Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года

Оглавление

Только факты

- → Число утечек информации выросло почти в два раза в мире и в полтора раза — в России (по сравнению с 1 полугодием 2021 года).
- → Во всем мире в первой половине года «утекло» около 3 млрд записей ПДн и платежной информации.
- → Количество скомпрометированных записей в России за первое полугодие превысило население страны — более 187 млн записей.
- → Доля утечек, вызванных умышленными нарушениями, превысила 96%.
- → Более 80% утечек информации спровоцированы хакерскими атаками.
- → Зафиксирован существенный рост утечек информации категории «коммерческая тайна» — ее доля превысила 13%.
- → Резко выросла доля утечек в промышленности и в торговле.
- → Более 30% информации, представленной на теневых форумах, украдено из компаний США, 13% — из российских компаний.

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 подготовил традиционный отчет по итогам исследования утечек за первое полугодие календарного года. Драматические события политического и экономического плана, случившиеся в первой половине 2022 г., не могли не оказать влияния на формирование мировой и российской картин утечек. С началом Специальной военной операции РФ многие вызовы в области кибербезопасности проявились еще сильнее, на фоне антироссийской истерики и формирования нового многополярного мира последовал очередной виток кибервойн. В новой реальности охота за персональными данными со стороны организованной киберпреступности становится все более интенсивной, количество атак неуклонно увеличивается[1], цена утечки возросла[2], и выявление внутренних злоумышленников стало еще более актуальной задачей для служб безопасности компаний по всему миру.

[1] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=331ab5d07864

[2] https://www.statista.com/statistics/987474/global-average-cost-data-breach/

Результаты исследования

Общая картина утечек в мире и в России

В процессе подготовки данных для отчета сотрудники ЭАЦ провели тщательный отбор источников информации, добавили ряд новых источников, осуществили ревизию ранее внесенных в базу утечек случаев, исходя из вновь полученных сообщений с целью проведения максимально релевантного сравнительного исследования (изменение различных параметров утечек в I полугодии 2022 г. по сравнению с аналогичным периодом 2021 г.).

В отчете по итогам 2021 г. мы констатировали, что практически во всем мире примерно на 28% произошло как снижение количества утечек, так и снижение количества скомпрометированных записей ПДн и платежной информации. Такая ситуация, на наш взгляд, была обусловлена комплексом факторов: рост латентности инцидентов (прежде всего внутреннего характера, то есть по вине сотрудников), эффект от ранее внедренных DLP и других систем защиты, временное насыщение подпольного рынка данных (ДаркВеба), внимание этого рынка к обогащению ранее украденных баз данных, а также распространение вредоносного ПО, операторы которого в первую очередь нацеливаются не на кражу данных, а на их блокировку с целью получения выкупа. Однако, с началом 2022 г. последовал значительный рост количества сообщений об утечках.

По итогам первой половины 2022 г. **в мире** Экспертно-аналитическим центром InfoWatch зарегистрирована **2101** утечка информации ограниченного доступа, что почти в два раза (на 93,2%) больше, чем за аналогичный период прошлого года. Количество утечек **в России** за первое полугодие 2022 г. составило 305 (+45,9% по сравнению с I полугодием 2021 г.) — см Рисунок 1.

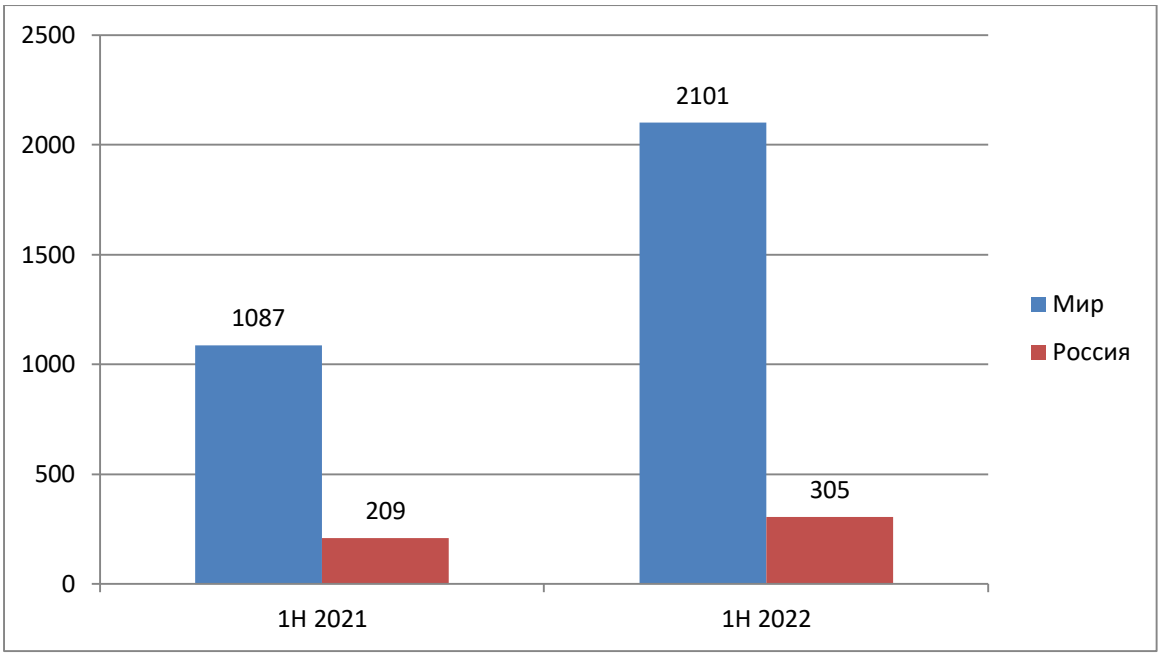


Рисунок 1. Число утечек: Мир — Россия, I полугодие 2021 г. — I полугодие 2022 г.

Обратные тенденции отмечены в отношении количества скомпрометированных записей персональных данных и платежной информации. В I полугодии 2022 г. в мире «утекло» на 27,8% меньше единиц информации, чем в I полугодии 2021 г. Судя по всему, это связано с избирательной активностью злоумышленников, которые старались похищать только действительно ликвидные на черном рынке данные. В то же время, компаниям, накопившим огромные базы персональных данных, в целом удалось устоять под натиском киберпреступников — в первые шесть месяцев 2022 г. зарегистрировано только семь случаев, в результате каждого из которых утекло от 100 млн записей ПДн. В I полугодии 2021 г. таких случаев было десять. Кроме того, удалось избежать случайных утечек подобного масштаба, вызванных неверными настройками облачных хранилищ, ошибками на веб-серверах и т.д. Судя по всему, компании уделили серьезное внимание защите своих ресурсов от случайных утечек информации.

В то же время в России объем «утекшей» информации вырос в 16,75 раза и составил 187,6 млн записей — см. Рисунок 2. Практически еженедельно в первой половине года публиковались сведения о крупных утечках из российских компаний и госорганов, в их числе: РЖД, авиакомпания «Победа», телекоммуникационные компании «Ростелеком» и «ВымпелКом», информационный портал Ykt.ru, сервисы «Мир Тесен», Fotostrana.ru и Text.ru, развлекательный ресурс Pikabu, сервисы доставки «Яндекс.Еда», Delivery Club и 2 Berega, школа управления «Сколково», образовательный портал GeekBrains.

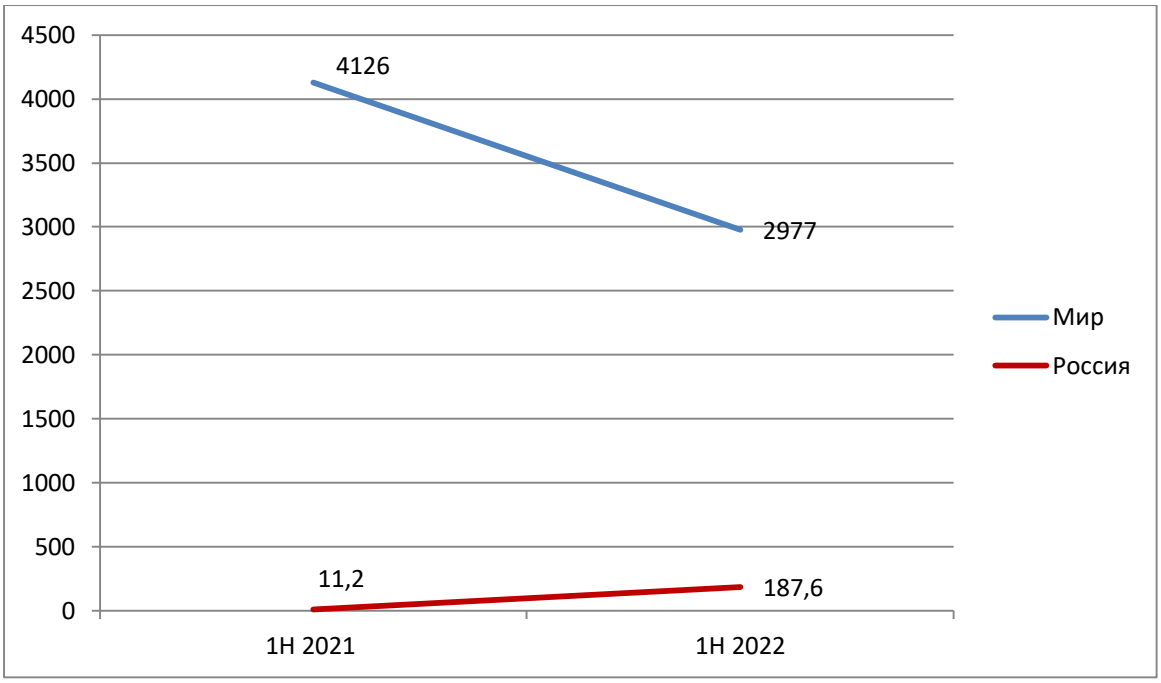


Рисунок 2. Количество утекших записей, млн: Мир — Россия, I полугодие 2021 г. — I полугодие 2022 г.

Таким образом всего за полгода в Сеть попало количество записей ПДн, которое превышает население России.

В первой половине 2022 г. резко выросла доля утечек, спровоцированных действиями внешних нарушителей. По сравнению с аналогичным периодом прошлого года в мире она выросла примерно с 60% до почти 90%, а в России в несколько раз — с 21,5% до 81% (Рисунок 3). Полагаем, что такая аномальная динамика связана с несколькими причинами.

Во-первых, произошел резкий всплеск хакерской активности, наметившийся еще в самом начале года, то есть до начала Специальной военной операции РФ и последующих событий в мире. Но уже с марта началось вовлечение в т.н. «кибервойска» большого количества жителей Украины и других стран, создание ресурсов, упрощающих участие в кибератаках «диванных войск», бесплатное распространение ряда профессиональных хакерских инструментов, которые можно использовать не только против сайтов госорганов. Также эксперты отмечают, что резко вырос спрос на киберботы, используемые для разведки ресурсов и различных видов кибератак.

Во-вторых, ослабление контроля за информационными активами в период пандемии спровоцировало объединение усилий внешних нарушителей (хакеров) с нарушителями внутренними (персоналом), то есть склонение сотрудников к хищению данных, внедрение инсайдеров.

В-третьих, вероятно, еще выше стала доля скрытых (так называемых, латентных) внутренних нарушений, то есть утечки, вызванные действиями или бездействием сотрудников, в последнее время фиксируются намного реже, чем еще в прошлом году.

В-четвертых, специфика законодательства США и ряда других стран предполагает суровую ответственность за сокрытие факта утечки или несвоевременное оповещение регуляторов, поэтому компаниям выгоднее обвинять в нарушениях «русских хакеров» и другие типы внешних нарушителей, нежели проводить объективные расследования, при которых зачастую приходится «выносить сор из избы».

Также важно отметить произошедшее на чёрном рынке разделение труда, создание новых хакерских инструментов и появление предложений по их сдаче в аренду, т.е. существенное расширение и развитие модели «киберкриминал как сервис».

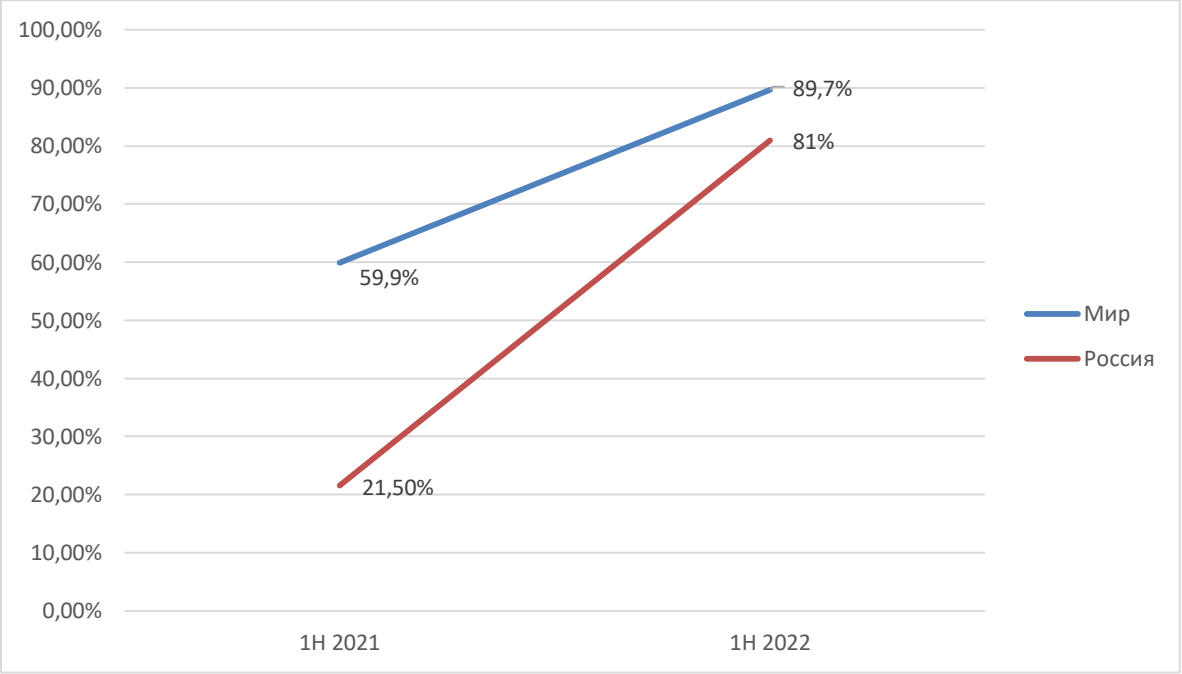


Рисунок 3. Динамика доли утечек вследствие внешнего воздействия: Мир — Россия, I полугодие 2021 г. — I полугодие 2022 г.

Вполне ожидаемо, что на фоне повышения ценности конфиденциальной информации в цифровую эпоху и снижения уровня защищенности цифровых активов в период пандемии, а также на новом витке кибервойн (кибератак, кибероперaций) продолжается рост доли утечек умышленного характера. Всплеск хакерской активности при одновременном увеличении латентности инцидентов, прежде всего случайного характера, приводит к превалирующей доле умышленных утечек. В мире и в России он превысил 96% по итогам I полугодия 2022 г. (Рисунок 4).

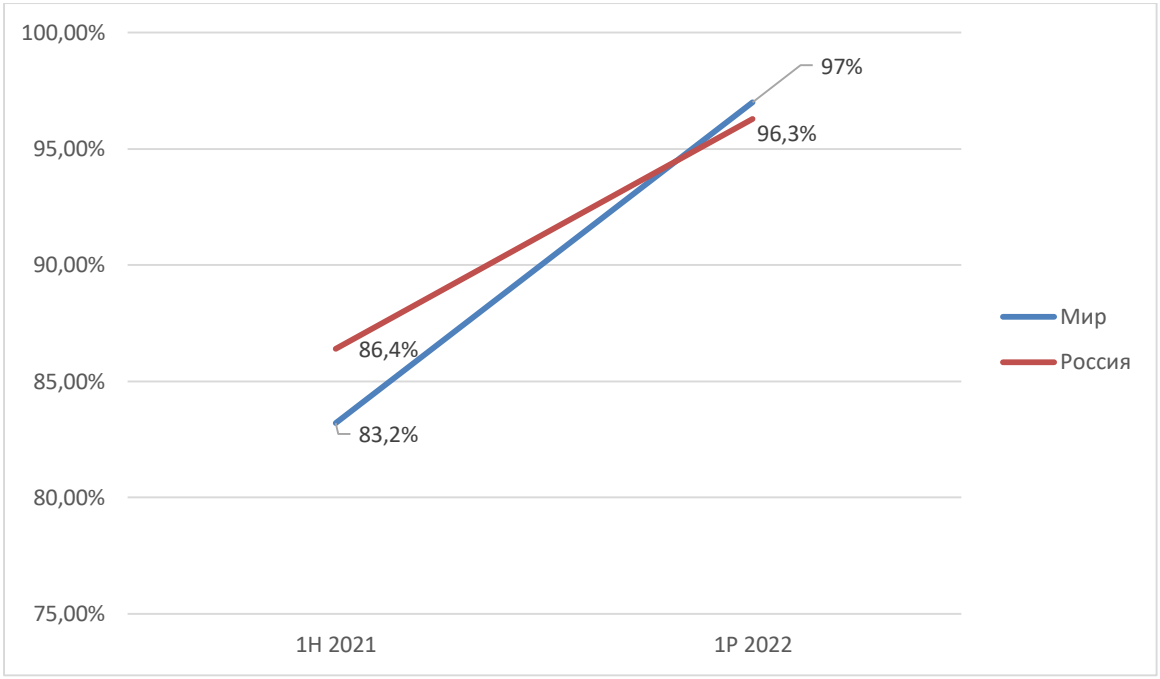


Рисунок 4. Доля умышленных нарушений: Мир — Россия, I полугодие 2021 г. — I полугодие 2022 г.

Одновременно с этим в мире с 57,4% до 67% выросла доля умышленных нарушений внутреннего характера (Рисунок 5).

Однако, стоит сделать важную оговорку: с учетом высокой латентности случайных нарушений реальная доля умышленных утечек может быть ниже. В России доля умышленных нарушений среди утечек по вине персонала и подрядчиков снизилась с 81,4% до 75,5%, что может быть следствием некоторого усиления мер контроля за сотрудниками.

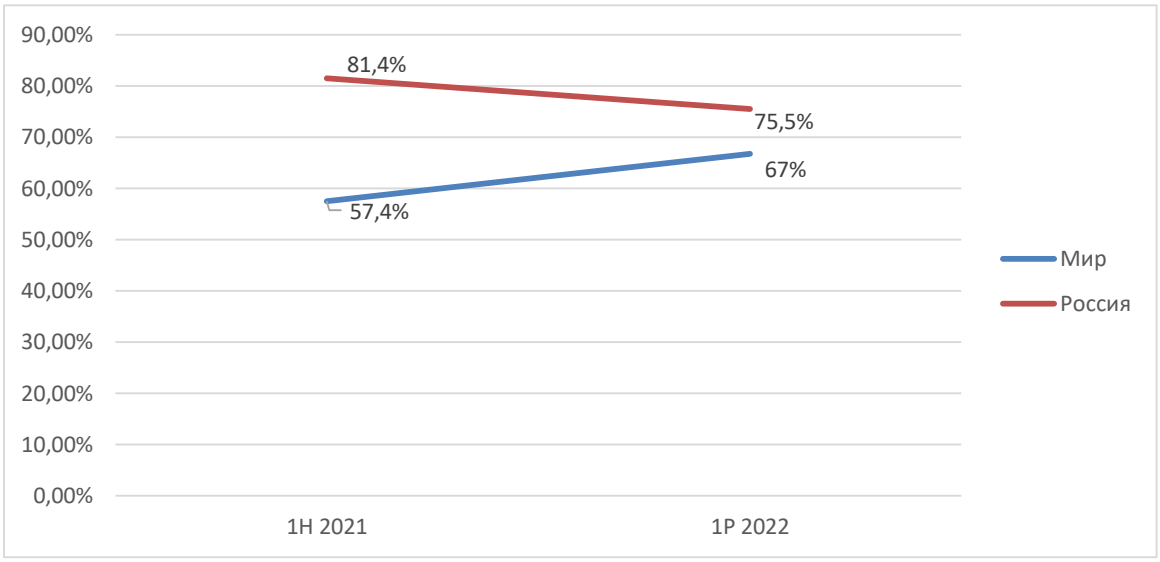


Рисунок 5. Доля умышленных нарушений внутреннего характера: Мир — Россия, I полугодие 2021 г. — I полугодие 2022 г.

Доминирующим типом информации на карте утечек информации остаются персональные данные (Рисунок 6). Но их доля в первой половине 2022 г. сократилась как в России, так и в мире. Это произошло за счет опережающего роста утечек коммерческих секретов — **интенсификация кибервойн по всем мире привела к более активной борьбе организованных групп хакеров за сведения экономического плана**. Вместе с тем, если судить по опубликованным данным, существенно снизилась доля утечек государственных секретов.

Рисунок 6. Распределение утечек по типам данных: Мир — Россия, I полугодие 2021 г. — I полугодие 2022 г.

Среди виновников утечек в мире превалируют хакеры и неизвестные лица. Эта же категория в первом полугодии 2022 г. впервые вышла на первый план и в России, где долгое время основными нарушителями выступали сотрудники (Рисунок 7). В условиях активизации хакеров основные силы компаний брошены на отражение внешних угроз. Возможно, в такой ситуации у служб безопасности не всегда хватает ресурсов на противодействие внутренним нарушениям: если инциденты случайного характера можно выявлять относительно успешно и в режиме цейтнота, используя правильно настроенные DLP, то умышленные действия сотрудников в новой реальности стало выявлять и предупреждать гораздо сложнее.

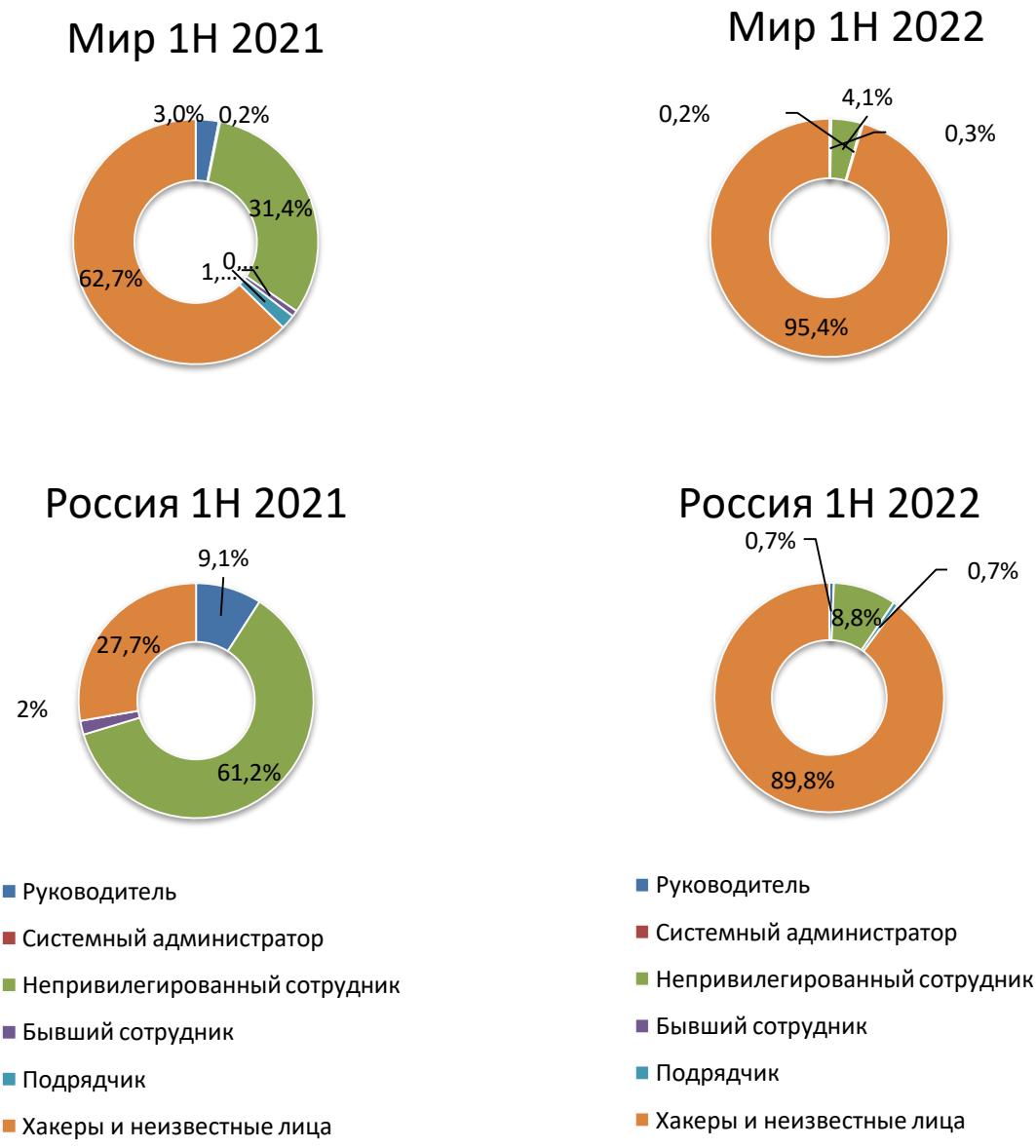


Рисунок 7. Распределение утечек по виновникам: Мир — Россия, I полугодие 2021 г. — I полугодие 2022 г.

В условиях чрезвычайно высокой хакерской активности и роста латентности внутренних нарушений еще более заметную роль в каналах начала играть Сеть. Вместе с тем, пока на второй план отошли сервисы мгновенных сообщений (IM) и электронная почта, резко упала доля бумажных носителей (Рисунок 8).

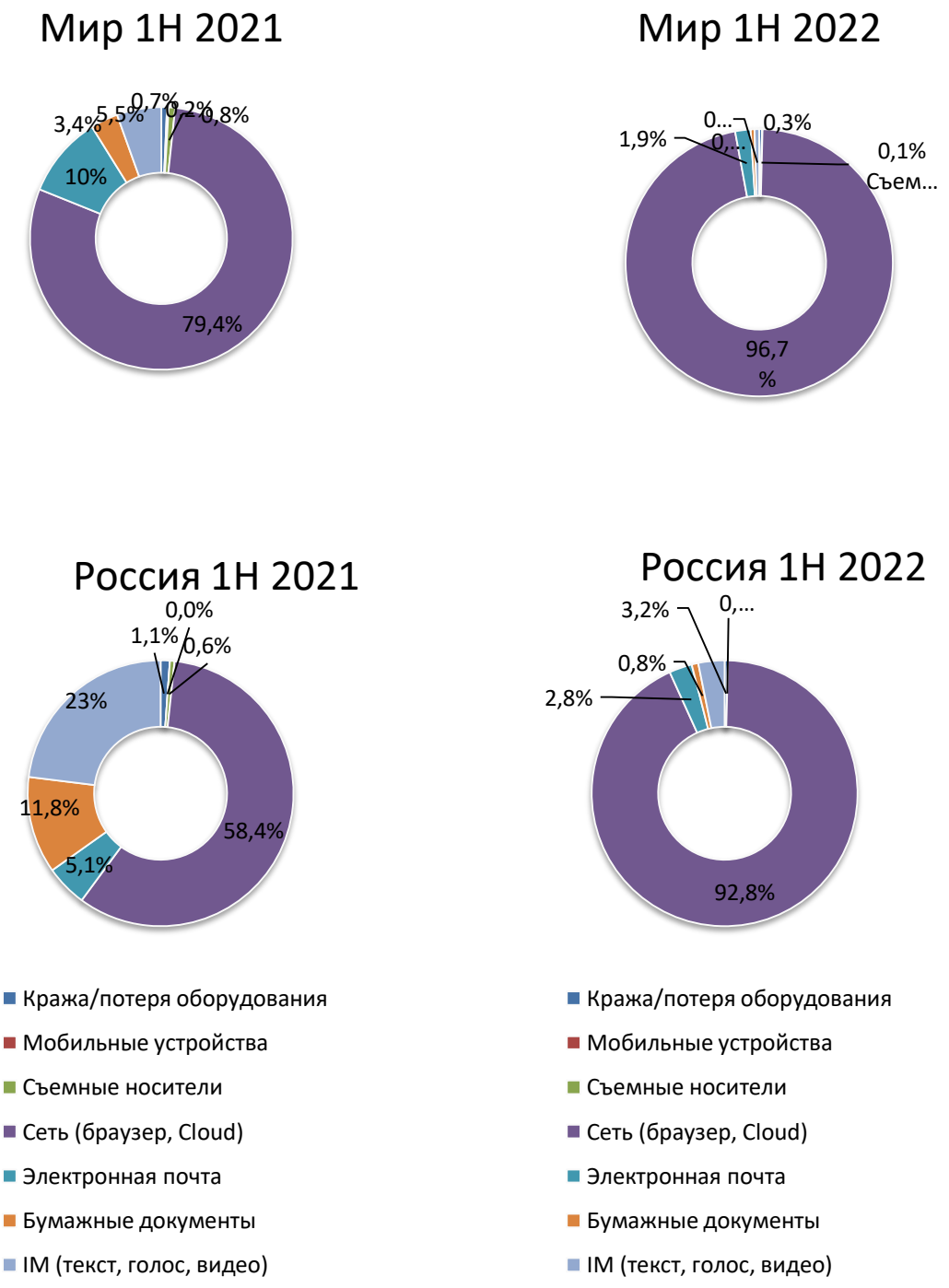
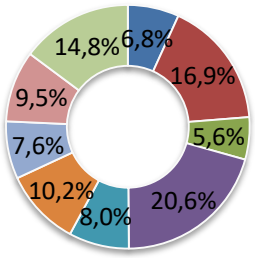


Рисунок 8. Распределение утечек по каналам: Мир — Россия, первое полугодие 2021 г. — первое полугодие 2022 г.

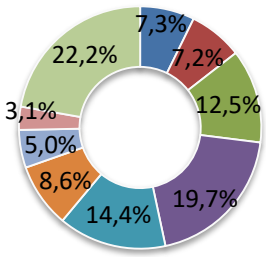
Как в мире, так и в России, резко выросла доля утечек в промышленности и в сегменте «Торговля и HoReCa» (Рисунок 9). Судя по всему, в первом случае организованная

киберпреступность выполняет заказы по добыче ценных производственных сведений, в том числе оборонного характера, а во втором — старается похитить клиентские базы, заручившись поддержкой инсайдеров в торговых компаниях, сетях отелей и общепита. Небольшое снижение долей финансового сегмента и госсектора не должно вселять оптимизма, поскольку в абсолютном выражении утечек в этих сферах стало больше. Вместе с тем, сюрпризом стало существенное снижение процента утечек в муниципальных органах власти и организациях. Можно предположить, что хакеры увлеклись другими направлениями и реже стали атаковать муниципальные структуры. Кроме того, на наш взгляд, сыграла свою роль высокая скрытность инцидентов в муниципалитетах, где часто отсутствуют необходимые ресурсы.

Мир 1H 2021

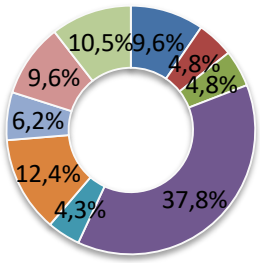


Мир 1H 2022

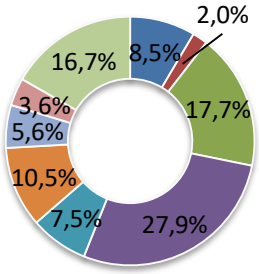


- Банки и финансы
- Здравоохранение
- Торговля, HoReCa
- Высокие технологии
- Промышленность и транспорт
- Госорганы и силовые структуры
- Образование
- Муниципальные учреждения
- Другое/не определено

Россия 1H 2021



Россия 1H 2022



- Банки и финансы
- Здравоохранение
- Торговля, HoReCa
- Высокие технологии
- Промышленность и транспорт
- Госорганы и силовые структуры
- Образование
- Муниципальные учреждения
- Другое/не определено

Рисунок 9. Отраслевое распределение утечек, Мир — Россия, первое полугодие 2021 г. — первое полугодие 2022 г.

Утечки информации ограниченного доступа — ДаркВеб

В этом отчете отдельную главу мы решили посвятить исследованию утечек информации ограниченного доступа, обнаруженных в ходе мониторинга теневых и «полутеневых» ресурсов, таких как форумы в ДаркВебе, а также закрытые, анонимные Telegram-каналы. В первую очередь такой интерес к теме связан с заметно возросшим числом кибератак с последующими утечками конфиденциальной информации, а также со снижением интенсивности потока сообщений об утечках в СМИ и в других открытых источниках.

Для исследования мы выбрали период публикации объявлений о продаже данных (а также сообщения, где данные предлагались для бесплатного скачивания) с 1 января по 30 июня 2022 г. В результате мы обнаружили сведения о **2036** утечках.

Необходимо пояснить, что сведения об одной утечке могут быть обнаружены как сразу в нескольких источниках (открытых и закрытых), так и только в одном. В данном случае выбраны публикации об утечках в ДаркВеб вне зависимости от наличия копий или сообщений в других источниках, в т.ч. СМИ.

Важно отметить, что в данной главе отчета относим все найденные утечки к категории умышленных, независимо от их «механизма»: кража данных сотрудников или следствие хакерской атаки. Из текстов таких объявлений мы не можем определить, кто стал виновников утечки — сотрудник или хакер. В то же время можно предположить, что, вероятнее всего, в основном речь идет о внешнем векторе воздействия, в результате преобладающая часть объявлений о продаже создается хакерами или их подельниками. Даже в том случае, если конфиденциальная информация утекла из-за потери физического носителя, такого как USB-флеш-накопитель, или по оплошности сотрудника компании, обнаружение данных злоумышленником и их выставление на продажу переводит такие утечки в категорию умышленных. Мы допускаем, что анонимно продавать данные может и укравший их сотрудник организации или его сообщник, но считаем долю таких сообщений небольшой.

На рисунке 10 представлено распределение обнаруженных утечек данных по странам, где действуют компании и организации, из которых «утекла» информация. Всего была найдена информация об утечках в 104 странах, для части утечек страна не установлена (9% найденных объявлений о продаже или бесплатном «сливе» данных).

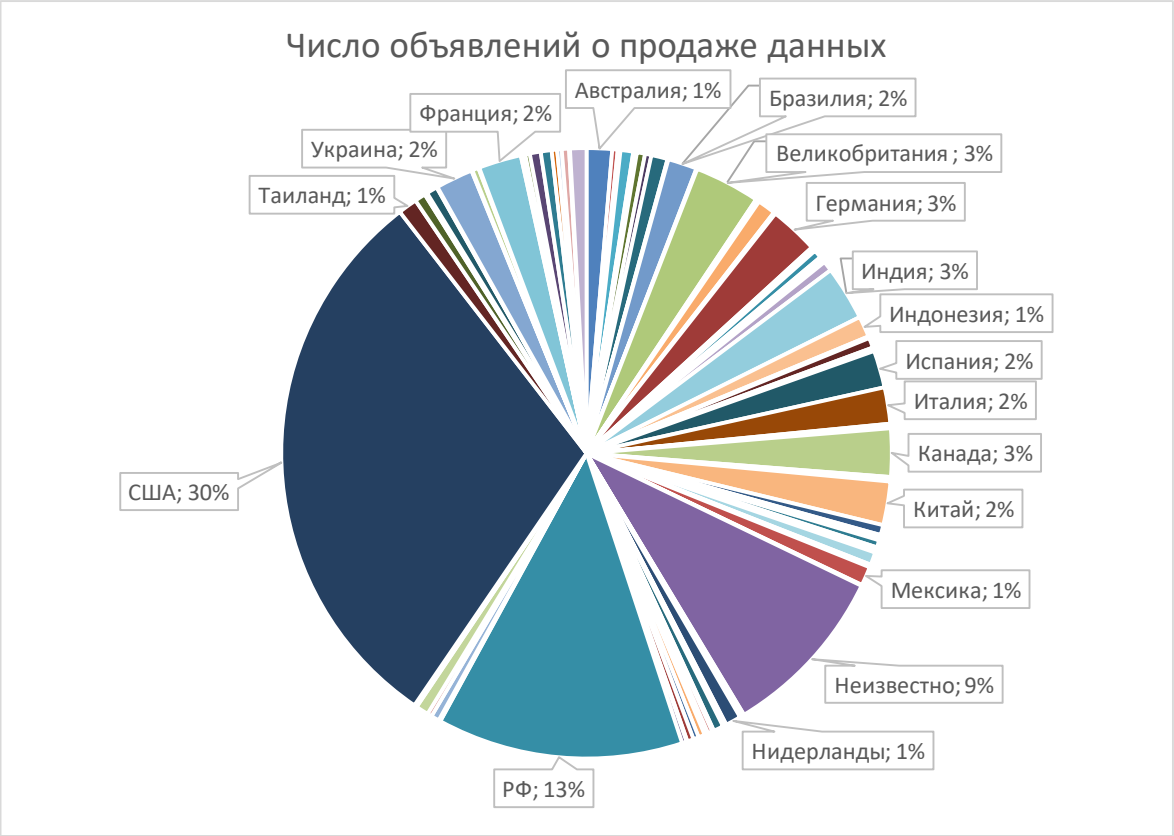


Рис 10. Распределение обнаруженных в ДаркВебе утечек по странам

Распределение по топ-11 странам выглядит следующим образом:

США — 30%;

РФ — 13%;

Великобритания/Германия/Индия/Канада/ — по 3%;

Бразилия/Испания/Италия/Китай/Украина/Франция — по 2%.

В своих отчетах мы регулярно отмечаем, что первое место по количеству утечек занимают США. Не является исключением и мониторинг утечек в ДаркВебе и закрытых Telegram-каналах. Такое положение вполне объяснимо: США все еще обладают самой мощной экономикой мира, именно здесь зарегистрированы сотни корпораций, ряд из которых оперируют данными миллиардов людей и обладают очень ценными ноу-хау. На втором месте — Российская Федерация, число кибератак на информационные ресурсы которой существенно возросло с марта этого года, что привело к большему, чем в аналогичном периоде 2021 года, числу утечек конфиденциальной информации.

На Рисунке 11 представлено отраслевое распределение утечек из компаний и организаций по всему миру, чьи данные оказались в ДаркВебе.

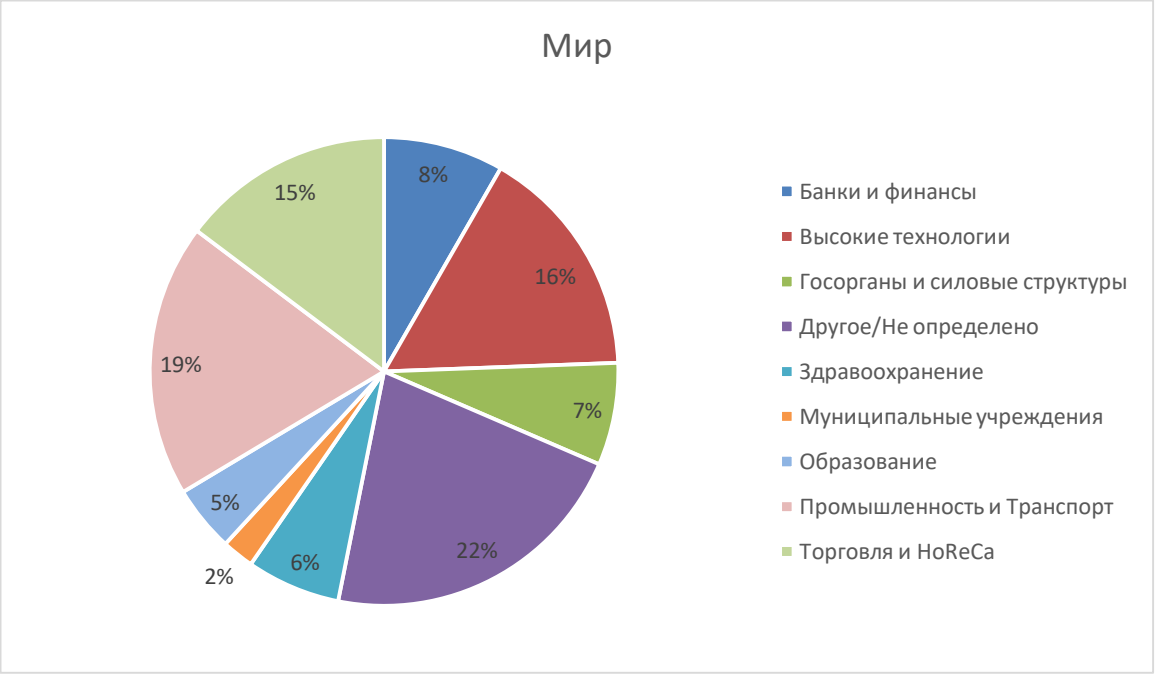


Рис 11. Распределение утечек в ДаркВебе по отраслям организаций в мире

Больше всего (19%) объявлений о продаже данных относилось к промышленным и транспортным компаниям, включая как пассажирские перевозки, так и грузовые. На втором месте (16%) — объявления о продаже данных высокотехнологичных компаний, а на третьем — торговых сетей и сектора HoReCa (15%).

Сравним распределение утечек в ДаркВебе по отраслям организаций в мире (рис. 11) и в России (рис. 12). Во многом распределения похожи за исключением нескольких аспектов:

1. В России доля утечек, которые пришлись на организации сферы «Торговля и HoReCa» несколько выше, чем в мире — 27% против 22%. По-видимому, хакеры в последнее время испытывали повышенный интерес к масштабным клиентским базам крупных российских ритейлеров и поставщиков услуг.

2. Доля утечек из промышленных и транспортных организаций в России (10%) оказалась ниже, чем в мире (19%).

Рис 12. Распределение утечек в ДаркВебе по отраслям организаций в России

При рассмотрении распределений по отраслям организаций утечек, обнаруженных в объявлениях в ДаркВебе, и утечек, суммарно зафиксированных ЭАЦ ИнфоВотч, хотим отметить, что во многом они хорошо коррелируют — см. таблица 1.

Таблица 1. Сравнение утечек, выявленных в ДаркВеб, со сводным количеством утечек, выявленных из различных источников

	Общая база		Утечки в ДаркВебе	
	Мир	Россия	Мир	Россия
Банки и финансы, %	7,3	8,5	8	10
Высокие технологии, %	19,7	27,9	16	16
Госорганы и силовые структуры, %	8,6	10,5	7	12
Другое/Не определено, %	22,2	16,7	22	27
Здравоохранение, %	7,2	2	6	1
Муниципальные учреждения, %	3,1	3,6	2	3
Образование, %	5	5,6	5	4
Промышленность и транспорт, %	14,4	7,5	19	10
Торговля и HoReCa, %	12,5	17,7	15	17

Значительнее всего отличаются доли утечек информации в высокотехнологичных компаниях: если **в мире** на такие компании приходится 19,7% утечек от общего

количества, то в ДаркВебе доля составляет 16%. Еще больше различия обнаруживаются, если рассматривать распределения утечек в секторе «Высокие технологии» **в России**: доля утечек от общего количества — 27,9%, а в объявлениях в ДаркВебе — 16%. Можно предположить, что целью хакеров при кибератаках в меньшей степени являются компании этого сегмента рынка. Такая же картина наблюдается и для организаций сферы «Здравоохранение».

Но если рассматривать промышленные и транспортные компании, то ситуация обратная. В мире (19%) и России (10%) чаще хакеры выкладывали объявления о продаже или передаче данных в ДаркВебе. В общем числе утечек информации доли в мире и России составили 14,4% и 7,5%, соответственно.

Как в глобальном масштабе, так и в России есть внушительная часть случаев, когда отраслевую принадлежность пострадавшей компании либо невозможно отнести ни к одной из обозначенных категорий, либо вообще нельзя определить. В общем количестве утечек доля случаев категории «Другое/не определено» составляет 22% в мире и 16,7% в России, среди утечек из ДаркВеба — 22% в мире и 27% в России. Такое значительное увеличение доли утечек в организациях «неопределенной отрасли» объясняется тем, что **зачастую в объявлениях не уточняют происхождение данных, предлагают приобрести базу «персональных данных россиян», «паспортов россиян» и т.д.**

В этом исследовании мы также распределили пострадавшие компании и организации по размеру: маленькие (<50 сотрудников), средние (<500 сотрудников) и крупные (≥500 сотрудников) — см. Рисунок 12. Распределение объявлений о продаже данных из организаций по их размеру выглядит следующим образом:

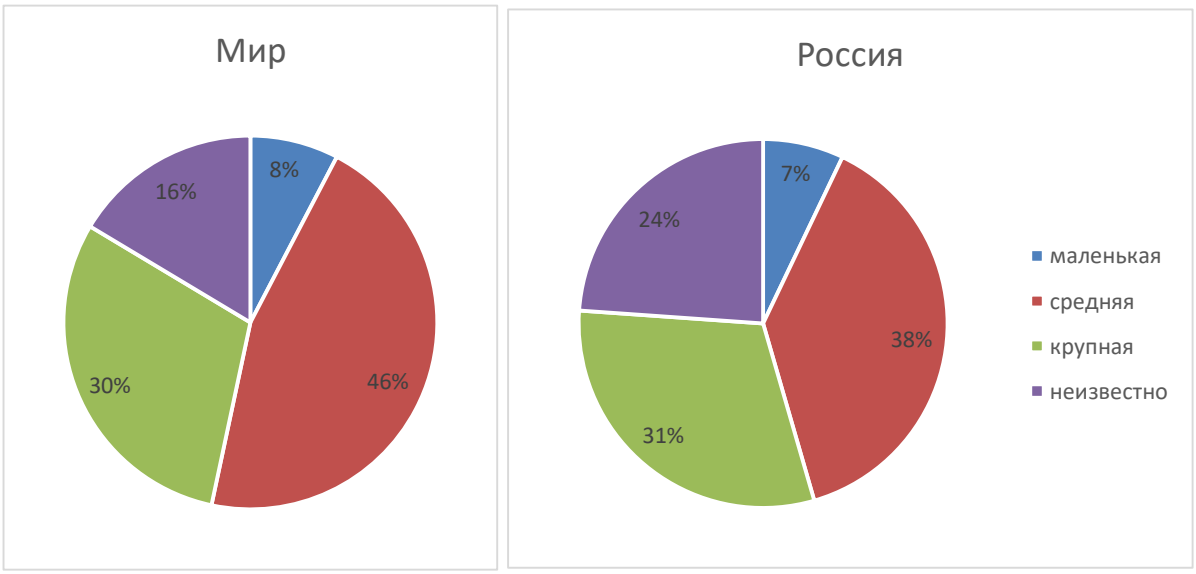


Рис 13. Распределение утечек из объявлений в ДаркВебе по размеру организаций

Из диаграммы утечек в мире заметно, что в ДаркВебе за период с 1 января по 30 июня 2022 г., в основном, продавали данные организаций среднего сегмента — 46%, но также на черном рынке продают и большое количество конфиденциальной информации крупных компаний — 30%. В 16% случаях нет возможности установить размер организации, в которой произошла утечка данных. Схожее распределение мы наблюдаем и в России за исключением того, что доля организаций, для которых не установлен их размер, выше — 24% в России против 16% в мире.

Отдельное внимание в исследовании решено было уделить изучению профилей авторов объявлений в ДаркВебе. Конечно, в аккаунтах теневых дельцов информации довольно немного, но даже представленные сведения позволяют судить об опыте этих людей. Мы распределили авторов объявлений о продаже данных по следующим четырем категориям: завсегдатай форума, старожил, новичок, администратор или создатель форума. Мы взяли только те объявления о продаже, где удалось установить статус автора и получили следующее распределение (Рисунок 14).

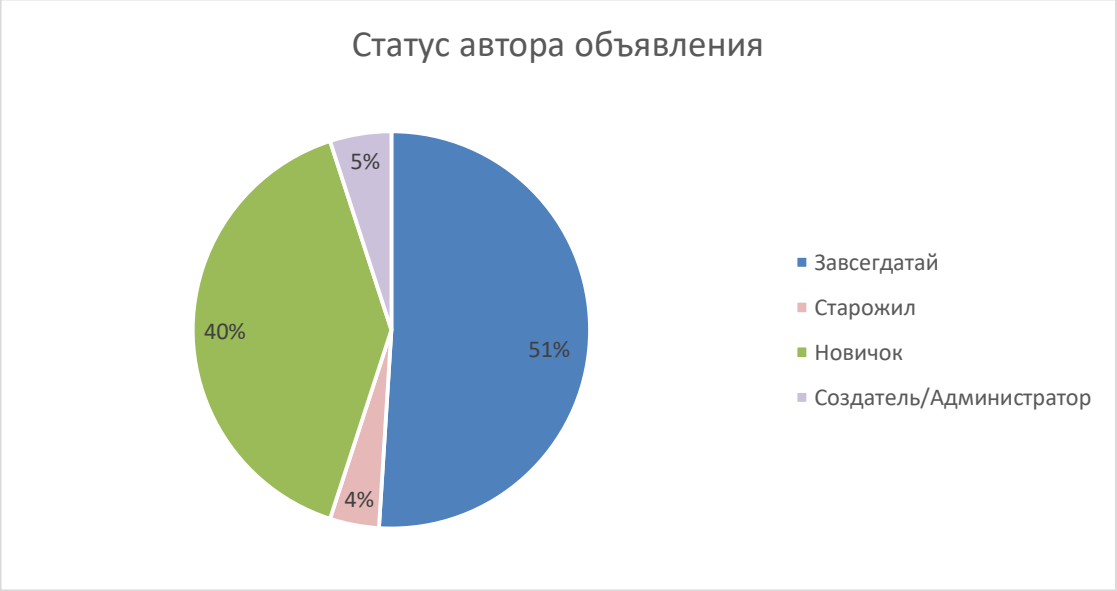


Рис. 14. Распределение объявлений в ДаркВебе по статусу авторов

Авторами наибольшего числа объявлений являются завсегдатаи форумов — 51%, вторые в списке новички — 40%. Примерно в равных долях создатели или администраторы и старожилы — 5% и 4%, соответственно.

Какой же тип данных наиболее часто продается на теневых форумах или в специализированных Telegram-каналах? Ответ на этом вопрос предсказуем. **Из всех объявлений, в которых удалось установить тип продаваемой информации, в 81% случаев продавцы на теневых форумах предлагали приобрести базы персональных данных клиентов компаний и государственных органов.** В 13%

случаев речь идет о продаже коммерческих тайн компаний, а 3% и 2% объявлений, соответственно, предлагают платежную информацию и сведения категории «государственная тайна».

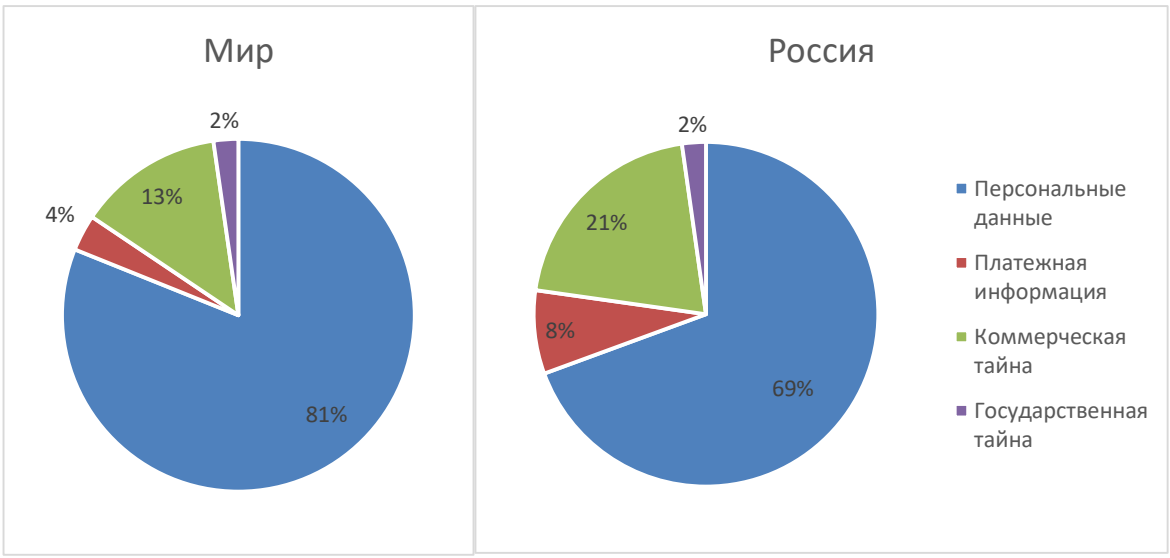


Рис. 14. Распределение объявлений по типу продаваемой информации.

И в мире, и в России основной целью хакеров остаются персональные данные: 81% инцидентов относятся к ПДн в мире и 60% в России. Интересно, что доля украденных коммерческий тайн в России в распределении выше, чем в мире: 21% против 13%. Вероятно, это связано с кибервойной, проводящейся против организаций, формирующих российскую экономику.

Две самые крупные с точки зрения числа скомпрометированных уникальных записей персональных данных утечки данных в мире — это утечка из бразильской компании-разработчика платежного инструмента (66 миллионов записей) и утечка пользователей онлайн-сайта для взрослых (65 миллионов записей). Встречаются в теневой Сети и совсем небольшие базы, содержащие около 1000 записей.

При сравнительном анализе распределения утечек из объявлений в Дарквебе с распределением общего количества утечек можно отметить, что **превалирующая доля утечек в обоих случаях относится к персональным данным — в мире 82,9% в общем распределении, 81% в распределении утечек в ДаркВебе.** На втором месте утечки, связанные с кражей коммерческих тайн компаний: в мире 13,4% в общем распределении и 13% в распределении утечек в ДаркВебе. В обоих источниках также невелика доля утечек сведений, составляющих государственную тайну, — порядка 2%. Доля утечек из объявлений в ДаркВебе, пришедшихся на платежную информацию, составляет 4% в мире. В общем распределении эта выборка несколько теряется и составляет уже 1,5%. А в России в объявлениях о продаже или бесплатной передаче данных платежная информация встречается достаточно часто — в 8% случаев. В общем распределении это значение снова теряется — всего 0,7%.

Заключение и выводы

Драматические события, происходящие в мире, не могли не отразиться на формировании картины утечек информации ограниченного доступа. Интенсификация кибератак, развязывание новых кибервойн, широкое распространение хакерских инструментов и повышение значимости информации в мире, а также стремление ее использовать как инструмент шантажа, экономического и политического давления, — все это привело к всплеску утечек, вызванных внешним воздействием. Вместе с тем, на наш взгляд, еще больше выросла латентность внутренних нарушений. Если в компании нет на вооружении современных инструментов защиты от действий персонала, службам безопасности крайне затруднительно проводить мероприятия по выявлению инцидентов и в сборе доказательной базы для проведения расследований. Ситуация осложняется тем, что вектор многих атак становится все более сложным, злоумышленники из-за пределов информационного контура организации все чаще вступают в сговор с сотрудниками и реализуют многоступенчатые схемы похищения информации.

Обращает на себя внимание тот факт, что значительно выросла доля утечек коммерческой тайны. Наибольшее давление злоумышленников в I полугодии 2022 г. испытывали производственные компании, в том числе связанные с оборонным сектором. От кражи персональных данных чаще всего страдал ритейл и традиционно высокотехнологические компании.

Исследование сообщений о продаже данных в ДаркВебе позволяет сделать вывод о процветании этого сегмента: ежедневно на подпольных форумах появляются десятки объявлений о продаже свежих баз данных, также злоумышленники предлагают (зачастую бесплатно или за символически деньги) базы из утечек прошлых лет. Усилия правоохранительных органов пока не дают ожидаемого эффекта — закрытие крупнейшей хакерской торговой площадки RaidForums и разгром ряда группировок киберпреступников походит на борьбу Геракла с Лернейской Гидрой: стоило ей отрубить одну голову, как на ее месте вырастала новая. Посмотрим, как на ситуацию в России повлияет ввод оборотных штрафов, заставит ли это организации изменить своё отношение к обеспечению безопасности персональных данных и к задачам специалистов по информационной безопасности.

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
- VK
- Telegram

Экспертно-аналитический центр InfoWatch

www.infowatch.ru/analytics

Методика

Исследование проводится на основе собственной базы утечек ЭАЦ, регулярно пополняемой специалистами ЭАЦ с 2004 года. Источником для этой базы являются публичные сообщения[3] о случаях утечек информации из учреждений, организаций, предприятий любых организационных форм и форм собственности, включая органы государственной власти и управления, а также данные из некоторых закрытых и условно-закрытых источников (форумы, чаты, каналы).

В настоящий момент количество записей в базе превышает 20 тысяч.

Исследования ЭАЦ, в основном, ориентированы на анализ сообщений об утечках данных на английском и русском языках. Во многом с этим связана большая доля информации о российских утечках, сообщений об утечках из компаний англосаксонских стран и Европы. Также используется некоторое количество источников на арабском, японском, немецком, французском, испанском и итальянском языках.

Исследования ЭАЦ, в основном, ориентированы на анализ сообщений об утечках данных на английском и русском языках. Во многом с этим связана большая доля в базе информации об утечках в России и сообщений об утечках из компаний англосаксонских стран и Европы. Для обеспечения и увеличения полноты охвата также используются источники на арабском, японском, немецком, французском, испанском и итальянском языках. В целях данного исследования использовались публикации только на русском языке.

В ходе наполнения базы утечек ЭАЦ каждое сообщение об утечке классифицируется по закрытому списку признаков. Каждый признак обладает ограниченной вариативностью. К примеру, при классификации по страновой принадлежности каждому сообщению присваивается один из вариантов (название страны, на территории которой работает обладатель информации и где, предположительно, произошла утечка информации.

В базу вносятся:

- текст заголовка и сообщения об утечке,
- ссылка на источник сообщения,
- дата публикации сообщения,
- название предприятия (организации, учреждения);
- государство (страна),
- сфера деятельности обладателя информации (отрасль),
- направление деятельности (коммерческая, некоммерческая),
- примерный размер организации (малая, средняя, крупная)[4],
- размер причиненного в результате утечки ущерба[5],
- количество скомпрометированных записей (только для ПДн и платёжной информации),
- субъект[6], непосредственно допустивший утечку.

Выделяются следующие сферы деятельности (отрасли, отраслевые группы):

---

[3] Сообщения об утечках данных, опубликованные официальными ведомствами, СМИ, авторами записей в блогах, интернет-форумах и иных открытых источниках по всему миру.

[4] По предполагаемому количеству персональных компьютеров в компании. Малые – до 50 ПК, средние – от 50 до 500 ПК, крупные — более 500 ПК.

[5] Данные об ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций в СМИ, или на сайтах пострадавших организаций, или из отчётов органов государственной власти, экспертных организаций.

[6] Авторы классифицируют утечки по виновнику инцидента. См. Глоссарий.

- банки, финансовые и страховые компании,
- медицина,
- торговля и HoReCa,
- высокие технологии (в основном, ИТ и телекоммуникационные компании),
- промышленность, энергетика и транспорт,
- госорганы и силовые структуры,
- образование,
- муниципальные органы власти и учреждения,
- другое (некоммерческие организации, спорт, медиа, консалтинг, недвижимость и т.д.).

Далее каждое сообщение классифицируется по:

- наличию умысла[7] (если по описанию или имеющимся признакам действия лица, допустившего утечку, являются умышленными, то утечка классифицируется как умышленная; в обратном случае — как неумышленная / случайная);
- каналу утечки,
- типам данных (относятся ли скомпрометированные сведения к персональным данным, платежной информации, государственной или коммерческой тайне, ноу-хау и т.п.),
- вектору воздействия («внешний», «внутренний», «не определено», также в ряде случаев выделяем так называемый «гибридный вектор», когда утечка связана с влиянием как внешних, так и внутренних нарушителей),
- типу нарушителя.

Все перечисленные признаки (конкретные варианты признаков) вносятся при наличии информации, определяются методом экспертной оценки, носят вероятностный характер, если информация неполная или противоречивая. При невозможности классифицировать сообщение (нельзя выявить вариант признака и отразить в базе, если в сообщении об утечке прямо или косвенно нет указания признака), в соответствующем поле проставляется значение «неизвестно». Иных признаков (категорий для классификации) база утечек ЭАЦ не содержит.

Также в базу попадают случаи, когда невозможно установить обладателя скомпрометированной информации, но совершенно точно известно, что утекшая информация не является скомпилированным набором данных на основе других утечек. Такие случаи при добавлении в базу классифицируются по всем известным параметрам, а в поле отраслевой принадлежности ставится «другое», поле «название компании» остается пустым.

В базу вносится количество скомпрометированных записей, содержащих только ПДн и/или платёжную информацию, т.к. в остальных случаях количественные характеристики обычно отсутствуют.

Важно отметить, что 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. Указанные признаки также устанавливаются на основе экспертной оценки.

В случаях, когда тип нарушителя неизвестен и удельный вес таких неизвестных в выборке незначителен (как правило, менее 3%), авторы исследования также добавляют их к внешним нарушителям, т.к. подобная выборка соответствует данным, полученным при изучении аналогичных случаев.

[7] Утечки данных разделяются на умышленные и неумышленные (случайные) См. Глоссарий.

Сообщения об утечках (единицы совокупности или элементы выборки) в базе ЭАЦ далее именуются «утечками». Т.е. каждая запись в базе ЭАЦ содержит сведения об одном событии, которое полностью соответствует приведенному выше определению утечки данных (информации).

Авторы считают, что большие шансы стать известными имеют случаи утечки данных, ставшие следствием:

- кражи в целях продажи неопределенному кругу лиц;
- действий хактивистов для достижения общественных и политических целей;

а также утечки из наиболее крупных и широко известных компаний, организаций, учреждений.

Кроме того, крупные утечки (объемом более 1 млн записей) и утечки из компаний с известными брендами чаще попадают в сферу внимания СМИ, блогеров и надзорных органов. Для анализа и корректного расчета среднего числа записей в одной публичной утечке выделена отдельная категория — «мега-утечка», то есть утечка, в результате которой было скомпрометировано 10 млн и более записей. Отдельно могут исследоваться и все утечки с числом скомпрометированных записей от 1 млн, а также вся совокупность утечек с числом записей до 1 млн.

Сведения об утечках представлены с использованием исторических данных — количественных показателей предыдущих лет.

Для повышения качества выводов использованы следующие подходы: исследования проводятся ежегодно на основе выборки, сформированной по единой методике (случайный поиск исходных сообщений об утечках, классификация сообщений по единому списку признаков). При формировании выводов авторы опираются на динамические показатели. Все данные в сравнительных исследованиях (сравнения с аналогичными показателями предыдущего периода) представляются в процентном виде. Исключение: сведения о совокупном количестве утечек, включенных в базу ЭАЦ, объеме записей, скомпрометированных в результате этих утечек, объеме скомпрометированных записей в расчете на одну утечку (только ПДн и платежная информация).

Указанные данные носят иллюстративный характер, дают представление, например, об изменении объемов определенных типов данных, хранимых и обрабатываемых обладателями информации.

В абсолютных показателях также представлены данные в виде так называемой «отраслевой карты утечек» — карта показывает фактическое распределение объема скомпрометированных персональных данных по отраслям (наглядно показывает зависимость объема ПДн в отрасли от размера компании-обладателя информации, числа утечек ПДн).

При анализе выборки по определенному признаку и построении сравнительных диаграмм (такие диаграммы авторы именуют разрезами или распределениями) все утечки, классифицированные по исследуемому признаку как «неизвестные» и с долей менее 5%, исключаются из выборки, после чего совокупность оставшихся утечек принимается за 100% для распределения по вариантам выбранного признака и последующего представления в диаграммах.[8] Такой подход позволяет проиллюстрировать динамические изменения отдельных показателей (долей, приходящихся на утечки, обладающие определенным признаком) более ярко, т.е. решает исключительно презентационные задачи. Но в случаях, когда доля утечек с признаком, классифицированным как «неизвестный», превышает 5%, представляются отдельные диаграммы.

ЭАЦ регулярно отслеживает обновления по ранее зарегистрированным утечкам.
В ходе такого мониторинга в базу вносится:

- информация об утечках, которые произошли в предыдущие периоды (прошлый год, позапрошлый и ранее),

[8] 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.

- обновлённая информация о составе (принадлежности) баз «мега-утечек»,
- уточнённые данные о дате (периоде), когда случилась ранее опубликованная утечка, об объёмах (количестве записей), векторе атаки и т.п.

То есть, при появлении новой информации, данные о количестве, а также векторах воздействия, каналах, суммах штрафов и т.п. утечек за прошлые периоды могут изменяться по сравнению с ранее опубликованными.

Но, как правило, эти данные не оказывают существенного влияния на общие показатели, отраженные в отчетах, а также на обозначенные в исследованиях тенденции.

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 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 (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 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.

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 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]

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 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.