Электронный журнал

Юрист компании

Компания / Корпоративные отношения

Как защитить корпоративные секреты. Готовые инструкции для коллег

Андрей Слепов
партнер, руководитель практики трудового и миграционного права московского офиса БАЙТЕН БУРКХАРДТ

Главное в статье

1	**2**	**3**
Режим коммерческой тайны ограничит доступ к документам	Работника можно привлечь к уголовной ответственности	Работодатель вправе контролировать доступ сотрудников в интернет
4	**5**	**6**
Компания может просматривать почту сотрудников	Работников не нужно предупреждать об установке видеокамер	Если сотрудник увольняется, его доступ к системам нужно технически ограничить

Мы нашли способы, как победить воровство информации сотрудниками. В статье — готовая инструкция, которая защитит данные компании, ее клиентов и технологии.

Введите режим коммерческой тайны

Режим коммерческой тайны ограничит доступ сотрудников к документам. А если работник нарушит режим и разгласит тайну, его гораздо проще привлечь к ответственности, в том числе уголовной. Сотрудники это понимают и реже действуют во вред компании.

---

98 ФЗ Ч. 1 ст. 10 Федерального закона от 29.07.04 № 98-ФЗ «О коммерческой тайне»

Что и как оформить.

Чтобы установить режим коммерческой тайны, выполните пять шагов.[98 ФЗ] Если не будет хотя бы одного, скорее всего суды посчитают, что режим коммерческой тайны не установлен, и наказать работника не сможете.

Со всеми документами знакомьте работников под подпись.

1

---

98 ФЗ-1 Ст. 5 Федерального закона от 29.07.04 № 98-ФЗ

Подготовьте перечень информации, которую относите к коммерческой тайне. Его можно прописать в положении о коммерческой тайне или прямо в трудовом договоре. К коммерческой тайне можно отнести любую информацию, за исключением указанной в законе.[98 ФЗ-1] Например, клиентские базы, ценовую политику, чертежи продукции, сведения о поставщиках. Чем шире перечень, тем проще доказать, что сотрудник что-то разгласил.

2

Пропишите в локальном акте ограничения при работе с коммерческой тайной. Запретите использовать такую информацию для личных целей. Определите, как следует использовать, хранить и маркировать документы и другие носители с информацией, которая составляет коммерческую тайну.

Установите, что любые документы с коммерческой тайной следует хранить в сейфах или шкафах, тумбочках, которые закрываются на ключ. Компания обязана обеспечить работников такой мебелью. Ценные файлы можно защитить паролем, а доступ к ним — ограничить.

Можно указать, что с коммерческой тайной разрешается работать только со служебного компьютера.

3

В локальном акте укажите, что работодатель ведет учет работников и контрагентов, которые получили доступ к информации. Для этого можно использовать специальные журналы. В них нужно фиксировать, у кого в данный момент находится информация с коммерческой тайной. Так будет проще отследить утечку.

ВС 2 П. 43 постановления Пленума ВС РФ от 17.03.04 № 2

Для учета работников включите в локальный акт перечень должностей, которые предполагают доступ к коммерческой тайне. Тогда в случае спора в суде сможете доказать, что сведения, которые разгласил работник, стали известны ему в связи с исполнением трудовых обязанностей.[ВС 2]

Включите в приложение к локальному акту также форму журнала для учета контрагентов, которым передана коммерческая тайна, и форму акта приемки-передачи информации.

4

Предусмотрите в локальном акте, что все носители с коммерческой тайной нужно грифовать. То есть наносить на них надпись «Коммерческая тайна». Также в грифе следует указывать полное наименование и местонахождение компании, которой принадлежит коммерческая тайна.

2–4 Решение Тверского районного суда города Москвы от 24.08.15 по делу № 2–4747/2015

Если на документах не окажется грифа, все равно есть шанс привлечь работника к ответственности, если остальные шаги выполнены. В таком случае суд поддержит работодателя.[2–4] Иначе работник мог бы легко обойти запрет на разглашение коммерческой тайны — просто переписать текст загрифованного документа.

Например, компания уволила работника за разглашение коммерческой тайны, которая стала ему известна в связи с исполнением трудовых обязанностей. Сотрудник оспорил увольнение в суде. Он указал, что из-за большой нагрузки не успел сделать работу в течение дня. Поэтому отправил базу клиентов себе на личную почту, чтобы доделать работу дома. Также истец указал, что на документах, которые он сам себе отправил, не было грифа.

Суд поддержал работодателя. Истец был ознакомлен со всеми локальными актами о режиме коммерческой тайны в компании. Несмотря на это, он отправил базу клиентов на ящики электронной почты, которые не находятся под контролем работодателя.

Суд отклонил ссылку на то, что у отправленных файлов не было грифа «Коммерческая тайна». Истец сам создал эти файлы на основе файлов, которые были размещены в системе работодателя с отметкой о конфиденциальности.

5

В трудовой договор и должностную инструкцию включите оговорку о том, что работник имеет доступ к коммерческой тайне и обязуется не разглашать ее.

---

81 ТК П. 5 ч. 1 ст. 81 ТК РФ

Как наказать работника.

Если работник нарушил режим коммерческой тайны, но не разгласил ее, его можно привлечь к дисциплинарной ответственности или уволить, если у него есть неснятое и непогашенное взыскание.[81 ТК]

---

81 ТК-1 П. 6 ч. 1 ст. 81 ТК РФ

183 УК Ч. 2 и 3 ст. 183 УК РФ

1–2 Приговор Лефортовского районного суда города Москвы от 18.08.15 по делу № 1–214/2015

1–6 Приговор Перовского районного суда г. Москвы от 02.09.14 по делу № 1–602/2014

В случае разглашения работника можно уволить[81 ТК-1] и потребовать возбудить в отношении него уголовное дело.[183 УК] Чаще всего сотрудников привлекают к уголовной

ответственности, если они сообщили данные о клиентах компании третьим лицам за вознаграждение.[1–2]

Например, работник скопировал клиентскую базу компании на флешки, а потом предложил конкуренту ее купить. Чтобы подтвердить достоверность базы, работник отправил конкуренту информацию о некоторых клиентах. В отношении нарушителя возбудили уголовное дело. В дальнейшем суд признал сотрудника виновным в разглашении коммерческой тайны и назначил ему штраф в 50 тыс. рублей.[1–6]

К материальной ответственности привлечь работника на практике сложно. Причина — доказать прямой ущерб от разглашения коммерческой тайны очень трудно.

Суды признают, что работодатель вправе просматривать почту с корпоративного ящика

Контролируйте доступ в интернет

Интернет — один из основных каналов утечки информации. Чтобы снизить риск, пропишите в локальных нормативных актах запрет использовать служебный доступ в интернет в личных целях.

Организация может ввести систему фильтрации веб-трафика. С помощью этой системы можно заблокировать доступ работников к определенным сайтам, например социальным сетям, видеохостингам, контролировать время работы в интернете, просматривать историю браузера любого сотрудника. Задача юриста — подготовить приказ о введении такой системы. С приказом ознакомьте работников под подпись.

Проверяйте электронную почту сотрудников

Работник может использовать корпоративную почту, чтобы пересылать секретные документы или вести переписку якобы от имени компании.

33–5 Апелляционное определение Московского городского суда от 14.02.17 по делу № 33–5694/2017

Укажите в локальных нормативных актах, что работодатель вправе проверять электронную почту сотрудников. Пропишите запрет на использование корпоративной почты в личных целях. Тогда сотрудник не сможет сослаться, что компания нарушила тайну переписки и вмешалась в его частную жизнь. Суды признают, что работодатель вправе просматривать почту с корпоративного ящика.[33–5]

33–1 Апелляционное определение Московского городского суда от 08.09.14 по делу № 33–18661/2014

Более того, компания вправе читать письма работника, если он отправил файлы через личную почту, но с рабочего компьютера, и система это автоматически зафиксировала. Суды считают такие действия законными.[33–1]

Чтобы подтвердить отправку документов, можно заверить у нотариуса снимки экрана или составить акт осмотра электронной почты работника. Если будете проводить осмотр, рекомендуется привлечь двух-трех специалистов, включая кадровика и специалиста ИТ. В случае судебного спора их можно использовать как свидетелей.

Установите видеокамеры

Если установить видеокамеры, это поможет снизить риск уничтожения, кражи документов или имущества. Видеокамеры помогут удержать сотрудников от противоправных действий.

Разработайте локальный нормативный акт, например положение о системе видеонаблюдения. В нем укажите цели наблюдения, сроки и порядок хранения данных, круг лиц, у которых будет доступ к видеозаписям. Пропишите в положении, что в помещениях с видеокамерами нужны предупредительные знаки. Например, наклейки на стенах с надписью «Ведется видеонаблюдение».

2–6 Решение Железногорского городского суда Курской области от 16.01.17 по делу № 2–63/2017 (2–2465/2016)

Получите письменное согласие у работников на обработку видеозаписей. Форму такого согласия можно подготовить отдельно или включить в трудовой договор. Если не сделать этого, есть риск, что в суде использовать видеозапись не получится. В практике есть

случаи, когда признается, что на видеозаписи зафиксированы биометрические персональные данные работников. А такие персональные данные, по общему правилу, можно обрабатывать только с письменного согласия сотрудников. Если согласия нет, суд может признать видеозапись недопустимым доказательством.[2–6]

РКН Разъяснения Роскомнадзора от 30.08.13 «О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностям их обработки»

33–4 Апелляционное определение Московского городского суда от 08.12.16 по делу № 33–49698/2016

Нужно ли уведомлять работников об установке видеокамер — спорный вопрос. Роскомнадзор разъяснил, что компания должна предупредить работников за два месяца до введения видеонаблюдения на основании статьи 74 Трудового кодекса.[РКН] Но суды чаще говорят об обратном — установка видеокамер не меняет условия трудового договора, которые определили стороны. Поэтому уведомлять работников заранее не нужно.[33–4] Если есть возможность — предупредите работников. Если нет — скорее всего это не повлияет на допустимость видеозаписей в качестве доказательства в суде.

Ограничьте доступ к корпоративным системам

Если поймали сотрудника на нарушении и собираетесь уволить, ограничьте его доступ к корпоративным системам. Когда сотрудник знает об увольнении, гораздо выше риск, что он захочет навредить компании.

---

243 ТК П. 3 ч. 1 ст. 243 ТК РФ

В суде удастся взыскать с работника только прямой ущерб, но не упущенную выгоду.[243 ТК] Фактически это значит, что компания не получит никакой компенсации, если работник, к примеру, удалит или скопирует важные файлы. Поэтому нужно создать условия, при которых сотрудник просто не сможет навредить.

Если есть подозрение, что сотрудник ведет параллельный бизнес, проверьте открытые источники: базы данных и социальные сети. Вероятно, он будет указан как член органов управления или работник другой компании.

Не прописывайте в трудовых договорах точное оборудование и системы, к которым работник должен иметь доступ для выполнения обязанностей. Иначе ограничить доступ к ним будет сложнее. Работник сможет сослаться на то, что работодатель незаконно не допускает его к работе в соответствии с трудовым договором.

Установите в трудовом договоре, что работник при увольнении в определенный срок обязан передать работодателю все его имущество и служебную информацию. В том числе пароли доступа к корпоративным ресурсам. Срок должен быть достаточным, чтобы проверить достоверность паролей.

Укажите в локальных актах, что права доступа сотрудника к системам можно менять. Это позволит технически ограничить копирование и удаление файлов с учетной записи работника.

Включите во внутренние документы ограничения на использование флеш-карт и других внешних носителей. Обеспечьте соблюдение этих ограничений технически. Также полезно прописать, что ИТ-специалисты обязаны регулярно создавать резервные копии электронной переписки и баз данных.

Компания потеряет секреты, если не будет их защищать

К нам обратилась компания, которая занималась разработкой программного обеспечения. Работодатель никак не защищал информацию и стремился создать максимально комфортные условия для сотрудников. Многие работали удаленно и с личных девайсов. У всех программистов был доступ к исходному коду продукта. Его можно было копировать на флешки и хранить в облачных сервисах.

Потом один из ключевых работников уволился. Стало известно, что он работает у основного конкурента компании. Это вызвало подозрения, что сотрудник может использовать информацию, которую получил в компании.

С помощью ИТ-экспертов и юристов провели внутреннее расследование, и подозрение подтвердилось. Перед увольнением работник скачал со своего компьютера исходный код и другие материалы. Компания не могла подтвердить этот факт документально, не принимала формальных мер по защите информации. Не было даже подтверждения, что компьютер предоставлен для работы именно этому сотруднику.

Когда об этом узнал конкурент компании, он отказался использовать код, который предоставил нарушитель. То есть убытков удалось избежать, но информация все равно оказалась раскрытой. Потом работник согласился вернуть все карты памяти с кодом, так как ему грозила уголовная ответственность.

Компания сделала выводы и приняла меры, чтобы защитить корпоративные секреты.

Юристы разработали соответствующие локальные акты и ознакомили с ними работников. При выдаче девайсов работников стали составлять специальный акт, чтобы закрепить устройство за конкретным человеком. Были приняты и технические меры: ограничение доступа к ресурсам компании, облачным хранилищам, запрет использовать ПО работодателя на личных девайсах.

Мария Гнутова,
старший консультант АЛРУД

Скачать документ в формате docx

Общество с ограниченной ответственностью «Альфа»

ПРИКАЗ №64
о введении контроля за доступом к сети Интернет

г. Москва 11.09.2017

Запретить работникам использовать доступ к сети Интернет на служебных компьютерах в целях, которые не связаны с должностными обязанностями.

Начальнику отдела информационной безопасности Андрееву А.А. обеспечить внедрение системы фильтрации веб-трафика на всех компьютерах компании в срок до 15.09.2017.

Начальнику отдела кадров Петрову П.П. довести до сведения работников настоящий приказ в срок до 12.09.2017.

Контроль за исполнением настоящего приказа возложить на начальника отдела информационной безопасности Андреева А.А.

Генеральный директор _____ /Иванов Иван Иванович

С настоящим приказом ознакомлены:

_____ /Андреев Андрей Андреевич
подпись

«11» сентября 2017 г.

_____ /Петров Петр Петрович
подпись

«11» сентября 2017 г.

Скачать документ в формате docx

Согласие работника
на обработку персональных данных

Я, Иванов Иван Иванович, зарегистрированный по адресу: г. N, ул. 9 Мая, дом 21, квартира 101, имеющий паспорт гражданина РФ 0000 № 000000, выданный 00.00.0000г. Отделом УФМС по N-скому району города N,

даю согласие ООО «Омега», расположенному по адресу: г. N, ул. Октябрьская, дом 9, с целью предотвращения правонарушений и преступлений, причинения вреда жизни и здоровью людей, а также имуществу ООО «Омега» на обработку моих персональных данных:

моих изображений на фотографиях и видеозаписях как в электронном виде, так и на материальных носителях информации.

Я согласен на обработку моих биометрических персональных данных путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (предоставления, доступа), блокирования, удаления, уничтожения персональных данных с использованием средств автоматизации или без использования таких средств.

Обработка вышеуказанных данных может быть поручена ООО «Альфа», расположенному по адресу: г. N, ул. Февральская, дом 26.

Срок действия моего согласия: в период действия трудового договора, а также в течение 30 дней после его прекращения.

Настоящее согласие может быть отозвано путем направления мной соответствующего запроса на адрес ООО «Омега».

Дата: 11.10.2017 г.

Подпись: _____ /Иванов И.И./

(подпись и собственноручная расшифровка подписи)