

Обзор судебной практики по защите коммерческой тайны в сфере ИТ в России

Фонд содействия цифровой трансформации «Атом»

<https://fondatom.ru>

Введение

- В обзоре рассмотрено более 50 судебных дел по защите коммерческой тайны.
- Приведённая в обзоре судебная практика охватывает период 2014 — 2017 гг.
- В работе разобраны судебные дела, связанные с разглашением коммерческой тайны с использованием информационных технологий и, в частности, таких сравнительно новых методов, как разглашение закрытых данных с помощью электронной почты, интернета и социальных сетей.
- Большая часть обзора отведена судебным делам, изучение которых позволяет обладателю коммерческой тайны эффективно установить режим коммерческой тайны на предприятии.
- Подробно разобраны ситуации, анализируя которые, можно соблюсти законную процедуру вынесения взысканий нарушителям, правильно подготовить доказательства и защитить свои интересы в суде.
- Рассмотрена возможность применения в качестве допустимых доказательств аудио- и видеозаписей, электронной переписки и интернет-страниц.
- Проанализирована практика привлечения нотариусов для фиксации факта разглашения.
- Обзор полезен широкому кругу владельцев и руководителей предприятий.

1. Виды нарушений

Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне» (ред. от 12.03.2014) (далее – Закон) определяет «разглашение информации, представляющей собой коммерческую тайну, как действие или бездействие, в результате которых закрытые сведения, в любой возможной форме (устной, письменной, другой форме, в том числе с использованием технических средств) становятся известными третьим лицам без согласия обладателя такой информации» (п. 9 ст. 3 Закона) [1].

Как это может происходить:

1. У сотрудника был доступ к тайне, и он нарушил режим коммерческой тайны (например, раскрыл кому-то ноу-хау).

В трудовых договорах оговаривается срок хранения тайны работником.

Пример из судебной практики 1: Если срок ещё действует, а работник уволился, то разглашение может произойти и после окончания трудового соглашения (апелляционное определение Санкт-Петербургского горсуда от 18.08.2015 № 33-13135/2015 по делу № 2-1146/2015).

2. Противозаконный доступ.

Пример из судебной практики 2: Злоумышленником получен доступ к конфиденциальной информации противозаконно, преступным путём, для обогащения (постановление Смоленского областного суда «Об отказе...» от 11.06.2015 № 4У-674/2015).

3. Лицензиар передал исключительные права или право использования ноу-хау, а лицензиат раскрыл кому-то секрет.

В любом случае незаконного разглашения конфиденциальной информации предполагается ответственность допустившего это нарушение лица [2].

Рассмотрим наиболее частые варианты таких нарушений, связанных с использованием IT-технологий.

Работник может скопировать информацию из базы компании на внешний накопитель (карту памяти, флешку, компакт-диск, внешний жёсткий диск и т.п.). Также работник может сохранить информацию в личный почтовый ящик, или в соцсетях.

Это уже является нарушением, даже если он ещё не передал накопитель третьему лицу, просто сохранил конфиденциальную информацию в черновиках личной почты или, например, на Facebook с доступом только для себя.

Если работодатель обнаружил этот факт после увольнения сотрудника, то можно написать заявление в полицию, однако вряд ли даже дело будет возбуждено, и вряд ли удастся возместить ущерб от разглашения тайны.

Если работодатель обнаружил факт разглашения до увольнения сотрудника, то работодатель может уволить работника по пп. «в» п. 6 ч. 1 ст. 81 ТК РФ (разглашение информации, составляющей коммерческую тайну) [3].

Для этого требуется выполнение ряда условий, которые подробнее рассмотрены в [главе 4 «Правильная процедура»](#).

Разглашение с помощью внешних накопителей

Работник скопировал конфиденциальную информацию на внешний накопитель для продажи конкурентам или для того, чтобы поработать с информацией дома.

В любом из этих случаев работодатель не может контролировать перемещение секретной информации. Даже если у работника нет злого умысла, он может этот накопитель потерять и таким образом сделать конфиденциальную информацию доступной третьим лицам.

Пример из судебной практики 3: Работник скопировал на флешку сведения о зарплате коллег. Работодатель провел служебную проверку, обнаружил нарушение и уволил работника. В компании существовали списки лиц, которые вправе обрабатывать персональные данные сотрудников. Нарушитель не входил в список. Работодатель выиграл трудовой спор, суд признал увольнение законным (апелляционное определение Московского городского суда от 04.08.2015 по делу № 33–24617/15) [4].

Однако, не всё так однозначно. Суд может принять решение и в пользу работника, и это зависит от того, какое взыскание было применено к работнику, что он собирался предпринять со скопированной информацией и установлен ли во внутренних нормативных актах компании запрет копирования конфиденциальной информации на внешние носители.

Пример из судебной практики 4: Сотрудница действительно скопировала на флешку информацию, составляющую коммерческую тайну общества, но только лишь для составления отчета. При этом работница не размещала эти сведения в интернете и не пересылала их по почте третьим лицам. По мнению суда, сам по себе факт копирования

секретной информации без доказательств ее передачи третьим лицам не может расцениваться как разглашение коммерческой тайны. Работницу восстановили в должности ([определение Московского городского суда от 12.12.2011 по делу № 42/8-10961/2011](#)).

И похожая ситуация – в следующем примере:

Пример из судебной практики 5: Верховный суд Республики Татарстан сослался на [п. 9 ст. 3 Закона № 98-ФЗ](#), где указаны признаки разглашения информации, составляющей коммерческую тайну. В частности, в нарушение всех правил она должна стать известной третьим лицам. Однако в рассматриваемом деле до этого не дошло, а значит, увольнять работника было нельзя (апелляционное определение от 29.08.2013 по делу № 33-10267/13).

Противоположный пример, в котором работник при приеме на работу подписал обязательство о неразглашении сведений, составляющих коммерческую тайну.

Пример из судебной практики 6: Локальный акт содержал перечень подобной информации и запрет на ее передачу (пересылку). Внутренняя проверка на предмет нарушения коммерческой тайны установила эпизоды нарушения режима коммерческой тайны. Они заключались в следующем: многократное копирование с персонального компьютера на личную флеш-карту файлов с конфиденциальной информацией и передача по электронной почте третьим лицам секретных сведений. Указанные факторы подтвердили разглашение работником охраняемой законом коммерческой тайны и законность его увольнения по подп. «в» п. 6 ч. 1 ст. 81 ТК РФ ([апелляционное определение Московского городского суда от 08.10.2013 по делу № 11-33789](#)).

В предыдущем примере работник передал конфиденциальную информацию третьим лицам, а примере ниже суд даже не пытался выяснить, стало ли известно о составе этих документов третьим лицам.

Пример из судебной практики 7: Шансы на выигрыш дела повышаются, если работник дал письменное обязательство не копировать документы компании. Например, в Кемеровском областном суде работнику не удалось оспорить выговор за копирование на флеш-карту секретных документов. Суд рассуждал так. Работник дал подписку о неразглашении сведений, составляющих коммерческую тайну, и подтвердил, что не будет копировать все разработки, схемы и другие документы работодателя. В локальном акте, с которым работника ознакомили под роспись, работодатель определил перечень информации и документов, составляющих коммерческую тайну. Работник имел доступ к этим сведениям и однажды несанкционированно скопировал на личный съемный USB-накопитель секретные файлы. За этот дисциплинарный проступок работодатель правомерно объявил ему выговор (определение от 29.06.2012 по делу № 33-6243-2012) [5].

Разглашение через электронную почту

Чаще всего сотрудники используют для разглашения бесплатную личную почту, которая не может предоставить такую же защиту переписки, как корпоративные почтовые сервисы, использующие меры усиленной информационной безопасности. Корпоративную почту компании защитить проще. При взломе личной почты на бесплатном сервисе

доступ к переписке получает неопределенные третьи лица. Кроме того, за безопасность корпоративной почты несёт ответственность компания, а не сотрудник [4].

Компания вправе контролировать переписку. Переписка сотрудников по рабочим вопросам — собственность компании. Поэтому уполномоченные представители компании могут ее открывать, просматривать, копировать и уничтожать [6].

Пример из судебной практики 8: *Сотрудница по запросам клиентов направляла информацию по электронной почте. Работодатель посчитал это разглашением конфиденциальной информации и уволил ее. Сотрудница обжаловала это решение в судебном порядке.*

Женщина указала, что сведения, которые были направлены клиентам компании, предоставлялись только на основе их официальных запросов. Кроме того, вся предоставленная информация направлялась по электронным адресам, которые были указаны в качестве контактных данных в доверенностях клиентов. Суд поддержал работницу. Он согласился, что разглашения конфиденциальной информации не было, и восстановил женщину на работе (апелляционное определение Московского городского суда от 28.06.2013 № 11–20217/2013) [7].

Ещё несколько примеров...

Пример из судебной практики 9: *Гражданин С. работал в ООО «Региональная страховая компания» в должности директора Департамента продаж. Был уволен после того как переправил по корпоративной почте на свой личный почтовый адрес и адрес супруги файлы, содержащие информацию о страховых продуктах Общества. Этот факт, вскрытый сотрудниками Департамента информационных технологий, проводивших контрольную проверку использования корпоративной почтовой системы, послужил основанием для проведения служебного расследования.*

С. в объяснительной записке написал, что файлы ему были нужны для проведения презентации потенциальным партнерам продуктов и услуг Общества. По его мнению, среди пересланных документов не было секретных. Комиссия с доводами С. не согласилась и постановила применить к нему дисциплинарное взыскание в виде увольнения. Приказ об увольнении ссылался на пп. «в» п.6 ч.1 ст. 81 ТК РФ.

Первая судебная инстанция, куда обратился С., встала на сторону истца и признала увольнение незаконным. Основанием для такого судебного решения послужило непредоставление ответчиком трудового договора с С., нечеткие формулировки Правил внутреннего трудового распорядка и отсутствие Положения о коммерческой тайне или иных нормативных документов, регламентирующих данный вопрос.

Однако суд апелляционной инстанции более внимательно отнесся к тем мерам, которые ответчик предпринимает для защиты своей конфиденциальной информации, и счел их достаточными для того, чтобы считать С. виновным в разглашении коммерческой и служебной тайны (Определение Московского городского суда по делу № 4г/9-9007/2014 от 20.10.2014) [8].

Пример из судебной практики 10: *Работник скопировал информацию и передал базу клиентов с рабочего компьютера на электронную почту третьего лица ([апелляционное определение Московского городского суда от 26.11.2015 по делу № 33–44248/2015](#)) [3].*

В этом случае сотрудник разгласил конфиденциальную информацию, передав её по электронной почте, не имея на это доверенности или приказа.

Пример из судебной практики 11: Работник передал конфиденциальную информацию на электронную почту третьего лица, ссылаясь на производственную необходимость ([определение Московского городского суда от 20.08.2014 по делу № 33–33182/14](#)).

А в следующем случае суд основывался на заключении экспертов и вынес решение в пользу уволенного работника:

Пример из судебной практики 12: *Специалисты подтвердили, что достоверных признаков отправки писем с адреса корпоративной почты на адрес третьего лица в указанное в этих письмах время либо позже не обнаружено. Более того, они выявили признаки имитации такой отправки и засвидетельствовали техническую возможность отправки данных писем в более поздний период. Оснований не доверять заключению эксперта у судебной коллегии не имелось, поэтому компания проиграла спор (апелляционное определение Санкт-Петербургского городского суда от 27.05.2014 № 33–8038/2013).*

В этом случае работник ссылался на то, что информация свободно присутствует в интернете и общедоступна, поэтому не является коммерческой тайной, и выиграл суд:

Пример из судебной практики 13: *Работодатель не установил в компании надлежащим образом режим коммерческой тайны (не ознакомил работника под роспись с конфиденциальной информацией, не получил обязательство не разглашать ее) и не доказал ущерб от действий сотрудника. С учетом этих факторов указание работодателя на наличие электронной переписки между работником и третьими лицами компании не помогло ([апелляционное определение Московского городского суда от 18.09.2013 по делу № 11–28840](#)).*

В данном же примере работодатель прописал в локальном акте запрет на направление через электронную почту, интернет или факсом сведений, составляющих конфиденциальную информацию и (или) коммерческую тайну, внешним адресатам без согласования. Также был составлен перечень такой информации, в котором были приведены признаки, указывающие на секретный статус информации.

Пример из судебной практики 14: *В компании использовали грифы «Конфиденциально», «Строго конфиденциально», «FOR INTERNAL USE ONLY», «Please do not forward» с пометкой «только для внутреннего пользования». Изучив доказательства работодателя, суд подтвердил правомерность увольнения за разглашение охраняемой законом тайны ([апелляционное определение Московского городского суда от 20.02.2015 по делу № 33–5528](#)).*

В примере ниже компания правильно установила режим коммерческой тайны, и суд принял её сторону.

Пример из судебной практики 15: *Заместитель управляющего директора Управления новых рынков ООО «Национальная служба взыскания» П. была уволена по пп. «в» п. 6 ч. 1 ст. 81 ТК РФ (разглашение охраняемой законом коммерческой тайны). Свое увольнение истец считала незаконным, поскольку факт разглашения охраняемой законом тайны с ее стороны отсутствует, увольнение произведено в связи с копированием сведений, которые являются незначительными, не повлекшими негативных правовых последствий, информация не была передана третьим лицам. Отправка рабочих материалов на личную почту была сделана для целей изучения данных материалов дома, а также возможности работать с ними в случае болезни.*

П. подписала соглашение о неразглашении конфиденциальной информации ООО «НСВ», обязательство о неразглашении сведений, составляющих коммерческую и банковскую тайну в соответствии с которыми, в том числе обязалась в период своей работы в ООО «НСВ» не делать несанкционированные выписки и копии (в том числе на магнитных носителях) документов, содержащих коммерческую и банковскую тайну.

Суд постановил решение Гагаринского районного суда города Москвы от 19 января 2015 года оставить без изменения, апелляционную жалобу П. — без удовлетворения ([апелляционное определение Московского городского суда от 20.04.2015 по делу № 33–12843](#)).

В компаниях с разветвленной сетью обособленных структурных подразделений без обмена электронными сообщениями не обойтись. Это же касается организаций с большой численностью персонала, который находится в одном населенном пункте, но на разных площадках. В этом примере компания выпустила локальный нормативный акт, в котором оговорила особые условия приема-передачи секретной информации с использованием защищенных каналов связи:

Пример из судебной практики 16: *В упомянутом акте за невыполнение требования было предусмотрена дисциплинарная ответственность вплоть до увольнения по статье, тем более, что работник не ограничился только своей почтой, а отправил сведения и по другим адресам ([апелляционное определение Московского городского суда от 06.04.2015 по делу № 33–11198/15](#)).*

За использование корпоративной почты для личных нужд работник может быть подвергнут взысканию, если локальный акт это прямо запрещает:

Пример из судебной практики 17: *Работодатель ввёл в действие локальный акт, в котором было описано, что компьютер предназначен только для работы, и его использование для личной переписки запрещено ввиду опасности заражения компьютера вирусом и разглашения коммерческой тайны ([определение Иркутского областного суда от 26.03.2014 № 33–2352/14](#)).*

Случается, что работники пытаются защищаться в суде тем, что документы, которые они переслали, малозначимы и не содержат коммерческой тайны.

Пример из судебной практики 18: На подобные обстоятельства сослался работник, который отправил по электронной почте сведения с коммерческой тайной себе и супруге. Но суд не принял их во внимание и подтвердил законность увольнения по [подп. «в» п. 6 ч. 1 ст. 81 ТК РФ](#) (определение Московского городского суда [от 28.01.2014 по делу № 33–5570/14](#)) [5].

Рассмотрим ещё один характерный пример увольнения за отправку служебных документов на адрес личной почты.

Примеры из судебной практики 19 и 20: Ведущему специалисту отдела МСФО крупной российской IT-компании руководитель предложил уволиться по собственному желанию. Та увольняться отказалась, и тогда с ней решили расстаться «по статье».

На предприятии сотрудники часто брали работу на дом, и сотрудница отправила на личную почту несколько писем с документами, чтобы поработать в выходные дни над срочным проектом. Об этом узнал руководитель, инициировал служебное расследование, по итогам которого Е. уволили по [подп. «в» п. 6 ч. 1 ст. 81 ТК РФ](#). Ее обвинили в том, что она разгласила корпоративные секреты.

Е. оспорила увольнение в судебном порядке. Сотрудница апеллировала к тому, что третьим лицам информацию она не разглашала, доступ к её ящику возможен только по паролю, а также у нее не запрашивали объяснения по факту отправки письма с конфиденциальной информацией компании, а только писем с учредительными документами, которые к тому же находятся на корпоративном сайте. Поэтому она просила суд признать ее увольнение незаконным, обязать компанию выплатить заработок за вынужденный прогул и компенсировать моральный вред.

Работодатель доказывал, что коммерческая тайна стала известна третьим лицам, следующим образом.

Пользовательское соглашение почтового сервиса Google.com предусматривает, что пользователь передает Google лицензию на использование материалов, которые пересылает в письмах. Следовательно, между Е. и Google действует лицензионный договор, заключенный в упрощенном порядке ([ч. 5 ст. 1286 ГК РФ](#)). Таким образом, к письмам на личную почту получило доступ к конфиденциальной информации третье лицо – компания Google, поэтому увольнение правомерно.

Суд согласился, что работница не имела права отправлять секреты компании на личную электронную почту. В результате таких действий третьи лица получили доступ к конфиденциальной информации компании.

Суд оставил без внимания довод работницы, что компания не запрашивала у нее объяснения по факту отправки конфиденциальной информации на личную почту, признал увольнение законным и отказал работнице в удовлетворении требований ([решение Мещанского районного суда г. Москвы от 21.12.2016 по делу № 2–11360/2016, апелляционное определение Московского городского суда от 16.05.2017 по делу № 33–17995/2017](#)) [9].

Ещё один свежий пример. Здесь дело дошло до Конституционного суда.

Пример из судебной практики 21: В 2016 году Александр С. был уволен с должности директора департамента по договорно-правовой работе ЗАО «Стройтрансгаз» за разглашение охраняемой законом тайны. Будучи ознакомленным с Положением об обеспечении режима конфиденциальности информации, являющимся частью его трудового договора, гр-н А.С. переслал с адреса служебной почты на свой внешний электронный адрес служебные документы, локальные нормативные акты работодателя и персональные данные его коллег. Операция была осуществлена через сервер компании ООО «Мэйл.ру», оказывающей услуги электросвязи и владеющей данным сервером.

Оспаривая увольнение в судах, заявитель ссылался на функции почтового оператора как представителя услуг связи, защищающего конфиденциальность переписки. Суды, однако, признали предоставляющую услуги электронной почты компанию обладателем пересылаемой пользователями информации, поскольку по условиям Пользовательского соглашения с клиентом «Мэйл.ру» может как ограничить, так и разрешить доступ к сведениям, содержащимся в электронных почтовых ящиках абонентов, что свидетельствует о разглашении конфиденциальной информации третьему лицу.

По мнению заявителя, оспариваемое законоположение пункта 5 статьи 2 ФЗ «Об информации, информационных технологиях и о защите информации», определяющее понятие «обладатель информации», не соответствует статьям 19 (часть 1), 23 (часть 2) и 55 (часть 3) Конституции РФ. Заявитель считает, что оно предоставляет лицу, оказывающему услуги электронной почты, право разрешать или ограничивать доступ к информации, содержащейся в пересылаемых электронных сообщениях абонентов, и тем самым позволяет привлекать работника, воспользовавшегося услугами почтового сервиса, к дисциплинарной ответственности за распространение охраняемой законом тайны. Конституция РФ гарантирует каждому право на свободное получение, передачу и распространение информации любым законным способом.

Применительно к праву граждан на тайну телефонных переговоров КС РФ ранее отмечал, что конституционно защищенной информацией считаются любые сведения, передаваемые по каналам телефонной связи. Для доступа к этим сведениям необходимо получить решение суда. Данная правовая позиция распространяется на правовое регулирование как тайны телефонных переговоров, так и переписки, почтовых, телеграфных и иных сообщений.

Отсутствие в законодательстве прямого указания на обязанность именно правообладателя интернет-сервиса обеспечивать тайну связи не означает отсутствие у него такой обязанности. И наличие у лица доступа к информации не означает, что оно становится ее обладателем. Также и условия пользовательского соглашения не могут трактоваться как предоставляющие владельцу интернет-сервиса право самостоятельно (в нарушение части 2 статьи 23 Конституции РФ) разрешать или ограничивать доступ к информации и тем самым признавать его обладателем этой информации.

Между тем отправка гражданином информации на свой электронный адрес создает условия для ее дальнейшего неконтролируемого использования.

Поэтому, если гражданин нарушил нормативные предписания компании, запрещающие отправку конфиденциальной информации на его личную почту, то такая ситуация может рассматриваться как нарушающая права обладателя информации безотносительно того установлено ее разглашение третьему лицу или нет.

Таким образом, оспоренная норма не противоречит Конституции РФ, поскольку:

- *не может рассматриваться как наделяющая интернет-сервис статусом обладателя информации в отношении сведений, содержащихся в сообщениях пользователей электронной почты;*
- *позволяет рассматривать отправку информации на личный адрес электронной почты гражданина как нарушение прав обладателя информации, который принял все меры, исключая несанкционированный доступ третьих лиц к этой информации, прямо запретил такие действия локальными нормативными актами и ознакомил сотрудника с их содержанием.*

Правоприменительные решения по делу Александра С. подлежат пересмотру ([постановление Конституционного суда РФ от 26.10.2017 № 25-П](#)) [10].

Разглашение по Интернету

SMM-менеджеры и маркетологи имеют право использовать соцсети. Во избежание разглашения коммерческой тайны эту деятельность необходимо контролировать.

В профессиональной среде распространено мнение, что остальным сотрудникам использование интернета стоит запрещать, в том числе и с личных мобильных устройств [4].

Кроме того, необходимо мониторить сайты, которые сотрудники посещают для выполнения служебных обязанностей. Контроль подразумевает, что компания будет получать персональные данные работника. Поэтому получите его согласие на обработку таких данных [6].

Фиксация факта разглашения

В тех случаях, когда установлен факт разглашения конфиденциальной информации в интернете, его нужно удостоверить, пока сотрудник или владелец интернет-ресурса не удалил или не изменил её. В противном случае применить взыскание к работнику будет невозможно.

Нотариус может зафиксировать наличие сообщения на конкретном сайте в протоколе осмотра интернет-страницы, и он станет основным доказательством нарушения.

Подробнее об этом – в [главе 6 «Рекомендации»](#).

Ответственность за разглашение

Ответственность за «слив» конфиденциальной информации в интернет должна быть прописана в локальном акте. Если этого не сделать, то наказание будет невозможно.

Пример из судебной практики 22: *Работник разместил в социальной сети «Одноклассники» сведения о том, что он сам работает в определенном месте и изготавливает стеклопакеты из китайских материалов. Работодатель посчитал, что распространение такой информации было нарушением, и уволил его. Но суд встал на сторону работника. Поскольку при приеме на работу работодатель письменно не запретил распространять информацию о методах ведения бизнеса и используемом сырье, суд посчитал, что в действиях работника не было признаков дисциплинарного проступка ([решение Борзинского городского суда Забайкальского края от 17.04.2015 по делу № 2–256/2015](#)) [11].*

Персональные данные

Используя мониторинг деятельности сотрудников в интернете, компания получает их персональные данные. Чтобы не нарушать закон, работники должны подписать согласие на их обработку [4].

2. Гриф необходим?

Установления режима коммерческой тайны п. 5 статьи 10. «Охрана конфиденциальности информации» Федерального закона от 29.07.2004 N 98-ФЗ «О коммерческой тайне» предусматривает, в том числе, нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна».

Однако, судебная практика показывает, что всё не так однозначно.

Пример из судебной практики 23: *Суд указал, что само по себе отсутствие на информации грифа «Коммерческая тайна» не освобождает работника от ответственности за разглашение информации, поскольку отсутствие грифа не означает, что в сведениях не содержится информация, составляющая коммерческую тайну. Работник имел возможность установить, что информация является коммерческой тайной, руководствуясь соответствующим локальным актом, с которым его ознакомили при приеме на работу ([апелляционное определение Московского городского суда от 26.11.2015 по делу № 33-44248/2015](#)) [2].*

Суды сейчас менее формально рассматривают дела об увольнении работников за разглашение коммерческой тайны.

Пример из судебной практики 24: *Суд указал, что на документах не было грифа «Конфиденциально» или «Строго конфиденциально». Тем не менее компания ознакомила работника с локальным актом, который предусматривал его обязанность не разглашать конфиденциальную информацию. С учетом этого суд признал увольнение работника законным ([апелляционное определение Московского городского суда от 02.02.2016 по делу № 33–3266/2016](#)).*

Здесь суд тоже встал на сторону работодателя:

Пример из судебной практики 25: Работодатель ознакомил работника под роспись с документами, которые определяли режим конфиденциальности. Дополнительно в его трудовом договоре было прописано обязательство о неразглашении такой информации. Поэтому в суде не сработал довод работника о том, что на документах не было грифа секретности ([определение Московского городского суда от 29.03.2016 № 4г-2218/2016](#)) [12].

3. Бездействие — тоже нарушение

Работник не заблокировал компьютер и ушёл.

Пункт 9 ст. 3 «Основные понятия, используемые в настоящем Федеральном законе» Федерального закона 98-ФЗ определяет разглашение информации, составляющей коммерческую тайну, как «действие или **бездействие**, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору».

Если работники не выполняют правила, исключаящие доступ к конфиденциальной информации других лиц, это может привести к разглашению коммерческой тайны.

Пример из судебной практики 26: Работника уволили, поскольку проверка установила, что он нарушил положения локальных актов. Эти документы предписывали не разглашать (не передавать) коммерческую тайну, включая пароли доступа в корпоративную информационную сеть. Кроме того, работник был обязан, оставляя рабочее место даже на короткое время, заблокировать доступ к работающему компьютеру путем нажатия клавиши Ctrl-Alt-Del и выбора в меню пункта «Блокировать компьютер». Работник проигнорировал указанный порядок, в результате чего доступ к его учетной записи получили другие сотрудники. Один из них совершил хищение денег с банковского счета клиента ([определение Московского городского суда от 18.02.2013 № 11-5312/2012](#)).

Пример из судебной практики 27: Работодатель обвинил сотрудника в разглашении коммерческой тайны в форме бездействия и допуске третьего лица к компьютеру. Все попытки работника оспорить увольнение по [подп. «в» п. 6 ч. 1 ст. 81 ТК РФ](#) остались безуспешными. Суд отказал в удовлетворении иска о восстановлении на работе ([определение Московского городского суда от 23.09.2013 № 4г/8-7616](#)).

Пример из судебной практики 28: Работодатель разработал порядок работы с документами, содержащими конфиденциальную информацию, но работник, вместо закрытого внутреннего помещения с ограниченным доступом, хранил часть документов вне этой зоны. По ошибке они оказались в мусоре, о чем сообщил клиент компании. Поскольку нарушение произошло из-за безответственности работника, обязанного контролировать работу с этими документами, то работодатель уволил его за разглашение банковской тайны и конфиденциальной информации. Попытка переложить вину на работодателя закончилась неудачей, так как он предпринял все меры по режиму хранения секретной информации (выделил помещение, разработал правила), но работник эти правила не соблюдал ([определение Московского городского суда от 19.08.2014 № 4г/8-7847](#)) [5].

4. Правильная процедура

Для защиты конфиденциальной информации работодатель должен установить режим защиты коммерческой тайны. Кроме этого, для выигрыша дела в суде необходимо соблюсти процедуру применения санкций, иначе суд их отменит. Суд будет смотреть на соблюдение следующих аспектов:

- Составлен акт о разглашении конфиденциальной информации?
- Запрошено ли у работника письменное объяснение?
- Составлен акт, если работник не предоставил объяснение?
- Работника уволили в течение месяца с момента выявления нарушения?
- Есть ли письменные доказательства факта разглашения?

Суд отменит взыскание, если на любой из этих вопросов работодатель ответит «нет» [7].

Во многих видах трудовых споров с целью определения бремени доказывания презюмируется незаконность поведения работодателя [13].

Введите режим защиты коммерческой тайны и соблюдайте процедуру

Суды – на стороне тех компаний, которые добросовестно хранят коммерческую тайну. «В 2015 и 2016 годах суды в 80% случаев признали увольнения за разглашение конфиденциальной информации законными».

Пример из судебной практики 29: Работодатель ознакомил работника под роспись с документами, которые определяли режим конфиденциальности. Дополнительно в его трудовом договоре было прописано обязательство о неразглашении такой информации. Поэтому в суде не сработал довод работника о том, что на документах не было грифа секретности ([определение Московского городского суда от 29.03.2016 № 4г-2218/2016](#)).

В этих же случаях суд встал на сторону работников:

Пример из судебной практики 30: Работодатель нарушал процедуру увольнения ([определение Московского городского суда от 19.08.2014 № 4г/8-7847](#)).

Пример из судебной практики 31: Работодатель не соблюдал требования по охране конфиденциальной информации ([определение Московского городского суда от 14.10.2014 по делу № 33-34636/14](#)) [12].

Если работник разгласит коммерческую тайну, то работодатель имеет право его уволить по статье. Для этого недостаточно составить перечень сведений, относящихся к коммерческой тайне, необходимо также вести учет лиц, имеющих к ней доступ. Если сотрудник нарушит положения локальных актов и трудового соглашения, взыскание будет законным.

Из судебной практики видно, что суды отменяют увольнения за разглашение коммерческой тайны ([подп. «в» п. 6 ч. 1 ст. 81 ТК РФ](#)) из-за нарушения процедуры

увольнения и отсутствие оснований для него. Привлекая работника к дисциплинарной ответственности за разглашение коммерческой тайны, работодатель обязан выполнить требования [ст. 193](#) ТК РФ.

Кроме того, компания обязана выполнить требования [ст. 10](#) Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне», и получить подпись работника под документами, относящимся к коммерческой тайне.

Пример из судебной практики 32: Работодатель тщательно выполнил перечисленные меры, и увольнение работника, разгласившего коммерческую тайну, суд признал правомерным (определение Московского городского суда [от 18.12.2014 № 4з/2–12790/14](#)) [5].

Обязательство о неразглашении коммерческой тайны

Обязательство о неразглашении коммерческой тайны является доказательством того, что сотрудник знал о конфиденциальности информации и принял обязательство хранить её в тайне.

В обязательстве не должно быть обязанности возместить упущенную выгоду;

Пример из судебной практики 33: Взыскать можно только прямой действительный ущерб (ст. 238 ТК РФ, п. 15 постановления Пленума ВС РФ от 16.11.2006 № 52, [определение Московского городского суда от 14.08.2014 № 33-28310](#)).

В обязательстве также нельзя запрещать переходить к конкуренту или организовывать похожий бизнес:

Пример из судебной практики 34: Работник вправе выбирать работу и вид деятельности (ст. 37 Конституции РФ, ст. 2 ТК РФ, [определение Ростовского областного суда от 11.12.2014 № 33-15622/2014](#));

В обязательстве нельзя штрафовать.

Примеры из судебной практики 35 и 36: Такой санкции в законе нет и нельзя договориться об ответственности выше, чем это предусмотрено законом (ч. 2 ст. 232 ТК РФ, [определения Свердловского областного суда от 23.05.2014 № 33-6628/2014](#) и [ВС Республики Татарстан от 23.03.2015 № 33-4126/2015](#)).

Увольнять можно по [подп. «в»](#) п. 6 ч. 1 ст. 81 ТК РФ после первого нарушения, т.к. оно грубое.

Примеры из судебной практики 37 — 39: Поскольку это дисциплинарное взыскание, запросите у работника объяснение. Приказ издавайте через 2 дня (ч. 3 ст. 192, ч. 1 ст.

[193 ТК РФ](#)). Вину работника подтвердят акт внутреннего расследования и служебные записки (определения Московского городского суда [от 20.10.2014 № 42/9-9007/2014](#), [от 20.11.2014 № 33-46279/14](#), [от 20.10.2015 № 42/8-9884](#)).

Увольнение без доказательств разглашения конфиденциальной информации — незаконно.

Пример из судебной практики 40: Суд его восстановит (апелляционное определение [Санкт-Петербургского городского суда от 30.09.2015 № 33-14813/2015](#)).

Рассчитайте ущерб и предоставьте суду.

Пример из судебной практики 41: Без доказательств того, что он разгласил коммерческую тайну, работодатель проиграет (определение [Санкт-Петербургского городского суда от 18.08.2015 № 33-13135/2015](#)).

Если конфиденциальная информация похищена с корыстными целями, наступает уголовная ответственность ([ст. 183 УК РФ](#)).

Примеры из судебной практики 42 и 43: Суды назначают штраф, исправительные или принудительные работы, лишают права занимать должности или даже свободы (приговоры [Лефортовского районного суда г. Москвы от 18.08.2015 № 1-214/2015](#), [Первомайского районного суда г. Пензы от 15.07.2015 № 1-159/2015](#)) [14].

Взыскание ущерба

Пример из судебной практики 44: Штраф за разглашение тайны в рамках трудовых отношений не взыскивается (апелляционное определение Верховного суда Республики Татарстан от 23.03.2015 по делу № 33-4126/2015).

С другой стороны, у компании есть право взыскать убытки, причиненные разглашением коммерческой тайны (ч. 4 ст. 11 закона № 98-ФЗ). Так, за разглашение ноу-хау (секрет производства — ст. 1465 ГК РФ) виновный возмещает убытки по правилам ст. 1472 ГК РФ.

Доказательства нарушения режима коммерческой тайны

Суду должно быть предоставлены следующие доказательства (ст. 11 закона № 98-ФЗ, ст. 192, 193 ТК РФ):

1. По закону № 98-ФЗ коммерческая тайна — любая информация, имеющая коммерческую ценность, неизвестная третьим лицам и отсутствующая в свободном доступе.

Компания должна составить перечень информации, составляющей коммерческую тайну, и закрепить его в положении.

Трудовое соглашение и обязательстве о неразглашении коммерческой тайны должно содержать ссылку на него и быть подписаны работником.

2. Конфиденциальная информация стала доступна работнику не из интернета, а в результате исполнения им трудовых обязанностей.

Это компания может доказать, т.к. обязана учитывать лиц с доступом к коммерческой тайне.

3. Работник обязался хранить конфиденциальную информацию в тайне.

Это фиксируется в трудовом соглашении, должностной инструкции, соглашении о неразглашении.

Пример из судебной практики 45: Подписывая документ о неразглашении, работник берет на себя обязанность выполнять приказы, инструкции и положения по обеспечению сохранности конфиденциальной информации работодателя (апелляционное определение Московского городского суда от 26.11.2015 по делу № 33-44248/2015) [2].

Допустимые доказательства

Аудио- и видеозаписи

Примет ли суд аудиозапись разговора в качестве доказательства?

Анализ судебной практики специалистами фонда «Атом» определил, что суд принимает аудиозаписи в качестве доказательства, если они соответствуют принципам относимости, допустимости и достоверности и можно доказать, когда, кто и в каких условиях их сделал (ст.ст. [59](#), [60](#) и [п. 3](#) ст. 67 ГПК РФ).

Работники этого сделать обычно не могут, поэтому суд не принимает у них такие доказательства, и ходатайства о приобщении записей суды не удовлетворяют.

Однако компания может это доказать, если работник при устройстве на работу был письменно предупреждён о таком контроле [3].

Согласие на аудио- и видеозапись:

Примеры из судебной практики 46 — 47: Большинство судов считает, что аудиозапись необходимо проводить с согласия другой стороны, иначе такое доказательство будет признано недопустимым. Обосновывают это нарушением требований [ст. 23](#) Конституции РФ, а именно права на неприкосновенность частной жизни (апелляционные

[определения Красноярского краевого суда от 24.09.2014 по делу № 33–9257/14, Московского городского суда от 30.07.2015 по делу № 33–26927/15](#)).

В единичных случаях суды приобщают к материалам дела аудиозаписи, которые не содержат в себе согласие другой стороны и подробную информацию о записи.

Пример из судебной практики 48: Суд отклонил довод работодателя о недопустимости аудиозаписи в силу нарушения требований [ст. 77](#) ГПК РФ. Довод суда: «в рамках судебного разбирательства в первой инстанции ответчик не был лишен права после прослушивания записи задать истцу уточняющие вопросы об обстоятельствах, в ней изложенных, ходатайствовать о назначении судебной фоноскопической экспертизы» ([апелляционное определение Омского областного суда от 28.01.2015 по делу № 33–394/2015](#)).

Требования к записям

Что будет, если работник, обвиняемый в разглашении конфиденциальной информации, например, по телефону, откажется признавать своим голос на аудиозаписи? Как минимум, придётся ходатайствовать о назначении судебной фоноскопической экспертизы, что затянет процесс.

Примеры из судебной практики 49 — 51: В самой аудиозаписи работник или работодатель должен указать, когда, кем и при каких обстоятельствах осуществлялись записи, чьи голоса на ней зафиксированы, а также представить распечатку ее содержания ([апелляционные определения ВС Республики Бурятия от 23.06.2014 по делу № 33–2560, Хабаровского краевого суда от 30.07.2014 по делу № 33–4619/2014, Московского городского суда от 16.12.2014 по делу № 33–40501/2014](#)) [13].

Использование видеоконтроля

Несмотря на то, что зачастую интересы компании идут вразрез с нормами о невмешательстве в приватную жизнь сотрудников, суды чаще всего принимают сторону компаний.

Мониторинг переписки, телефонные переговоры, серфинг в интернете сотрудников, компания обязана уведомить о таких действиях сотрудников, иначе возможно, что суд не признает судом эти доказательства допустимыми (ст. 60 ГПК РФ).

Однако, согласия работников на видео- и аудиозапись действий и разговоров персонала не требуется.

Пример из судебной практики 52: Мнение работника не повлияет на право снимать его на камеру или записывать разговоры на диктофон ([определение Московского областного суда от 19.04.2012 № 33–9255/2012](#)).

Контроль за работниками с нарушением законодательства о защите персональных данных может послужить поводом для привлечения работодателя к ответственности вплоть до уголовной [6].

Электронная переписка

В судебной практике немало случаев использования переписки по e-mail в качестве доказательства как работниками, так и работодателями.

Примеры из судебной практики 53 — 54: Работники активно используют ее в делах о доказывании факта возникновения между сторонами трудовых отношений. Но если у работника кроме электронной переписки других доказательств нет, суды встают на сторону работодателя (определения [Санкт-Петербургского городского суда от 03.02.2016 по делу № 33–2200/2016](#), [Московского городского суда от 26.08.2016 по делу № 33–33392/2016](#)).

Работодатели также используют как доказательства электронную переписку в делах об увольнении за разглашение коммерческой тайны. Изучая письма, можно понять, что и кому переслал работник. Важный момент при контроле переписки работника — не переступать черту.

Пример из судебной практики 55: Проверка личных средств связи работника — нарушение конституционных прав на личную переписку и частную жизнь ([решение Ворошиловского районного суда г. Волгограда от 25.07.2011 по делу № 2–2770/2011](#)) [13].

6. Рекомендации

Нотариальное заверение электронной переписки

Для того, чтобы суд признал переписку по e-mail в качестве допустимого доказательства, распечатку скриншота с экрана или простую распечатку лучше нотариально заверить [13].

Нотариус делает это у себя или у работодателя.

Кроме того, по делу о разглашении коммерческой тайны нотариус может допросить свидетелей, если по делу много свидетелей и суд отказывается всех слушать в заседании (Закон № 457-ФЗ) [15].

Протокол осмотра интернет-страницы

Четких правил, как составлять протокол, нет. Каждый нотариус составляет его сам исходя из своего опыта и знаний. Но есть несколько моментов, на которые суды обращают внимание. Из-за их отсутствия суд может не принять протокол. Вот эти требования:

1 Разъяснение терминов, которые нотариус использует в протоколе. Судья может не знать, например, что такое «утилита». Поэтому попросит растолковать значение. Если вы не сможете это сделать, придется вызывать технического специалиста, что затянет процесс.

2 Очистка кэша. Кэш — специальное место на жестком диске компьютера, где хранятся копии страниц, которые пользователь компьютера посещал в Интернете. Если его не очистить, работник может этим воспользоваться. Довод — нотариус искусственно создал страницу с оскорблениями и загрузил её из кэша.

3 Проверка браузера на вирусы. Отсутствие антивирусной проверки — повод признать протокол недопустимым доказательством. Вирусы негативно влияют на работу браузера и системы в целом, вследствие чего он не может отражать достоверную информацию на страницах сети Интернет.

4 Подтверждение системными утилитами подлинности отображения содержимого осматриваемого сайта. Нотариус должен подтвердить, что зашел на реальную страницу в Интернете. Для этого, обычно, используют служебную программу трассировки, которая есть в операционной системе (Tracert в Windows, Traceroute в Linux). Она показывает путь от компьютера пользователя до интересующей его страницы в Интернете.

5 Переход от главной страницы сайта к нужной странице. Это доказательство того, что страница находится на конкретном сайте в Интернете.

Пример из судебной практики 56: Суд не принял протокол, так как нотариус начал осмотр с интересующей заявителя страницы ([постановление СИП от 27.11.2014 по делу № А40-1849/2013](#)).

6 Контактная информация работника на странице в соцсети. Кроме фиксации сообщения нужно подтвердить, что страница принадлежит работнику, а не иному лицу. Нотариус откроет вкладку «Контактная информация», сделает скриншот и подошьет его к протоколу [16].

ПРОТОКОЛ осмотра

Город Москва, шестое октября две тысячи семнадцатого года.

Я, Миллер Николай Николаевич, нотариус города Москвы (лицензия № 000651 на право нотариальной деятельности от 10 мая 1995 года, приказ № 42-ч от 02 марта 1998 года, выданные Управлением юстиции города Москвы), в соответствии со статьями 35, 102, 103 Основ законодательства Российской Федерации о нотариате произвел осмотр сайта в информационно-телекоммуникационной сети «Интернет».

Место и время проведения осмотра:

Осмотр производился в помещении нотариуса города Москвы Миллера Н. Н. по адресу: город Москва, Пресненская набережная, дом 12, Комплекс «Федерация», Башня «Восток», этаж 12, офис Д2.

Осмотр начал: 06 октября 2017 года в 10:35.

Осмотр окончен: 06 октября 2017 года в 11:00.

Основание для проведения осмотра:

Заявление от 06 октября 2017 года общества с ограниченной ответственностью «Ромашка» (ОГРН 12345121211, ИНН 77123456, место нахождения: 123000, город Москва, улица Ленина, дом 1) о проведении осмотра с целью обеспечения доказательств, необходимых в случае возникновения дела в суде или административном органе.

Цели осмотра:

Заявитель просит произвести осмотр сайта в информационно-телекоммуникационной сети общего пользования «Интернет» по адресу: facebook.com с целью фиксации информации, размещенной на странице зарегистрированного пользователя «Петр Петров» указанного сайта по адресу: <https://www.facebook.com/profile.php?id=1111234578906>, а именно — записи «Петров Петр — отзывы о работодателях... 22 июня 11:50», информации в разделе «Информация» (подраздел «Контактная и основная информация»), и в связи с имеющимися основаниями полагать, что последующее доказывание наличия данной информации на указанном сайте может оказаться затруднительным и (или) невозможным из-за того, что информация находится в электронном виде, в любой момент времени может быть изменена или удалена, а заявитель не является администратором осматриваемого сайта и доменного имени.

Протокол осмотра интернет-страницы, <http://e.tspor.ru/article.aspx?aid=598063>

7. Выводы

Суды по делам о защите коммерческой тайны принимают во внимание в первую очередь следующие обстоятельства.

1. На предприятии установлен режим защиты коммерческой тайны в соответствии с Законом № 98-ФЗ, для чего:

- Утверждён перечень сведений, составляющих коммерческую тайну,
- Утверждено Положение о коммерческой тайне,
- Разработаны средства и методы защиты конфиденциальной информации компании,
- Прогрифованы носители конфиденциальной информации,
- Введены изменения в должностные инструкции сотрудников и иную организационно-распорядительную документацию,
- Разработаны положения, инструкций, правила и методики по обеспечению режима работы для исполнителей закрытых работ,
- Работники, допущенные к работе с закрытыми сведениями, ознакомлены под роспись с Положением,
- Взяты письменные обязательства по сохранению конфиденциальности сведений, составляющих коммерческую тайну,
- Ведётся учет допуска сотрудников к закрытой информации,
- В договоры с контрагентами введены положения о неразглашении коммерческой тайны.

2. Соблюдена процедура применения санкций, а именно:

- Составлен акт о разглашении конфиденциальной информации,
- Запрошено письменное объяснение,
- Составлен акт, если работник объяснение не предоставил,
- Работника уволили в течение месяца с момента выявления нарушения,
- Есть письменные доказательства факта разглашения.

3. Работники предупреждены о применении аудио- и видеоконтроля за их действиями и разговорами.

4. Доказательства разглашения конфиденциальной информации в электронной переписке и в интернете заверены нотариально.

Если все эти условия выполнены, защитить права обладателя конфиденциальной информации в суде будет намного проще.

8. Источники

1. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне», http://www.consultant.ru/document/cons_doc_LAW_48699/
2. Служебная и коммерческая тайна – нюансы, http://rusjurist.ru/tajna/kommercheskaya_tajna/sluzhebnyaya_i_kommercheskaya_tajna_nyuansy/
3. 12 неприятных сюрпризов от уволенного работника. Как сделать так, чтобы вас не застали врасплох, <http://e.tspor.ru/article.aspx?aid=473831>
4. Как помешать разглашению конфиденциальной информации, <https://www.tspor.ru/article/2177-qqe-17-m4-04-04-2017-kak-pomeshat-razglasheniyu-konfidentsialnoy-informatsii>

5. Работника подозревают в разглашении коммерческой тайны. Четыре ситуации, которые закончатся увольнением, <http://e.tspor.ru/article.aspx?aid=403198>
6. Коммерческая тайна. Принципы защиты секретов от конкурентов, <http://e.tspor.ru/article.aspx?aid=529962>
7. В каком случае удастся наказать за разглашение конфиденциальной информации, <https://www.tspor.ru/article/2287-nakazat-za-razglashenie-konfidentsialnoy-informatsii>
8. Обзор судебной практики по делам, связанным с разглашением коммерческой тайны, <http://naar.ru/articles/obzor-sudebnoi-praktiki-po-delam-sviazannym/>
9. Использование бесплатной почты может стать поводом для увольнения, <http://e.tspor.ru/article.aspx?aid=574203>
10. Подробно: КС защитил тайну переписки по электронной почте, <http://www.ksrf.ru/ru/News/Pages/ViewItem.aspx?ParamId=3360>
11. Работник в иске сослался на смс-переписку. Примет ли суд такое доказательство, <http://e.tspor.ru/article.aspx?aid=473835>
12. Конкуренты узнали о тайнах компании. Привлекаем виновника к ответственности, <http://e.tspor.ru/article.aspx?aid=529966>
13. Доказательства в трудовых спорах. Правила подготовки материалов для суда, <http://e.tspor.ru/article.aspx?aid=529970>
14. Обязательство о неразглашении коммерческой тайны, <http://e.tspor.ru/article.aspx?aid=443219>
15. У компании нет доказательств вины работника. Чем поможет нотариус, <http://e.tspor.ru/article.aspx?aid=529969>
16. Протокол осмотра интернет-страницы, <http://e.tspor.ru/article.aspx?aid=598063>

Аналитик и автор исследования: Баублис Борис Петрович,
главный аналитик Фонда содействия цифровой трансформации «Атом»,
<https://fondatom.ru>

Актуальные материалы по этой и другим темам вы сможете найти на сайте <https://fondatom.ru>