Составлен: 22.06.2026

GIS ГАЗИНФОРМ СЕРВИС

УТЕЧКИ ДАННЫХ

Публичный отчёт от Аналитического центра кибербезопасности компании «Газинформсервис»

ТРАНСФОРМАЦИЯ 2022–2025

ГАЗИНФОРМ СЕРВИС

СОДЕРЖАНИЕ

GIS ГАЗИНФОРМ СЕРВИС

СОДЕРЖАНИЕ

ОТ АВТОРОВ

Утечки данных в Российской Федерации в 2022–2026 гг. трансформировались из серии резонансных эпизодов в устойчивый структурный риск для организаций из любого сектора экономики. Если в 2022 г. ключевым контекстом выступали массовые хактивистские кампании, то к 2024–2025 гг. ландшафт утечек стал более сложным.

Кибератаки сегодня интегрированы в общие стратегии противодействия, поэтому уязвимость любого участника цифровой экономики автоматически создает риски для всех. Компрометация одного звена, будь то подрядчик, сервисный интегратор или отраслевой сервис, открывает злоумышленникам возможность каскадного проникновения в смежные организации и объекты критической инфраструктуры. Это усложнение угроз нашло отражение не только в изменении самой анатомии инцидентов, но и в расширении спектра компрометируемых данных.

Так, в период с 2022 по 2026 год в России сформировалась новая модель **атак на данные**, включающая три последовательных этапа:

компрометация → ***публикация*** → ***монетизация***

На каждом из них могут быть задействованы разные, не связанные между собой напрямую участники. При переходе к количественному анализу важно учитывать, что наши представления о реальном масштабе утечек опираются на неполные и часто искаженные данные.

Важным фактором стала и трансформация понятия «утечка». Когда-то речь шла про утечки персональных данных, но к 2025 экспертное сообщество в своих отчетах и докладах все чаще подразумевает под этим термином утечку данных, в которых может содержаться любая информация. Это могут быть и персональные данные, и не отнесенная к той или иной категории информация.

Публичная статистика по утечкам всегда неполна по двум причинам. Во-первых, организации не раскрывают значительную часть инцидентов. Кроме того, иногда цифры в аналитических отчетах строятся на сообщениях злоумышленников, публикациях на форумах или в каналах мессенджеров.

Такие источники требуют осторожности, так как преступные группировки нередко намеренно вводят сообщество в заблуждение. Последующая проверка показывает, что утечка произошла несколько лет назад, а данные оказались устаревшими.

Тем не менее динамика утечек персональных данных уже получила отчетливый регуляторный ответ, выразившийся в ужесточении нормативной среды. С мая 2025 года вступил в силу Федеральный закон от 30.11.2024 №420-ФЗ, вносящий изменения в том числе в статью 13.11 КоАП РФ и предусматривающий более строгие штрафные механизмы за недостаточные меры по защите персональных данных.

В Аналитическом центре кибербезопасности компании «Газинформсервис» мы анализируем тенденции и статистику по утечкам данных и видим, что сегодня ни один бизнес или организация не могут считать себя застрахованными от инцидента. Угрозы приобрели системный характер, а регуляторное давление делает финансовые последствия утечек сопоставимыми с ущербом от остановки производства.

При этом для многих компаний построение «достаточно безопасной» инфраструктуры экономически затруднительно, что иногда приводит к откладыванию необходимых мер или отказу от них. В этой связи мы предлагаем подход, позволяющий заранее оценить риски, спрогнозировать возможные потери и выбрать модель информационной безопасности, оптимальную по соотношению уровня защиты, стоимости и потенциального ущерба. Такой подход, на наш взгляд, способствует принятию более взвешенных и экономически обоснованных решений.

К отчету прилагается калькулятор*, позволяющий на основе собственных данных и экспертных оценок рассчитать возможные затраты. Также представлен пример расчета на синтетическом кейсе.

Калькулятор рисков от GIS
https://www.gaz-is.ru/risk-calculator

Мы будем признательны за обратную связь, замечания и предложения. Убеждены, что только совместными усилиями возможно повысить устойчивость цифровой экономики к подобным угрозам.

Команда Аналитического центра кибербезопасности компании «Газинформсервис»

2022–2025
ТРАНСФОРМАЦИЯ АТАК НА ДАННЫЕ

2022 — БАЗОВАЯ ЛИНИЯ УГРОЗ

2022 год целесообразно рассматривать как базовую точку нового цикла утечек данных в России. В этот период фиксируется резкий рост числа инцидентов, усложнение моделей компрометации и качественное изменение профиля угроз.

По данным InfoWatch*, в 2022 году в российских организациях зафиксировано 835 инцидентов утечек и 747 млн скомпрометированных записей, что значительно превышает показатели 2020–2021 гг. В нашей выборке за тот же год, среди проанализированных 95 публичных утечек, содержащих 457 млн строк данных пользователей из РФ, крупнейшие инциденты пришлись на сегменты доставки еды, ритейла и интернет-сервисов.

InfoWatch
Аналитический отчет «Россия: утечки информации ограниченного доступа 2023-2024»

2022 год важен не только количественным всплеском, но и закреплением устойчивых закономерностей. Утечки данных все чаще становились следствием многошаговых атак с элементами социальной инженерии, компрометации внешнего периметра и последующего распространения данных. Заметно выросла роль публично доступных сервисов, открытых хранилищ и неактуализированного ПО. Атаки разворачивались в условиях мощного хактивистского давления, формировавшего «шумовой фон», маскирующий действия злоумышленников и затрудняющий своевременное обнаружение утечек.

Фишинг стал одним из ключевых стартовых механизмов компрометации, перейдя на более сложный, многокомпонентный уровень и использовался против организаций госсектора и КИИ. Глобальный контекст совпадал с трансформацией атак в России. Так, например, по данным CrowdStrike*, в 2022 году наблюдался рост социального инжиниринга, включая фишинг и обход многофакторной аутентификации. Фишинг уже выполнял не только функцию доставки вредоносного кода, но и функцию получения доступа к учетной записи, который стал самостоятельным товаром в криминальном подполье и основой для последующей атаки.

CrowdStrike
2023 Global Threat report

Наряду с фишингом, вторым значимым каналом компрометации в 2022 году стали технические недостатки внешнего периметра и ошибки в настройках и конфигурациях сервисов. При этом существенная часть крупных инцидентов была связана со спланированными атаками, что свидетельствует о переходе от случайных дефектов к целенаправленной компрометации доступных извне систем. Но и за этими техническими проблемами стояли более глубокие системные причины, связанные с изменением условий эксплуатации ИТ-инфраструктуры.

В условиях динамического изменения геополитического фактора в ландшафте ИБ в 2022 году многие организации столкнулись с проблемами ухода вендоров, нарушения поддержки и лицензирования, дефицита оборудования и образования незакрытых уязвимостей.. В совокупности это создало ситуацию, при которой внешний периметр российских организаций оказался одновременно более широким, менее однородным и хуже обслуживаемым, чем в предыдущие периоды.

Анализируя совокупность факторов, определивших всплеск утечек данных в России в 2022 году, можно утверждать, что ключевую роль сыграло не одно внешнее событие, а системная неготовность инфраструктуры защиты к резкому изменению внешнего контекста. На фоне кратного роста числа атак организации столкнулись с недостаточностью существующих мер безопасности: технические уязвимости, слабый контроль за действиями пользователей и подрядчиков, отсутствие глубокого мониторинга в сочетании с активизацией фишинга создали благоприятную среду для злоумышленников. При этом беспрецедентная активизация хактивистских группировок придала процессу качественно иной масштаб — идеологически мотивированные атаки многократно увеличили число целей и скорость распространения угроз, превратив утечки из единичных инцидентов в массовое явление, охватившее все ключевые сектора экономики.

2023/2024 — ТРАНСФОРМАЦИЯ УТЕЧЕК ДАННЫХ

Период с начала 2023 и до середины 2024 г. следует рассматривать как переходную фазу между кратным ростом количества утечек персональных данных 2022 года и структурированным ландшафтом утечек информации в общем, сформировавшимся к 2025 г.

Количество инцидентов стабилизировалось (786 в 2023 г., 778 в 2024 г.), однако масштаб последствий вырос: объем скомпрометированных записей ПДн в 2024 г. превысил 1,5 млрд, а доля России в мировых утечках информации увеличилась с 6,4% до 8,5%*. При этом важно учитывать латентный характер части инцидентов: некоторые утечки 2023 года не были публично раскрыты в момент совершения кибератаки и попали в статистику только в 2024 г., после обнаружения дампов в открытых источниках или базах данных. Это означает не снижение риска, а его качественную перестройку, то есть инциденты становятся сложнее и масштабнее, а временной разрыв между компрометацией и публичным раскрытием увеличивается, затрудняя своевременное реагирование.

InfoWatch
Аналитический отчет «Россия: утечки информации ограниченного доступа 2023-2024»

Сдвиг в механизмах компрометации: подрядчики и среда разработки

Одним из наиболее значимых признаков переходного этапа является усиление роли подрядчиков и иных доверенных контрагентов в механизме компрометации. Атаки все чаще реализуются через поставщиков, уже имеющих легитимный доступ к корпоративным системам. Недостаточный контроль прав доступа, слабая сегментация сетей и формальная верификация партнеров позволяют злоумышленникам обходить традиционные защитные барьеры через доверенные отношения.

Это означает качественный сдвиг по сравнению с 2022 годом. С 2023 г. цепочка поставок начинает выступать не как среда накопления риска, а как самостоятельный канал утечек данных.

Компрометация подрядчика часто менее заметна для жертвы, чем прямая атака на внешний периметр, и злоумышленники используют уже существующие доверенные каналы доступа, маскируя активность под штатное взаимодействие.

Этот сдвиг подтверждается и расследованиями F.A.C.C.T.*: в инструментарии группировки Shadow фигурируют AnyDesk, PuTTY, WinSCP, Rclone, ngrok, PsExec, wmiexec и другие средства удаленного доступа. Набор хорошо показывает логику переходного периода, когда атакующие эксплуатируют легитимные инструменты и уже имеющиеся точки входа, а не только классические вредоносные сценарии.

F.A.C.C.T.
«Тени не скроются»: Расследование атак группировки Shadow

Логика использования доверенных каналов естественным образом распространилась и на среду разработки, которая за переходный период превратилась в самостоятельную зону риска. Инциденты все чаще были связаны с несанкционированным доступом к исходному коду, к базам данных и конфигурационным файлам через уязвимости систем управления версиями и CI/CD-конвейеров. В этот период утекает уже и информация об уязвимостях, точках входа, о самой инфраструктуре. То есть недостаточная защита репозиториев и отсутствие принципа минимальных привилегий приводили к утечкам не только пользовательских данных, но и архитектурных артефактов, сервисных ключей и другой критически значимой технической информации.

За период 2023–2024 гг. утечка перестает быть просто выгрузкой клиентской базы. Компрометации затрагивают инженерные контуры: хранилища кода, среды сборки, внутренние wiki-системы. Показателен кейс компании «Микорд»*, где в сеть попали техническая информация по ЕРВУ (единый государственный реестр воинского учета), выгрузки из Jira и Confluence, а также скриншоты переписок после взлома. Такой тип инцидента принципиально отличается от классической утечки персональных данных: объектом становится не только массив данных о людях, но и конфиденциальные данные производства, компании, ИТ-инфраструктуры.

Кейс компании «Микорд»
стр. 23

В результате к концу 2024 г. формируется переход от логики «взломали базу персональных данных» к логике «скомпрометировали цифровую среду».

Telegram как канал утечек и витрина давления

Вторая важнейшая характеристика переходного этапа — это изменение каналов публикации скомпрометированных данных. Если в 2022 и некоторое время в 2023 году основная видимость утечек была сосредоточена на форумах и даркнет-площадках, то к 2024 году Telegram становится доминирующим каналом. Исследования показали, в 2024 году через Telegram распространялось 72% зафиксированных публикаций утечек, через специализированные форумы — 26%.

Таким образом значение Telegram становится шире, чем роль просто «площадки размещения». Он снижает порог публикации, с этого момента злоумышленнику не требуется встраиваться в

репутационную систему даркнет-форумов. Telegram позволяет совмещать несколько функций, таких как: демонстрация факта компрометации, давление на жертву, вброс фрагментов данных, продажа дампа и медиатизация инцидента. Формат канала или чата превращает утечку в элемент информационно-психологического воздействия, и публикация фрагмента базы или схем инфраструктуры служит публичным доказательством, что усиливает репутационный ущерб.

Но и специализированные форумы сохраняют свою роль — они используются атакующими для публикации логинов, паролей и технических деталей атак. В 2023–2024 гг. формируется многоуровневая экосистема: Telegram выполняет функцию быстрой витрины и давления, форумы — функцию детализированной монетизации и обмена.

Смешанный профиль нарушителя

В 2024 году формально внешний нарушитель остается доминирующим (76,9%)*, однако успешность атак все сильнее зависит от внутренних условий, таких как: ошибки настройки, избыточность прав, низкая цифровая гигиена сотрудников и недостаточность контроля за подрядчиками. Доля умышленных и неумышленных действий персонала как значимых факторов утечек, по опросам, достигает 37% и 44% соответственно. Происходит переход от чисто внешнего вектора к смешанной модели, где внешняя атака реализуется через внутренние уязвимости организационного уровня.

InfoWatch
Аналитический отчет «Россия: утечки информации ограниченного доступа 2023-2024»

Исследования показали, что в 2023–2024 гг. ландшафт утечек в России качественно изменился. При стабилизации числа инцидентов масштаб последствий вырос. Произошел сдвиг в механизмах компрометации, получили широкое распространение атаки через подрядчиков и цепочки поставок, среда разработки стала самостоятельной зоной риска. Утечки перестали сводиться к выгрузке клиентских баз. Telegram превратился в доминирующий канал публикации, совмещая функции витрины, давления и медиатизации, а форумы сохранили роль площадки для монетизации. Профиль нарушителя стал гибридным, и внешняя атака стала чаще реализовываться через внутренние уязвимости. Эти изменения заложили основу для структурированного ландшафта утечек, закрепившегося в 2025.

2024/2025 — СТРУКТУРИРОВАННЫЙ ЛАНДШАФТ УТЕЧЕК

Период второй половины 2024 и 2025 г. — это фаза окончательного оформления ландшафта утечек данных в России.

Если 2022 год выступал базовой линией угроз, когда к атакующим присоединились хактивисты и массово утекали персональные данные, то в 2023 и в первой половине 2024 г. накопленные базы использовались злоумышленниками для старта множества новых атак. Получила массовое развитие социальная инженерия, мошенничество, вымогательство — но этот период был только переходным этапом. К 2025 г. в публичной аналитике уже прослеживается устойчивая четырехканальная схема компрометации цифровой инфраструктуры организаций и утечек данных.

Рис. 1
Квадрат утечек информации 2025

2024–2025 КРУПНЕЙШИЕ УТЕЧКИ

КРУПНЕЙШИЕ УТЕЧКИ 2024

Эффективная оценка киберрисков начинается с изучения реальных инцидентов. Анализ резонансных утечек данных формирует понимание актуальных угроз и их бизнес-воздействия.

Компрометация данных Rendez-Vous

Источник: anti-malware.ru

В 11 SQL-дампах размещена следующая информация:

- ФИО
- email (4,5 млн уникальных)
- телефон (7,6 млн уникальных)
- дата рождения
- пол
- адрес прописки
- хешированный пароль (MD5 с солью)
- даты регистрации и последней активности
- стоимость покупки, размер скидки
- накопленные бонусы
- код подарочного сертификата и ПИН для активации

Компромат данных ДИТ Москвы (mos.ru)

Источник: ib-bank.ru

В открытом доступе оказались 13 462 446 строк, содержащих:

- ФИО
- даты и места рождения
- адреса регистрации и фактического места проживания
- номера паспортов и свидетельств о рождении
- телефон (7,2 млн уникальных)
- email (4,8 млн уникальных)

Утечка Burgerkingrus

Источник: telesputnik.ru

В открытый доступ были выложены данные клиентов, предположительно сети быстрого питания Burger King, пишут аналитики DLBI. Всего 5 627 676 строк за период времени с 31.05.2018 по 25.08.2024. Данные, которые попали в Сеть:

- имя
- телефон (4,8 млн уникальных)
- email (3,1 млн уникальных)
- дата рождения
- пол
- город
- любимая категория/блюдо
- дата заказа

КРУПНЕЙШИЕ УТЕЧКИ 2025

Федеральная служба государственной регистрации, кадастра и картографии (Росреестр)

Источник: masksafe.ru

В январе Silent Crow заявили о компрометации инфраструктуры Росреестра — ФОИВ имущественного учета. По их утверждению, им удалось получить доступ к более чем 2 миллиардам строк информации общим объемом около 1 терабайта. В качестве доказательства хакеры опубликовали фрагмент базы данных на 81 990 606 строк, где содержится свыше 12,5 тыс. вхождений слова «rosreestr». Последняя запись в утекшем дампе датируется 10.03.2024. Ведомство официально отрицает факт утечки и заявляет, что проводит дополнительные проверки.

Данные, которые попали в Сеть:

- ФИО
- email (401 тыс. уникальных)
- Телефон (7,5 млн уникальных)
- Адрес
- Дата рождения
- СНИЛС
- Дата
- Компания

ПАО «Аэрофлот»

Источник: reuters.com , www.ec-rs.ru

ПАО «Аэрофлот» пережило крупную хакерскую атаку. Ответственность за нее взяли группировки «Киберпартизаны BY» и Silent Crow.

- ФИО
- Даты рождения
- Сканы нагрузочных тестов
- Заключения врачебно-летных экспертных комиссий
- Медицинские данные

Ростелеком

Источник: masksafe.ru

В том же месяце Silent Crow заявили о компрометации «Ростелекома». По заявлению компании, инцидент произошел из инфраструктуры подрядчика, а не из основных систем компании. В опубликованных образцах фигурируют 154 тыс. адресов электронной почты и 101 тыс. телефонных номеров. «Ростелеком» утверждает, что особо чувствительных персональных данных в утечке не было, и рекомендует пользователям сменить пароли и включить двухфакторную аутентификацию.

Данные, которые попали в Сеть:

- Имя
- email (154 тыс. уникальных)
- Телефон (101 тыс. уникальных)
- Текст обращения
- Название компетентного департамента

Утечка информации Микорд

Источник: storage.googleapis.com

Анонимная хакерская группировка опубликовала заявление о компрометации разработчика единого реестра воинского учета, компании «Микорд». Часть полученных ими данных была выложена в сеть. По заявлению СМИ, утечка содержит:

- Техническую информацию по ЕРВУ (единый реестр воинского учета)
- Выгрузки из Jira и Confluence
- Скриншоты переписок и реакции в чатах после взлома

КРУПНЕЙШИЕ УТЕЧКИ 2025

Департамент информационных технологий города Москвы

Источник: vademec.ru

Хакерская группировка заявила об атаке на ЕМИАС. В результате атаки был получен полный доступ к внутренней сети крупной информационной системы, обслуживающей значительное количество пользователей. Общий объем извлеченных данных составил около 17 ТБ, включая базы данных и другие корпоративные ресурсы.

- ФИО
- Даты рождения
- Номера полисов
- Адреса прописки
- Телефоны
- Электронная почта
- Логины

АльфаСтрахование-Жизнь

Источник: computerra.ru

В сети оказались данные 60 тыс. человек:

- ФИО
- Дата рождения
- Телефон (68 тыс. уникальных)
- email (34 тыс. уникальных)
- Пароль в хеше
- Должность и место работы

ОТРАСЛЕВОЙ АНАЛИЗ РФ

Отраслевой анализ утечек данных в Российской Федерации за 2022–2026 гг. показывает, что структура риска менялась не линейно, а по двум различным траекториям. Первая траектория отражает масштаб компрометации — то есть объем строк и записей, попавших в открытый доступ в публично наблюдаемых кейсах. Вторая — частоту инцидентов по отраслям, зафиксированных в годовой статистике.

Именно поэтому в разные годы лидерами оказываются разные сектора: в 2022 году доминировали доставка еды и ритейл по объему утекших данных, в 2023 году — ритейл и финансы, в 2024 году — торговля и госсектор по числу инцидентов, а в 2025 году торговля сохранила лидерство по частоте, тогда как государственный сектор вышел в лидеры по масштабу компрометации*.

«Газинформсервис»
Отчёт об утечках 2022–2023

Методически важно учитывать, что 2022–2023 гг. в доступных материалах хорошо описываются через объем публично выложенных строк, тогда как 2024–2025 гг. — через зарегистрированные утечки и отраслевые доли. Поэтому отраслевой анализ должен сопоставлять не только числа, но и характер риска: где утечки происходят чаще, где они крупнее, где выше доля чувствительных данных и где атака опирается на наиболее зрелые каналы компрометации, внешний периметр, подрядчиков, среды разработки и легитимные доступы.

В «текущей картине» (как ориентире для 2026) лидируют по атакуемости: госуправление (14%), финансы (11%), транспорт и логистика (10%), электронная коммерция/ритейл (10%), далее IT (6%), производство/промышленность (5%)*.

BI.ZONE
Исследование ландшафта киберугроз в России и странах СНГ

ГОСУДАРСТВЕННЫЙ СЕКТОР

Государственный сектор в 2022 году еще не выглядел главным источником массовых публичных утечек по объему строк: в выборке публично проанализированных кейсов на него приходилось около 583 тыс. строк.

Однако уже в 2023 году объем публично утекших данных из госорганов вырос до 5,5 млн строк, а в 2024 году государственные организации заняли третье место по числу утечек персональных данных с долей 9,8%, причем сам InfoWatch* подчеркивает, что в госсекторе фиксируется рост уже третий год подряд.

InfoWatch
Аналитический отчет «Россия: утечки информации ограниченного доступа 2023-2024»

В 2025 году государственный сектор стал ключевым не столько по числу инцидентов, сколько по масштабу последствий. В кейсовом массиве за первую половину 2025 года на государственный сектор пришлось 26% всех зафиксированных утечек, но при этом 92% общего объема утекших строк. В том же массиве фигурируют наиболее крупные и системно значимые инциденты: предполагаемая компрометация Росреестра с заявлением о более чем 2 млрд строк и публикацией фрагмента на 81,99 млн строк, а также атака на ЕМИАС / ДИТ Москвы с заявленным извлечением около 17 ТБ данных. Даже с учетом неполной верификации таких заявлений отраслевой профиль очевиден: государственные структуры в 2025 году концентрировали максимальный объем гражданских и инфраструктурных данных, а значит, и максимальный потенциальный ущерб.

В аналитической логике 2026 года госсектор следует квалифицировать как отрасль с наивысшим системным риском: не обязательно с максимальной частотой утечек, но с наибольшим масштабом компрометации, высокой чувствительностью данных и выраженным эффектом каскадного ущерба для граждан и критических сервисов.

ФИНАНСЫ

Финансовая отрасль еще в 2022 году не была лидером по объему публично утекших данных — в выборке публичных кейсов на нее приходилось около 244 тыс. строк.

Однако уже в 2023 году финансы вышли в число наиболее пострадавших отраслей: объем утекших данных составил 154,9 млн строк, практически сравнявшись с ритейлом (158,6 млн). Это подтверждает, что финсектор остается для злоумышленников одним из наиболее привлекательных объектов из-за высокой ценности клиентских, платежных и идентификационных данных.

В 2024 году доля финансового сектора в зарегистрированных утечках, напротив, снизилась: по всем утечкам она составила 3,2% против 10,1% в 2023 году, а по утечкам персональных данных — 3,9% против 12,1% годом ранее. Однако это снижение не означает устойчивого ослабления риска. Уже по итогам 2025 года InfoWatch зафиксировал 44 инцидента в

InfoWatch
Аналитический отчет «Россия: утечки информации ограниченного доступа 2023-2024»

российском финсекторе против 29 в 2024 году, то есть рост примерно в полтора раза. При этом объем известных скомпрометированных ПДн составил 3,6 млн записей против 77,5 млн годом ранее, но сам источник оговаривает, что около 35% российских сообщений об утечках в финсекторе вообще не содержат сведений о числе записей. Одновременно около 16% инцидентов в российской финансовой отрасли были связаны с внутренними нарушителями, что существенно выше мирового уровня.

Следовательно, финансы в 2022–2025 гг. демонстрируют не максимальную частоту инцидентов, а высокую концентрацию экономически ценных данных, устойчивую привлекательность для атакующих и заметную роль внутренних рисков.

ЭЛЕКТРОННАЯ КОММЕРЦИЯ И РИТЕЙЛ

Ритейл и электронная коммерция являются наиболее устойчивым лидером российского ландшафта утечек.

Уже в 2022 году в публичной выборке на ритейл приходилось 37,9 млн строк*, а если учитывать еще и связанный с потребительским рынком сегмент ресторанов и доставки еды, то крупнейший объем — 311,9 млн строк — вообще приходился именно на эту группу сервисов массового спроса. В 2023 году ритейл стал главным сектором по объему утекших данных — 158,6 млн строк, опередив финансы.

«Газинформсервис»
Отчёт об утечках
2022–2023

В 2024 году лидерство ритейла только укрепилось. По всем зарегистрированным утечкам доля торговли составила 27,8% против 16,8% в 2023 году, а по утечкам персональных данных — уже 35,1% против 21,3%. InfoWatch прямо отмечает, что в 2024 году на торговлю пришлось больше трети всех инцидентов с персональными данными*. В 2025 году эта тенденция сохранилась: по официальным итогам InfoWatch торговля второй год подряд занимает первое место по числу инцидентов с долей 25,4%.

InfoWatch
Аналитический отчет
«Россия: утечки информации ограниченного доступа 2023-2024»

В сводном виде российский отраслевой профиль 2022–2026 гг. можно интерпретировать следующим образом: ритейл лидирует по частоте и устойчивости инцидентов; госсектор — по масштабу и чувствительности последствий; финансы — по экономической ценности данных и значимости внутренних рисков.

Отсюда следует и ключевой вывод для 2026 года: наиболее опасны не просто отрасли с самым большим числом утечек, а отрасли, где сочетаются большие массивы данных, высокая связность с внешними сервисами, зависимость от подрядчиков и значительный общественный либо экономический ущерб. Именно поэтому в российском контексте в 2026 году к наиболее рискованным с точки зрения информационной безопасности следует отнести госсектор, ритейл и финансы.

АНАЛИЗ ЭКОНОМИЧЕСКИХ ПОТЕРЬ ПРИ УТЕЧКАХ ИНФОРМАЦИИ

Структурированный анализ утечек информации позволил оценить масштаб и динамику угрозы. Теперь от статистики инцидентов перейдём к экономике их последствий. Для этого необходимо сместить фокус с операционных метрик на анализ прямого и косвенного ущерба.

Сюда входят регуляторные штрафы и судебные издержки при утечках персональных данных, прямая потеря выручки из-за остановки бизнес-процессов, расходы на восстановление повреждённых данных и, как наиболее трудно измеримая, но от того не менее разрушительная статья — репутационные потери, ведущие к оттоку клиентской базы. Совокупность этих затрат превращает киберинцидент из технического сбоя в финансовое событие, требующее оценки окупаемости защитных мер.

В этой логике становится очевидным, что превентивные затраты на построение системы защиты данных, как правило, на порядки ниже суммы совокупного ущерба от реализации даже одного крупного инцидента, что переводит вопрос безопасности из разряда технического в разряд финансово обоснованного управления рисками.

ИЗДЕРЖКИ КОМПАНИИ ПРИ УТЕЧКАХ ИНФОРМАЦИИ

Как было сказано выше, любая утечка информации, помимо правовых и репутационных последствий, имеет прямое финансовое измерение, которое складывается из нескольких обязательных статей затрат.

Потери выручки от простоя компании во время восстановления данных при утечке информации

По статистике минимальное время простоя и восстановления систем после атаки, вследствие которой утеряна информация, составляет от 3-5 дней, средний период простоя составляет около 10 дней.

Этот процесс включает:

- **Диагностику**
  Выявление скомпрометированных данных и пораженных систем.
- **Восстановление данных**
  Восстановление информации и функциональности систем из резервных копий.
- **Устранение уязвимостей**
  Патчинг и обновление ПО, через которое произошел взлом.
- **Административные и коммуникационные задачи**
  Уведомление клиентов, партнеров и регуляторов (например, Роскомнадзора), восстановление рабочих процессов.

Штрафы

Закон от 27.07.2006 № 152-ФЗ «О персональных данных» обязывает операторов персональных данных применять меры по обеспечению безопасности и сохранению конфиденциальности сведений. К операторам персональных данных относятся практически все ИП, компании и даже самозанятые, если они взаимодействуют с личной информацией физлиц.

С 30 мая 2025 года действуют поправки (Федеральный закон от 30 ноября 2024 г. № 420-ФЗ) в статью 13.11 Кодекса РФ об административных правонарушениях «Нарушение законодательства Российской Федерации в области персональных данных» (далее — 13.11 КоАП РФ), предусматривающие ужесточение ответственности за нарушения в данной области.

Во-первых, выросли штрафы за обработку персональных данных в не предусмотренных законом случаях. Компании заплатят от 150 000 до 300 000 рублей (ч. 1 ст. 13.11 КоАП РФ). За повторное нарушение придется перечислить в бюджет в несколько раз больше (ч. 1.1 ст. 13.11 КоАП РФ).

Во-вторых, за утечку ПДн ввели штрафы, размеры которых зависят от количества пострадавших:

- **от 1000 до 10 000 субъектов ПДн**
  от 200 000 до 400 000 рублей для должностных лиц, от 3 000 000 до 5 000 000 рублей для компаний (ч. 12 ст. 13.11 КоАП РФ);
- **от 10 000 до 100 000 субъектов ПДн**
  от 300 000 до 500 000 рублей для должностных лиц, от 5 000 000 до 10 000 000 рублей для компаний (ч. 13 ст. 13.11 КоАП РФ);
- **более 100 000 субъектов ПДн**
  от 400 000 до 600 000 рублей для должностных лиц, от 10 000 000 до 15 000 000 рублей для компаний (ч. 14 ст. 13.11 КоАП РФ).
- **За повторное нарушение** для компаний предусмотрен «оборотный» штраф – от 1% до 3% годовой выручки, но не менее 20 000 000 рублей и не более 500 000 000 рублей (ч. 15 ст. 13.11 КоАП РФ). Оборотный штраф — это процент от совокупной годовой выручки компании за год, предшествующий году выявления правонарушения.
- **При утечке специальных категорий ПДн** грозит штраф до 15 000 000 рублей, биометрических ПДн – до 20 000 000 рублей (ч. 16 и 17 ст. 13.11 КоАП РФ).

В-третьих, установили штрафы за неуведомление Роскомнадзора о намерении обрабатывать ПДн или об их утечке (ч. 10 и 11 ст. 13.11 КоАП РФ). С 30 мая 2025 года штрафы по ч. 11 ст. 13.11 КоАП РФ: для должностных лиц — от 400 000 до 800 000 рублей; для ИП — от 1 до 3 млн рублей; для организаций — от 1 до 3 млн рублей.

Чтобы избежать штрафа, оператор должен отправить уведомление в Роскомнадзор в течение 24 часов с момента выявления факта «неправомерной передачи, предоставления, распространения или доступа к персональной информации без согласия субъекта данных»; за **72 часа** провести расследование и отправить в РКН отчёт о его результатах (ч. 3.1 ст. 21 Федерального закона от 27.07.2006 N°152-ФЗ).

Причем, исходя из судебной практики, можно сказать, что суды учитывают наличие у оператора организационных и технических мер.

Издержки от судебных исков физических лиц, чьи данные были скомпрометированы

Судебные издержки, связанные с исками физических лиц, чьи персональные данные были скомпрометированы, представляют собой хотя и регулярную, но относительно сдержанную по масштабу статью ущерба. Сам по себе факт существования такого рода претензий создаёт для организации дополнительную правовую и финансовую нагрузку.

На основе практики РФ иски предъявляют 0,1–0,5% от числа пострадавших, а размер компенсации составляет 10–15 тыс. рублей на человека.

Репутационные потери вследствие оттока клиентов при утечке информации

Репутационные потери, пожалуй, наиболее трудно формализуемый, но при этом один из самых разрушительных видов косвенного ущерба от утечки информации. Они не фиксируются в бухгалтерской отчётности непосредственно в момент инцидента, однако именно через них удар наносится по будущим денежным потокам компании.

Оценочные потери от оттока клиентов и снижения продаж на основании экспертной оценки составляют в среднем 1,5% от совокупной годовой выручки компании.

Затраты на восстановление утерянных данных

Компания в случае инцидента по утечке информации дополнительно несет следующие затраты:

1. Восстановление утерянной информации.
2. Работа по восстановлению может выполняться штатными сотрудниками профильных подразделений или с привлечением наемных специалистов. Затраты зависят от масштаба утечки данных и складываются из срока выполняемых работ по восстановлению, количества задействованного персонала, дополнительных материальных затрат (при необходимости).
3. Выкуп скомпрометированной информации.
4. PR на проведение дополнительных исследований и разработки новой рыночной стратегии для предприятия в связи с отказом от организационных, научно-технических, коммерческих решений, ставших неэффективными в результате утечки сведений.

ВАРИАНТЫ ЗАЩИТНЫХ СИСТЕМ В КОМПАНИИ

Насколько дорого обеспечить безопасность инфраструктуры? В зависимости от выбранной модели организации работ — полное внутреннее внедрение или полный аутсорсинг — существенно меняется структура затрат и уровень контроля над инфраструктурой. Рассмотрим два основных варианта внедрения защитных систем в компании.

Вариант 1

Защитой информации занимается полностью внутренняя ИБ-команда

Все работы по внедрению и сопровождению систем защиты данных выполняются штатными сотрудниками службы ИБ компании.

Этот путь включает в себя расходы на:

1. Приобретение и настройку оборудования, затраты на техническое обслуживание оборудования или затраты на аренду оборудования.
2. Приобретение, настройку, интеграцию ПО.
3. ФОТ сотрудников службы ИБ (заработная плата, налоги с ФОТ).
4. Обучение и повышение квалификации персонала.
5. Поиск и подбор персонала.
6. Оборудование рабочего места сотрудников службы ИБ.

Минусы данного варианта:

1. Единовременные высокие инвестиции на покупку оборудования, ПО.
2. Поиск качественного оборудования, закупка, поиск подрядчиков по проектированию и настройке, внедрение и интеграция занимает длительное время.
3. Поиск специалистов службы ИБ в условиях «кадрового голода».
4. Результат работы зависит от квалификации персонала, следовательно необходимо постоянное и качественное обучение персонала. В условиях высокой текучести кадров данные затраты могут быть выше запланированных. Найти и удержать готовых людей очень дорого. С новичками в ИБ ситуация тоже непростая – их нужно обучить, а затем суметь удержать, потому что спрос огромный.

Вариант 2
Полный аутсорсинг безопасности

В модели полного аутсорсинга ИБ, известной также как услуги MSSP (Managed Security Service Provider), компания делегирует внешнему провайдеру ответственность за весь комплекс мер защиты информации.

За абонентскую плату компании предоставляется готовая инфраструктура, которая включает в себя аренду и настройку оборудования, обновления, мониторинг и техподдержку.

Услуги MSSP различаются по объему ответственности провайдера. Условно их можно разделить на три уровня сервиса:

- **Базовый уровень** фокусируется на мониторинге и базовой защите конечных точек без глубокого реагирования. Включает EDR/антивирус, базовый SOC-мониторинг (SOC L1), обновления СЗИ. Обеспечивает соответствие минимальным требованиям ФСТЭК.

- **Средний уровень** добавляет управляемое обнаружение и реагирование (MDR). Входит SIEM, XDR/EDR с автоматизацией, Threat Hunting, DLP, WAF для веб-приложений. Провайдер берет на себя постоянный мониторинг, начальное реагирование и отчетность по инцидентам.
- **Премиум-уровень** предполагает полный аутсорсинг ИБ с проактивной защитой. Комплекс: SIEM/SOAR + SOC/MDR, криптография, расследование инцидентов, аудит соответствия (ФСБ, ГосСОПКА). Включает пост-анализ атак.

Коммерческий SOC обеспечивает доступ к enterprise-уровню безопасности без капитальных затрат и операционных сложностей.

Детализированные выгоды коммерческого SOC заключаются в следующем:

1. Экспертиза и знания, глубокая специализация аналитиков (специалисты по различным типам атак (APT, ransomware, DDoS), аналитики с отраслевой экспертизой (финансы, retail, производство), постоянное обучение за счет провайдера, накопленная база знаний по 1000+ инцидентам)
2. Технологическое превосходство — современные SIEM/SOAR-платформы (системы поведенческого анализа (UEBA), платформы Threat intelligence, системы машинного обучения для обнаружения аномалий)
3. Экономия на масштабе (инфраструктура распределяется между 50+ клиентами, автоматизация рутинных операций, стандартизированные процессы, общие базы знаний и детекторы)
4. Гарантированное качество обслуживания (время обнаружения угроз: < 15 минут, время реагирования: < 30 минут, ложные срабатывания: < 5%, доступность платформы: 99.9%)
5. Управление рисками и комплаенс (подготовка отчетов для регуляторов, соответствие 152-ФЗ, 187-ФЗ, PCI DSS, аудит безопасности партнеров, управление инцидентами по NIST/ISO)
6. Проактивная безопасность (поиск скрытых угроз в инфраструктуре, анализ тактик и техник злоумышленников (MITRE ATT&CK), расследование сложных инцидентов, рекомендации по усилению защиты)
7. Бизнес-преимущества (защита репутации бренда, обеспечение непрерывности бизнеса, повышение доверия клиентов и инвесторов, снижение стоимости киберстрахования).

СРАВНЕНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧЕК С РАЗНОЙ ВАРИАЦИЕЙ СЗИ

Для наглядного сопоставления двух моделей рассмотрим синтетический кейс компании ООО «Атлет-супер-Ритейл».

Оценим прогнозируемый ущерб от потенциальной утечки, затраты на построение собственной службы ИБ и стоимость подключения внешнего центра мониторинга и реагирования на инциденты. Для удобства такой оценки к настоящему отчёту прилагается экономический калькулятор, позволяющий на основе индивидуальных параметров бизнеса рассчитать окупаемость инвестиций в тот или иной способ защиты.

Экономический калькулятор рисков

https://www.gaz-is.ru/risk-calculator

КЕЙС: ТОРГОВАЯ СЕТЬ «АТЛЕТ-СУПЕР»
ВЫБОР МОДЕЛИ ЦЕНТРА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Общая информация об организации

- **Наименование**
  Торговая сеть «Атлет-супер» (ООО «Атлет-супер-Ритейл»).
- **Сфера деятельности**
  Розничная торговля продуктами питания и сопутствующими товарами (форматы: супермаркеты у дома, дискаунтеры).
- **Годовая выручка**
  6,75 млрд рублей.
- **Численность сотрудников**
  980 человек (из них 850 — персонал магазинов и складов, 130 — офисные сотрудники и ИТ-персонал).
- **География**
  Центральный офис (г. Москва), распределительный центр (Московская область), 69 магазинов в Московской, Тульской и Калужской областях, собственный интернет-магазин с доставкой.

Компания активно развивает омниканальные продажи: покупатели оформляют заказы онлайн и забирают в магазинах, действует программа лояльности с обработкой персональных данных. Бизнес критически зависит от непрерывной работы кассового оборудования (каждая минута простоя — потеря выручки) и соответствия требованиям индустрии платежных карт. Маржинальность в ритейле низкая, поэтому любые незапланированные расходы, включая штрафы регуляторов или простой, оказывают значительное давление на финансовые показатели.

Характеристика ИТ-инфраструктуры

ИТ-инфраструктура является высокораспределенной и территориально разнесенной. Для расчетов стоимости SOC активы классифицированы по типам и точкам сбора событий.

Категория	Характеристика	Количество активов/ параметров
Серверное оборудование	ЦОД (2 хоста виртуализации), серверы в магазинах (фискальные серверы, контроллеры)	75 шт. (включая виртуальные машины)
Кассовое и терминальное оборудование	POS-терминалы (кассы), платежные терминалы, весовое оборудование	345 единиц
Пользовательские устройства	Рабочие станции офиса, ноутбуки сотрудников, планшеты для приемки товара	330 шт.
Сетевое оборудование	Маршрутизаторы, коммутаторы, точки доступа Wi-Fi, VPN-концентраторы для связи с магазинами	170 шт. (включая 69 комплектов оборудования в магазинах)
Системы защиты	EDR-агенты (только офис и серверы), DLP (для офиса), почтовый шлюз, антивирус для касс	350 лицензий EDR; 200 лицензий для POS-систем (для точек продаж)
Критичные активы	Серверы баз данных (1С, система лояльности, интернет-магазин), процессинговые узлы платежных шлюзов	25 шт.
EPS (Events per second)	Средняя нагрузка генерации событий безопасности	4000 EPS

Контекст для расчета: основной вызов для ритейлера — обеспечение безопасности удаленных объектов (магазинов), где нет локальных ИТ-специалистов. Мониторинг должен охватывать:

- 69 торговых точек с кассовым оборудованием;
- Распределительный центр с WMS-системой;
- Интернет-магазин и процессинг платежей.

Для соблюдения требований безопасности необходимо контролировать доступ к среде платежных карт, что требует строгого логирования и мониторинга всех операций с данными держателей карт.

Команда ИБ и текущие вызовы

На момент принятия решения в компании функционировал отдел информационной безопасности из 3 человек:

- Руководитель отдела ИБ;
- 1 специалист по сетевым экранам;
- 1 специалист по защите периметра и антивирусной защите.

Существующие проблемы:

1. **Отсутствие мониторинга 24/7**
   Атаки на ритейлеров (особенно программы-шифровальщики и компрометация касс) происходят преимущественно в ночное время и выходные. Штатный отдел работает 5/2 с 9:00 до 18:00.

2. **Несвязанность событий**
   В компании есть разрозненные средства защиты (антивирус, DLP, межсетевые экраны), но отсутствует SIEM-платформа. Аналитики не видят цепочку атаки. Расследование инцидента (например, подозрительная активность на кассе) занимает 2–3 дня.

3. **Кадровый голод**
   Попытки нанять аналитика уровня L1 с опытом работы в ритейле или знанием специфики кассового ПО не увенчались успехом в течение 4 месяцев. Зарплатные ожидания (от 180 тыс. руб. на руки) превышают утвержденный бюджет.

Бюджетирование и расчет стоимости владения

Совет директоров, учитывая высокие риски простоев торговых точек, выделил бюджет на развитие системы мониторинга инцидентов. Рассматриваются два сценария.

Сценарий А: Создание собственного центра мониторинга
Расчет затрат на 1 год (в рублях):

Категория затрат	Статья	Сумма (руб)	Примечание
CapEx (Капитальные)		**23 500 000 ₽**	
	SIEM-платформа (с учетом лицензий на активы)	9 000 000 ₽	Для 4000 EPS и 4000 активов
	Внедрение SIEM и настройка сбора событий под кассовое ПО	5 500 000 ₽	Сложность: несколько типов кассового ПО
	Настройка сбора логов с 69 магазинов (VPN, агенты)	4 000 000 ₽	Необходима организация защищенных каналов передачи данных

Категория затрат	Статья	Сумма (руб)	Примечание
	Дополнительные инвестиции: доступ к Threat Intelligence и UEBA-системам enterprise-уровня	5 000 000 ₽	Собственная команда не имеет доступа к Threat Intelligence и UEBA-системам enterprise-уровня, которые требуют дополнительных инвестиций
OpEx (Операционные)		**32 499 047 ₽**	**в год**
	ФОТ (Фонд оплаты труда с учетом налогов)	26 399 047 ₽	10 аналитиков (L1-L2) + 1 инженер поддержки инфраструктуры + 1 руководитель SOC / L3. Средняя заработная плата аналитиков 120 000 руб./мес. после вычета налогов, руководителя — 150 000 руб./мес. после вычета налогов.
	Техподдержка ПО (20% от CapEx)	3 700 000 ₽	Ежегодное обновление лицензий SIEM и EDR
	Затраты на формирование отчетности (формирование логов для аудита)	600 000 ₽	Доработки отчетов под требования аудиторов
	Обучение аналитиков	1 500 000 ₽	Специализация по защите ритейла (из расчета 150 000 руб./год на одного специалиста)
	Поиск аналитиков	300 000 ₽	Из расчета 30 000 руб./год на одного специалиста
ИТОГО за 1 год		**55 999 047 ₽**	

Риски сценария А:

1. **Запуск**
   Оптимистичный минимальный срок запуска полноценного мониторинга всех 69 магазинов 10-12 месяцев. Все это время магазины остаются без централизованного контроля.

2. **Кадровая проблема**
   Обеспечить круглосуточную работу (24/7) штатом аналитиков из 8 человек невозможно — физически требуется минимум 10-12 человек для работы в комфортном режиме. Увеличение ФОТ практически неизбежно.

3. **Текучка**
   Аналитики L1, работающие только с инфраструктурой одной компании, быстро выгорают из-за отсутствия разнообразия задач и карьерного роста. Рынок перегрет, удержание специалистов требует постоянного пересмотра зарплат.

Сценарий Б: Коммерческий центр мониторинга «SOC» (аутсорсинг мониторинга)
Расчет затрат на 1 год (в рублях):

Услуга	Стоимость (руб)	Комментарий
Лицензии MSSP (SIEM, EDR)	8 500 000 ₽	Стоимость в год
Мониторинг до 4000 активов (включая кассы, серверы, сетевое оборудование)	7 800 000 ₽	Круглосуточный мониторинг 24/7, аналитика L1-L2 (1 год)
Услуги ЦОД (центра обработки данных)	2 400 000 ₽	Сервер + СХД (система хранения данных)
Услуги расследования инцидентов	2 900 000 ₽	5 обращений в год
Расширенная аналитика (UEBA, Threat Intelligence)	3 500 000 ₽	Поведенческий анализ аномалий на кассах и в офисе
Интеграция и поддержка агентов сбора событий под кассовое ПО	2 000 000 ₽	Настройка сбора событий со специфического ритейл-оборудования
ИТОГО	**27 100 000 ₽**	**в год**

Ключевые параметры сценария Б:

1. **Скорость запуска**
   21–30 дней до начала полноценного мониторинга (за счет готовой инфраструктуры провайдера).
2. **Фиксированная стоимость**
   Отсутствие незапланированных капитальных затрат.
3. **Доступ к экспертизе**
   Коммерческий центр мониторинга имеет опыт работы с ритейл-клиентами, что означает готовые детекторы для атак на POS-терминалы, кассовое ПО и процессинговые системы.
4. **Соглашение об уровне обслуживания**
   Время обнаружения инцидента меньше 15 минут. Время реагирования меньше 30 минут. Ложные срабатывания меньше 5%.

Детализация специфических требований ритейлера

Для точного расчета стоимости работы центра мониторинга (своего или коммерческого) в торговой сети «Атлет-супер» были определены следующие отраслевые требования:

Пункт 1 Объекты мониторинга с отраслевой спецификой

Тип актива	Особенности мониторинга	Количество
POS-терминалы (кассы)	Контроль целостности ПО, мониторинг несанкционированного доступа к платежным данным, логи фискальных операций	330
Платежный шлюз	Мониторинг попыток компрометации транзакций, логи доступа к записям о действиях пользователей	2 узла
Серверы системы лояльности	Контроль доступа к ПДн клиентов, логи изменений	4 сервера
Торговые точки	VPN-соединения, сетевое оборудование, отсутствие локального ИТ-персонала	69 точек

Пункт 2 Требования к команде (для сценария «свой центр мониторинга»)

Для обеспечения мониторинга 24/7 с учетом распределенной инфраструктуры минимальная численность команды центра мониторинга для «Атлет-супер» составляет:

Роль	Количество	Функции	ФОТ (год, с налогами)
L1-аналитики (сменный график)	6	Первичный анализ алертов, эскалация, мониторинг касс	12 930 206 ₽
L2-аналитики (расследование)	4	Расследование инцидентов, настройка корреляций, взаимодействие с магазинами	8 620 014 ₽
Инженер SIEM / инфраструктуры	1	Поддержка платформы, обновление парсеров (особенно для касс)	2 155 034 ₽
Руководитель SOC / L3	1	Threat Hunting, взаимодействие с аудиторами PCI DSS, развитие	2 693 793 ₽
ИТОГО	**10**		**26 399 047 ₽**

Пункт 3 Требования к технологиям

1. **Центр мониторинга должен обеспечивать выполнение требований:** тестирование на проникновение, план реагирования на инциденты.
2. **Интеграция с кассовым ПО:** необходима поддержка парсеров для нестандартных форматов логов кассовых систем (например, «Штрих-М», «Атол», EVOTOR).
3. **Работа с удаленными точками:** возможность мониторинга магазинов, где интернет-канал может быть нестабильным (буферизация логов на месте).

Расчет экономической эффективности для ритейлера

Используя методологию оценки предотвращенного ущерба, рассчитаем эффективность для торговой сети «Атлет-супер». Для ритейла характерны специфические риски.

Пункт 1 Потенциальные угрозы и ущерб

Тип актива	Сценарий без SOC	Расчет ущерба
Программа-шифровальщик	Шифрование кассового сервера и 30% касс в пик торговли (пятница, вечер). Простой 2 торговых дня.	*Потеря выручки* = $\frac{6\ 750\ 000\ руб.}{365\ дней * 2\ день}$ **37 000 000 руб.**
Утечка данных программы лояльности	Утечка ПДн 500 000 клиентов. Первичный инцидент (фиксированные штрафы)	Штрафы: статья 13.11 Кодекса РФ об административных правонарушениях с изменениями от 30.05.2025 (более 100 000 записей) **10 000 000 руб.**
Судебные издержки от исков	На основе практики РФ иски предъявляют 0,1–0,5% от числа пострадавших, а размер компенсации составляет 10–15 тыс. рублей на человека	*500 000 человек * 0,1% * 10 000 руб* **5 000 000 руб.**
Репутационные потери	Оценочные потери от оттока клиентов и снижения продаж на основании экспертной оценки составляют в среднем 1,5% от совокупной годовой выручки компании.	*6 750 000 000 руб.* * 1,5%* **101 250 000 руб.**
Затраты на восстановление	Дополнительные затраты на рекламу при утечке данных.	**6 075 000 руб.**
	Восстановление информации (работа штатных или привлеченных специалистов по восстановлению данных)	**1 800 000 руб.**

Тип актива	Сценарий без SOC	Расчет ущерба
Итого ущерб в случае атаки и потери информации		**161 125 000 руб.**
Итого ущерб в случае атаки и потери информации с учетом вероятности инцидента	Вероятность инцидента 30%	**48 337 500 руб.**

При расчете потенциального ущерба не учтено:

1. Повторный инцидент, который влечет за собой оборотные штрафы в размере от 1–3% от выручки (67 500 000–202 500 000 руб.)
2. Выкуп информации — не менее 6 000 000 руб.
3. Штрафы за неуведомление Роскомнадзора — 1 000 000–3 000 000 руб.
4. Фишинговые атаки на бухгалтерию и прямой перевод средств.

Пункт 2 Сводный расчет эффективности (3 года)

Показатель	Собственный центр мониторинга	Коммерческий центр мониторинга
Затраты 1-й год	55 999 047 руб.	27 100 000 руб.
Затраты 2-й год	32 499 047 руб.	27 100 000 руб.
Затраты 3-й год	32 499 047 руб.	27 100 000 руб.
Итого за 3 года	**120 997 141 руб.**	**81 300 000 руб.**
Экономия при выборе коммерческого SOC		**39 697 141 руб.**

Предотвращенный ущерб за 3 года (консервативная оценка):

48 337 500 * 3 = 145 012 500 руб.

(что полностью покрывает разницу в стоимости между двумя подходами за 3 года)

Заключение

Для торговой сети «Атлет-супер» как представителя крупного ритейл-бизнеса с выручкой 6,75 млрд рублей, распределенной инфраструктурой из 69 магазинов и высокими требованиями к защите платежных данных экономическая и операционная целесообразность склоняется в пользу коммерческого центра мониторинга.

Обоснование:

1. **Финансовая предсказуемость**
   Коммерческий центр мониторинга предлагает модель с фиксированными годовыми затратами без капитальных вложений, что критически важно для ритейлера с низкой маржинальностью. Собственный центр мониторинга требует единовременных вложений.

2. **Покрытие удаленных точек**
   Коммерческий центр мониторинга имеет опыт работы с распределенными объектами (филиальная сеть, магазины) и готовую методологию мониторинга кассового оборудования, что сокращает время настройки с 12 месяцев до 1 месяца.

3. **Кадровая стабильность**
   В условиях острого кадрового голода (особенно для специалистов, понимающих специфику ритейла) коммерческий центр мониторинга предоставляет готовую команду из 10+ аналитиков с подтвержденной экспертизой, исключая риски простоя из-за увольнений.

Рекомендация:

Принять стратегию использования коммерческого центра мониторинга с передачей на аутсорсинг функций мониторинга 24/7, Threat Hunting и подготовки отчетности аудиторов. На уровне штатного отдела ИБ сохранить функции управления доступом, архитектурного контроля кассового ПО и взаимодействия с магазинами при инцидентах, требующих физического присутствия.

ЗАКЛЮЧЕНИЕ И ВЫВОДЫ

2022 год следует рассматривать как отправную точку нового цикла утечек данных в России, когда произошёл кратный рост числа инцидентов, усложнение моделей компрометации и качественная трансформация профиля угроз. При этом хактивистская активность сформировала «шумовой фон», затруднявший своевременное выявление и интерпретацию атак.

Период 2023 – первой половины 2024 года стал переходной фазой: при относительной стабилизации числа инцидентов существенно вырос масштаб последствий и глубина компрометации. К 2025 году сформировался устойчивый ландшафт утечек, в котором атаки реализуются по многоэтапной модели, а публикация данных сместилась в открытые цифровые каналы, прежде всего мессенджеры. Одновременно социальная инженерия, мошенничество и вымогательство приобрели массовый и системный характер.

Отраслевой анализ показывает нелинейную структуру риска, развивавшуюся по двум траекториям — частоте инцидентов и масштабу компрометации. Это объясняет смену отраслевых лидеров: по количеству утечек устойчиво лидирует торговля, тогда как государственный сектор демонстрирует максимальный масштаб и чувствительность последствий.

Ключевым уязвимым активом на протяжении всего периода остаются данные, при этом их состав существенно расширился: от персональных данных к корпоративной, технической и инфраструктурной информации. Утечка таких данных влечёт не только регуляторные риски, но и прямые операционные и финансовые потери — от штрафов и простоев до репутационного ущерба и оттока клиентов. Ключевой вывод исследования заключается в том, что предотвращение инцидентов и системное управление рисками утечек экономически эффективнее, чем ликвидация их последствий. При этом выбор модели защиты — собственная служба ИБ или аутсорсинг — определяется зрелостью процессов, доступностью экспертизы и готовностью инвестировать в инфраструктуру, однако в

обоих случаях критичным становится не только уровень защиты, но и её экономическая обоснованность. Для перехода от декларативной оценки угроз к практическому управлению рисками в отчёте предложен экономический калькулятор*. Он позволяет на основе параметров конкретной организации оценить потенциальный ущерб от утечки и сопоставить его со стоимостью различных моделей защиты, обеспечивая количественное обоснование управленческих решений.

Калькулятор рисков от GIS
https://www.gaz-is.ru/risk-calculator

Исследование проведено Аналитическим центром кибербезопасности компании «Газинформсервис» и основано на анализе открытых источников, отраслевой статистики и данных профессионального сообщества.

ИСТОЧНИКИ

1. Infowatch: Аналитический отчет «Россия: утечки информации ограниченного доступа 2023-2024»
2. BI.ZONE: Исследование ландшафта киберугроз в РОссии и странах СНГ
3. CrowdStrike: 2023 Global Threat report
4. F.A.C.C.T.: «Тени не скроются» Расследование атак группировки Shadow
5. Закон №152-ФЗ «О персональных данных»
6. Закон №420-ФЗ ««Об информации, информационных технологиях и о защите информации»
7. КоАП 13.11 «Нарушение законодательства Российской Федерации в области персональных данных»
8. Онлайн-журнал Телеспутник
   telesputnik.ru
9. Сайт IT-компании MaskSafe
   masksafe.ru
10. Информационно-аналитический центр по информационной безопасности Anti-Malware
    www.anti-malware.ru
11. Информационное агентство «Газета.Ру»
    www.gazeta.ru
12. Информационный портал «Крым.Ньюс»
    crimea-news.com
13. Портал «Ваш МедЭксперт» о медицине и фармацевтике
    vademec.ru
14. Международное новостное агентство «Рейтер»
    www.reuters.com

GIS ГАЗИНФОРМ СЕРВИС

Над отчётом работали:

АЦКБ

ARKTIS

Л.А. Виткова

Начальник Аналитического центра кибербезопасности (АЦКБ)

Постановка задачи исследования, разработка методологического подхода, сбор и системный анализ информации, подготовка и написание аналитических разделов отчёта, формирование выводов и итоговых обобщений, редактирование.

И.Н. Дмитриева

Лаборатория исследований кибербезопасности, АЦКБ

Сбор и систематизация информации, аналитика, системный анализ.

В.В. Пучков

Лаборатория развития и продвижения компетенций кибербезопасности, АЦКБ

Разработка практического кейса, участие в создании модели экономической оценки и сравнительного анализа эффективности стратегий защиты.

А.В. Максимов

Лаборатория исследований кибербезопасности, АЦКБ

Систематизация, аналитика.

Е.Д. Едемская

Лаборатория исследований кибербезопасности, АЦКБ

Верификация данных, аналитика, системный анализ.

И.А. Пучкова

Независимый экономист, консультант

Разработка экономической модели, создание калькулятора оценки рисков, подготовка раздела об экономической эффективности, формирование системы показателей и критериев для оценки ущерба и эффективности мер защиты.

Д.А. Лебедева

Лаборатория исследований кибербезопасности, АЦКБ

Сбор и систематизация информации, аналитика.

Е.В. Можелянская

Лаборатория исследований кибербезопасности, АЦКБ

Дизайн, вёрстка, коррекция.

А.А. Тасюк

Лаборатория исследований кибербезопасности, АЦКБ

Систематизация, редактирование, аналитика.

ARKTIS (Advanced Recon & Knowledge for Threat Intelligence Systems)

TI-команда «Газинформсервис»

Сбор и систематизация информации.