

Как дело РЖД демонстрирует новый подход судов к утечкам данных

Актуальность материала: **21.02.2026**

Девятый арбитражный апелляционный суд 16 февраля отменил решение о привлечении ОАО «РЖД» к ответственности за утечку персональных данных, учтя факт внешней кибератаки и возбужденное уголовное дело. Это может стать началом нового тренда, [считает Алексей Мунтян](#): по его мнению, суды начинают оценивать реальные меры киберзащиты, отходя от практики формальных наказаний бизнеса за сам факт утечки данных.

Долгое время в российской судебной практике превалировал подход, который можно охарактеризовать как объективное вменение. Если персональные данные оказались скомпрометированы, компания признавалась виновной по умолчанию. Надзорному органу было достаточно зафиксировать факт утечки, чтобы суд назначил административное наказание, не погружаясь в детали того, насколько эффективно и добросовестно была выстроена защита корпоративной ИТ-инфраструктуры.

В начале 2025 года Роскомнадзор обнаружил в открытом доступе базу данных объемом более 17 млн строк, содержащую персональные сведения сотрудников ОАО «РЖД», включая их ФИО, должности и электронные почты. Утечка была опубликована в закрытом Telegram-канале хакерской группировки. По итогам внеплановой проверки надзорный орган обратился в суд, который привлек РЖД к административной ответственности по ч.1 ст.13.11 КоАП РФ, назначив компании штраф в размере 150 000 рублей за нарушение законодательства в области персональных данных.

Однако РЖД не согласились со штрафом и обратились в апелляционную инстанцию. Их ключевой аргумент состоял в том, что утечка произошла не из-за халатности компании, а в результате целенаправленной кибератаки. И 27 января 2026 года было оглашено [постановление Девятого арбитражного апелляционного суда](#), которое демонстрирует иной, более взвешенный подход к оценке вины бизнеса в утечках.

От констатации факта к оценке мер защиты

Ключевой вывод суда заключается в напоминании о базовых принципах права, согласно которым юридическое лицо признается виновным только в том случае, если у него была возможность соблюсти правила, но оно не приняло всех зависящих от него мер (ч.2 ст.2.1 КоАП РФ).

В случае с РЖД суд указал, что выводы Роскомнадзора о единоличной вине компании преждевременны. В материалах административного дела отсутствовали доказательства того, что компания не соблюдала требования законодательства к защите персональных данных. Зато присутствовали данные о неправомерном доступе неустановленного лица, обладавшего специальными познаниями и использовавшего программы для обхода защиты серверной инфраструктуры РЖД.

Суды постепенно повышают стандарты доказывания для обеих сторон конфликта. Это

подтверждается и другими разбирательствами (например, находящиеся на рассмотрении суда дела ГК «Орион Телеком» — №А74-10378/2025 и №А33-29369/2025). Теперь от уполномоченных органов требуют конкретики: какие именно меры защиты должна была, но не предприняла компания, в какой момент правонарушение считается окончанным и как технически был осуществлен доступ. В свою очередь, от бизнеса суды ждут документального подтверждения как соблюдения всех предусмотренных законом мер защиты, так и в целом добросовестного и осмотрительного поведения в отношении обеспечения безопасности персональных данных.

Уголовное дело как фактор судебной оценки

Особого внимания заслуживает принятая судом апелляция РЖД к возбужденному уголовному делу по ч.1 ст.272.1 УК РФ (незаконная обработка компьютерной информации, содержащей персональные данные). Суд также учел общеизвестный факт значительного роста с 2022 года количества хакерских атак на российские компании и организации на фоне нынешней напряженной геополитической обстановки.

Логика суда, в целом, ясна: если ИТ-инфраструктура была взломана в результате целенаправленной профессиональной кибератаки, возлагать всю ответственность исключительно на оператора персональных данных несправедливо. Однако этот аргумент таит в себе и правовую неопределенность.

Подача заявления о преступлении и сам факт возбуждения дела — это не итоговый приговор, устанавливающий все юридически значимые обстоятельства утечки. Уголовное расследование киберинцидентов может длиться годами, дело может быть преквалифицировано или вовсе прекращено. Возникает закономерный вопрос: означает ли логика суда, что административное производство должно быть поставлено на паузу до завершения уголовного? И что произойдет, если виновные так и не будут найдены? Пока правоприменительная практика не дает однозначных ответов на эти вопросы.

Практические выводы для бизнеса

Важно оговориться, что дело РЖД формально не создает прецедента. Кроме того, спор рассматривался в арбитражном суде, тогда как с 1 января 2026 года дела по утечкам и другим нарушениям в области персональных данных возвращаются в ведение судов общей юрисдикции. Пока неясно, воспримут ли они арбитражную практику, к тому же решение апелляции может быть оспорено Роскомнадзором в вышестоящих инстанциях.

Тем не менее, для бизнеса это дело лишний раз показывает актуальность понимания, что утечка — это не «если», а «когда». Кроме того, уже сейчас можно сформулировать ряд практических выводов для бизнеса:

1. Документирование превентивных мер. Компаниям необходимо иметь четкую, актуальную и документально подтвержденную историю выполнения мероприятий и внедрения мер защиты персональных данных. В случае инцидента именно эти документы станут главным аргументом, подтверждающим, что бизнес принял все зависящие от него меры для недопущения утечки.
2. Проактивная позиция при инцидентах. Замалчивание утечки — худшая стратегия. подача заявления в правоохранительные органы, информирование уполномоченных

органов (Роскомнадзор, НКЦКИ) и активное содействие расследованию инцидента становятся необходимыми элементами юридической защиты компании и её партнеров.

3. Обоснование мастерства кибератаки. В суде потребуются доказывать не просто факт взлома систем компании, а уровень его сложности и профессионализма: использование злоумышленниками специфического ПО, обход существующих (и работающих) контуров безопасности, изощрённость техник кибератаки.

Судебная практика показывает все большую погруженность судов в суть и обстоятельства киберинцидентов. Для бизнеса это означает, что инвестиции в реальную, а не бумажную информационную безопасность теперь могут не только предотвратить утечку (или хотя бы уменьшить ее масштаб и последствия), но и защитить от разорительных штрафов, ведь наличие реальных мер защиты доказывает меньшую степень вины, а значит, гарантирует соразмерное и более мягкое наказание.

[системы](#), [инциденты](#), [инфобез](#), [уведомление](#), [надзор](#), [ответственность](#)

From:

<https://wiki.privacy-advocates.ru/> - **Privacy Advocates | Альманах**

Permanent link:

https://wiki.privacy-advocates.ru/rzhd_novyj_podxod_k_utechkam

Last update: **2026/03/01 18:09**

