INFOWATCH®

Аналитический отчёт

ИССЛЕДОВАНИЕ УТЕЧЕК ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА В ПЕРВОЙ ПОЛОВИНЕ 2022

Читайте материалы экспертно-аналитического центра InfoWatch

Оглавление

Только факты 3

Сокращения 3

Аннотация 3

Результаты исследования 4

Заключение и выводы 13

Только факты

- **Число утечек информации выросло почти в два раза в мире и в полтора раза — в России** (по сравнению с H1 2021)
- Во всём мире в первой половине года «утекло» около 3 млрд записей ПДн и платёжной информации
- Количество скомпрометированных записей в России за H1 2022 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» — её 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

Сокращения

GDPR General Data Protection Regulation (Регламент Евросоюза о персданных от 27.4.2016, вступил в силу 25.5.2018)

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

Методика исследования и глоссарий доступны в электронной версии отчёта: infowatch.ru/analytics

1 forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know
2 statista.com/statistics/987474/global-average-cost-data-breach

Результаты исследования

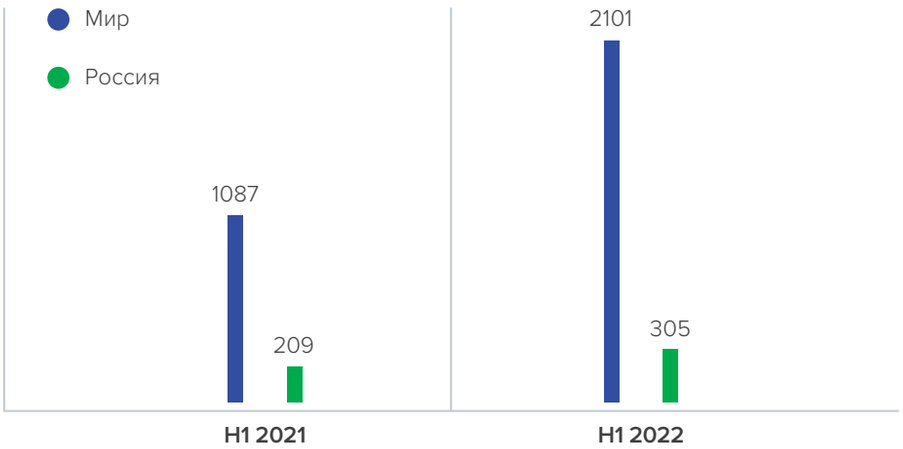
Общая картина утечек в мире и в России

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

В отчёте по итогам 2021 мы констатировали, что практически во всём мире примерно на 28% произошло как снижение количества утечек, так и снижение количества скомпрометированных записей ПДн и платёжной 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 внедрённых 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 последовал значительный рост количества сообщений об утечках.

По итогам первой половины 2022 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 I полугодие 2022 составило 305 (+45,9% по сравнению с I полугодием 2021) (рисунок 1).

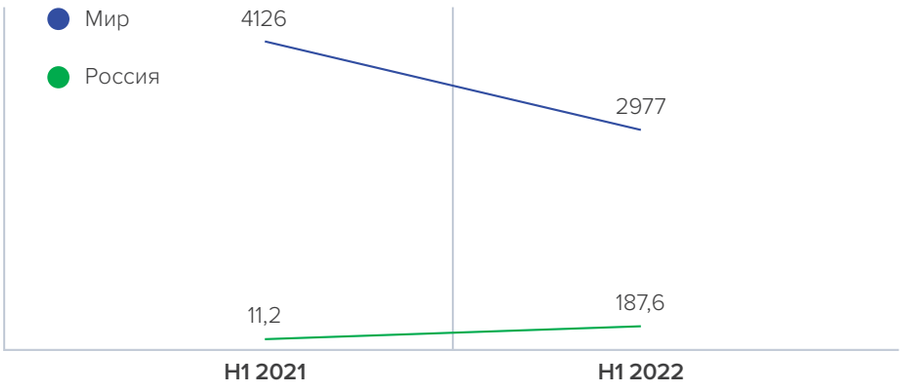
Рисунок 1. Число утечек: мир — Россия, I полугодие 2021 — I полугодие 2022



Обратные тенденции отмечены в отношении количества скомпрометированных записей персональных данных и платёжной информации. В I полугодии 2022 в мире «утекло» на 27,8% меньше единиц информации, чем в I полугодии 2021. Судя по всему, это связано с избирательной активностью злоумышленников, которые старались похищать только действительно ликвидные на чёрном рынке данные. В то же время компаниям, накопившим огромные базы персональных данных, в целом удалось устоять под натиском киберпреступников — в первые шесть месяцев 2022 зарегистрировано только семь случаев, в результате каждого из которых утекло от 100 млн записей ПДн. В I полугодии 2021 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 серьёзное внимание защите своих ресурсов от случайных утечек информации.

В то же время в России объём «утёкшей» информации вырос в 16,75 раза и составил 187,6 млн записей (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 утёкших записей, млн: мир — Россия, I полугодие 2021 — I полугодие 2022



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

В первой половине 2022 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, произошёл резкий всплеск хакерской активности, наметившийся ещё 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.

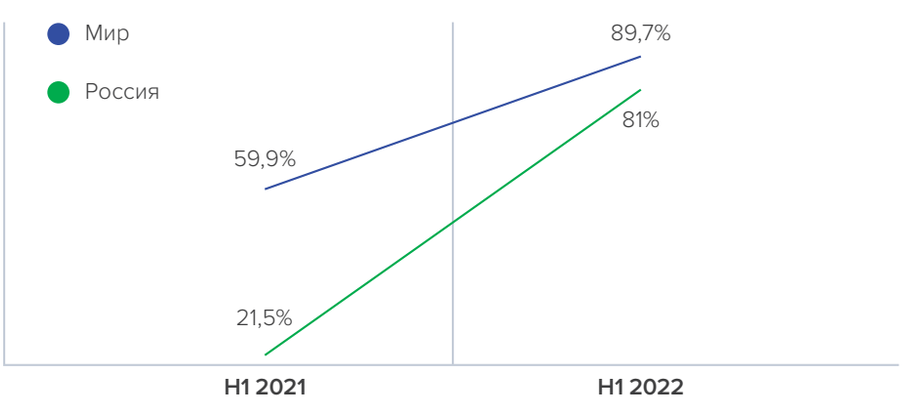
Во-вторых, ослабление контроля за информационными активами в период пандемии спровоцировало объединение усилий внешних нарушителей (хакеров) с нарушителями внутренними (персоналом), то есть склонение сотрудников к хищению данных, внедрение инсайдеров.

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

В-четвёртых, 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 приходится «выносить сор из избы».

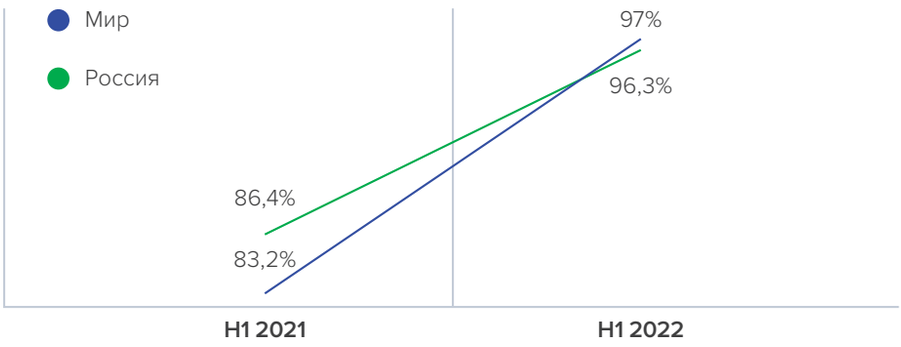
Также важно отметить произошедшее на чёрном рынке разделение труда, создание новых хакерских инструментов и появление предложений по их сдаче в аренду, то есть существенное расширение и развитие модели «киберкриминал как сервис».

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



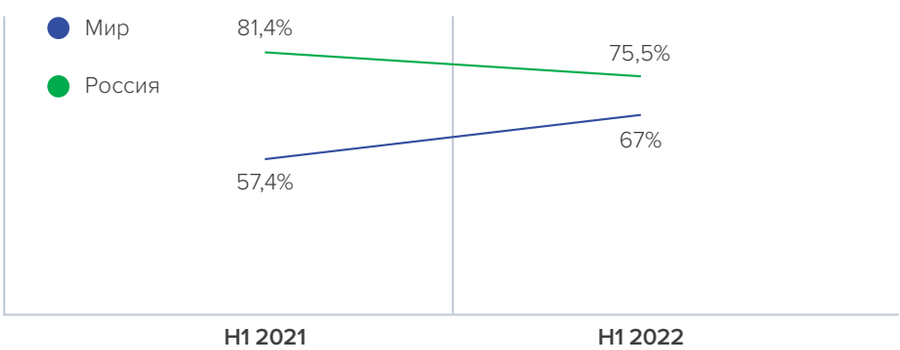
Вполне ожидаемо, что на фоне повышения ценности конфиденциальной информации в цифровую эпоху и снижения уровня защищённости цифровых активов в период пандемии, а также на новом витке кибервойн (кибератак, кибероперaций) продолжается рост доли утечек умышленного характера. Всплеск хакерской активности 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 (рисунок 4).

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



Одновременно с этим в мире с 57,4% до 67% выросла доля умышленных нарушений внутреннего характера (рисунок 5). Однако стоит сделать важную оговорку: с учётом 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.

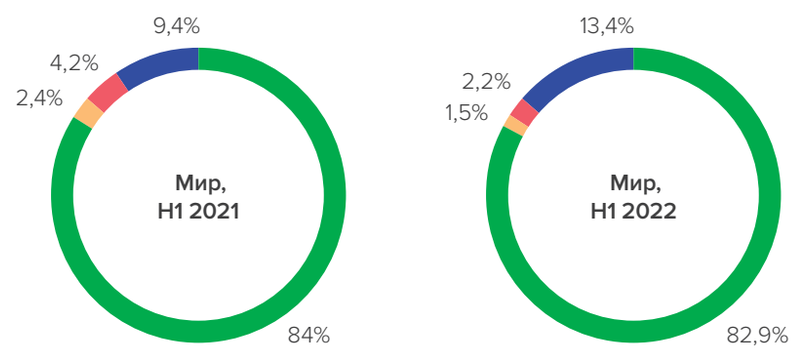
Рисунок 5. Доля умышленных нарушений внутреннего характера: мир — Россия, I полугодие 2021 — I полугодие 2022



Доминирующим типом информации на карте утечек остаются персональные данные

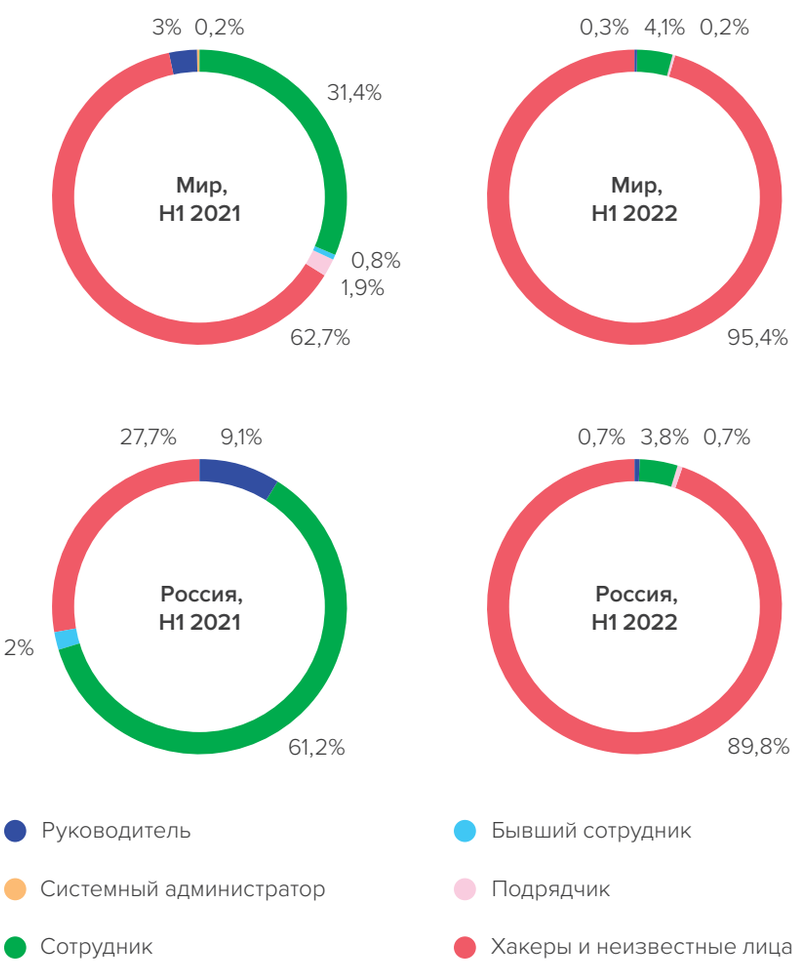
См. рисунок 6. Но их доля в первой половине 2022 сократилась как в России, так и в мире. Это произошло за счёт опережающего роста утечек коммерческих секретов — интенсификация кибервойн по всем мире привела к более активной борьбе организованных групп хакеров за сведения экономического плана. Вместе 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 — I полугодие 2022



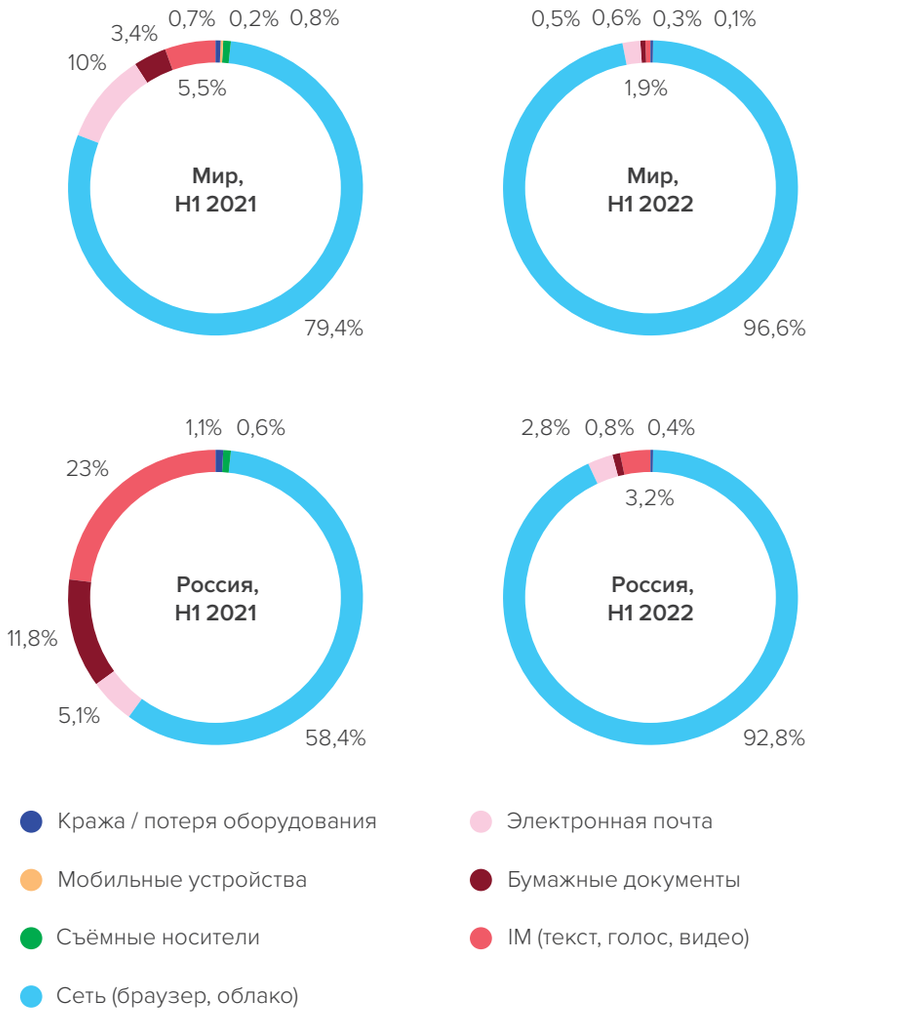
Среди виновников утечек в мире превалируют хакеры и неизвестные лица. Эта же категория в первом полугодии 2022 впервые вышла на первый план и в России, где долгое время основными нарушителями выступали сотрудники (рисунок 7). В условиях активизации хакеров основные силы компаний брошены на отражение 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 — I полугодие 2022



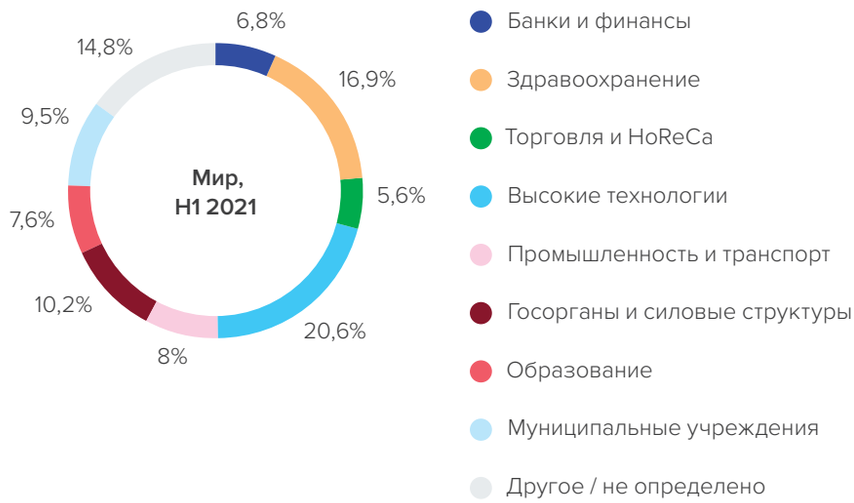
В условиях чрезвычайно высокой хакерской активности и роста латентности внутренних нарушений ещё более заметную роль в каналах начала играть сеть. Вместе с тем, пока на второй план отошли сервисы мгновенных сообщений (IM) и электронная почта, резко упала доля бумажных носителей (рисунок 8).

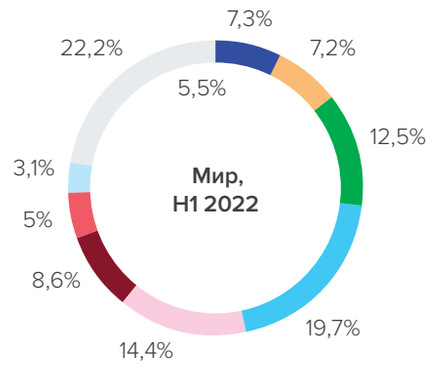
Рисунок 8. Распределение утечек по каналам: мир — Россия, I полугодие 2021 — I полугодие 2022



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.

Рисунок 9. Отраслевое распределение утечек, мир — Россия, I полугодие 2021 — I полугодие 2022





Утечки информации ограниченного доступа — дарквеб

В этом отчёте 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 телеграм-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. 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 дарквебе вне зависимости от наличия копий или сообщений в других источниках, в т. ч. СМИ.

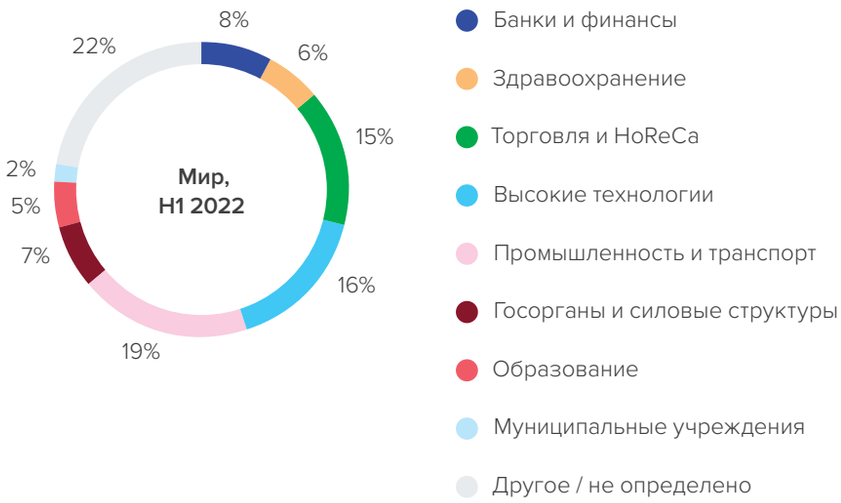
Важно отметить, что в данной главе отчёта относим все найденные утечки к категории умышленных, независимо от их «механизма»: кража данных сотрудников или следствие хакерской атаки. Из текстов таких объявлений мы не можем определить, кто стал виновников утечки — сотрудник или хакер. В то же время можно предположить, что, вероятнее всего, в основном речь идёт о внешнем векторе воздействия, в результате преобладающая часть объявлений о продаже создаётся 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.

Распределение обнаруженных утечек данных по странам, где действуют компании и организации, из которых «утекла» информация, выглядит следующим образом: США — 30%, РФ — 13%, Великобритания, Германия, Индия, Канада — по 3%, Бразилия, Испания, Италия, Китай, Украина, Франция — по 2%. Всего была найдена информация об утечках в 104 странах, для части утечек страна не установлена (9% найденных объявлений о продаже или бесплатном «сливе» данных).

В своих отчётах мы регулярно отмечаем, что первое место по количеству утечек занимают США. Не является исключением и мониторинг утечек в дарквебе и закрытых телеграм-каналах. Такое положение вполне объяснимо: США всё ещё 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 10 представлено отраслевое распределение утечек из компаний и организаций по всему миру, чьи данные оказались в дарквебе.

Рисунок 10. 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 (рисунок 10) и в России (рисунок 11). Во многом распределения похожи за исключением нескольких аспектов:

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

Рисунок 11. 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 InfoWatch, хотим отметить, что во многом они хорошо коррелируют (таблица 1).

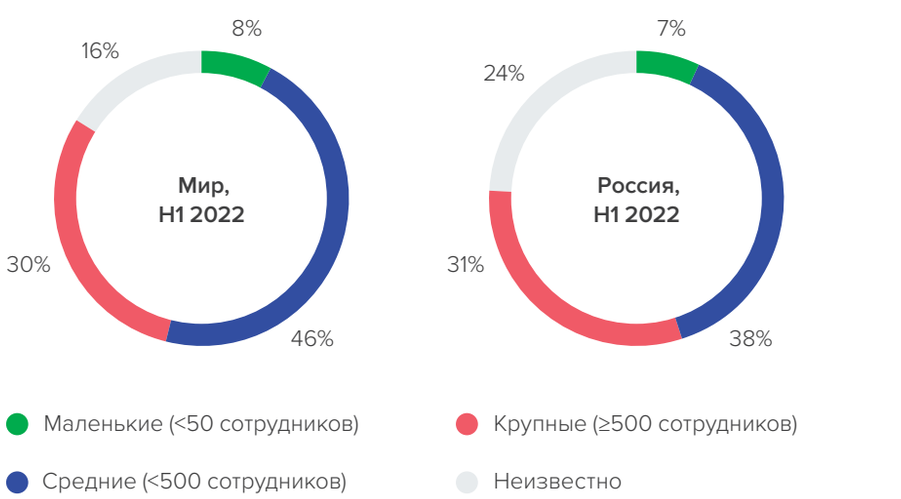
Таблица 1. Сравнение утечек, выявленных в дарквебе, со сводным количеством утечек, выявленных из различных источников

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

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%. Ещё 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 «неопределённой отрасли» объясняется тем, что зачастую в объявлениях не уточняют происхождение данных, предлагают приобрести базу «персональных данных россиян», «паспортов россиян» и т. д.**

Рисунок 12. Распределение утечек из объявлений в дарквебе по размеру организаций

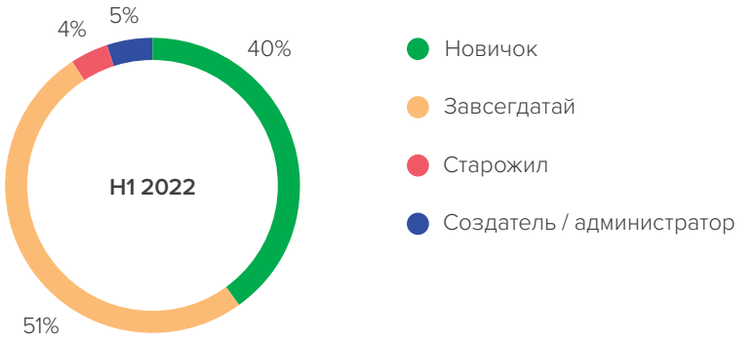


Из диаграммы утечек в мире заметно, что в дарквебе за период с 1 января по 30 июня 2022, в основном, продавали данные организаций среднего сегмента — 46%, но также на чёрном рынке продают и большое количество конфиденциальной информации крупных компаний — 30%. В 16% случаях нет возможности установить 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 13).

Рисунок 13. Распределение утечек 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%. Какой же тип данных наиболее часто продаётся на теневых форумах или в специализированных телеграм-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 идёт о продаже коммерческих тайн компаний, а 3% и 2% объявлений, соответственно, предлагают платёжную информацию и сведения категории «государственная тайна».

Рисунок 14. Распределение утечек в дарквебе 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 платёжного 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 платёжную 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 платёжная информация встречается достаточно часто — в 8% случаев. В общем распределении это значение снова теряется — всего 0,7%.

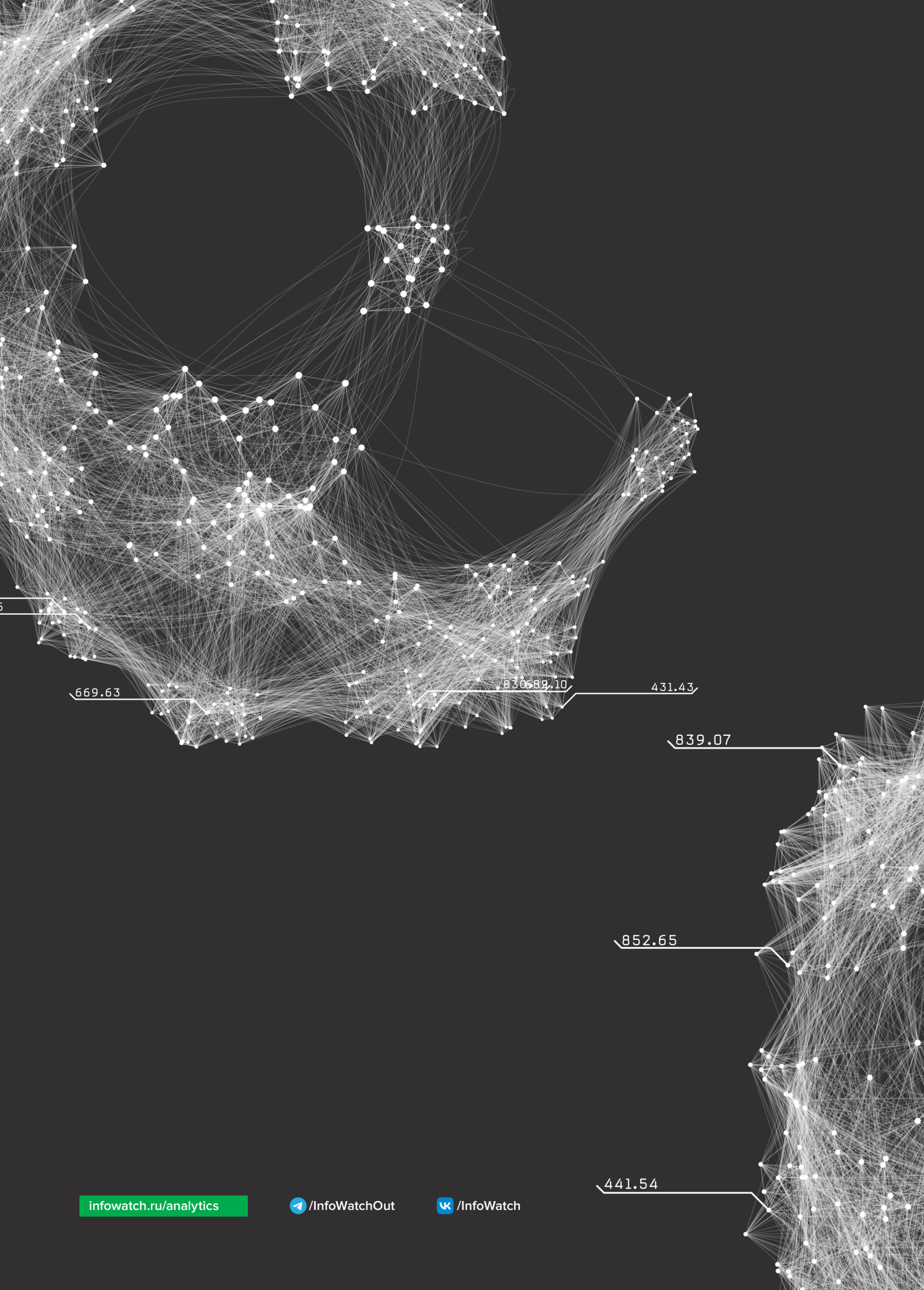
Заключение и выводы

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 использовать её как инструмент шантажа, экономического и политического давления, — всё это привело к всплеску утечек, вызванных внешним воздействием. Вместе с тем, на наш взгляд, ещё 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 всё более сложным, злоумышленники из-за пределов информационного контура организации всё 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 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 её 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.


669.63
830689.10
431.43
839.07
852.65
441.54