INFOWATCH®

ФИНАНСОВЫЙ СЕКТОР: УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Мир — Россия, 2021–2023

Оглавление

Только факты

- Количество утечек в финансовой отрасли за 2023 выросло на 79,5% в мире и на 12,3% в России
- Всего в финсекторе за 2023 утекло более 4,3 млрд. записей ПДн, из российских финансовых организаций — более 170 млн.
- Доля банков среди утечек информации в мировой финансовой отрасли составила 26,2%, в российской — 46,9%
- Более 98% утечек из финансовых организаций в России и мире случились в результате нарушений умышленного характера
- Среди нарушений со стороны сотрудников доля умышленных выросла и составила 48,2% в мире и 75% в России
- В 2023 на долю США пришлось 44,3% всех утечек информации в финансовой сфере, на долю России — 6,1%
- Треть опрошенных российских специалистов считает, что в финсекторе сосредоточены наиболее ценные информационные ресурсы
- 58% опрошенных российских специалистов считают финсектор наиболее защищённым от утечек данных
- 67% специалистов ИБ и СБ крупных частных финансовых организаций на первое место ставят угрозы утечек по вине сотрудников

Сокращения

GDPR	General Data Protection Regulation (регламент Евросоюза о персданных от 27 апреля 2016, вступил в силу 25 мая 2018
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
ЭАЦ	Экспертно-аналитический центр ГК InfoWatch

Аннотация

Экспертно-аналитический центр ГК InfoWatch представляет отчёт по результатам исследования утечек конфиденциальной информации из организаций отраслевой группы «Банки и финансовые услуги»: банки, кредитные организации, страховые компании, биржи, криптобиржи, платёжные сервисы и т. д. Эта отрасль обеспечивает устойчивость экономики, является её кровеносной системой. Обеспечение защиты финансовой системы входит в число государственных приоритетов. В условиях, когда похищение денег из финансовых организаций требует нетривиальных знаний и серьёзных усилий по реализации преступных схем, злоумышленники давно поставили во главу угла похищение конфиденциальной информации. Персональные данные клиентов, платёжная информация, коммерческие секреты и другие сведения стали привлекательным объектом для организованной киберпреступности, так как эта информация легко монетизируется на чёрном рынке и становится мощным инструментом для шантажа, а также эффективным средством нарушения устойчивости финансовых систем. В частности, речь идёт о попытках хактивистов оказать политическое давление на те или иные государства посредством атак на их ключевые финансовые организации, а также о спланированных акциях, направленных на то, чтобы посеять панику среди клиентов и подорвать их доверие к финансовым институтам.

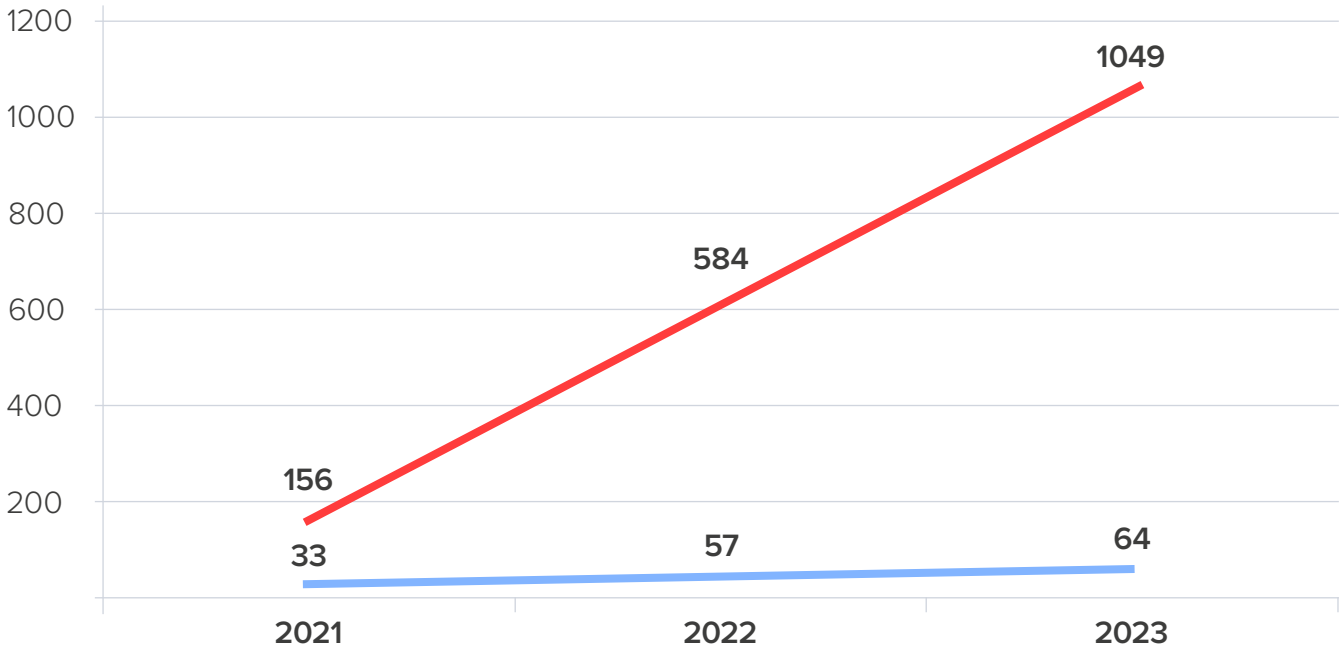
В отчёте приведена статистика по количеству зарегистрированных утечек конфиденциальной информации в отрасли «Банки и финансовые услуги», а также по количеству скомпрометированных записей персональных данных. Аналитики представляют картину утечек данных в таких разрезах, как типы инцидентов, характер умысла, типы нарушителей, типы утекших данных, каналы утечек и т. д. Также в отчёте приведён ряд данных из опроса, проведённого ЭАЦ при участии «Код ИБ» в декабре 2023 — январе 2024, в отношении уровня ИБ различных российских организаций.

Отчёт будет особенно полезен руководителям, специалистам по защите информации и экономической безопасности, риск-менеджменту, работающим в финансовых организациях, а также всем, кто интересуется темой обеспечения информационной безопасности в ключевых отраслях экономики.

Результаты исследования

Утечек в финансовой отрасли стало больше на 80%

Экспертно-аналитический центр InfoWatch в 2023 зарегистрировал 1049 утечек конфиденциальной информации из организаций, представляющих мировую отрасль «Банки и финансовые услуги»: банки, финансовые и страховые компании, биржи и т. д. Это на 79,5% больше, чем в 2022, когда в данной отрасли были зарегистрировано 584 утечки. По сравнению с 2021 рост ещё более значительный — 572% (в 6,7 раза) — см. рисунок 1. В условиях, когда похищение денежных средств из хранилищ и со счетов финансовых организаций требует специальных знаний и сложных инструментов, по мере совершенствования различных средств защиты, преступники в качестве основной цели выбирают конфиденциальную информацию как ключевой актив постиндустриальной эпохи. Киберкриминал находит различные уязвимые точки в корпоративной инфраструктуре банков и других организаций финсектора. Хакеры проникают в сети компаний, применяя вредоносное ПО (главный тренд — вирусы-вымогатели и вирусы-«вайперы»), взламывают ресурсы посредством использования скомпрометированных данных, активно атакуют по цепочке поставок ПО. Последняя угроза особенно широко проявилась в 2023, когда злоумышленники из группировки Clop, используя уязвимость нулевого дня в программном обеспечении MOVEit Transfer (отправка файлов большого объёма), успешно атаковали более 2600 организаций по всему миру, включая сотни организаций финансовой отрасли.



Австралийская небанковская кредитная организация Latitude по итогам первого полугодия оценила ущерб от утечки данных в 76 млн. долларов. В результате атаки в марте 2023 хакеры похитили данные до 14 млн. клиентов Latitude.

Источник: Information Age

Рисунок 1. Количество утечек данных в отрасли «Банки и финансовые услуги»

Роскомнадзор подтвердил утечку данных клиентов МТС-банка и составил административный протокол о нарушении законодательства в области персональных данных. В начале сентября 2023 канал «Утечки информации» сообщил, что в сеть попала база данных с информацией о клиентах МТС-банка, включая частичную информацию о картах. В базе было около 1 млн. строк данных о клиентах. В частности, утекли такие сведения, как ФИО, даты рождения, пол, гражданство и ИНН.

Источник: РБК

Значительную часть ПДн и платёжной информации клиентов возможно использовать для похищения денежных средств без взлома систем, обеспечивающих переводы, а используя методы социальной инженерии. Часто клиент под воздействием телефонного разговора с мошенником по сути добровольно переводит средства на его счета, что значительно затрудняет привлечение к ответственности. В российском финсекторе рост количества утечек не такой резкий: 64 утечки в 2023, что на 12,3% больше, чем в 2022, и на 93,9% больше по сравнению с 2021. Существенный рост количества инцидентов связан с активизацией организованных групп хакеров, прежде всего — политически мотивированных хактивистов, на фоне проведения СВО. Их главными задачами стали подрыв устойчивости, психологическое давление на финансовые организации и запугивание клиентов. Когда злоумышленникам удавалось взломать системы российских банков и других компаний, украденные данные как правило размещались в открытом доступе. Это сопровождалось угрозами с обсценной лексикой и политическими заявлениями. Проукраинские хакеры рассматривали кибератаки как форму войны.

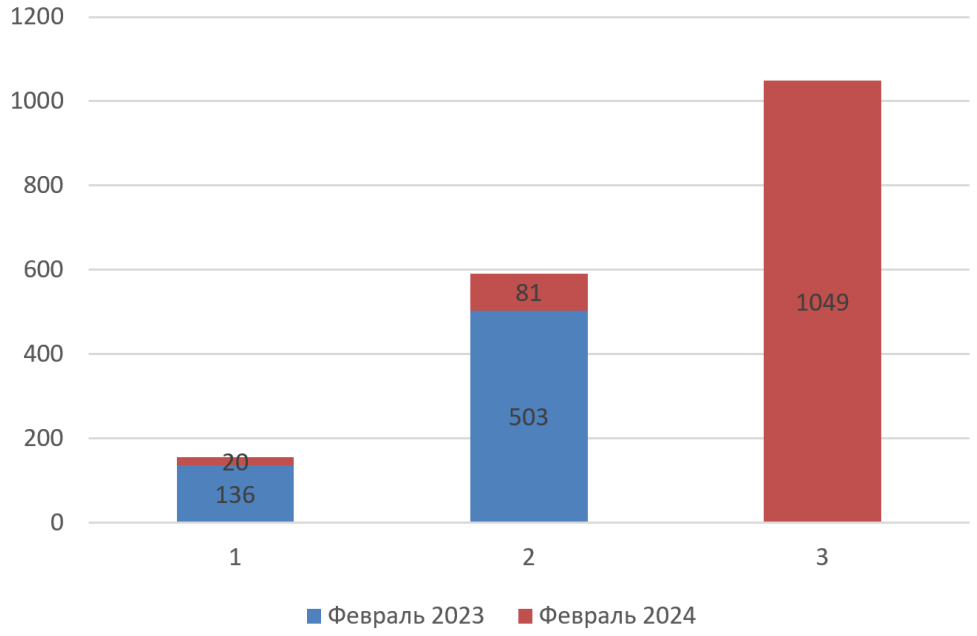


Рисунок 2. Утечки данных в финсекторе, мир

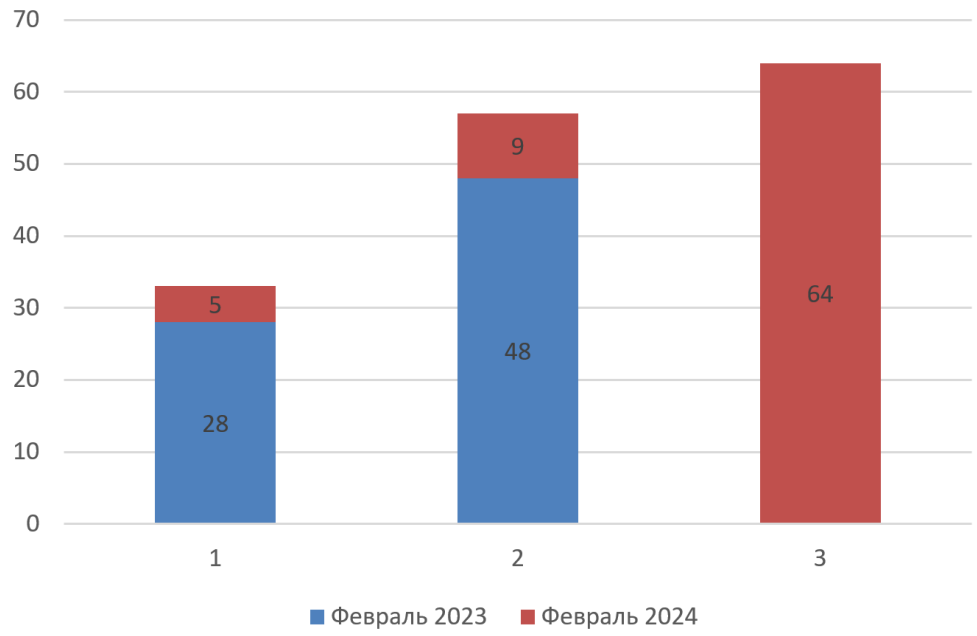


Рисунок 3. Утечки данных в финсекторе, Россия

Аналитики ЭАЦ регулярно проводят мониторинг различных источников об утечках информации, в том числе опираясь на разработанную ими методику определения латентности инцидентов. На рисунках 2 и 3 приведено количество утечек с учётом новых выявленных случаев компрометации данных в 2021–2022, начиная с 1 февраля 2023 (ряд 1) и до 1 февраля 2024 (ряд 2). За этот период ЭАЦ добавил в базу утечек информации сведения о 20 утечках в мировой финансовой сфере за 2021 и 81 утечке за 2022. Соответственно, за год после публикации исследования об утечках информации в финансовом секторе за 2021–2022 дополнительно внесено в базу случившиеся в 2021–2022 14 утечек из российских финансовых компаний.

В российской финансовой отрасли половина утечек пришлась на банки, значительно выросла доля страхования

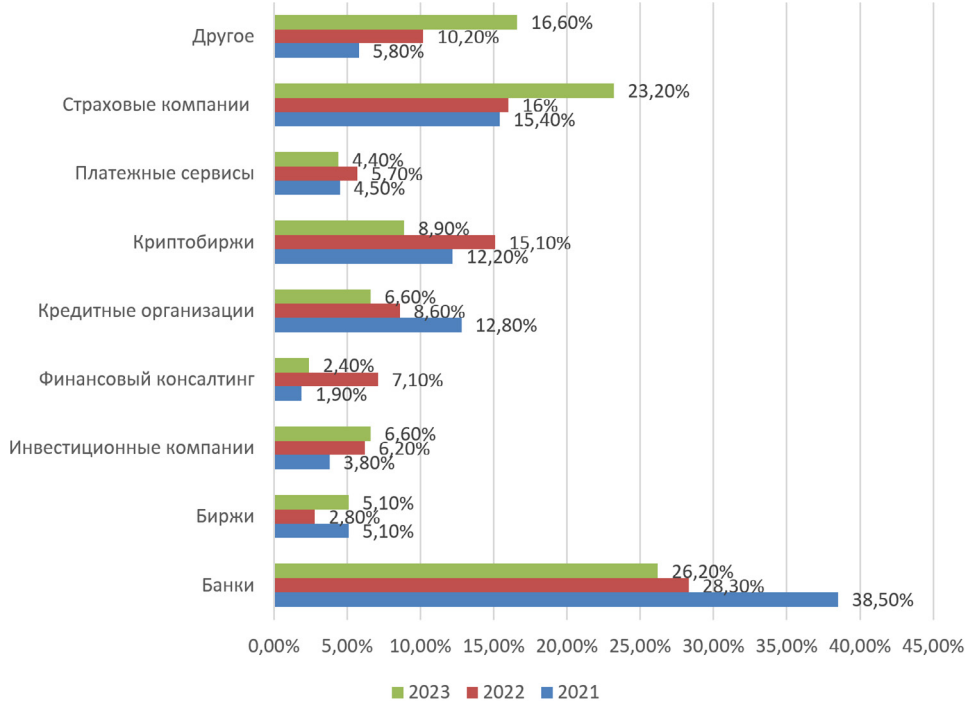


Рисунок 4. Утечки данных в финсекторе по отраслям, мир

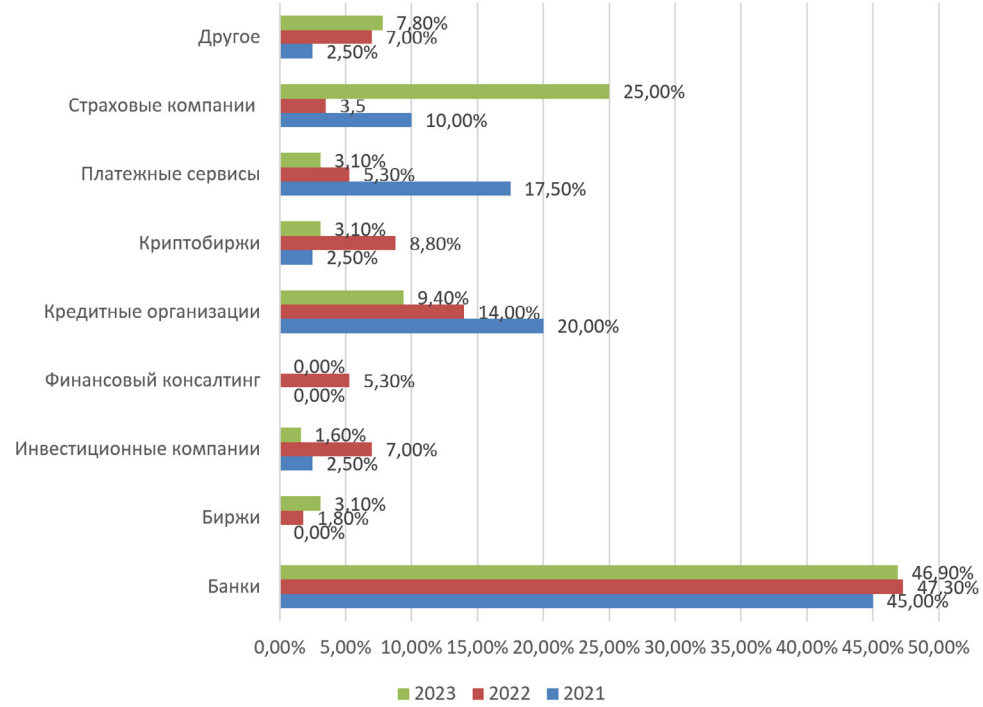


Рисунок 5. Утечки данных в финсекторе по отраслям, Россия

В мире в течение 2021–2023 сократилась доля банков, из которых зафиксированы утечки данных, но при этом выросла доля страховых компаний. Процент утечек из кредитных организаций небанковского сектора в 2023 уменьшился вдвое по сравнению с 2021.

На рисунках 4 и 5 представлено распределение утечек конфиденциальной информации в финсекторе по сегментам. Довольно высока доля скомпрометированных данных среди криптобирж, однако она существенно снизилась по сравнению с 2022. Цифровые активы —

сравнительно молодое направление финансового рынка. Вероятно, операторы криптобирж стали больше времени уделять обеспечению кибербезопасности, что позволило сдержать рост утечек информации, а значит, и снизить риски кражи криптовалюты из кошельков пользователей. Кроме того, растёт квалификация самих пользователей.

Сегодня цифровые валюты востребованы не только продвинутыми технофанатами, как ещё несколько лет назад, но уже довольно широкими слоями населения. При этом неофиты крипторынка в основном довольно быстро осваивают правила безопасного обращения с активами. По данным Bitfinex, к 1 декабря 2023 количество держателей криптовалютных активов в мире выросло до 575 млн. (с 432 млн. в начале 2023). Ожидается, что к концу 2024 цифровой валютой будут обладать 850 млн человек.

В России доля банков в распределении утечек по категориям оставалась стабильно высокой на протяжении всех трёх лет — не ниже 45%. При этом в 2,5 раза в общем распределении инцидентов выросла доля страховых компаний

В то же время снизился процент утечек, пришедшихся на кредитные организации (МФО и другие) — с 20% в 2021 до 9,4% в 2023.

Утекло более 4,3 млрд. записей ПДн в мировой финансовой сфере и более 170 млн. в российской

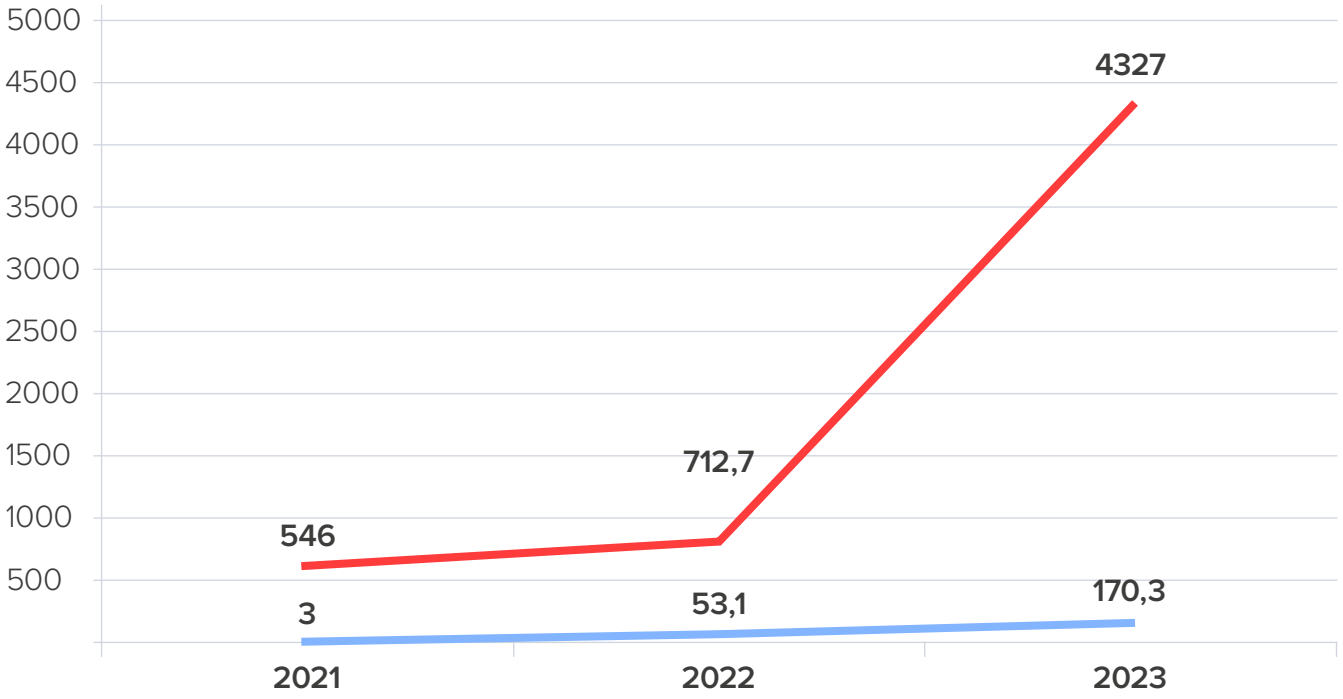


Рисунок 6. Скомпрометированные записи ПДн в финсекторе, млн.

В 2022–2023 в финансовой сфере отмечен резкий рост количества скомпрометированных записей ПДн. В первую очередь это обусловлено повышением результативности хакерских атак — взломы информационных систем регулярно приводили к утечкам крупных баз данных. Всего за 2023 из сферы «Банки и финансовые услуги» утекло 4,324 млрд. записей ПДн (рисунок 6). Фактически утекла информация более половины населения Земли. Однако, скорее всего, реальное количество пострадавших от утечек людей всё-таки меньше, поскольку некоторые вкладчики банков, клиенты страховых компаний и держатели криптокошельков могли стать жертвами инцидентов неоднократно.

Из российских финансовых организаций в 2023 утекло более 170 млн. записей ПДн (без учёта платёжных данных). Эта цифра больше, чем население России. По сравнению с 2022 скомпрометировано в три с лишним раза больше ПДн, а по сравнению с 2021 — больше почти в 57 раз!

Особую тревогу вызывает тот факт, что многие украденные базы данных выкладывались в открытый доступ, то есть быстро становились ценным источником для проведения фишинговых атак, а также могли использоваться различными преступными группировками для обогащения уже имеющихся баз, дополнения цифровых профилей потенциальных жертв мошеннических схем.

Доля умышленных нарушений превысила 98%

В последние два года среди инцидентов ИБ, приведших к утечкам, более 95% в мире и более 84% в России — кибератаки (рисунки 7 и 8).

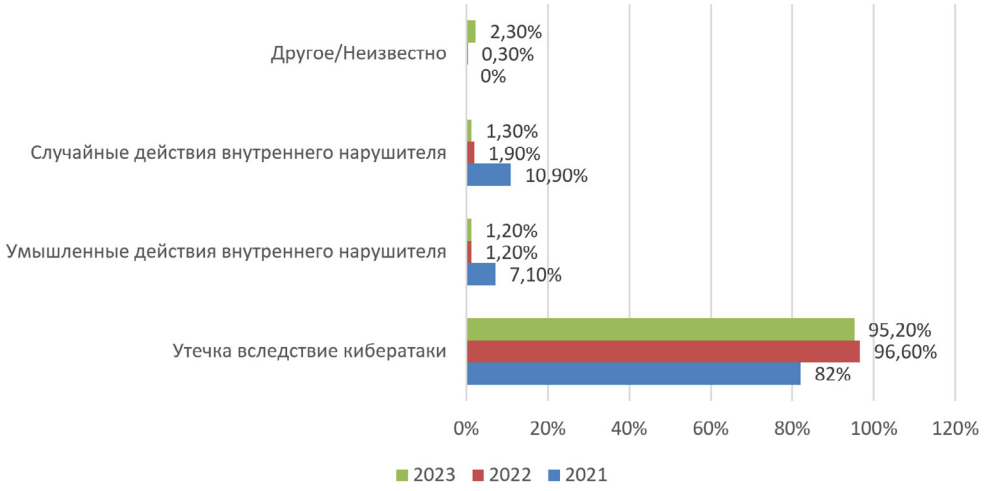


Рисунок 7. Утечки в финсекторе по типам инцидентов, мир

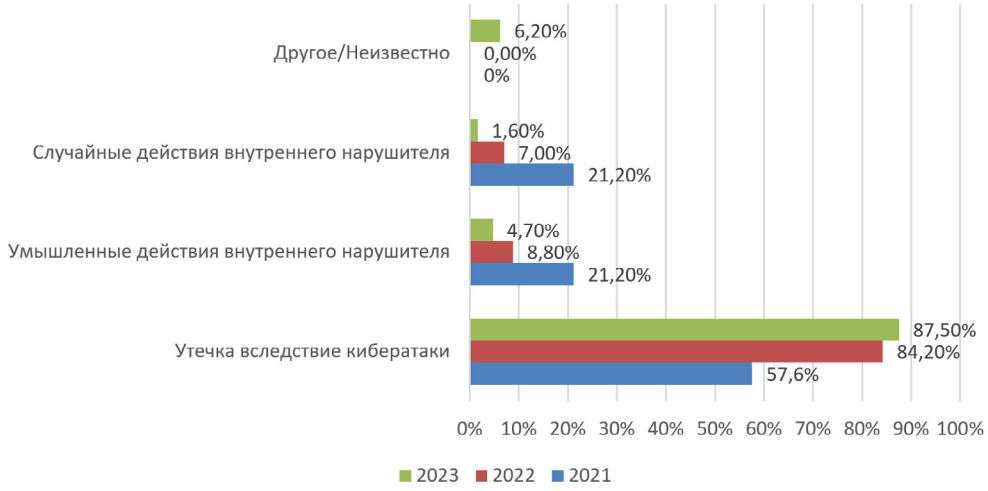


Рисунок 8. Утечки в финсекторе по типам инцидентов, Россия

Угрозы и меры

Важно отметить, что часть кибератак может носить гибридный характер, то есть, вероятно, они совершаются с привлечением лиц, работающих в финансовых организациях, или являются прикрытием для внутренних хищений. Исходя из этого, доля инцидентов, связанных с действиями внутренних нарушителей, формально снизилась — до 2,5% в мире и 6,3% в России. Это может быть связано с несколькими факторами.

Во-первых, происходил взрывной рост количества результативных кибератак, что во многом предопределено обострением политической борьбы на фоне СВО и других конфликтов в разных частях планеты. Во-вторых, могли дать плоды усилия финансовых организаций по предотвращению нарушений внутреннего характера. В частности, это касается настройки более эффективных DLP-систем нового поколения, основанных на интеллектуальном исследовании поведенческих факторов сотрудников, внедрении совершенных систем управления доступом, организации организационных и обучающих мероприятий среди персонала, концентрации служб ИБ на предотвращении нарушений со стороны персонала.

В-третьих, вероятно, выросла латентность злонамеренной деятельности сотрудников: смычка усилий внутренних и внешних нарушителей (т. н. «гибридный вектор» атак), о которой уже несколько лет говорят эксперты InfoWatch и их коллеги, приводит к тому, что существенную часть инцидентов становится трудно идентифицировать с точки зрения типов и причин инцидентов. По факту подавляющее большинство утечек данных последнего времени произошли в результате хакерской активности, но в совокупности этих нарушений есть доля инцидентов гибридного характера, когда информация утекала в результате объединения усилий недобросовестных сотрудников с внешними злоумышленниками (внедрение инсайдеров в финансовые организации, шантаж сотрудников и доверенных подрядчиков организованными преступными группами, добровольная передача сотрудниками учётных данных и коммерческих сведений хакерам).

Согласно опросу, проведенному ЭАЦ в декабре 2023, специалисты ИБ и СБ крупных частных финансовых организаций (в России) назвали наибольшим риском за прошедший год внутренние угрозы — утечки данных по вине сотрудников (67%). Также они назвали риски роста фишинговых (50%) и DDoS-атак (50%). В 2024 специалисты ИБ и СБ финансовых организаций, напротив, ожидают снижения риска DDoS-атак (33% против 50% за 2023), при этом, как и в прошедшем году, по-прежнему считают самым высоким риск утечек по вине сотрудников (67%). Что примечательно, если в 2023 риск взлома внешнего ИТ-периметра организации отметили 8%, то на следующий год — уже 25%.

Дополнительно отмечено, что одна из крупнейших проблем — мошенничество со стороны третьих лиц в отношении клиентов финансовых организаций, с использованием их персональных данных. За 2023 по мнению половины респондентов из финсектора самыми популярными мерами по информационной безопасности, принятыми в финансовых организациях, стали (допускалось несколько вариантов ответа):

- Проведение обучающих мероприятий по ИБ и информационной гигиене среди сотрудников — 58%
- Внедрение системы защиты от вторжений (IDS / IPS / FW / NGFW) — 33%
- Внедрение всех мер прошло до 2023 года, но сделали модернизацию — 33%)
- Внедрение DLP-системы — 25%

Другая половина респондентов ответила, что внедрение всех мер прошло до 2023 и модернизация систем ИБ не потребовалась (50%). При этом, когда респондентов из финансовой отрасли попросили сказать, какая из принятых мер показала наибольшую эффективность, специалисты в основном признали, что это проведение обучающих мероприятий для сотрудников (42% ответивших) и внедрение DLP (33% ответивших), которые принесли более значительный эффект, нежели внедрение системы защиты от вторжений.

В 2023 доля инцидентов умышленного характера как в мире, так и в России превысила 98%

См. рисунки 9 и 10. Но небольшой процент утечек случайного характера не должен вводить в заблуждение. Вероятно, достоянием общественности становятся далеко не все непреднамеренные нарушения. Кроме того, ряд из них приводит к утечкам довольно крупных баз данных и важной коммерческой информации — в основном это происходит в результате ошибок сотрудников при настройке облачных хранилищ и доступа к проектным репозиториям.

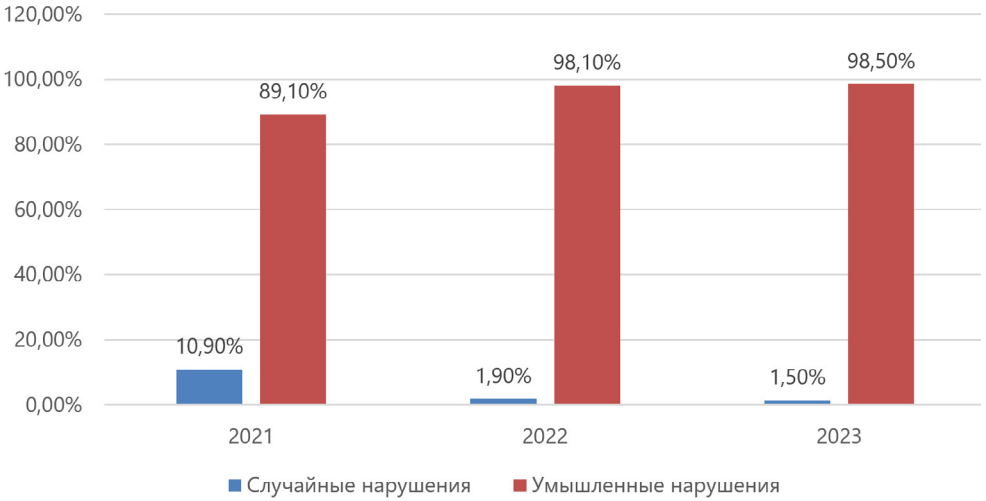


Рисунок 9. Утечки в финсекторе по характеру умысла, мир

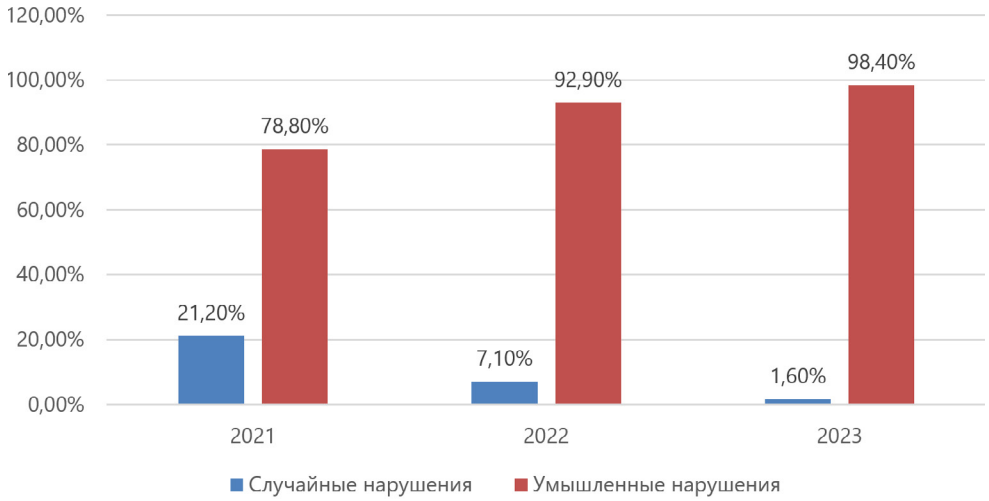


Рисунок 10. Утечки в финсекторе по характеру умысла, Россия

Более миллиона служебных документов финтех-компании NorthOne оказались в открытом доступе. Файлы включали счета клиентов финансового приложения, в инвойсах встречались персональные данные: имена, адреса электронной почты, физические адреса и т. д. Хранилище находилось в открытом доступе более десяти дней.

Источник: Website Planet

В мире доля умышленных нарушений со стороны персонала в 2023 выросла до 48,2%, а в России — до 75%

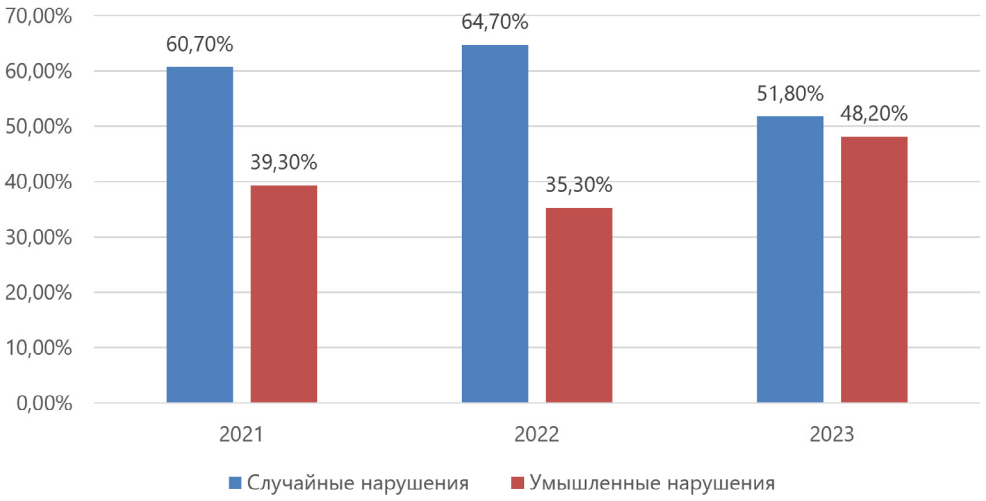


Рисунок 11. Внутренние утечки в финсекторе по умыслу, мир

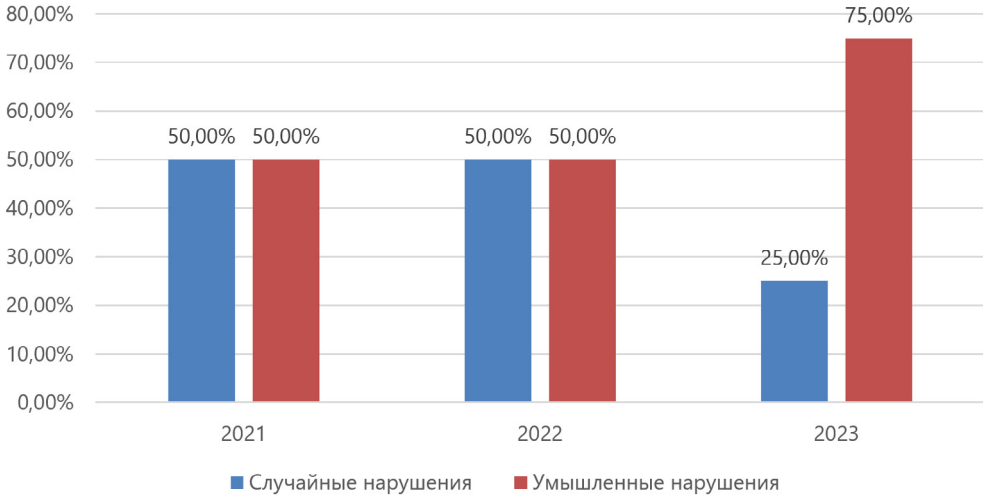


Рисунок 12. Внутренние утечки в финсекторе по умыслу, Россия

Сотрудники ушли в тень: доля утечек по вине внешних нарушителей выросла до 96,9% в мире и до 93,7% — в России

Снижение доли внутренних нарушителей в последние годы можно объяснить значительным ростом хакерской активности и плодотворной работой многих компаний по настройке DLP и принятии других мер против внутренних нарушений различного характера. То есть, если сдержать волну кибератак финансовым организациям пока не удается, то возможностей для внутреннего мошенничества с данными и рисков непреднамеренных утечек информации стало меньше.

Из опроса ЭАЦ. Интересно, что в отношении признания и информирования об утечках данных, подавляющее респондентов из финансовой отрасли (42%) считают, что утечки данных признают лишь 4–10% организаций. 25% участников опроса настроены более оптимистично и считают, что утечки признают 21–30% организаций. В то же время 17% ответивших придерживаются мнения, что случаи компрометации данных признают только 1–3% организаций. Таким образом, можно сказать, что почти 60% специалистов служб безопасности крупных финансовых организаций согласны с утверждением, что об утечках данных сообщают не более 10% организаций. На основе этого можно предположить, что повышенное внимание к финсектору в плане предотвращения внутренних угроз, а также методичная работа по обучению работников и внедрению DLP-систем, которые показывают свою эффективность, способствуют снижению количества утечек. Также стоит обратить внимание на пессимистичный настрой большинства респондентов в отношении признания утечек организациями.

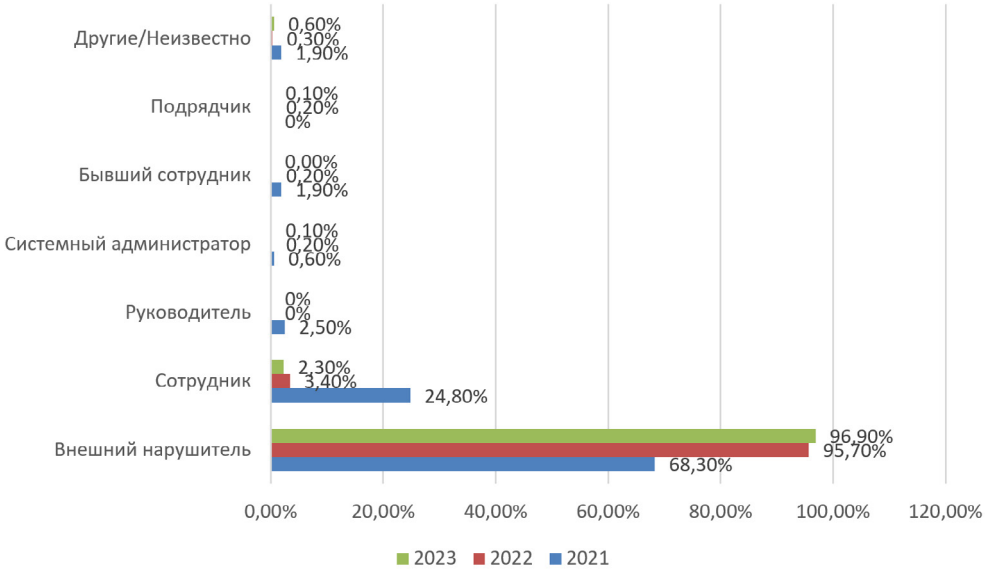


Рисунок 13. Утечки в финсекторе по типу нарушителей, мир

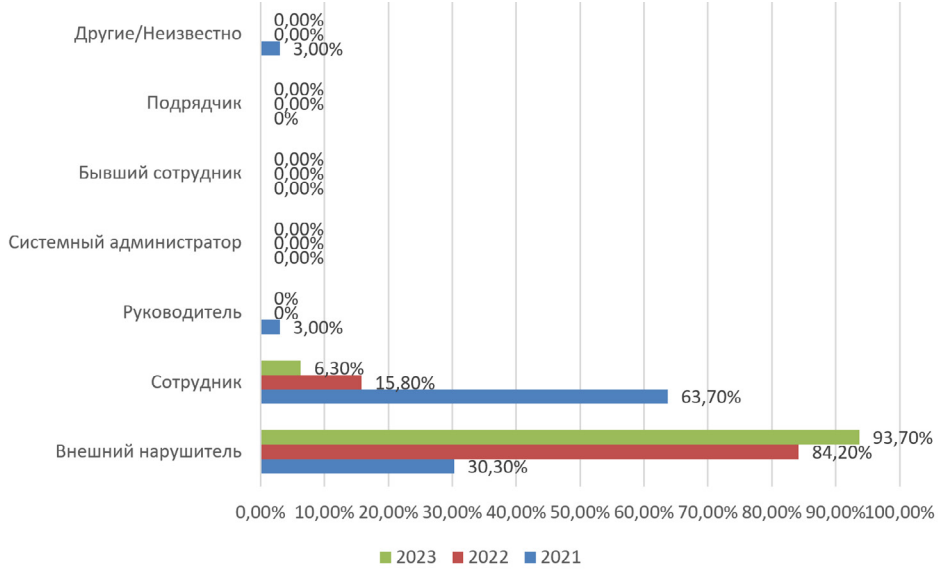


Рисунок 14. Утечки в финсекторе по типу нарушителей, Россия

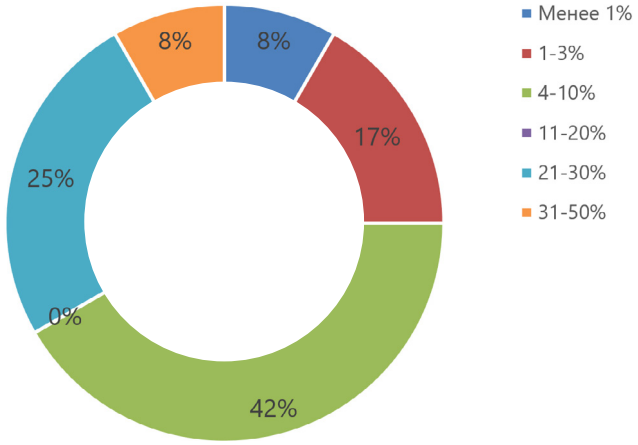


Рисунок 15

Сколько организаций в России, по вашему мнению, признает свои утечки данных?
Ответы специалистов финансовых организаций

Вывод

Несмотря на то, что по статистике значительная часть утечек может быть отнесена к последствиям кибератак, наибольшую опасность для конфиденциальной информации специалисты ИБ и СБ финансовых организаций видят именно в угрозах со стороны сотрудников, в том числе вследствие неумышленных действий.

Утечки информации на бумажных носителях сходят на нет

Распределение утечек в финансовой отрасли приведено на рисунках 16 и 17. Доминирующим каналом является сеть. В результате тотальной цифровизации финансовых услуг практически перестали фиксироваться утечки в результате кражи или потери бумажных документов.

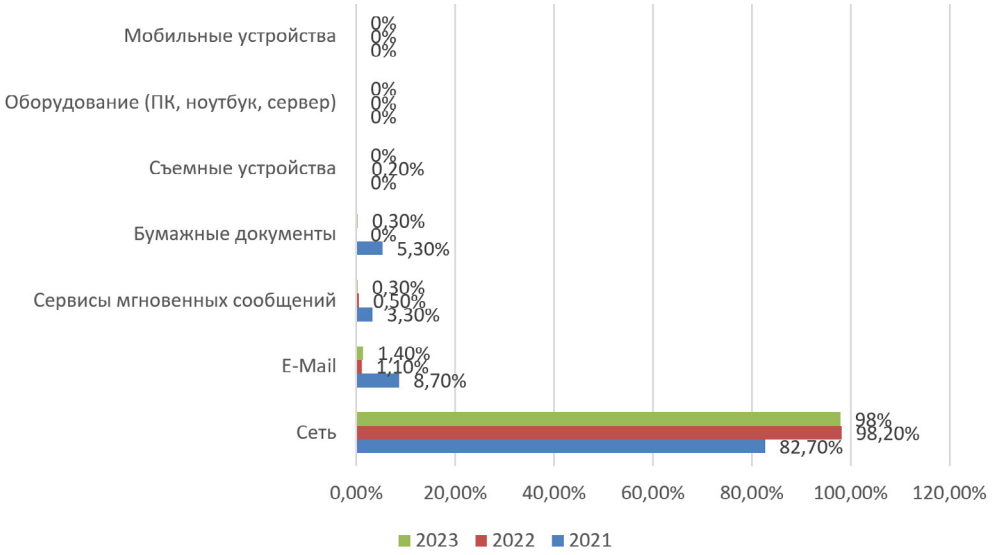


Рисунок 16. Утечки в финсекторе по каналам, мир

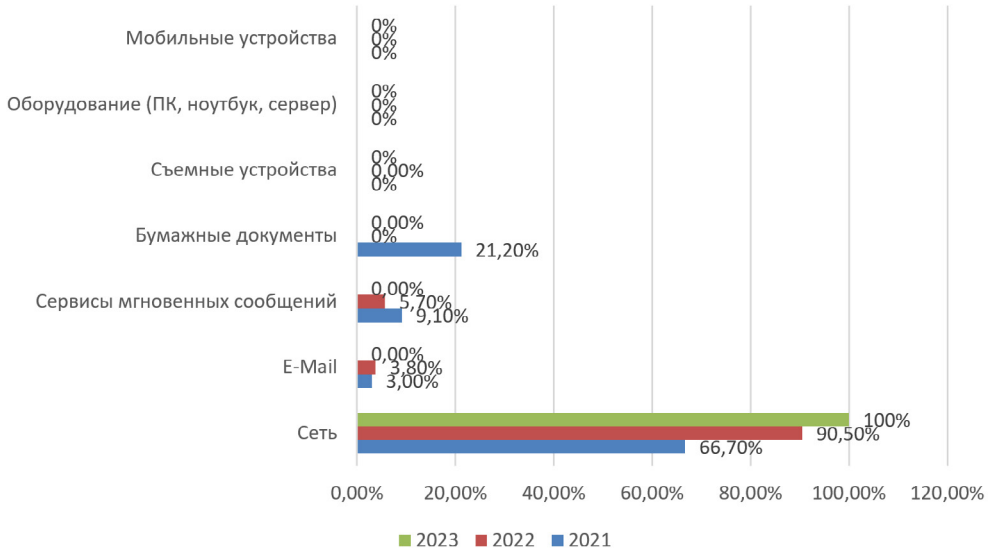


Рисунок 17. Утечки в финсекторе по каналам, Россия

Ценные ресурсы

На рисунках 18 и 19 приведено распределение утечек в финсекторе по типам скомпрометированных данных. Сумма долей превышает 100%, поскольку исследована структура данных на основе всей доступной информации об инцидентах. В ряде случаев утекли несколько типов данных.

Обращает на себя внимание рост доли утечек коммерческой тайны в мире за 2023. На наш взгляд, это прежде всего связано с тактикой хакерских группировок: внутренние данные бизнеса финансовой организации выступают весомым аргументом при шантаже

Кроме того, эту информацию можно быстро монетизировать на чёрном рынке, она может представлять интерес для разведок многих стран, так как позволяет узнать о «внутренней кухне» ключевых финансовых институтов конкурирующих и враждебных государств.

Также ЭАЦ в составе ПДн начал выделять долю аутентификационной информации (в связи с ростом), то есть логинов, паролей и других данных, которые позволяют верифицировать пользователя в системе или сервисе. В данном отчёте выделена доля биометрических персональных данных.

В мировой финансовой отрасли доля аутентификационной информации в составе ПДн среди утечек 2021 составила 1,6%, в 2022 — 2,9%, в 2023 — 4,3%. В 2021–2022 утечек биометрических данных не выявлено, в 2023 их доля в составе утекших из финансового сектора ПДн составила 0,1%.

Среди российских организаций финансовой отрасли в 2021 утечек аутентификационной информации не зарегистрировано, в 2022 её доля составила 2,1%, а в 2023 — 1,8%. Утечек биометрических данных не зарегистрировано.

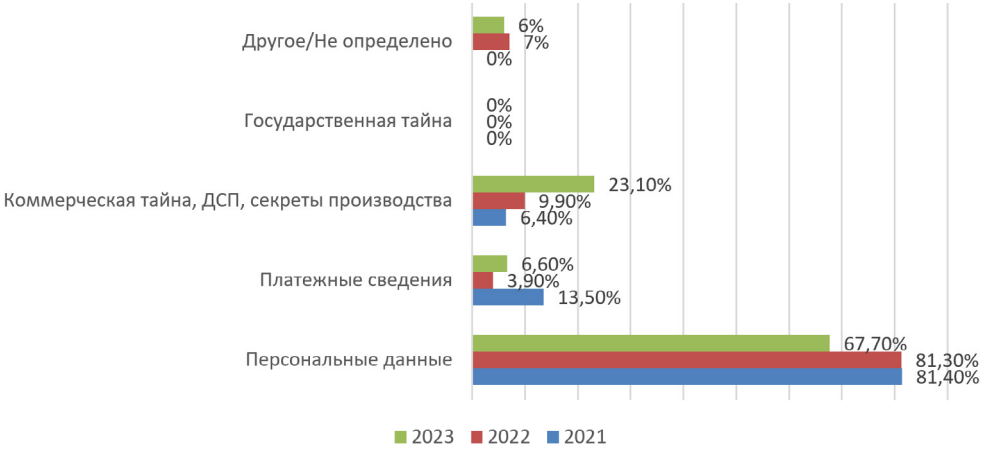


Рисунок 18. Утечки в финсекторе по типам данных, мир

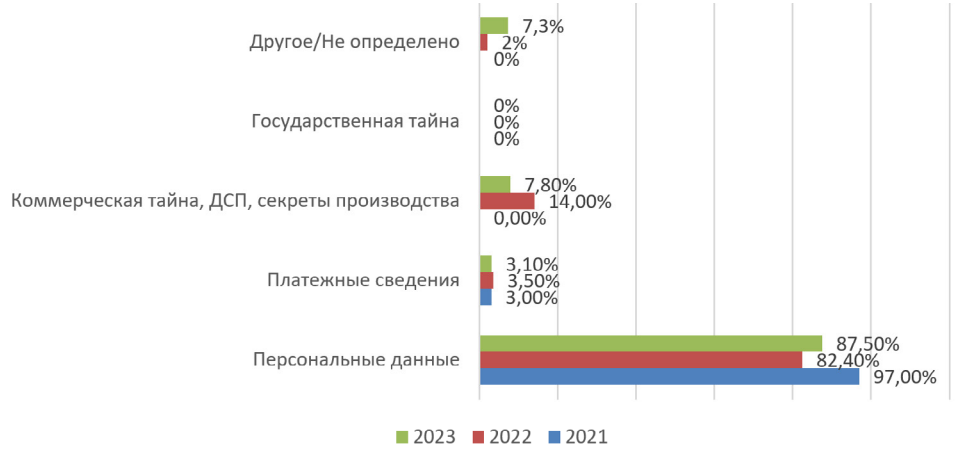


Рисунок 19. Утечки в финсекторе по типам данных, Россия

Из опроса ЭАЦ. На вопрос о том, в какой отрасли сосредоточены наиболее ценные (критичные для устойчивости организации) цифровые (информационные) ресурсы, 58% ИБ и СБ специалистов, работающих в финансовых организациях, ответили, что в финансовом секторе (58%). Другие их коллеги считают, что эти ресурсы сосредоточены: 25% — в государственном секторе, 8% — в промышленности и 8% — в энергетике. Также участники опроса считают, что на текущий момент наиболее защищена от утечек финансовая отрасль — так ответили 75% опрошенных сотрудников ИБ и СБ специалистов, работающих в финансовых организациях. Но 17% посчитали, что лучше всего защищены государственные учреждения, а 8% назвали самой устойчивой отрасль телекоммуникаций.

Поскольку опрос проводился не только среди финансовых организаций, стоит отметить, что большинство респондентов указали, что наиболее ценные ресурсы сосредоточены в финансовом секторе — 31% от всех опрошенных. На втором месте по результатам ответов находится госсектор (16%), далее идут телекоммуникации и энергетика (по 12%), промышленность (10%).

Также большинство опрошенных специалистов считают, что от утечек данных лучше всего защищен финансовый сектор (58%). С большим отрывом на втором месте находится госсектор (15%), далее расположились ИТ и ИБ-отрасль (4%).

На организации США приходится более 44% утечек в финансовой отрасли

По-прежнему основная часть утечек информации в отрасли «Банки и финансовые услуги» приходится на организации США. В 2021 эта доля составила 31,4%, в 2022 — 34,4%, а в 2023 — 44,3%.

Несмотря на рост количества утечек данных в российском финансовом секторе, доля нашей страны в общем распределении инцидентов сократилась с 21,2% в 2021 до 6,1% в 2023 (рисунок 20). Это происходит за счёт опережающего роста количества утечек в мире, прежде всего в США.

Общая доля утечек в англосаксонских странах (США, Великобритания, Канада, Австралия), в России, Индии, Китае, а также в крупнейших государствах Южной Америки (Бразилия) и Юго-Восточной Азии (Индонезия) составляет 67,3%. Соответственно, на долю других государств приходится 32,7% утечек в финансовой отрасли.

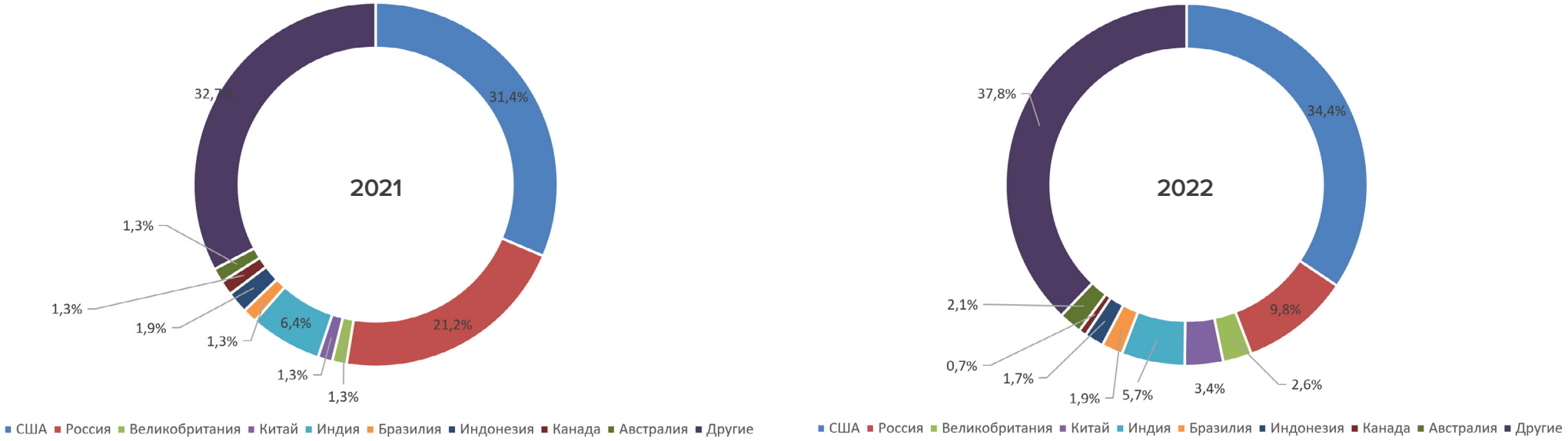
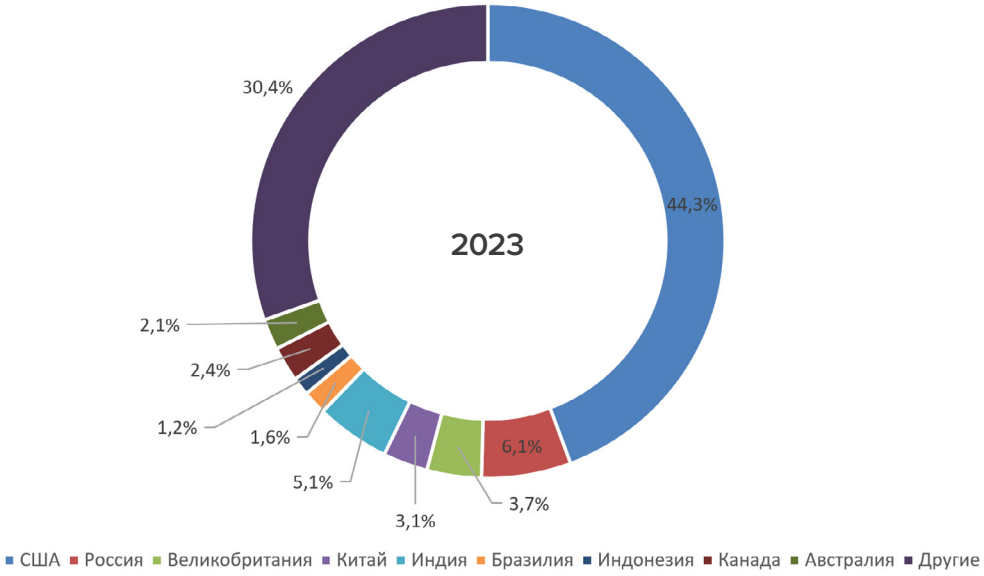


Рисунок 20. Утечки в финсекторе по странам



Заключение и выводы

Финансовая отрасль исторически является очень привлекательной для преступников, поскольку обладает солидными денежными ресурсами. Но в цифровую эпоху порой не менее желанной для злоумышленников целью становятся конфиденциальные данные. Банки, страховые компании и другие участники финансового сектора обладают значимой информацией о клиентах (ПДн, платежные сведения) и ценными коммерческими данными. Переход на «цифру» вдохнул в каждую единицу информации новый смысл. Если раньше данные были наполнением архивов и справочников, то в постиндустриальный период они приобрели осязаемую ценность, так как во многих случаях могут использоваться для получения доступа к финансовым счетам, а также выступать средством экономического и политического давления и мошеннических кампаний. Стремительное развитие цифровизации в финансовом секторе способствовало ускорению операций, повышению удобства обслуживания клиентов, созданию ряда полезных сервисов и удобных форм работы с данными. Значительное количество новых рисков появилось в связи с развитием платёжных сервисов, которые теперь в основном предоставляются дистанционно.

По результатам проведённого опроса, специалисты служб ИБ и СБ из российских организаций различных секторов экономики отметили, что наиболее ценные ресурсы сосредоточены в финансовом секторе — 31% от всех опрошенных.

На втором месте по мнению респондентов находится госсектор (16%), далее идут телекоммуникации и энергетика (по 12%) и промышленность (10%). По данным ЭАЦ, в 2023 среди финансовых организаций более 95% утечек конфиденциальной информации в мире и более 87% в России были спровоцированы кибератаками. Особую озабоченность вызывает распространение программ-вымогателей.

Используя их, злоумышленники блокируют взломанные ресурсы и требуют выкуп у организации-жертвы. Процветанию этого вида киберактивности способствует широкое распространение модели RaaS (вирус-вымогатель как сервис), когда опытные разработчики вредоносного ПО сдают его в аренду молодым хакерским группировкам.

Кроме того, финансовый сектор подвержен атакам по цепочке поставок программных продуктов. Например, современный банк может взаимодействовать с сотнями разработчиков ПО для информационных систем, платёжных сервисов, API, а также с поставщиками интеграционных сервисов. В результате эксплуатации уязвимостей в ПО Accelion, GoAnywhere и MOVEit были взломаны тысячи организаций, в том числе немало банков и страховых компаний.

Одна из главных функций современных ИТ — обеспечение удобства коммуникаций. И здесь в диалектике цифрового мира тоже возникает противоречие: помимо комфортного общения, технологии несут серьёзные риски, поскольку позволяют упростить взаимодействие злоумышленников. Сокращение доли внутренних нарушений в распределении утечек среди финансовых организация (в 2023 она составила примерно 2,5% в мире и порядка 6% в России) может не только свидетельствовать об успехах корпоративных служб ИБ и ЭБ, но и говорить о повышении латентности инцидентов по вине персонала. Вместе с тем выросла доля утечек умышленного характера по вине сотрудников — в финансовой отрасли России он составила 75% в 2023 Согласно опросу ЭАЦ, наибольшим риском утечки данных специалисты ИБ и СБ финансовых организаций считают действия сотрудников (внутренних нарушителей), поэтому планируют более половины бюджетов потратить на их обучение и тренинги в 2023–2024.

В отношении признания и информирования об утечках данных опрос показал весьма пессимистичную картину: подавляющее число респондентов из финансовой отрасли (42%) считают, что утечки данных признают лишь 4–10% организаций.

Полагаем, что всё большее количество утечек информации, которые классифицируются как внешние после появления украденной информации в дарквебе, имеют смешанную форму происхождения (т. н. гибридный вектор атаки), то есть происходят в результате сговора внешних и внутренних нарушителей. Поэтому перед специалистами ИБ в банках, страховых компаниях и других организациях стоят всё более сложные задачи по выявлению нарушений, связанных с утечками данных, и идентификации нарушителей. Значительную поддержку в решении этих задач оказывают DLP-системы нового поколения, позволяющие на основе моделей искусственного интеллекта анализировать потоки событий, брать под контроль движение всех конфиденциальных данных в компании, идентифицировать и прогнозировать риски, проводить быстрое и эффективное расследование инцидентов на основе визуализации данных.