Утечка баз данных и коммерческой тайны: как привлечь бывшего сотрудника к ответственности и взыскать убытки

Пушков Дмитрий Андреевич, юрист «Леганта Групп»

Почему "утечки" превратились в критический риск

Клиентские базы, CRM и исходный код копируются за минуты и уходят через почту, мессенджеры и облака. Для суда решающими остаются режим коммерческой тайны, ограниченный доступ, маркировка и доказанный ущерб, а не сама ценность данных как таковая.

Что признается коммерческой тайной по № 98-ФЗ

Три обязательных признака
Коммерческая тайна должна иметь реальную или потенциальную ценность, быть неизвестной третьим лицам и не находиться в свободном законном доступе. Без совокупности этих признаков режим не работает.

Что обычно охраняют
Под режим КТ обычно подпадают клиентские базы, CRM, условия договоров, исходный код, технологические решения и иные сведения, дающие конкурентное преимущество или позволяющие удерживать рынок.

Что исключено законом
Открытые сведения, данные ЕГРЮЛ и ФНС, а также штатные и учредительные документы не могут считаться коммерческой тайной, даже если компания обозначает их как конфиденциальные.

Режим важнее названия
Термины вроде «секретная информация» или «ДСП» не заменяют установленный по статье 10 Закона № 98-ФЗ режим КТ. Для суда юридически значим именно оформленный режим, а не внутреннее название.

Четыре кита режима коммерческой тайны

Кит режима	Что должно быть оформлено	Зачем это в суде
1. Идентификация информации	Перечень сведений, составляющих КТ, грифы/пометки; основания отнесения	Подтверждает объект и предмет спора: именно «эта» информация — коммерческая тайна
2. Определение круга допущенных	Порядок доступа: перечень должностей/лиц; уровни доступа; журналирование	Показывает осведомленность и возможность контроля: сведения не «утекали сами по себе»
3. Организационно-правовой режим	ЛНА: положение о КТ, инструкции; режим ИТ/документооборота, запреты/обязательства; маркировка носителей	Дает доказательства дисциплинируемости и реальности ограничений, а также выполнения работодателем «разумных мер»
4. Контроль и ответственность	Контроль соблюдения режима; обучение/инструктажи; фиксация нарушений; условия в договорах/подписях	Подкрепляет причинную связь и вину: работник знал режим и нарушил его; база для убытков/взыскания

ФЗ № 98-ФЗ «О коммерческой тайне», ст. 10; судебная практика 2024–2025 годов

Без этих элементов спор о разглашении и о возмещении убытков обычно «рассыпается» уже на стадии оценки доказательств: суды проверяют, была ли информация действительно отнесена к коммерческой тайне, соблюдался ли режим, и подтверждается ли, что работник/контрагент действовал вопреки установленным правилам.

Каждый элемент «закрывает» отдельный процессуальный и фактический риск: (1) что именно является КТ, (2) кому и на каких условиях она доступна, (3) какие меры работодатель реально предпринимал, (4) как подтверждается осведомлённость и нарушение. Отсутствие хотя бы одного «кита» чаще всего приводит к отказу во взыскании убытков и осложняет привлечение к ответственности, включая дисциплинарную меру, поскольку суд оценивает не только поведение лица, но и качество доказательственной базы со стороны бизнеса.

Практика 2023–2025: главные правовые выводы

Личный Telegram больше не «личное пространство»

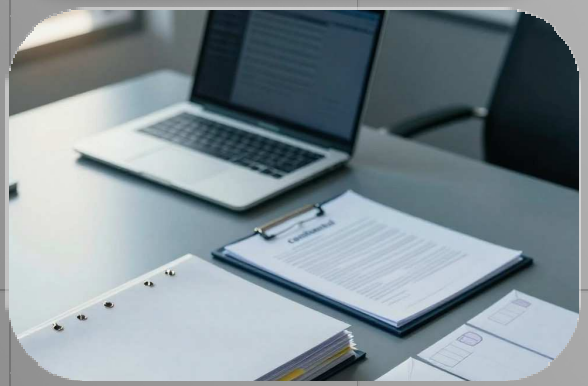
Суды всё чаще рассматривают пересылку рабочих файлов в личный Telegram или облачный сервис как разглашение, если работодатель ввёл режим коммерческой тайны и ограничил доступ. Ключевым становится не намерение сотрудника, а утрата контроля над информацией после копирования на сторонний ресурс.

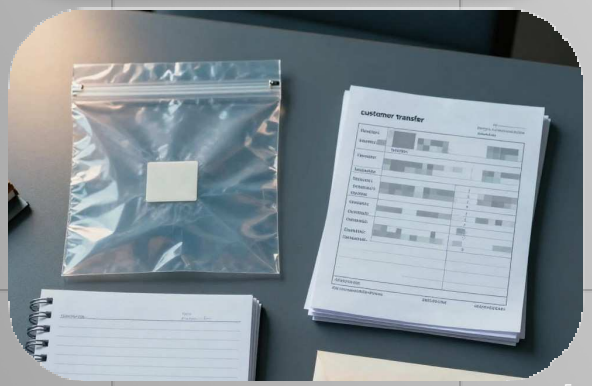
Успех иска начинается с режима, а не с эмоций

В делах о клиентских базах и CRM суд проверяет не только ценность данных, но и наличие маркировки, перечня сведений, допусков и NDA. Если режим КТ оформлен формально или неполно, даже очевидная утечка часто не приводит к взысканию убытков.
Определение Первого кассационного суда общей юрисдикции от 17.04.2023 № 88-12649/2023

Убытки нужно доказывать, а не предполагать

Арбитражная практика 2024–2025 годов показывает: суды отказывают, когда истец пытается связать потерю клиентов лишь с фактом их перехода к конкуренту. Нужна прямая причинная связь, корректный расчёт ущерба и подтверждение того, что именно утечка повлияла на хозяйственный результат.





Три уровня ответственности и логика выбора механизма

1

1) Действующий сотрудник

Цель — уволить нелояльного сотрудника без выходного пособия. Основание — пп. «в» п. 6 ч. 1 ст. 81 ТК РФ. Что нужно: акт служебного расследования, письменное объяснение сотрудника, фиксация факта разглашения. Срок — один месяц со дня обнаружения проступка, если сотрудник уже уволился — ТК РФ здесь бессилен.

2

2) Цель спора — расходы и убытки

Если требуется взыскать расходы или обеспечить компенсацию, выбирают требование о возмещении вреда и убытков. Ключевым становится доказательство связи между нарушением и наступившими последствиями для бизнеса.

3

3) После увольнения — гражданско-правовой путь

Если вы хотите взыскать упущенную выгоду с уже уволившегося сотрудника, нужно идти по пути гражданско-правовой (деликтной) ответственности — через ст. 15 и 1064 ГК РФ, доказывая, что вред причинён умышленным нарушением соглашения о конфиденциальности, которое продолжает действовать и после увольнения.

Уголовная ответственность по ст. 183 УК РФ после реформы 2025 года

1. **Новые санкции**
   С 5 июля 2025 года ч. 3 ст. 183 УК РФ предусматривает лишение свободы на срок от 2 до 5 лет и штраф до 5 млн рублей, а ч. 4 — от 3 до 7 лет и штраф от 1 до 5 млн рублей.
2. **Крупный ущерб**
   Для целей статьи 183 крупный ущерб начинается со суммы свыше 2,5 млн рублей. Это позволяет переводить серьёзные утечки из корпоративного конфликта в уголовно-правовую плоскость.
3. **Практическое значение**
   При сливе клиентской базы, ноу-хау или исходного кода заявление в МВД должно подаваться незамедлительно. Уголовное дело расширяет инструменты поиска и фиксации цифровых следов.
4. **Что важно не упустить**
   Заявление должно быть юридически выверенным: ошибки в формулировках, квалификации и описании ущерба часто приводят к отказу в возбуждении дела и потере времени.

Как привлечь нового работодателя к ответственности

Жалоба в ФАС

Если компания использует чужую КТ в интересах бизнеса, это может квалифицироваться как недобросовестная конкуренция. ФАС вправе выдать предписание и назначить оборотный штраф до 15% выручки.

Иск о нарушении прав

При незаконном использовании базы данных, ноу-хау или программного обеспечения возможен иск о нарушении исключительных прав. В таком случае допустимо требовать компенсацию или убытки в полном объёме.

Солидарное взыскание

Когда вред причинили сотрудник и компания-конкурент, возможно предъявление требований солидарно по статье 1080 ГК РФ. Это повышает шансы на реальное исполнение и взыскание.

Пошаговый сбор доказательств после утечки

Зафиксируйте режим коммерческой тайны

Подготовьте пакет подтверждений: положения о режиме, перечень сведений, грифы «коммерческая тайна», внутренние инструкции, договоры о неразглашении и доказательства ознакомления работника под подпись.

Докажите факт разглашения и причинно-следственную связь

Зафиксируйте, какие именно сведения утрачены, кому и в какой форме стали доступны. Привяжите данные к действиям работника и к последствиям: потерям, снижению выручки, контрактным рискам, конкурентному ущербу.

Соберите следы утечки и доступ к данным

Запросите и сохраните логи ИТ-систем, записи контроля доступа, сетевые журналы, файлы выгрузок и переписку. Обеспечьте неизменность носителей, ведите журнал цепочки хранения доказательств.

Оформите доказательственную базу для требований к ответственности

Систематизируйте материалы под заявляемые основания ответственности: дисциплинарную, гражданско-правовую (материальную) и уголовную. Учитывайте актуальную судебную практику 2024–2025 и соблюдайте процессуальные требования.

Что фиксировать для суда и следствия

1 Логи систем

Сохраняйте логи CRM, почты и DLP: они показывают, кто, когда и к каким данным обращался. Их ценность максимальна при немедленном извлечении и правильной фиксации.

2 Акт комиссии

Акт служебной комиссии подтверждает факт обнаружения утечки, состав участников и первичные выводы. Чем подробнее описаны обстоятельства, тем труднее оспорить документ в споре.

3 Нотариальный протокол

Протокол нотариуса особенно полезен для переписки, веб-страниц и облачных ресурсов. Он снижает риск спора о подлинности и времени существования цифрового следа.

4 Заключение эксперта

Компьютерно-техническая экспертиза устанавливает копирование, пересылку, подключение носителей и временные параметры действий. Это один из самых убедительных источников для суда и следствия.

5 Расчёт ущерба

Фиксируйте прямой ущерб, а при гражданском иске — также убытки и упущенную выгоду. Любые сторонние сведения используйте только законным способом и с учётом риска оспаривания.

Профилактика в трудовых отношениях

1. **Закрепите обязанность письменно**
   В трудовой договор и допсоглашение включите прямое обязательство не разглашать коммерческую тайну. Отдельно укажите, что оно действует и после увольнения в течение установленного срока.
2. **Ознакомьте под подпись**
   Сотрудник должен получить Положение о коммерческой тайне и NDA не формально, а с личной подписью и датой. Это подтверждает осознанное принятие ограничений и снижает риск спора.
3. **Свяжите увольнение с возвратом носителей**
   В обходной лист включите передачу документов, флеш-носителей и иных материальных носителей. Отдельно зафиксируйте подтверждение, что копии данных у работника отсутствуют.
4. **Проверьте процедуры до конфликта**
   Регулярно обновляйте локальные акты и перечни сведений, чтобы условия были актуальны на момент спора. Иначе даже дисциплинарная мера может быть оспорена как недостаточно обоснованная.

Контроль корпоративных каналов и DLP

Уведомление о мониторинге
Правила пользования корпоративной связью должны прямо сообщать сотрудникам, что переписка, файлы и действия в корпоративных каналах могут проверяться в целях безопасности и соблюдения режима КТ.

Блокировка массовой выгрузки
DLP-система должна выявлять нетипичную передачу больших массивов данных, отправку на внешние адреса и копирование на съёмные носители. Это позволяет остановить утечку до выхода информации за пределы компании.

Автоматическая маркировка файлов
Для документов, содержащих чувствительные сведения, настройте автоматическое присвоение грифа «Коммерческая тайна». Маркировка помогает подтвердить режим защиты и снижает вероятность спора о статусе файла.

Контроль рисков в сети
Мониторинг серверов, почты и рабочих станций должен сопровождаться журналированием событий и уведомлением ответственных лиц. Это создаёт доказательственную базу и дисциплинирует пользователей корпоративной инфраструктуры.

Аудит режима КТ: что проверять в первую очередь

Проверка	Что смотрим	Риск
Перечень сведений	Точность	Спор о предмете
Маркировка	Гриф на носителях	Слабая защита
Допуск	Журналы доступа	Нельзя связать утечку
Увольнение	NDA и возврат носителей	Срыв взыскания

Федеральный закон № 98-ФЗ, локальные акты работодателя, судебная практика 2024–2025 годов

Краткий аудит показывает, где режим коммерческой тайны работает, а где создаёт уязвимость для спора, увольнения или взыскания убытков.

Чем точнее оформлены перечни, доступ и увольнение, тем выше шансы на взыскание убытков и правовую перспективу дела.

Главный вывод для бизнеса: Эффективный режим КТ - возможность недопущения или компенсации потерь!

Успех спора определяют точный режим КТ, ограниченный доступ и быстрый сбор доказательств. Без этих элементов утечку почти невозможно эффективно квалифицировать, доказать и взыскать по ней убытки.