

Обстоятельства дела

Истец с 18 апреля 2025 по 09 сентября 2025 состоял в трудовых отношениях с ответчиком. Впоследствии трудовой договор был расторгнут в связи с разглашением истцом коммерческой тайны работодателя - ответчика.

У работодателя действовали положение о коммерческой тайне и конфиденциальной информации, перечни охраняемых сведений и правила информационной безопасности. Работник был ознакомлен с этими документами под подпись и принял обязательство не разглашать информацию, полученную при исполнении трудовых обязанностей.

В ходе внутренней проверки работодатель установил, что работник направлял корпоративные документы на личную электронную почту и адрес сторонней организации. Переданные материалы содержали сведения о тендерах, каналах сбыта, финансовых показателях, заработной плате сотрудников и планах деятельности компании. Кроме того, истец загружал охраняемые сведения из внутреннего защищённого ресурса Power Bi в сторонний сервис DeepSeek.

Работник оспаривал увольнение, ссылаясь на отсутствие доказательств разглашения охраняемой законом тайны. Он также просил изменить основание увольнения на соглашение сторон и взыскать 5 млн руб., предусмотренные дополнительным соглашением к трудовому договору для такого основания прекращения трудовых отношений.

Работодатель представил скриншоты с рабочего компьютера работника, данные системы мониторинга, результаты проверки службы информационной безопасности, материалы служебного расследования и свидетельские показания. Эти материалы доказывали нарушение работником установленного режима защиты информации.

Правовая позиция суда

Суд признал увольнение законным и отказал в удовлетворении связанных с ним требований, так как в рассматриваемом деле все условия для увольнения по основанию разглашения работником охраняемой законом тайны были соблюдены, а именно:

- обязанность сохранять конфиденциальность была закреплена в трудовом договоре и должностной инструкции работника;
- локальные нормативные акты работодателя определяли конкретные категории охраняемой информации;
- работник был ознакомлен с этими актами под подпись;
- сведения стали известны работнику при исполнении им своих трудовых обязанностей;
- был установлен факт разглашения охраняемой законом тайны, так как исходя из обстоятельств дела у истца не было служебной необходимости разглашать упомянутые сведения, а сам факт разглашения подтверждался различными доказательствами и материалами служебного расследования.

При этом, основной вывод суда заключался в том, что для квалификации действий работника как разглашения охраняемой законом тайны не требуется устанавливать фактическое ознакомление конкретного третьего лица с переданной информацией.

Сославшись на [Постановление Конституционного Суда РФ от 26 октября 2017 г. № 25-П](#), суд указал, что передача корпоративной информации на ресурс, который не контролируется работодателем, создает условия для ее неконтролируемого использования. В связи с этим отсутствует необходимость устанавливать факт доведения информации до третьих лиц. На этом основании выгрузка сведений, составляющих коммерческую тайну или конфиденциальную информацию, во внешний сервис искусственного интеллекта была квалифицирована как разглашение.

Данное решение суда имеет важное значение как для работодателей, которые вводят режим коммерческой тайны и допускают применение работниками внешних цифровых сервисов, так и для самих работников.

Рекомендации для работодателей:

- определить в локальных нормативных актах конкретные категории защищаемой информации;
- урегулировать использование личной почты, облачных хранилищ и внешних ИИ-сервисов;
- установить порядок согласования передачи корпоративных данных на внешние ресурсы;
- ознакомить работников с соответствующими правилами под подпись;
- при выявлении нарушения зафиксировать содержание переданных файлов, способ и время передачи, используемый ресурс и отсутствие производственной необходимости передачи данных.

Рекомендации для работников:

- не направлять служебные документы на личную почту и иные внешние адреса без согласования с работодателем;
- внимательно изучать локальные нормативные акты о коммерческой тайне, конфиденциальности и информационной безопасности;
- использовать только разрешенные работодателем сервисы и соблюдать установленный порядок работы с корпоративной информацией;
- при необходимости передачи данных получать письменное согласование и сохранять подтверждение служебной цели таких действий;
- при проведении служебного расследования предоставлять письменные объяснения и документы, подтверждающие производственную необходимость использования информации.



Мы будем рады ответить на ваши вопросы



Анна Максименко

Партнер

Anna.Maximenko@kkmp.legal



Ева Лазовская

Стажер

Eva.Lazovskaya@kkmp.legal