



«ДОРОГИЕ УТЕЧКИ» КАК РЕАГИРОВАТЬ НА УТЕЧКИ ИНФОРМАЦИИ РАЗНЫХ ВИДОВ

КИБЕРАТАКИ – ЭТО РЫНОК

① Реализация кибератаки требует ресурса, а также влечет риски. Сфера кибератак подвержена влиянию рыночных механизмов, а в современной реальности – политическим факторам

КЛЮЧЕВЫЕ ТРЕНДЫ:

ЦЕНА МОЛЧАНИЯ

1

Угроза опубликования данных становится одним из главных инструментов вымогательства

МЕНЬШЕ, НО ГЛУБЖЕ

2

Рыночная стоимость массовых утечек падает из-за медленного устаревания данных. В фокусе злоумышленников – редкие и адресные данные

ЧЕЛОВЕК – САМОЕ УЯЗВИМОЕ ЗВЕНО

3

Развитие систем информационной безопасности приводит к увеличению числа атак через социальную инженерию

ХАРАКТЕРНЫЕ ОТЛИЧИЯ

- высокие инвестиции в НИОКР в сравнении с другими отраслями – ценные информационные активы;
- высокая автономия каждого сотрудника;
- доступ к нескольким централизованным информационным системам;
- частые случаи целевых атак на специалистов (врачей, научных сотрудников)

ТОЛЬКО ЦИФРЫ

- в 2025 году в **два раза** увеличилось количество утечек коммерческой тайны в сфере здравоохранения;
- **21,6% инцидентов** по вине внутреннего нарушителя – самый высокий показатель среди всех отраслей;
- **66+ млн. записей** о персональных данных и медицинской тайне утекло за 3 года в России;

ЦЕННЫЕ АКТИВЫ:

Специальные категории ПДн

Крайне высокая ценность для мошеннических атак на субъектов

Статистика и исследования

Коммерчески-ценные стратегические информационные активы

Базы поставщиков и клиентов

Конкурентное преимущество для развития собственного бизнеса

ТИПЫ ДАННЫХ В УТЕЧКАХ (2025)



#1 ПДн УТЕКАЮТ ЧАЩЕ ВСЕГО

67% скомпрометированных персональных данных – это аутентификационная информация, которая может использоваться для получения доступа к системам

#2 ТОРГОВЛЯ – ЛИДЕР ПО ЧИСЛУ ИНЦИДЕНТОВ

25% утечек произошло в торговом секторе. По 9% - в сфере туризма, и в сфере телекоммуникаций, 7,3% - образование, 5,4% - промышленность, 4,6% - **медицинский сектор**

#3 В 8 ИЗ 10 СЛУЧАЕВ ПРИЧИНА - КИБЕРАТАКА

Однако для реализации кибератаки часто используются данные сотрудников, а также действия внутренних нарушителей

«ДОРОГИЕ» УТЕЧКИ

УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ



Структура убытков:

- административный штраф (до 20 млн. руб.);
- репутационные риски и отток потребителей (СМИ освещают кибератаки и утечки, как острые инфоповоды);
- расходы на сопровождение административного дела и приведение процессов в соответствие;
- расходы на повышение безопасности

ВНУТРЕННИЕ НАРУШЕНИЯ



Структура убытков:

- непредсказуемые сценарии развития угроз: от копирования данных до уничтожения инфраструктуры;
- усиление конкурентов и потеря преимуществ;
- нарушения внутри коллектива, остановка бизнес-процессов и простой;
- все, что актуально для утечки ПДн

КИБЕРАТАКИ

/ 70%

реализованные из иностранных юрисдикций формируют крупные утечки

ОШИБКИ

/ 30%

работника в ходе исполнения обязанностей формирует пул мелких утечек по ч. 1 ст. 13.11



Обращение в МВД по ст. 272 УК РФ не исключает вины оператора, но является важным действием для защиты интересов

Выводы из судебной практики:

- Оператор отвечает за действия своих работников: совершенные без умысла (А51-17988/2025), случайные (МС города Москвы №5-791/413/2026) и намеренные (А40-199062/2025)
- После передачи дел в подсудность мировых судов доказать отсутствие вины оператора сложно, а суммы штрафов не уменьшаются ниже минимального размера (исключение – микропредприятия)
- Отвечают не только операторы, но и руководители (МС города Москвы №05-0749/365/2026 – 05-/0752/2026, А33-36164/2025)
- Высокая активность Прокуратуры РФ – в отличие от РКН у нее нет моратория, административного регламента, а в сферу надзора попадает соблюдение всех требований законодательства

РАССМАТРИВАЮТ ЛИ СУДЫ ТЕХНИЧЕСКУЮ СТОРОНУ?

А19-25808/2025

Суд подробно изучил материалы экспертизы и выделил конкретные недостатки, особенно отметив неверную конфигурацию системы, позволяющую **повышать права доступа без ввода пароля** и использование учётки уволенного в 2022

А40-263206/2025

Хотя суд пришел к выводу о недоказанности вины оператора в утечке, подробное исследование мер защиты информации отсутствует



Выполнение требований к безопасности может являться доказательством в совокупности с материалами экспертизы. При этом такие доказательства должны быть надлежащим образом оформлены, к примеру, актом оценки уровня защищенности ИСПДн в порядке п. 6 Приказа ФСТЭК №21



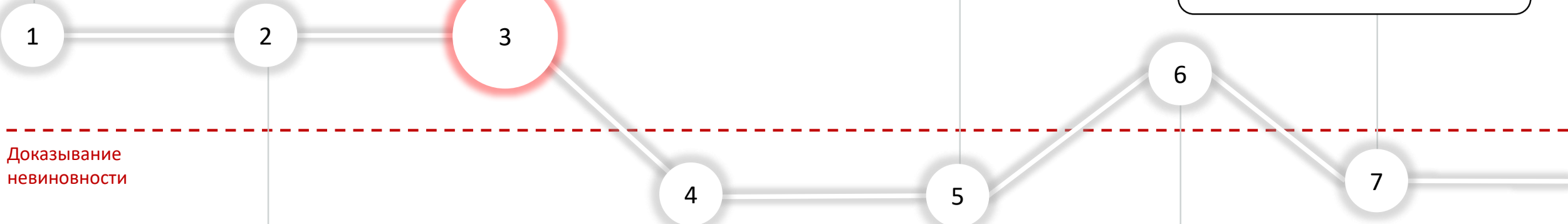
ДИНАМИКА СПОРОВ ПО УТЕЧКАМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Спортмастер и АльфаСтрахование 2023
Сделали все возможное? Нет состава правонарушения

Введены штрафы, подсудность АС

Суды применяют предупреждения,
штрафы минимальны, но вина признается повсеместно

Подсудность СОЮ
Мировые суды строго оценивают действия оператора и применяют штрафы согласно КоАП, предупреждений почти нет



Доказывание
невиновности

Банки доказывают разумность мер, 2024
Отсутствие ИБ приводит к выплатам вкладчику

Факт утечки означает бездействие
Характерный пример: дело №А55-36038/2025

Дело РЖД – вывод о вине преждевременный, надо расследовать атаку и доказать вину
Дело «Орион Телеком» - проведена экспертиза

УВЕДОМЛЕНИЕ – КОГДА НАЧИНАЕТСЯ ОТСЧЕТ?

ВХОДЯЩЕЕ СООБЩЕНИЕ

Например, запрос РКН, Прокуратуры и Субъекта. Если ответить РКН уведомлением – это не будет нарушением по ч. 11 КоАП (*Постановление ВС РФ от 21.01.2026 №5-АД25-119-К2*)

ВНУТРЕННЕЕ СООБЩЕНИЕ

«24 часа» часто привязаны к рабочим часам безопасности. Тем не менее, события в DLP/SOC/SIEM и иных системах являются объективными.

«72 часа» - строго с момента, обозначенном в первом уведомлении, но таких уведомлений может быть несколько

На следующий день

За редким исключением (дело №А40-341776/25) уведомление подается на следующий день

Пара часов – это погрешность

В деле А56-4733/2026 уведомление подали через 26,5 часов, РКН это проигнорировал

Второе – строго в течение 72 часов

Если первое подано в среду-четверг, придется подать второе в выходные (А474-10378/2025)

УВЕДОМЛЕНИЕ – ЕСЛИ «НЕ УСПЕВАЕМ!»



- ① Цель второго уведомления – дать РКН материалы для реагирования. «Второе уведомление» на самом деле может быть серией из нескольких уведомлений.

A74-10378/2025



По истечении 72 часов оператор уведомил РКН о том, что расследование еще идет и на этот процесс нужно больше времени.

Новые уведомления РКН содержали информацию о выявленных в сети утечках. В старых решениях* такая информация была расценена, как доказательство добросовестного поведения оператора

*

Ждем информацию от подрядчика

Обязанность каждого оператора является индивидуальной и не зависит от действий третьих лиц. Сроки для каждого свои

Нашли новые обстоятельства

информацию в сети, установили причину – лучше сообщить

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ – ОСНОВА ДЛЯ ЗАЩИТЫ ИНТЕРЕСОВ ОПЕРАТОРА ВО ВСЕХ СЦЕНАРИЯХ РАЗВИТИЯ СОБЫТИЙ

НАИБОЛЕЕ АКТУАЛЬНЫЕ ДЕЙСТВИЯ:

Остановка инцидента

Немедленное ограничение доступа, сброс пользовательских паролей, сканирование системы

1

Проведение экспертизы

Необходимо и для сопровождения обращения в МВД, и для позиции в деле об административном правонарушении

2

Подготовка к работе с безопасностью и обращениями субъектов

Необходима для исполнения прав субъектов и предотвращения развития рисков (в частности, жалоб и требований субъектов)

3

Уведомление РКН об утечке персданных - что нужно знать перед направлением:

!

- в текущей практике уведомление оператора является началом для административного расследования;
- данные из уведомления часто переходят в позицию РКН, само уведомление рассматривается, как обязанность оператора (то же дело А40-351064/2025), а не признак добросовестности;
- отсутствие уведомления – гарантия дополнительного штрафа до 3 млн. руб.

ВНУТРЕННИЙ НАРУШИТЕЛЬ

i

Зачастую причина утраты, утечки или уничтожения информации – это не хакер в кофте с капюшоном. Это рядовой менеджер в рубашке, который захотел получить (незаконным способом) бонус к зарплате или отомстить. Такой менеджер опаснее хакера – он знает про внутренние конфликты, слабые места в защите. Он знает про папки, в которых хранится информации и то, какая информация по-настоящему представляет ценность. Или угрозу

10%



нарушений происходят исключительно по вине внутреннего нарушителя

86%



нарушений носят умышленный характер и совершаются намеренно

Увольнение в топе рисков



При увольнении работники стараются взять от организации максимум ресурсов

Месть становится мотивацией к нарушению



В уголовной практике все чаще встречаются преступления, совершенные против работодателя из мести. Их цель — причинение максимального вреда

Человек — наименее защищенный элемент любой системы



Реализовать атаку через внутреннего нарушителя проще, чем через уязвимость в системе. Существует практика атак через непосредственное подключение к системам

СЦЕНАРИИ И ПОСЛЕДСТВИЯ В ПРАКТИКЕ

УХОД К КОНКУРЕНТУ С ЦЕННЫМИ МАТЕРИАЛАМИ



Дело №10-22639/2025



Руководитель скопировал план проекта на незарегистрированную флешку перед увольнением. DLP зафиксировал копирование.

РЕЗУЛЬТАТ

Суд признал вину по ст. 183 УК РФ (утечка данных), но освободил от наказания из-за **истечения срока давности** (ст. 272 УК РФ).

РАБОТА НА КОНКУРЕНТА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИИ РАБОТОДАТЕЛЯ



Дело №88-3378/2024



Начальник отдела логистики передавал данные конкурентам через систему. После обнаружения – уволен, работодатель обратился в МВД.

РЕЗУЛЬТАТ

В трудовом споре увольнение признано обоснованным. Работодатель признан потерпевшим по уголовному делу.

ЗАМЕЧАНИЯ И ВЫГОВОРЫ ЗА НАРУШЕНИЕ МЕР ИБ

Хотя утечки и не случилось, сами действия работника могут быть признаны **нарушением трудовых обязанностей**

- ✓ **ИБ не спит** – привлечение кадровой службы может показать нарушителю, что его действия не просто выявляются и блокируются, но и могут встретить сопротивление **в правовом поле**
- ✓ Нарушение формирует почву для применения п. 5 ст. 81 ТК РФ – **увольнения за неоднократное несоблюдение обязанностей**

Использование ответственности возможно при наличии грамотно построенной системы ЛНА



Апелляционное определение СПбГС от 31.01.2025 №33-2515/2025

Суд признал правоммерным вынесения **замечания** за **фотографирование** экрана рабочего компьютера на личный телефон, даже с учетом рабочей цели



Апелляционное определение СПбГС от 08.12.2025 №33-23711/2025

Выговор за то, что работник **забыл заблокировать** компьютер, уйдя в отпуск, был признан правоммерным даже с учетом автоматической блокировки экрана



Определение 6-го КСОЮ от 05.03.2026 №88-3939/2026

Суд признал **замечание** о недопустимости **хранения паролей на «рабочем столе»** компьютера, хотя работнику и не рассказали о наличии спец. ПО для хранения паролей.

The background features two large, overlapping, curved green shapes that sweep across the frame from the corners towards the center, creating a dynamic, modern aesthetic.

УГОЛОВНАЯ ПРАКТИКА

В СФЕРЕ УГРОЗ ВНУТРЕННЕГО НАРУШИТЕЛЯ

272.1 УК РФ

Ответственность за неправомерное обращение персональных данных

272, 274 УК РФ

Неправомерный доступ к компьютерной информации, нарушение правил обработки информации

274.1 УК РФ

Неправомерное воздействие на критическую информационную инфраструктуру

Общий обзор:

- В суды попадают дела с разной мотивацией нарушителей. Зачастую это корысть (прямая и косвенная), реже – месть.
- В некоторых случаях нарушитель может быть обнаружен вне информационного периметра компании, например, при предложении услуг на специализированных площадках (Приговор Головинского районного суда города Москвы от 04.08.2026 по делу N 1-383/2026).
- В исключительных случаях уголовные дела открываются против руководства или специалистов ИБ за халатность или нарушение инструкций.
- Основа практики – прямой умысел на совершение преступных действий.

272.1 УК РФ

Ответственность за неправомерное обращение персональных данных

272, 274 УК РФ

Неправомерный доступ к компьютерной информации, нарушение правил обработки информации

274.1 УК РФ

Неправомерное воздействие на критическую информационную инфраструктуру

Особенности:

- наступательная безопасность – поиск утечек и слитых баз является законным в случае, если целью является изучение утечки, а не обработка использованных данных (А40-201075/2025);
- 80% фигурантов дел - работники, которые торгуют данными, оставшиеся 20% - «специалисты» по пробиву и организаторы профильных сервисов;

Приговор Рудничного районного суда города Кемерово от 29.06.2026 по делу N 1-179/2026



Работник МФО в составе ОПГ копировал паспорта заемщиков и передавал их подельникам для создания фальшивых личностей. 4 года условно

272.1 УК РФ

Ответственность за неправомерное обращение персональных данных

272, 274 УК РФ

Неправомерный доступ к компьютерной информации, нарушение правил обработки информации

274.1 УК РФ

Неправомерное воздействие на критическую информационную инфраструктуру

Особенности 272 УК РФ:

- использование рабочего доступа для совершения противоправных действий является неправомерным воздействием – парируем основную ссылку работников;
- основной фигурант – сотрудник, использующий корпоративный доступ

Особенности 274 УК РФ:

- фигурант – человек, которому поставлена прямая обязанность выполнять **инструкцию** при работе с системой;

*Обвинение считает, что вина господина Ройтмана состоит в том, что он **в нарушение инструкции** хранил логин и пароль от входа в систему бронирования билетов в персональном компьютере... Александр Кальчук «не выполнил комплекс мер по защите информации», что прямо входило в его должностные обязанности*

Сирена Трэвел,
репортаж
Коммерсантъ

272.1 УК РФ

Ответственность за неправомерное обращение персональных данных

272, 274 УК РФ

Неправомерный доступ к компьютерной информации, нарушение правил обработки информации

274.1 УК РФ

Неправомерное воздействие на критическую информационную инфраструктуру

Особенности:

- большое число дел объясняется привлечением работников, которые вносили в систему недостоверные данные или наоборот, выгружали их из нее;
- уголовные дела для эксплуатантов систем ИБ являются исключением и связаны с бездействием или крайней небрежностью (например, установкой несертифицированного антивируса).

«Неправомерное воздействие» - это изменение данных системы (в том числе добавление в нее подложных данных), поскольку такие действия нарушают целостность системы

Определение ВС РФ от 15 апреля 2026 года № 9-УД26-2-К

Определение ВС РФ от 5 марта 2026 года № 12-УД25-2К6

ЛИЧНОЕ ОБОГАЩЕНИЕ: ПРЯМОЕ И КОСВЕННОЕ

РАБОТНИК ЗАЧИСЛИЛ СЕБЕ ДЕНЬГИ



Определение БКСОЮ от 01.07.2026 N 77-1892/2026

Работник-программист банка использовал технические навыки и изменил данные в кредитной системе банка, начислив на свой счет более 31 миллиона рублей

В ходе внутренней проверки Работник понял, что «на него выйдут», и самостоятельно сообщил в полицию о преступлении, вернув 15 миллионов добровольно

Итог: компенсация 16 млн. банку, и 2 года колонии общего режима

СОТРУДНИЦА ХОТЕЛА ВЫПОЛНИТЬ ПЛАН



Приговор Славянского ГС Краснодарского края от 23.07.2025 по делу N 1-155/2025

Сотрудница попросила подчиненную предоставить ей доступ к системе банка и через него оформила ЭЦП и вклад от имени клиента, чтобы закрыть план по открытию счетов

Суд усмотрел в этом корыстную заинтересованность в форме желания получить премию

① Уничтожение информации (и информационной инфраструктуры) из мести – это состав ст. 272 УК РФ.

Кассационное постановление 3 КСОЮ от 23.04.2026 №77-667/2026



После увольнения работник вошел в свою учетную запись (она не была заблокирована) и удалил виртуальные машины работодателя. Была уничтожена бухгалтерия, полностью остановлены административные процессы и оказание образовательных услуг.

Суд признал вину работника в преступлении, предусмотренном ст. 272 УК РФ, удовлетворил гражданский иск работодателя о компенсации вреда, причиненного преступлением

Кассационное определение 2КСОЮ от 09.10.2025 №77-2714/2025



Уволенный директор уничтожил данные в CRM-системе, что привело к нарушению работы коммерческого департамента на протяжении 7 месяцев. Работодатель оценил ущерб в 5.2 миллиона рублей – 1.1 млн. на восстановление инфраструктуры, 4.1 млн. – заработная плата сотрудникам за период простоя.

Суд признал вину работника и обязал его компенсировать причиненный ущерб в полном объеме

DLP - СИСТЕМЫ

«Остановка» утечек и сбор доказательств – основа и для борьбы с нарушениями, и для их профилактики

РАМ - СИСТЕМЫ

Жесткое ограничение доступа к системам для подрядчиков и администраторов – исключение самого частого сценария атаки

UBA

User Behavior Analytics – позволяют предсказывать поведение пользователей исходя из аномалий

Юридический аспект:

- Определение и защита информационных активов (коммерческая тайна, служебное произведение, интеллектуальная собственность);
- Управление обязанностями, правами и компенсационными механизмами.

Организационный аспект:

- Работа с атмосферой в коллективе, построение культуры взаимного уважения;
- Предотвращение конфликтов внутри команд;
- Методическая и учебная работа в вопросах цифровой гигиены и обработки персональных данных;

ЗАЩИТА ИНФОРМАЦИОННЫХ АКТИВОВ – ЭТО МНОГОСОСТАВНАЯ **СТРАТЕГИЧЕСКАЯ** ЗАДАЧА, ВКЛЮЧАЮЩАЯ РАЗНЫЕ ЭТАПЫ И КОМПЕТЕНЦИИ

Аудит информационных активов

1

Позволяет выявить ценные категории и группы информации, определить тактику их защиты и использования в бизнесе.

Позволяет не только защитить активы, но и создать конкурентные преимущества

Внедрение средств, систем и процессов защиты

2

Включает три аспекта. **Технический** аспект обеспечивает устойчивость к атакам. **Организационный** аспект минимизирует ошибки и выстраивает операционную надежность и подконтрольность. **Юридический** - позволяет создать основу для компенсации убытков и ответственности нарушителей

Реагирование на инциденты безопасности

3

Позволяет минимизировать ущерб и определить виновных, снизить санкции регуляторов и управлять репутацией



Илья Башкиров

Руководитель группы консалтинга

ilia.bashkirov@infowatch.com

+7(915)390-11-30