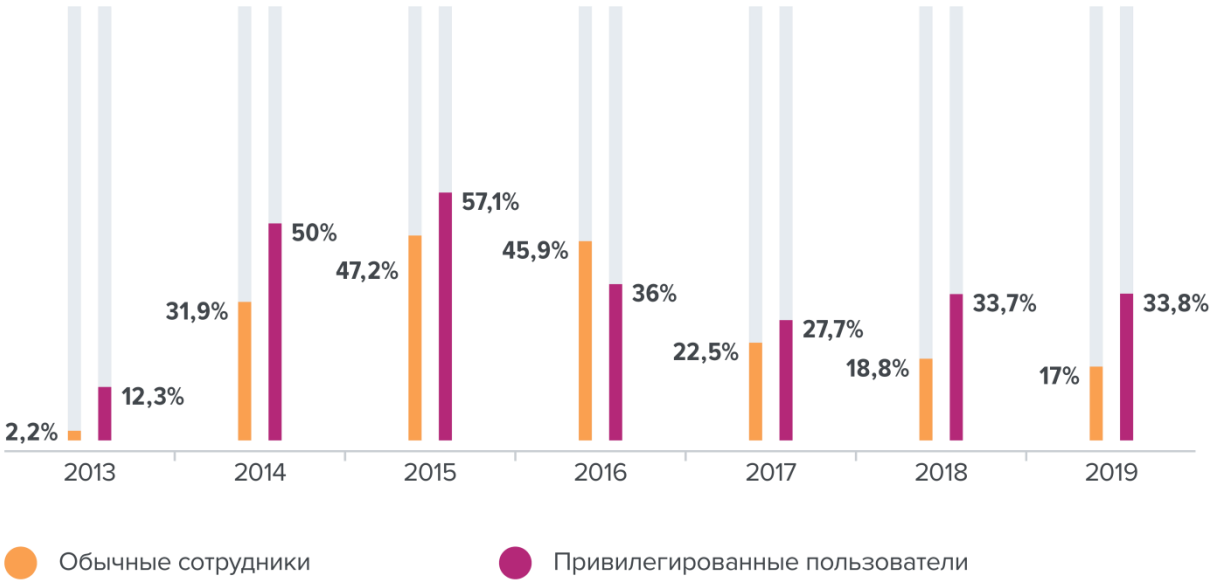


Рисунок 15. Доля «квалифицированных» утечек от общего числа инцидентов в распределении по обычному и привилегированному пользователю. 2013 - 2019 гг.

В силу высокой латентности умышленных утечек все попытки распределение этих утечек по каналам, отражающее реальную картину для генеральной совокупности, скорее всего, обречены на неудачу. Ведущим каналом как для умышленных, так и для случайных утечек остается сетевой. Говорить о динамике остальных каналов применительно к умышленным утечкам пока все еще затруднительно.[8]

Случайные утечки, очевидно, менее латентны, чем умышленные, поэтому распределение случайных утечек даже на относительно небольшой выборке вполне репрезентативно и позволяет составить представление о том, какие каналы передачи информации наиболее опасны, как меняется распределение утечек по каналам во времени.

В 2019 году вполне ожидаемо выросла доля случайных утечек через сеть (в том числе из-за неверных настроек облачных хранилищ, неправомерного использования таких ресурсов, ошибок при публикации данных на сайтах компаний и ведомств), составив 61,6% (Рисунок 16).

[8] В силу высокой латентности и небольшого количества умышленных утечек, зафиксированных на отличных от сетевого каналах, представленная картина умышленных утечек (в части распределения по каналам) с вероятностью, не отражает реальную картину утечек, случившихся в мире в период 2013-2019 гг.

Рисунок 16. Распределение случайных утечек по каналам передачи информации, 2013 – 2019 гг.

Сетевой канал остается наиболее «проблемным» еще и потому, что практически не имеет ограничений по объему данных, которые могут быть скомпрометированы.

> *wired.com: В Сети на незащищенном сервере найдены персональные данные 1,2 млрд подписчиков Facebook, Twitter, LinkedIn и GitHub. Среди скомпрометированной информации не оказалось таких чувствительных данных, как пароли, номера кредитных карт или номера социального страхования. Утекли только профили сотен миллионов людей в соцсетях, а также данные о карьере (по-видимому, скопированы из LinkedIn), почти 50 млн уникальных телефонных номеров и 622 млн уникальных адресов электронной почты.*

По-прежнему актуальны утечки, случившиеся в результате потери или кражи оборудования. Порой такие случаи довольно курьезны.

> *bloomberg.com: Неизвестный похитил жесткие диски с информацией о 29 тыс. работников Facebook. Ситуацию усугубляет тот факт, что данные на носителях не были зашифрованы. Инцидент произошел еще 17 ноября. Злоумышленник вскрыл автомобиль бухгалтера по начислению зарплаты и унес с собой находившуюся в салоне сумку с жесткими дисками. На них без использования шифрования были записаны данные сотрудников: имена, номера банковских счетов, последние четыре цифры номеров социального*

страхования (SSN), а также сведения о зарплатах, бонусах и участии в акционерном капитале.

С той же легкостью, что и несколько лет назад, злоумышленники копируют секреты своих работодателей на USB-носитель.

> *bloomberg.com: Американская автомобилестроительная корпорация General Motors (GM) заявила, что один из ее руководителей был подкуплен южнокорейской Hyundai Motor с целью получения доступа к секретной информации о разработке электромобилей и беспилотных транспортных средств. GM считают, что этот руководитель незаконно получил конфиденциальную информацию о технологиях безопасности автомобилей, передовых функциях помощи водителю и процессах разработки автономных транспортных средств. Согласно иску, перед уходом из General Motors мужчина скопировал секретные данные с корпоративного ноутбука на незарегистрированные USB-носители.*

Появляются сравнительно новые каналы утечек данных, близкие по технологии к сетевому, но все же имеющие свою специфику. Например, в 2019 году зафиксирован ряд утечек, случившихся по вине или неосторожности авторов мобильных приложений.

> *bbc.com: Ошибка в API мобильного приложения могла привести к компрометации персональных данных порядка 325 млн абонентов индийского мобильного оператора Airtel. По номеру абонента через интерфейс можно было узнать такую информацию, как имена, адреса электронной почты, даты рождения, адреса, а также номера IMEI — уникальные числовые идентификаторы для мобильных устройств.*

Распределение утечек по каналам позволяет сделать два важных наблюдения. Во-первых, доля сетевого канала растет, и это порождает у разработчиков и пользователей технических решений для защиты информации ошибочное представление о том, что можно сосредоточиться на защите сети и не уделять внимание остальным каналам. Степень ошибочности этого заблуждения хорошо иллюстрируют показатели ущерба операторов информации от действий недобросовестных сотрудников, которые «вынесли» значимую информацию на флэшках, на бумажных носителях, посредством использования фотокамер смартфонов, мобильных приложений.

Отсюда второе наблюдение: в эпоху, когда информация действительно имеет ценность, когда сведения о прорывной технологии стоимостью миллионы долларов можно украсть, просто отправив сообщение в мессенджер, неважных, незначительных или недостойных внимания каналов потенциальной утечки информации быть не может.

Заключение и выводы

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

Внутренние утечки обладают мощным разрушительным потенциалом. Последствия ошибок или злонамеренных действий персонала могут проявляться не только в имущественных или репутационных потерях, но и в приостановке или ликвидации бизнеса как такового.

Распределение внутренних утечек по типу данных со всей очевидностью демонстрирует особенность двух групп данных — группы пользовательских данных и группы, куда вошли остальные типы данных. Это означает, что не только каналы передачи информации, но и сами данные, обрабатываемые в компании, обладают спецификой, прямо влияющей на итоговую эффективность используемых защитных мер, будь то технические средства защиты или организационные изменения.

В практической плоскости специфика персональных данных, например, проявляется в том, что для достаточно эффективной защиты ПДн, утечки которых носят преимущественно случайный характер, в целом достаточно применения технических средств защиты, ориентированных на выявление в потоке трафика формализованной информации. И наоборот, только технических мер совершенно недостаточно для защиты секретов производства, информации, составляющей коммерческую тайну — для действительно эффективного противодействия утечкам этой группы данных уже необходимо сочетание технических и организационных мер.

Нельзя не отметить определенную стабильность картины внутренних утечек, где основным каналом компрометации данных остается сетевой, основным субъектом, по чьей вине или неосторожности утекает информация ограниченного доступа, является рядовой персонал компаний и организаций. Вместе с тем следует помнить, что любой канал передачи информации является потенциально опасным, любой сотрудник может стать источником бед для своего работодателя. Стратегия построения системы защиты, направленная на контроль исключительно рядовых сотрудников, только или с выявлением утечек данных преимущественно на сетевом канале, скорее всего, окажется проигрышной. Поэтому очень важно создавать модель защиты с учетом контроля привилегированных пользователей – топ-менеджеров и системных администраторов.

Мониторинг утечек на сайте InfoWatch

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

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

- Почтовая рассылка
- Facebook
- Telegram

Экспертно-аналитический центр InfoWatch

www.infowatch.ru/analytics

Глоссарий

Атака – см. компьютерная атака, сетевая атака, вторжение.

Вторжение (атака) – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам [Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ. Утвержден ФСТЭК России. 3 февраля 2012 г.].

Вектор воздействия – критерий классификации в отношении действий лиц, спровоцировавших утечку (в рамках данного отчета InfoWatch).

Различаются действия внешних нарушителей (злоумышленников) (хакеров и других лиц) – внешние атаки, направленные против компании, воздействующие на веб-ресурсы, информационную инфраструктуру, носители корпоративной информации с целью компрометации информации, и действия внутренних нарушителей, (сотрудники компании и подрядчики, получившие права доступа к ресурсам компании) атакующих системы защиты изнутри (нелегитимный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.).

Внешняя атака – атака, совершенная внешним нарушителем.

Внутренний нарушитель – см. Нарушитель информационной безопасности организации (нарушитель).

Внешний нарушитель – см. Нарушитель информационной безопасности организации (нарушитель).

Деструктивные действия сотрудников – в рамках данного отчета об утечках информации аналитики InfoWatch к таким действиям относят действия сотрудников, повлекшие компрометацию информации ограниченного доступа: использование информации ограниченного доступа в личных целях, в том числе сопряженное с мошенничеством; нелегитимный доступ к информации (превышение прав доступа).

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными] разведками и другими заинтересованными субъектами [ГОСТ Р 50922-2006, статья 2.3.2].

Примечание – Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Инцидент – см. инцидент безопасности, инцидент информационной безопасности, компьютерный инцидент.

Инцидент безопасности (Security incident) – неблагоприятное событие в системе или сети, а также угроза такого события.

Примечание – Иногда используется термин ≪несостоявшийся инцидент≫ для описания события, которое могло обернуться инцидентом при несколько других обстоятельствах [ГОСТ 56205-2014, статья 3.2.106]

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность [ГОСТ Р 53114-2008, статья 3.2.7. ГОСТ Р ИСО/МЭК 27001-2006, статья 3.6].

Примечание – Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Канал утечки информации – способ утечки информации; предполагает сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность.

На данный момент аналитики InfoWatch выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

- «Оборудование (сервер, СХД, ноутбук, ПК)», – компрометация информации в ходе обслуживания, в результате кражи 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, USB, карты памяти и др.).
- «Сеть (сетевой канал)» – утечка через браузер (отправка данных через веб-интерфейс 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 на бумаге).
- «IM –сервисы мгновенных сообщений» - утечка информации при передаче ее голосом, в текстовом виде, а также через видео - при использовании мессенджеров.

- «Не определено» - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки.

Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, п.7 ст.2].

Конфиденциальная информация – сведения конфиденциального характера, в соответствии с Указом Президента РФ от 6 марта 1997 г. №188.

В данном отчете (исследовании) авторы относят к таким сведениям информацию, доступ к которой осуществляется строго ограниченным и известным кругом лиц с условием, что информация не будет передана третьим лицам без согласия владельца информации. Помимо персональных данных, это платежная информация, коммерческие секреты и ноу-хау, а также государственные и военные секреты. В некоторых случаях при анализе полученных сведений определить тип конфиденциальной информации не представляется возможным, поэтому она относится в категории «не определено».

Нарушитель информационной безопасности организации (нарушитель) – физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации [ГОСТ Р 53114-2008, статья 3.3.5].

В БДУ ФСТЭК России bdu.fstec.ru приведены следующие виды нарушителей/ источников угроз:

- внутренний нарушитель (потенциал низкий, средний, высокий);
- внешний нарушитель (потенциал низкий, средний, высокий).

В данном отчете (исследовании) к категории «нарушитель» авторы относят лицо, которое по ошибке или осознанно (с умыслом – злоумышленник) совершило определенные запрещенные действия, повлекшие утечку информации.

InfoWatch различает два вида нарушителей – «внешний нарушитель» и «внутренний нарушитель», а также шесть категорий нарушителей:

- Внешний нарушитель – Хакер/неизвестное лицо: взломщики компьютерных сетей, в том числе представляющие организованную киберпреступность; владельцы хакерского инструментария (библиотек); взломщики, действующие в политических и социальных целях, - хактивисты; сотрудники иностранных разведок и армий; похитители оборудования с конфиденциальной информацией.
- Рядовой сотрудник.
- Топ-менеджер (руководитель).
- Системный администратор.
- Подрядчик: сторонние исполнители работ по заказу компании, партнеры и внештатные сотрудники.
- Бывший сотрудник.

В рамках исследования топ-менеджеров, системных администраторов, а в отдельных случаях и подрядчиков авторы включают в категорию привилегированных пользователей, то есть пользователей, наделенных повышенными правами доступа к информации. Как правило, действия таких пользователей в информационной системе службами информационной безопасности контролируются слабо либо не контролируются.

Иных пользователей корпоративной информационной системы (рядовых сотрудников) авторы относят к непривилегированным, обычным пользователям.

Неправомерный доступ – см. несанкционированный доступ.

Несанкционированный доступ – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа [ГОСТ Р 53114-2008, статья 3.3.6].

Примечания:

1. Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.
2. Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них.

В данном отчете (исследовании) авторы используют также словосочетание «нелегитимный доступ».

Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [ГОСТ Р 50922-2006, статья 2.6.6]

Правонарушение – неправомерное поведение, запрещенное законом под угрозой наступления ответственности общественно вредное или опасное деяние.

Выделяют: преступление (в рамках УК РФ и УПК РФ), административное правонарушение (в рамках КОАП РФ), налоговое правонарушение (в рамках НК РФ).

В данном отчете (исследовании) авторы используют понятие «правонарушение» как родовое (общее) по отношению к преступлению и административному правонарушению.

Привилегированный пользователь – к таким пользователям InfoWatch относит категории лиц, имеющие расширенные права доступа в информационные системы, полномочия по изменению конфигураций и назначения прав администраторов другим пользователям. К привилегированным пользователям относятся руководители различного уровня, системные администраторы, в некоторых случаях подрядчики и другие категории.

Разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации [ГОСТ Р 53114-2008, статья 3.3.11].

Разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору [98-ФЗ «О коммерческой тайне» п.9 ст.3]

Событие: Возникновение или наличие определенной совокупности обстоятельств [ГОСТ Р 53114-2008, статья 3.2.8].

Примечания:

1. Характер, вероятность и последствия события могут быть не полностью известны.
2. Событие может возникать один или несколько раз.
3. Вероятность, связанная с событием, может быть оценена.
4. Событие может состоять из невозникновения одного или нескольких обстоятельств.
5. Непредсказуемое событие иногда называют «инцидентом».
6. Событие, при котором не происходит никаких потерь, иногда называют предпосылкой к происшествию [инциденту], опасным состоянием, опасным стечением обстоятельств и т.д.

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками [ГОСТ Р 53114-2008, статья 3.3.10].

В данном отчете (исследовании) InfoWatch к категории «утечка информации» относится событие, когда в результате умышленных или неумышленных действий внутреннего или внешнего нарушителя обладатель информации ограниченного доступа (компания) утрачивает контроль над этой информацией.

Умышленная (злонамеренная) утечка информации – InfoWatch понимает под ней такую утечку, когда пользователь, работающий с информацией ограниченного доступа, предполагал возможные негативные последствия своих действий, осознавал их противоправный характер, был предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду, или руководствовался иными мотивами (месть, зависть, личная неприязнь и т.д.). При этом в результате таких действий контроль над информацией со стороны ее обладателя был утрачен. При этом неважно, повлекли ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. Также к умышленным утечкам относятся все утечки, спровоцированные хакерскими атаками или физическим доступом извне к носителям информации ограниченного доступа, принадлежащей компании.