



Аналитический отчет

**Утечки информации
ограниченного доступа
в мире и России,
первое полугодие 2023 г.**



Оглавление

| | |
|--|----|
| Только факты | 3 |
| Сокращения | 4 |
| Аннотация | 4 |
| Результаты исследования | 5 |
| – Утечек информации стало больше в 2,4 раза..... | 5 |
| – Утечки персональных данных | 6 |
| – Типы данных, содержащихся в утечках | 8 |
| Заключение и выводы..... | 10 |
| Мониторинг утечек на сайте InfoWatch | 11 |
| Методика | 12 |
| Глоссарий..... | 13 |



Только факты

- Количество утечек информации в мире выросло в 2,4 раза.
- Количество скомпрометированных записей ПДн в мире за полгода составило 18,3 млрд.
- В России утекло 705 млн записей ПДн — на 72% больше, чем в I полугодии 2022 г.
- На один случай утечки данных в мире пришлось в среднем 3,3 млн записей, в России — 2,45 млн записей.
- В мире резко выросла доля утечек коммерческой тайны — с 11% до 30,4%.
- В России стало вдвое больше утечек государственной тайны.

Данные приведены за 1 полугодие 2023 года по сравнению с аналогичным периодом 2022 года.



Сокращения

| | |
|------|---|
| GDPR | General Data Protection Regulation (Регламент Евросоюза о персональных данных от 27.04.2016 г., вступил в силу 25.05.2018 г.) |
| ИБ | Информационная безопасность |
| ИС | Информационная система |
| ИТ | Информационные технологии |
| НСД | Несанкционированный доступ |
| ПДн | Персональные данные |
| ПО | Программное обеспечение |
| ЭАЦ | Экспертно-аналитический центр ГК ИнфоВотч |

Аннотация

Экспертно-аналитический центр ГК InfoWatch выпустил отчет по результатам исследования утечек сведений ограниченного доступа в мире и в России за I полугодие 2023 г. Приведено сравнение количества утечек и количества скомпрометированных записей ПДн с первым и вторым полугодием 2022 года. Представлены сравнительные диаграммы по типам скомпрометированных данных. В отчете приведены выводы о динамике картины утечек информации в мире и в России.



Результаты исследования

Утечек информации стало больше в 2,4 раза

В мировом масштабе в I полугодии 2023 г. продолжился рост количества утечек информации ограниченного доступа. Как мы отмечали в предыдущих отчетах, ключевым фактором, влияющим на динамику утечек данных в 2022 году, стала международная ситуация, обострившаяся на фоне Специальной военной операции. В 2023 году влияние этого фактора продолжается. Тектонические изменения в мировой политике и экономике провоцируют рост хакерской активности, прежде всего, действия хактивистов — политически мотивированных лиц, основным мотивом которых, как правило, выступает привлечение внимания к той или иной стороне конфликта. Как следствие, количество утечек информации в мире растет третье полугодие подряд.

В первой половине 2023 г. ЭАЦ зарегистрировал 5532 утечки информации, что на 141,2% (в 2,4 раза) больше по сравнению с аналогичным периодом 2022 г. Печальное лидерство по количеству утечек удерживает США – в первой половине 2023 г. ЭАЦ зарегистрировал 1957 случаев компрометации данных из коммерческих компаний и государственных организаций этой страны. По темпам роста утечек информации впереди Индонезия — там случаев кражи и потери данных стало больше почти в 7 раз. Для сравнения: в государствах Европы и Северной Америки случаев компрометации данных стало больше в 2,5-3 раза.

Почти во всех странах по сравнению с I полугодием 2022 года количество утечек данных выросло, причем кратно. Правда, по сравнению со вторым полугодием 2022 г. рост куда менее существенный — он составил 16,5% (см. Рисунок 1). В плане тенденций многое будет зависеть от политической ситуации в мире, от насыщения черного рынка данных и, конечно, от усилий самих компаний по укреплению систем защиты информации.

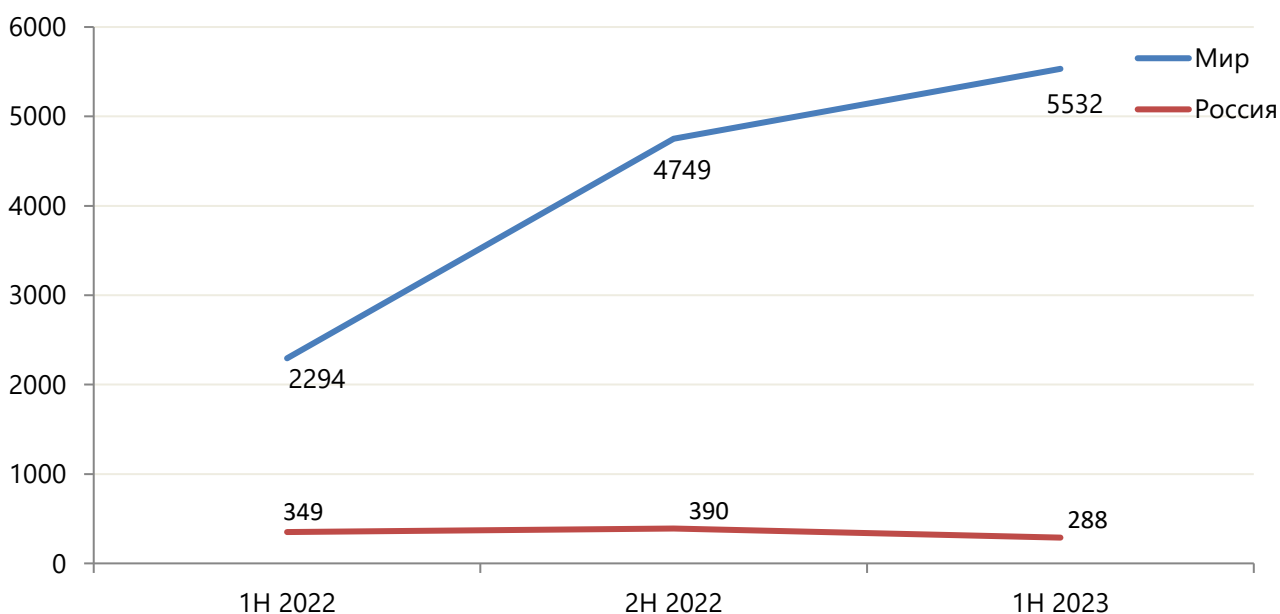


Рис 1. Количество утечек данных: Мир - Россия, 1Н 2022, 2Н 2022, 1Н 2023.



При этом в России в I полугодии 2023 г. зарегистрированных утечек информации немного уменьшилось. По сравнению с аналогичным периодом прошлого года инцидентов, приведших к компрометации данных, стало меньше на 17,5%.

Мы полагаем, что такая ситуация может быть связана с постепенной адаптацией подразделений ИТ и ИБ российских компаний и госорганов к ландшафту киберугроз, складывающемуся после начала СВО. Вместе с тем, в рамках борьбы с внутренними угрозами расширяется практика использования современных DLP-систем с мощными возможностями контентного анализа и обработки больших объемов данных с помощью искусственного интеллекта. Помимо этого, инициативы Президента и Правительства по импортозамещению средств защиты информации уже могут приносить реальные плоды — в России, прежде всего, в госсекторе, быстро снижается доля иностранного ПО, часть из которого могла содержать опасные уязвимости. Также, судя по всему, снижается давление хакеров на российские компании. Исключение составляют проукраинские группировки, которые путем кражи данных регулярно стремятся нанести репутационный ущерб организациям практически из всех отраслей российской экономики вплоть до библиотечных сайтов.

***Engadget:** Проект Reddit подвергся хакерской атаке, что позволило злоумышленникам получить доступ к ряду внутренних документов. Также хакеры могли украсть исходный код компании. Компания Reddit заявляет, что в качестве вектора атаки служил фишинг. Хакеры использовали для сотрудников «приманку» в виде страницы, имитирующей внутренний сайт. Авторизация персонала на этой ложной странице позволяла злоумышленникам получить учетные данные и токены.*

***Forbes:** «Ашан» подтвердил утечку данных клиентов, компания проводит внутреннее расследование. Данные скольких людей оказались в открытом доступе, не уточняется. Ранее Telegram-канал, посвященный утечкам, сообщил, что в файлах с данными «Ашана» почти 8 млн строк, в которых указаны имена и фамилии, телефоны, адреса электронной почты.*

Утечки персональных данных

По уточненным данным, в течение 2022 г. во всем мире утекло более 20,4 млрд записей персональных данных (включая платежную информацию). При этом второе полугодие оказалось в пять с лишним раз «урожайнее» по объему сливов информации, чем первое (Рисунок 2).

В первой половине 2023 г. было скомпрометировано почти столько же единиц ПДн, сколько за весь прошлый год — около 18,3 млрд записей.

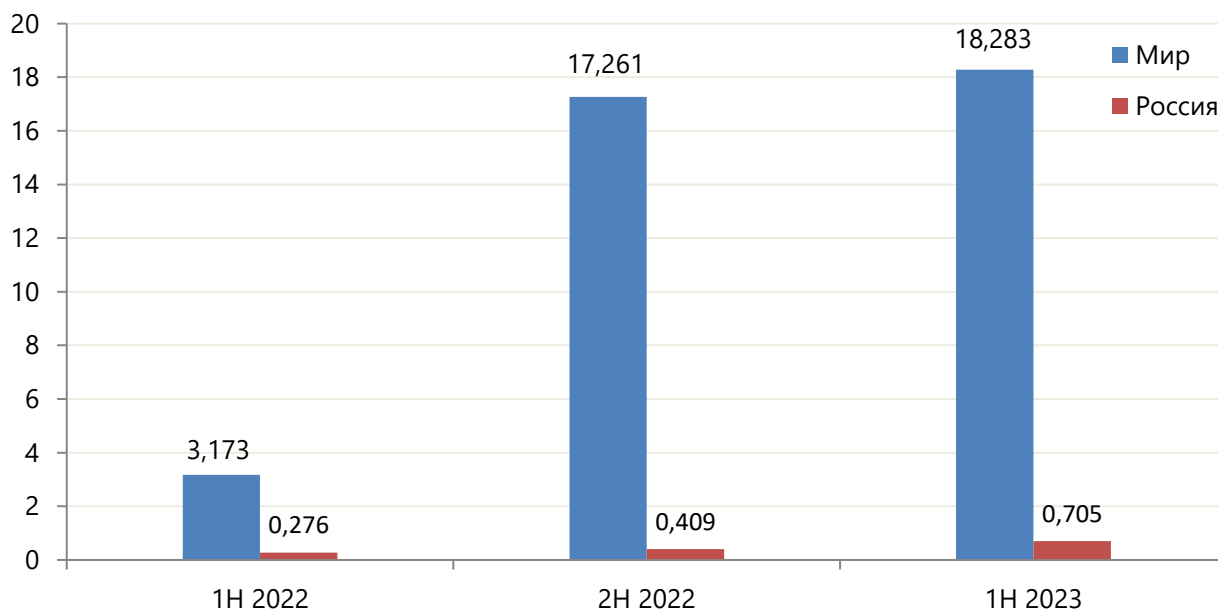


Рис 2. Количество скомпрометированных записей ПДн, млрд: Мир - Россия, 1H 2022, 2H 2022, 1H 2023.

Bleeping Computer: Компания PeopleConnect, владелец сервисов проверки биографических сведений TruthFinder и Instant CheckMate, подтвердила, что хакеры украли персональные данные порядка 20 млн подписчиков, получив доступ к резервной базе данных. Похищенные персональные данные были выставлены на хакерский форум в дарквебе.

Infosecurity: Хакеры выложили в открытый доступ дампы, который может относиться к сети ресторанов быстрого питания «Вкусно – и точка». Слитый файл содержит информацию о почти 300 тысячах соискателях компании.

На рисунке 2 можно заметить, что **в России количество скомпрометированных ПДн в последнее время неуклонно растет. Даже несмотря на снижение количества утечек, объем «слитых» данных вырос более чем на 72% и составил 705 млн записей.** Практически ежедневно поступают сообщения о взломе тех или иных крупных баз данных.

В I полугодии 2023 г. на одну утечку в мире приходилось в среднем 3,3 млн записей персональных данных, тогда как в России 2,45 млн записей (Рисунок 3). По сравнению с аналогичным периодом прошлого года среднестатистическая российская утечка «потяжелела» в три раза, что подтверждает тезис о том, что злоумышленники стали чаще получать доступ к крупным хранилищам конфиденциальной информации в нашей стране.

Здесь стоит сделать важную оговорку. **Количество скомпрометированных записей ПДн в России — 705 млн записей — необходимо рассматривать как минимальное значение, поскольку во многих сообщениях об утечках (таких случаев более 40%) не указано точное количество скомпрометированных данных и нет возможности скачать и сосчитать.**

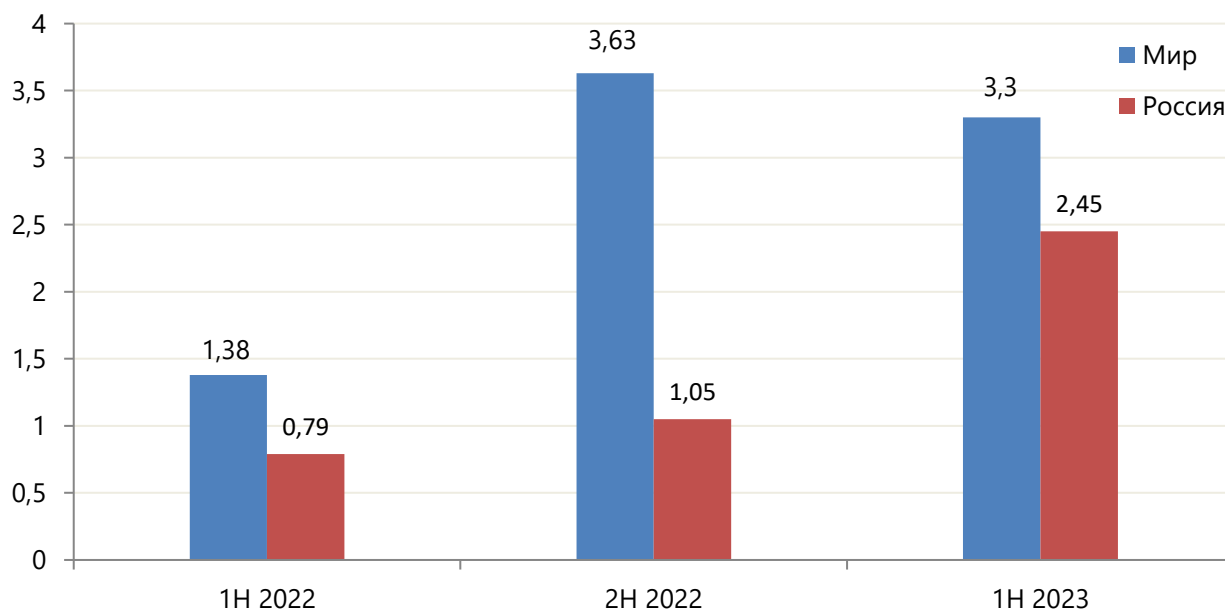


Рис 3. Среднее количество записей ПДн на одну утечку, млн: Мир - Россия, 1H 2022, 2H 2022, 1H 2023.

Dark Reading: Британский ритейлер JD Sports предупредил около 10 млн клиентов о том, что их данные были раскрыты в ходе хакерской атаки. Пострадали клиенты, которые несколько лет назад делали онлайн-заказы на товары брендов JD Sports, Size?, Millets, Blacks, Scotts и MilletSport. Были раскрыты такие персональные данные, как адреса доставки, адреса электронной почты, номера телефонов, детали заказов и последние четыре цифры платежных карт.

Habr: неизвестный хакер выложил в открытый доступ базу данных 9,8 млн клиентов интернет-магазина «Читай-город», а также информацию о пользователях книжного портала «Эксмо» (размер утечки 452 тыс. строк) и издательства «АСТ» (87 тыс. строк).

Почти каждая третья утечка конфиденциальной информации в России связана с компрометацией крупных баз данных (от 100 тыс. записей ПДн). Всего в первом полугодии 2023 г. утекло 92 таких базы, тогда как в первом полугодии 2022 г. — 72 базы.

Типы данных, содержащихся в утечках

На Рисунке 4 показано распределение скомпрометированной информации по типам данных. Отметим, что в мире в I полугодии 2023 г. существенно выросла доля утечек коммерческой тайны, ноу-хау и секретов производства. Главным образом это связано с тем, что в условиях насыщения черного рынка большими объемами персональных данных, в том числе бесплатным распространением со стороны хактивистов, многие хакерские группировки объектом своего преступного промысла стали чаще выбирать именно информацию коммерческого характера: закрытые отчеты, финансовые планы, чертежи, запатентованные изобретения и т.д. — все то, что имеет большую ценность в условиях жесткой конкурентной борьбы и за возврат чего можно потребовать крупный выкуп у компании-жертвы. В то же время в России выросла доля утечек гостайны. Кроме того, злоумышленники по-прежнему активно взламывают хранилища персональных данных. Часто это связано с неэкономическими мотивами, а с активностью хактивистов.

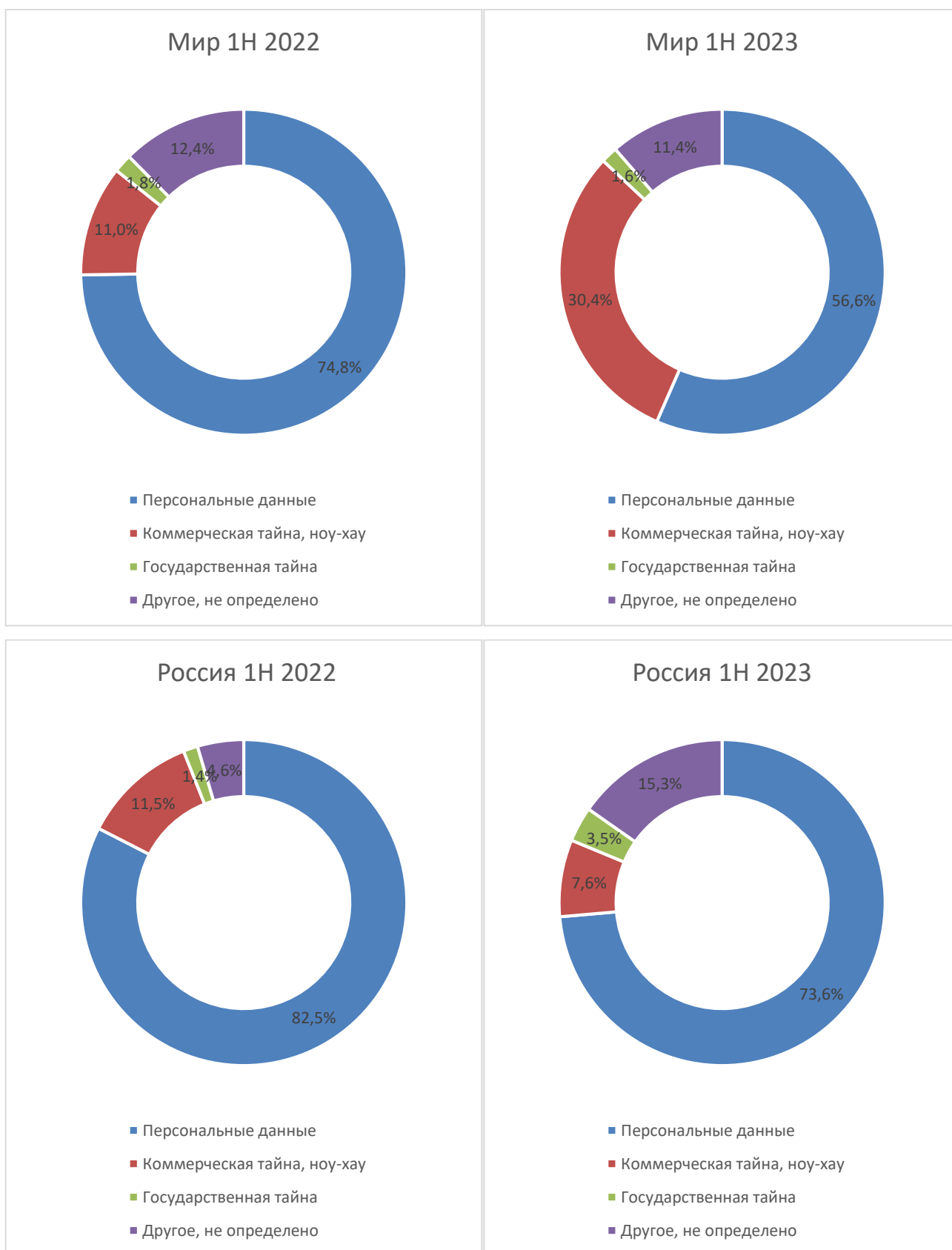


Рисунок 4. Распределение утечек по типам данных: Мир - Россия, I полугодие 2022 г. – I полугодие 2023 г.



Заключение и выводы

На мировую картину утечек информации продолжают оказывать сильнейшее влияние политические изменения, начавшиеся с февраля 2022 г. В этом контексте хакерская активность массово обусловлена не только мотивами извлечения выгоды, но и стремлением нанести репутационный вред тому или иному государству путем кибератаки на его организации. В эпоху коренного изменения мировой экономики и разгорающихся в разных частях света политических конфликтов хактивизм находит плодородную почву для роста.

Однако, основные итоги первого полугодия вселяют некоторый оптимизм. Если по сравнению с I полугодием 2022 года в мире утечек информации стало больше в 2,4 раза, то по сравнению со второй половиной прошлого года темпы роста сравнительно невелики, а в России за I полугодие этого года ЭАЦ и вовсе зафиксировал небольшое снижение количества случаев хищения и потери данных. В то же время не может не вызывать тревогу продолжающийся рост объема скомпрометированных данных (из расчета количества ПДн). Подпольный рынок пока не пришел к состоянию насыщения — ежедневно на нем публикуются десятки, а то и сотни объявлений о продаже (а часто — и бесплатном распространении) крупных баз данных. За счёт этого фактора, а также усиления защиты объектов критической информационной инфраструктуры можно было бы во втором полугодии ожидать снижения темпов роста как случаев утечек информации, так и количества утекших записей персональных данных, но полагаем, что политический хактивизм будет по-прежнему отрицательно влиять на ситуацию. Особенно он опасен, если у хакеров в организации есть «свой человек», в т.ч. сочувствующий различным течениям хактивизма или привилегированный пользователь, готовый за деньги продать аутентификационную информацию, скачать базы, заразить изнутри систему и т.п.

По итогам 2023 г. можно будет сделать более обоснованные выводы о том, какой будет динамика и структура утечек информации в ближайшее время.






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:

-  Рассылка InfoWatch
-  ВКонтакте
-  Telegram

© InfoWatch

Полное воспроизведение, опубликование материалов запрещено.

Цитирование возможно только при указании ссылки на источник.



Методика

Исследование проводится на основе собственной базы утечек информации (данных) ЭАЦ, регулярно пополняемой специалистами ЭАЦ с 2004 года.

«Методика сбора, обработки и анализа сведений об утечках охраняемой законом информации. Версия от 28.02.2023 г.»

Настоящим свидетельством Акционерное общество «Национальный Реестр интеллектуальной собственности» подтверждает, что 05.04.2023 г. файл «Методика сбора, обработки и анализа сведений об утечках охраняемой законом информации. Версия от 28.02.2023 г.» по заявлению: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ЛАБОРАТОРИЯ ИНФОВОТЧ" (ОГРН 1087746543367, ИНН 7734583888), зашифрован и помещен в виртуальную ячейку АПК НРИС.

Объект интеллектуальной собственности может быть предоставлен Депоненту на основании заявления или по запросу органов государственной власти.



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 (нарушителей - хакеров и других лиц, как известных, так и не известных) — внешние атаки, направленные против организации, воздействующие на веб-ресурсы, информационную инфраструктуру, носители корпоративной информации с целью компрометации информации, и действия внутренних нарушителей (сотрудники организации и подрядчики, получившие права доступа к ресурсам организации), атакующих системы защиты изнутри (неправомерный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.), а также допускающих утечки данных своими случайными действиями (бездействием).

Внешняя атака — атака, совершенная внешним нарушителем.

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

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

ГАС «Правосудие» — Государственная автоматизированная система Российской Федерации.

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).

Запись в ГАС «Правосудие» — запись на сайте <https://bsr.sudrf.ru/>, включающая информацию об одном судебном решении.

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 нескольких 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:

1. утрата услуг, оборудования или устройств;



2. системные сбои или перегрузки;
3. ошибки пользователей;
4. несоблюдение политики или рекомендаций по ИБ;
5. нарушение физических мер защиты;
6. неконтролируемые изменения систем;
7. сбои программного обеспечения и отказы технических средств;
8. 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):

1. «Оборудование (сервер, СХД, ноутбук, ПК)», — компрометация информации в ходе обслуживания, в результате кражи или потери оборудования.
2. «Мобильные устройства» — утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.
3. «Съемные носители» — потеря/кража съемных носителей (CD, USB, карты памяти и др.).
4. «Сеть (сетевой канал)»:
 - сетевое соединение - проникновение в сеть организации из Интернет или другую сеть общего пользования (взлом, открытый вход, наличие аутентификационной информации), нелегитимное использование внутренних ресурсов сети, в т.ч. FTP;
 - облачные сервисы (неверная настройка внешних ресурсов - серверов в «облаке» и т.п.);
 - нелегитимная публикация информации на внешнем веб-сервисе (сайт организации, GitHub и т.п.);
 - нелегитимная публикация информации на неофициальных (личных) Интернет-сервисах (яндекс-диск и т.п.), в соцсетях или мессенджерах, отправка данных через веб-интерфейс в личную почту, формы ввода в браузере, в соцсети, мессенджеры (ранее - утечка через браузер).
5. «Электронная почта» — утечка данных через корпоративную электронную почту.
6. «Бумажные документы» — утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации на бумаге).
7. «IM-сервисы мгновенных сообщений» — утечка информации при передаче ее голосом, в текстовом виде, а также через видео — при использовании мессенджеров.
8. «Не определено» — категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки.

Критическая информационная инфраструктура Российской Федерации — объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

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».

Нарушение с применением средств автоматизации — нарушение положений (требований) статей Кодекса об административных нарушениях РФ или Уголовного кодекса РФ с использованием компьютера, средств связи и сети Интернет.

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 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:

1. 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.
2. Рядовой сотрудник.
3. Топ-менеджер (руководитель).
4. Системный администратор.
5. Подрядчик: сторонние исполнители работ по заказу организации, партнеры и внештатные сотрудники.
6. 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:

- Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.
- 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]

Объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

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 отчетах (исследованиях) 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.



Субъекты критической информационной инфраструктуры — государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Судебное дело — совокупность судебных решений всех инстанций, которые относятся к одному факту нарушения Кодекса об административных нарушениях или уголовного кодекса РФ.

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 целях исследований, проводимых по данной Методике, к категории «утечка информации» относится событие, когда в результате умышленных действий внешнего нарушителя, или умышленных или неумышленных действий внутреннего нарушителя, или совместных действий внутреннего и внешних нарушителей обладатель информации ограниченного доступа (организация) утратил контроль над этой информацией.

Утечка информации неумышленная - к данной категории относятся ситуации, если к утечке информации привели действия (бездействие) пользователя (внутреннего нарушителя), которые не носят признаков умысла (случайно отправил данные по неправильному адресу, забыл закрыть доступ к сетевому серверу, Elastic-серверу или GitHub, потерял бумажные документы или другой носитель информации). Если в результате случайных действий пользователя, доступ к данным получило третье лицо, не имеющее корыстных намерений (исследователь сетевой безопасности, в том числе с применением сетевых программ-роботов, этичный хакер, прохожий), такая утечка также признается случайной.

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 организация убытки, связанные с действиями пользователя, причинён ли реальный вред субъектам персональных данных.

В целях исследований, проводимых по данной Методике, к умышленным также относятся те утечки, в результате которых данные получены внешними по отношению к организации лицами, проводившими целенаправленный поиск определённых типов данных и/или искавших возможность получить подобные или любые данные конкретных организаций. При этом на характер умысла не влияет то, вследствие чего получены данные - в результате взлома системы или за счёт ошибки сотрудника организации, не ограничившего доступ к данным. Таким образом решающим фактором при установлении характера умысла в каждой конкретной утечке выступает наличие корыстной заинтересованности сотрудников, подрядчиков и третьих лиц в отношении информационных активов организации.

Также к умышленным утечкам относятся все утечки, спровоцированные хакерскими атаками или физическим доступом извне к носителям информации ограниченного доступа, принадлежащей организации, в том числе в результате совместных действий внешнего нарушителя и внутреннего нарушителя (**гибридные утечки**).