

ПАМЯТКА:

## ПРОБЛЕМЫ ЛЕГИТИМИЗАЦИИ ПРИ ИСПОЛЬЗОВАНИИ DLP-СИСТЕМ



### 1. ПРАВА И ОБЯЗАННОСТИ СОТРУДНИКА НА РАБОЧЕМ МЕСТЕ

#### Сотрудник имеет право на:

- неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ст. 23 Конституции РФ);
- тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23 Конституции РФ).

Причем, тайна переписки должна соблюдаться вне зависимости от того, содержится в ней или нет информация, содержащая тайну частной жизни, личную или семейную тайну (п. 6 Постановления Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)»).

Собирать, хранить и использовать эти данные можно лишь с согласия сотрудника (ч.1 ст. 24 Конституции РФ, п. 1 ст. 152.2 ГК РФ), а нарушение прав влечет уголовную ответственность (ст. 137-138 Уголовного кодекса РФ).

С точки зрения трудового законодательства, человек, являющийся работником организации, обязан посвящать рабочее время исполнению трудовых обязанностей, а работодатель обязан учитывать фактически отработанное время (ст. 91 ТК РФ) и вправе контролировать количество и качество работы сотрудника (п. 1 ст. 86 ТК РФ), а также его рабочее место (ст. 209 ТК РФ). Более того, в отношении своего имущества работодатель может совершать любые действия, не противоречащие закону (п. 2 ст. 209 ГК РФ), в частности, устанавливать на оборудование системы контроля.

Исходя из этого, использовать предоставленные нанимателем средства работник должен исключительно для выполнения своей трудовой функции. Выполнение личных задач на корпоративных ресурсах может трактоваться как нарушение трудовой дисциплины.



## 2. ФИКСАЦИЯ ПРАВ И ОБЯЗАННОСТЕЙ РАБОТОДАТЕЛЕМ

Обязанность работника использовать информационные ресурсы нанимателя и его технические средства исключительно для выполнения должностных обязанностей фиксирует трудовой договор.

В нем должен содержаться прямой запрет на хранение личной информации на корпоративных ресурсах (ПК и файловые хранилища) и передачу ее по корпоративным каналам связи (электронная почта, мессенджер и др.).

Такой же запрет должен быть наложен на хранение корпоративной информации на личных ресурсах и ее передачу с использованием личных средств

Необходимо закрепить эти положения в локальных нормативных правовых актах организации. Например, в Правилах внутреннего трудового распорядка или должностной инструкции сотрудника они могут быть сформулированы как:

- «Предоставляемые работнику для выполнения трудовых обязанностей ЭВМ и другая техника, имеющая доступ к сети Интернет, а также предоставленный работнику корпоративный адрес электронной почты должны использоваться работником исключительно для получения и передачи информации рабочего характера в рамках должностных обязанностей. Пользование ЭВМ и техникой в личных целях запрещается».
- «То же распространяется на средства видеоконференцсвязи, мессенджеры и иные средства связи при условии, что для их использования в служебных целях формируются отдельные аккаунты работников».

Кроме того, в должностной инструкции сотрудников различных категорий можно отразить запрет на использование отдельных информационных ресурсов в рабочее время. К таким ресурсам могут относиться, например, развлекательные сайты, сервисы поиска работы, публичные файлообменные сервисы.



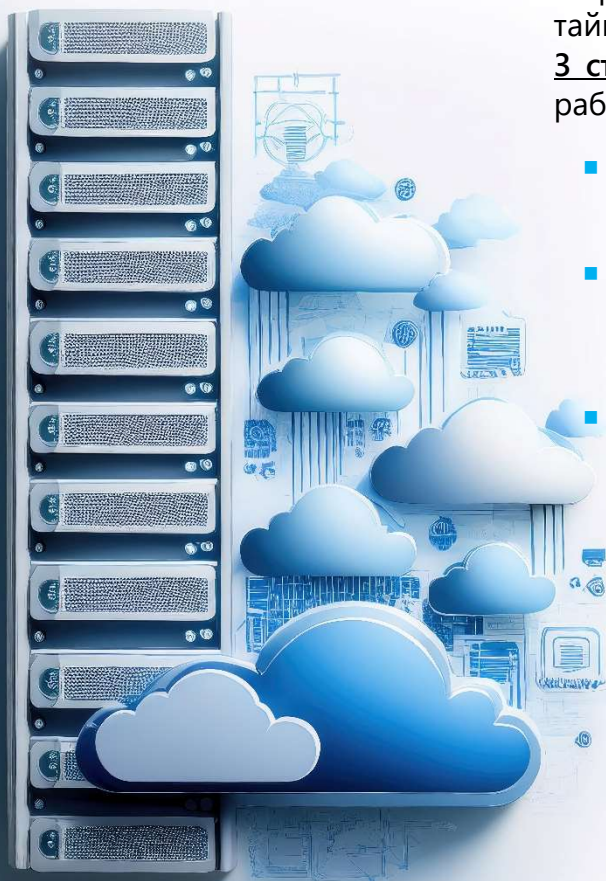
### 3. ОБЯЗАННОСТИ РАБОТОДАТЕЛЯ В ЧАСТИ КОНТРОЛЯ

По законодательству РФ работодатель уполномочен контролировать сотрудников, обеспечивая информационную безопасность в следующих направлениях:

- ▶ защита персональных данных  
(ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»);
- ▶ защита банковской тайны  
(ФЗ от 02.12.1990 № 395-1 «О банках и банковской деятельности»);
- ▶ защита информации, содержащейся в государственных информационных системах  
(ФЗ от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Приказ ФСТЭК от 11.02.2013 № 17);
- ▶ защита информации на объектах критической информационной инфраструктуры  
(ФЗ от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ», Приказ ФСТЭК от 25.12.2017 № 239);
- ▶ защита коммерческой тайны  
(ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне»).

Работодатель уполномочен регулировать использование сотрудниками информации, составляющей коммерческую тайну (ч. 1 ст. 10 Закона «О коммерческой тайне»). Часть 3 статьи 11 Закона «О коммерческой тайне» обязывает работника:

- выполнять установленный работодателем режим коммерческой тайны;
- не разглашать эту информацию и не использовать ее в личных целях без согласия владельцев даже после прекращения действия трудового договора;
- передать работодателю материальные носители с данной информацией при прекращении или расторжении трудового договора.





## 4. ПОРЯДОК ВВЕДЕНИЯ ЛЕГАЛЬНОГО КОНТРОЛЯ

### ШАГ 1

Внесите упомянутые правки в трудовые договоры и должностные инструкции сотрудников, подготовьте или актуализируйте внутренние нормативные акты: Правила внутреннего распорядка, Положение о коммерческой тайне, Приказ о неразглашении информации, содержащей коммерческую тайну. Так вы установите режим использования информационных ресурсов и технических средств компании.

### ШАГ 2

Получите у всех сотрудников подписанные обязательства о неразглашении конфиденциальной информации и соблюдении правил ее обработки по форме, приведенной в приложении к этой статье.

### ШАГ 3

Получите от каждого работника письменное согласие на ознакомление работодателя со сведениями о частной жизни работника, если они вскроются в ходе осуществляемого с использованием программных и технических средств или без такового контроля использования ресурсов, техники и хранилищ информации компании, а также соблюдения правил внутреннего распорядка и выполнения должностных обязанностей.

### ШАГ 4

Введите локальным актом DLP-систему в эксплуатацию, отразите цели ее использования:

- контроль соблюдения правил внутреннего трудового распорядка и должностных обязанностей;
- выполнение требований законодательства и иных нормативных актов по обеспечению конфиденциальности информации и коммерческой тайны;
- контроль использования предоставленных нанимателем технических средств.

Также пропишите порядок использования DLP-системы перечень лиц, которые будут ее использовать и обязательно отразите цели, для которых будет применяться эта система.

Учитывая эти уведомления, запреты и обязательства сотрудников по их соблюдению, компания не может и не должна знать, что нарушит право человека на тайну личной переписки, если прочтет его рабочее сообщение. То есть действия работодателя в случае получения информации о частной жизни сотрудника неумышленны. Кроме того, об отсутствии нарушения со стороны работодателя говорит согласие работника на ознакомление со сведениями его частной жизни в случае их наличия в корпоративной информационной системе.

В пользу легальности использования DLP говорит и специфика работы этих систем: как правило, анализирует перехваченные данные не человек, а сама программа, которая к уголовной ответственности привлечена быть не может (ст. 19 УК РФ).

## 5. СУДЕБНАЯ ПРАКТИКА



### **Апелляционное постановление Кемеровского областного суда от 05.03.2021 по делу № 22-604/2021.**

#### **Кратко:**

Сотрудник предприятия сохранил данные, составляющие коммерческую тайну, на личный флеш-накопитель. Нарушение обнаружено с помощью DLP.

На предприятии был подготовлен полный пакет локальных актов по защите коммерческой тайны, работники были с ними ознакомлены. Суд установил, что сохранение на внешний незарегистрированный носитель информации, составляющей коммерческую тайну, любыми сотрудниками предприятия и вне зависимости от цели и наступления последствий, составляет преступление, предусмотренное ст. 183 УК РФ.

### **Определение Второго кассационного суда общей юрисдикции от 14.05. 2024 по делу № 2-16587/2022.**

#### **Кратко:**

Сотрудница регулярно опаздывала на работу, не выполняла поручения, рабочее время проводила на сайтах, не связанных с выполнением ее обязанностей. Кроме того, работница разместила конфиденциальные данные в незащищенном облаке.

Ее действия зафиксированы DLP-системой. За нарушения сотрудница подверглась 6 дисциплинарным взысканиям.

В Правилах внутреннего трудового распорядка предприятия был зафиксирован запрет на посещение сайтов, не связанных с работой и размещение данных на незащищенных ресурсах. Использование внешних хранилищ для корпоративной информации также было запрещено Положением о коммерческой тайне. Сотрудники предприятия были ознакомлены с этими актами. Суды трех инстанций признали действия компании законными.



**Апелляционное определение Судебной коллегии  
по гражданским делам Московского городского суда  
от 08.07.2024 по делу № 33-24525/2024.**

**Кратко:**

ИТ-специалист регулярно в рабочее время посещал сайты, не связанные с его должностными обязанностями. Кроме того, для доступа к ним он создал аккаунты с корпоративной почтой. Этот факт зафиксирован DLP-системой и послужил причиной дисциплинарного взыскания.

Сотрудник обратился в суд, чтобы оспорить действия работодателя.

Компания предоставила суду скриншоты системы и полный комплект внутренних документов, в том числе положение о контроле информационных ресурсов, правила внутреннего распорядка.

В требованиях сотрудника и жалобе на решение суда было отказано.



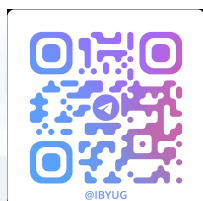
**Апелляционное постановление Суда Еврейской автономной  
области от 31.10.2023 по делу № 22-541/2023.**

**Кратко:**

Начальница ИБ-отдела государственной организации целенаправленно находила, читала, сохраняла, передавала коллегам и обсуждала с ними личную переписку сотрудников в корпоративном мессенджере.

Сотрудники не давали работодателю согласия на ознакомление со сведениями из своей частной жизни в случае их обнаружения при контроле информационных ресурсов и оборудования работодателя. Использование мессенджера для служебной коммуникации не было регламентировано.

Суд признал указанную сотрудницу виновной в преступлениях, предусмотренных ч. 2 ст. 2 138 УК РФ и ч. 3 ст. 278 УК РФ и приговорил ее к 2 годам лишения свободы условно. Апелляционный суд оставил это решение в силе.



**Обязательство**  
**о неразглашении конфиденциальной информации и соблюдении правил ее обработки**

Я,

---

(фамилия, имя, отчество)

---

(должность, наименование структурного подразделения, организация)

предупрежден (а), что вследствие наличия трудовых или иных отношений с КОМПАНИЕЙ на период действия данных отношений мне может быть предоставлен доступ к сведениям конфиденциального характера, включая персональные данные и информацию, составляющую коммерческую тайну (далее – Конфиденциальные сведения).

1. Настоящим добровольно принимаю на себя обязательства:

- 1.1. Не разглашать Конфиденциальные сведения, доверенные или ставшие мне известными вследствие наличия трудовых или иных отношений с КОМПАНИЕЙ.
- 1.2. Не сообщать устно или письменно, не передавать третьим лицам и не раскрывать публично Конфиденциальные сведения без соответствующего разрешения руководителя структурного подразделения и подразделения КОМПАНИИ, ответственного за защиту информации.
- 1.3. Прекратить обработку ставших мне известными Конфиденциальных сведений в случае расторжения со мной трудового договора, освобождения от замещаемой должности, увольнения или прекращения отношений иным образом.
- 1.4. Выполнять требования действующего законодательства Российской Федерации, приказов, инструкций, положений и иных нормативных актов КОМПАНИИ, по обеспечению информационной безопасности.
- 1.5. В случае попытки посторонних лиц получить Конфиденциальные сведения, немедленно сообщать об этом непосредственному руководителю.
- 1.6. Не использовать, прямо или косвенно, Конфиденциальные сведения для осуществления деятельности, не связанной с выполнением трудовых или иных отношений с КОМПАНИЕЙ, для получения выгоды.
- 1.7. Обращивать Конфиденциальные сведения только на технических средствах обработки, хранения и передачи информации, предоставленных КОМПАНИЕЙ, либо разрешенных для обработки Конфиденциальных сведений подразделением по информационной безопасности КОМПАНИИ.
- 1.8. Не устанавливать и не использовать сторонние программные и технические средства, не предусмотренные КОМПАНИЕЙ.
- 1.9. Незамедлительно сообщать непосредственному руководителю об утрате носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению Конфиденциальных сведений.
- 1.10. При прекращении трудовых отношений с КОМПАНИЕЙ, все материальные носители, содержащие Конфиденциальные сведения (флеш-накопители, компакт-диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы и пр.), которые находились в моем распоряжении, передать непосредственному руководителю.
- 1.11. Использовать информационные ресурсы КОМПАНИИ и переданные КОМПАНИЕЙ в мое распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения должностных обязанностей или обязанностей, определенных иными отношениями с КОМПАНИЕЙ.

2. Я согласен на проведение со стороны КОМПАНИИ контроля использования мной информационных ресурсов КОМПАНИИ, а также использования мной технических средств обработки, хранения и передачи информации, соблюдения мной требований нормативных актов КОМПАНИИ по обеспечению информационной безопасности.

3. Я уведомлен о том, что на территории КОМПАНИИ осуществляется видеосъемка.

4. Я подтверждаю, что не имею никаких обязательств перед какими-либо физическими или юридическими лицами, которые входят в противоречие с моими обязанностями по осуществлению отношений с КОМПАНИЕЙ или которые ограничивают исполнение мной должностных обязанностей сотрудника КОМПАНИИ.

5. Я прошел инструктаж по вопросам информационной безопасности и ознакомлен с документами по обеспечению информационной безопасности, действующими в КОМПАНИИ, в том числе с требованиями к защите персональных данных.

6. Мне известно, что нарушение требований по обеспечению информационной безопасности может повлечь административную, гражданско-правовую, уголовную и дисциплинарную (вплоть до увольнения) ответственность в соответствии с действующим законодательством Российской Федерации.