searchinform.ru

Правовые аспекты применения DLP

SEARCHINFORM
INFORMATION SECURITY

Moscow Digital School

[руководство по защите от внутренних угроз]

Информационная безопасность

О чем этот документ

Использование всех технических возможностей DLP-системы – это только половина защиты. Недостаточно просто вовремя выявить нарушение со стороны работника. Необходимо грамотно его расследовать и наказать виновника, чтобы подобные инциденты не повторялись. Но не все работодатели готовы идти до конца и доводить дело до суда. По данным исследования «СёрчИнформ», в 2020 году только 12% российских компаний обращались в суд, чтобы возместить ущерб от действий инсайдеров.

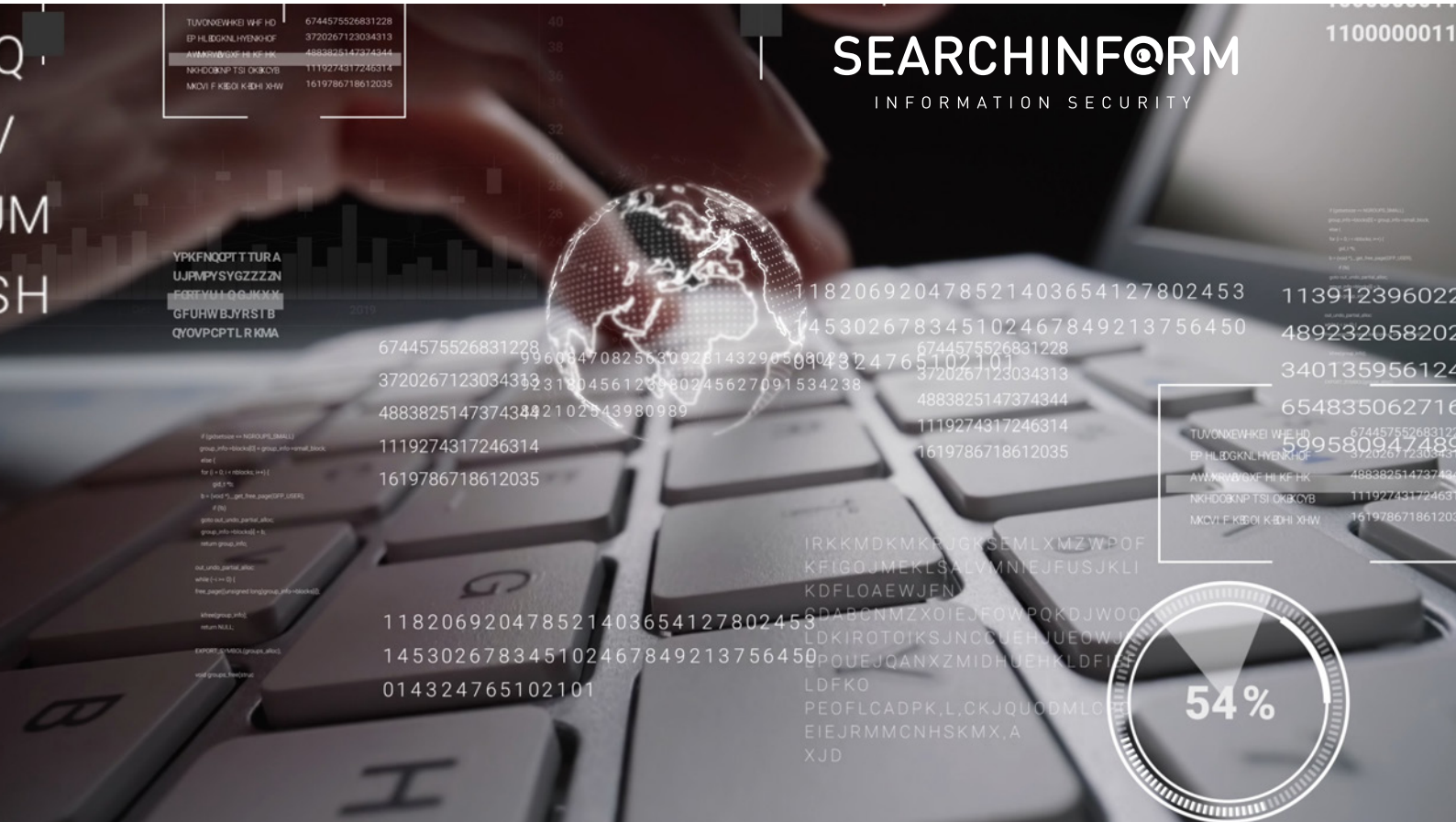
Причина простая: работодателю сложно документально обосновать и доказать в таких делах связь между действиями работника и причинённым ущербом. Но если знать, как правильно фиксировать нарушения и работать с этой информацией, такой проблемы не возникнет. Вместе с экспертами Ассоциации юристов России и Moscow Digital School мы проанализировали место ИБ-инструментов в юридическом поле и сделали выводы, как применять их для защиты законных интересов компании.

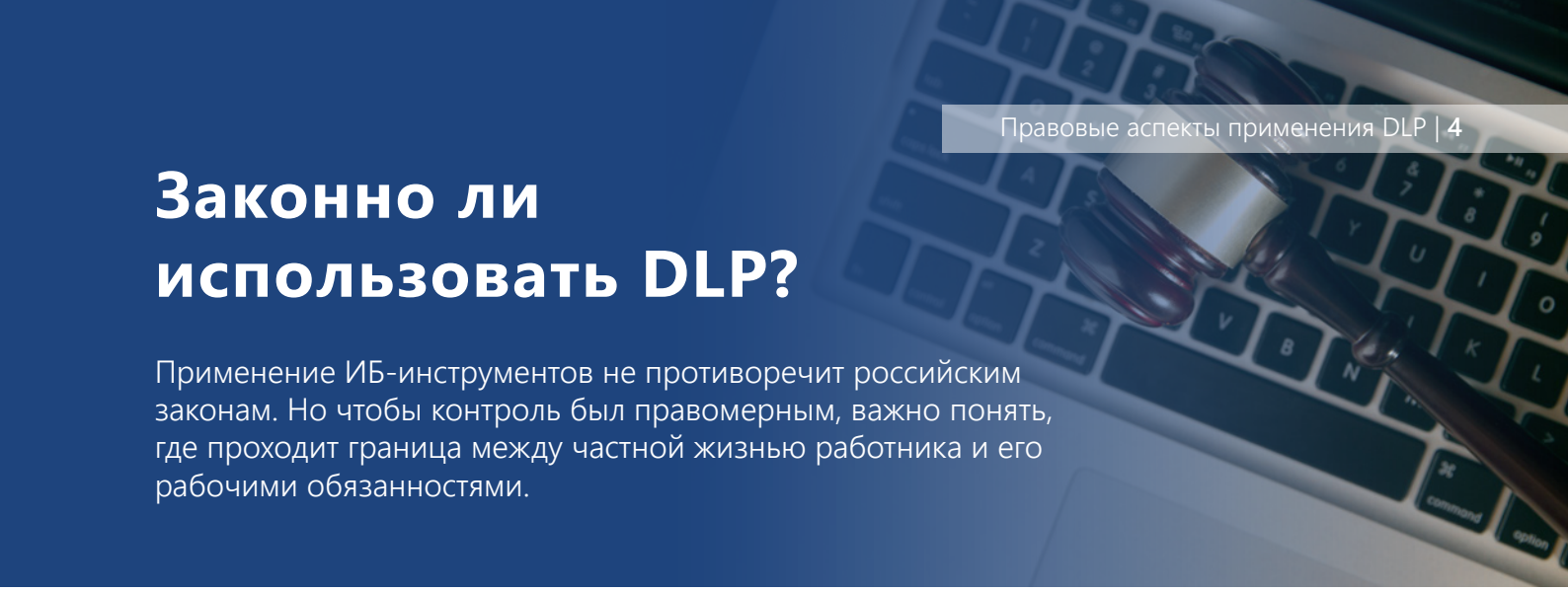
В этой книге мы:

- Разберём, законно ли использовать DLP-систему в бизнесе.
- Дадим рекомендации, как грамотно оформить внедрение DLP.
- Расскажем, зачем нужна система контроля и как правильно использовать выявленные инциденты в суде.
- Проиллюстрируем советы реальными примерами из ИБ-практики компаний.

SEARCHINFORM
INFORMATION SECURITY

Содержание





Законно ли использовать DLP?

Применение ИБ-инструментов не противоречит российским законам. Но чтобы контроль был правомерным, важно понять, где проходит граница между частной жизнью работника и его рабочими обязанностями.

Технически в вопросах контроля за сотрудниками закон на стороне работодателя, прежде всего об этом говорит Трудовой кодекс:

- ✓ Сотрудник в рабочее время обязан трудиться (**ст. 91 ТК РФ**).
- ✓ Работодатель имеет право требовать от работника исполнения трудовых обязанностей (**ст. 22 ТК РФ**), а без соответствующего контроля сделать это практически нереально.
- ✓ Работодатель организует сотруднику условия труда и снабжает необходимым оборудованием (**ст. 209 ТК РФ**), так что может распоряжаться своим имуществом по собственному усмотрению (**ч. 2 ст. 209 ГК РФ**). И в том числе устанавливать на него системы контроля.

SEARCHINFORM
INFORMATION SECURITY

Еще один довод в пользу компаний: **по законодательству вы** не только вправе, но и **обязаны контролировать сотрудников**, чтобы защитить персональные данные, банковскую и коммерческую тайну, информацию в государственных информационных системах, а также данные в АСУ на объектах критической инфраструктуры. Это закреплено в федеральных законах: «О персональных данных», «О банках и банковской деятельности», «Об информации, информационных технологиях и о защите информации», «О коммерческой тайне» – и других нормативных актах.

В конце концов, анализировать действия сотрудника будете не вы, а программа, которую невозможно привлечь к уголовной ответственности (ст. 19 Уголовного кодекса).

При этом неправильное внедрение ПО для контроля – без должного юридического сопровождения и в тайне от коллектива – может обернуться против компании.

Если посмотреть на это с точки зрения законодательства, такое использование DLP-систем предполагает ограничение прав работника на:

- полную достоверную информацию об условиях труда (ст. 22 ТК РФ);
- неприкосновенность частной жизни (ст. 23 Конституции РФ);
- тайну переписки в той мере, в которой система позволяет следить за перепиской работника по электронной почте и в онлайн-мессенджерах (ст. 24 Конституции РФ);
- защиту персональных данных, поскольку любая относящаяся к работнику информация охраняется в качестве его персональных данных;
- на соблюдение иных видов тайн – врачебной, адвокатской и т.п., если в результате негласного использования DLP-систем работодателю станут известны соответствующие факты.

При использовании системы компания может нечаянно раскрыть секреты не только своих работников, но и иных лиц, с которыми они состоят в личной переписке.

Елена Мышливец – эксперт Moscow Digital School:

Moscow Digital School

Нарушение указанных выше прав работников и иных лиц может привести не только к гражданско-правовой или административной, но и к уголовной ответственности. Например, ст. 5.53, 13.11 Кодекса РФ об административных правонарушениях, ст. 137, 138, 183, 272 УК РФ.

Чтобы исключить подобные проблемы, следует зафиксировать в трудовом контракте, что работник может использовать информационные ресурсы нанимателя и его технические средства **исключительно для выполнения должностных обязанностей**.

Там же нужно прописать запрет на хранение личной информации на корпоративных ресурсах (ПК и файловые хранилища) и передачу ее по корпоративным каналам связи (электронная почта, сеть Интернет и др.).

SEARCHINFORM
INFORMATION SECURITY

Как оформить внедрение DLP?

Чтобы обезопасить себя с точки зрения закона, закрыть вопрос этики и иметь возможность использовать данные из DLP в качестве доказательств в суде, нужно соблюсти необходимые процедуры при внедрении IT-решения.

Приводим примерный перечень мер, актуальный для большинства компаний.

1. Внедрите режим коммерческой тайны (КТ)

Зачем?

Во-первых, это покажет, что контроль за рабочими местами сотрудников необходим.

Во-вторых, поможет наказать нарушителей.

Как?

Определите, какая информация составляет КТ. Закон «О коммерческой тайне» обещает защиту любых сведений – производственного, технического, экономического, организационного характера и т.п. – которые реально или потенциально имеют коммерческую ценность.

!

По закону нельзя прятать под гриф конфиденциальности кадровую информацию (количество работников, систему оплаты и условия труда) или сведения, которые влияют на безопасность людей (например, о токсичности производства или реализуемой продукции).

В отношении других данных решает компания. Главный признак коммерчески значимой информации такой: если она случайно попадет не в те руки, законный обладатель понесёт реальный ущерб.

Елена Мышливец – эксперт Moscow Digital School:

Чтобы ценные данные стали «тайной», необходимо составить подробный перечень конфиденциальной информации с максимально конкретными сведениями о типах, форматах таких данных и их отличительных признаках: от названий конкретных документов до целых категорий, например, «базы 1С» или «приказы за подписью директора».

Файлы и бумаги, не попавшие в перечень и под гриф, тайной считаться не будут, даже если реально содержат конфиденциальные сведения. Работника, уволенного за их разглашение, могут восстановить на работе с компенсацией морального вреда и зарплаты за вынужденный прогул.

Исключения составляют документы, которые охраняются на других основаниях: налоговая, банковская, медицинская тайна, персональные данные, ноу-хау (последние необязательно включать в коммерческую тайну, если предварительно оформить в соответствии со ст. 1495 ГК РФ как самостоятельный результат интеллектуальной деятельности).

Выберите перечень лиц, допущенных к работе с тайной.

Круг сотрудников, которым будет доступна тайна, нужно четко закрепить в документах с указанием имён, должностей, личных и обязательно учётных данных в корпоративных системах. Последнее нужно, чтобы при необходимости суд мог достоверно установить виновника утечки.

SEARCHINFORM
INFORMATION SECURITY

Вадим Перевалов – преподаватель Moscow Digital School:

Закрепите за работниками их учётные записи – чтобы это сделать, опишите во внутренних документах организации, каким образом учётная запись закрепляется за конкретным работником. Например, в дополнительных соглашениях с сотрудником можно указать, что работодатель предоставляет ему ПК и корпоративные средства связи, доступ к которым осуществляется с помощью такого-то логина. В этом же документе обяжите сотрудника сохранять в тайне логин и пароль от учётной записи.

Это нужно на случай судебного спора. Даже если вы приведёте исчерпывающие доказательства из DLP, что из-под определённой учётной записи распространяли сведения ограниченного доступа, вам ещё предстоит документально обосновать, как эта учётка связана с конкретным работником.

Ограничьте доступ к конфиденциальным данным.

Одного грифа «коммерческая тайна» недостаточно: важно, чтобы люди без допуска к ней не смогли даже случайно её увидеть. Чтобы этого добиться, нужно:

- **Хранить документы**, содержащие конфиденциальные сведения, **в защищённых хранилищах** (например, сейфах или отдельных помещениях), а выдавать только при предъявлении документов, подтверждающих уровень доступа.

- **В электронных хранилищах настроить и строго контролировать права доступа** для сотрудников к коммерческой тайне. У сотрудников без права работать с ней не должно быть возможности зайти на серверы, сетевые папки и на отдельные ПК, где лежит такая информация, открыть, прочитать, скопировать или удалить её.

  С задачей цифрового разграничения доступов справляются встроенные средства операционных систем (например, Active Directory для корпоративных версий Windows), а также соответствующие настройки в отдельных сервисах вроде CRM.

  Чтобы удостовериться, что настройки заданы правильно, полезны DCAP-системы: они проводят аудит прав доступа и операций с конфиденциальными файлами. А продвинутые DCAP-решения заодно могут блокировать нежелательные действия с критичными документами.

- **Разработать чёткие правила работы с коммерческой тайной** и включить их в должностные инструкции сотрудников, допущенных к работе с ней. Регламент должен содержать правила хранения, учёта, уничтожения и оборота таких данных.

- **Контролировать исполнение регламентов и выявлять нарушения**. Здесь на помощь как раз придут DLP, а также другие системы безопасности – от видеонаблюдения до СКУД.

Вадим Перевалов – преподаватель Moscow Digital School:

Moscow Digital School

«Установите требования по обеспечению конфиденциальности иной критичной информации: персданных, врачебной, банковской, адвокатской тайны и т.п. То есть всех потенциально уязвимых и защищённых законом данных, которые не включены в ваш перечень КТ.

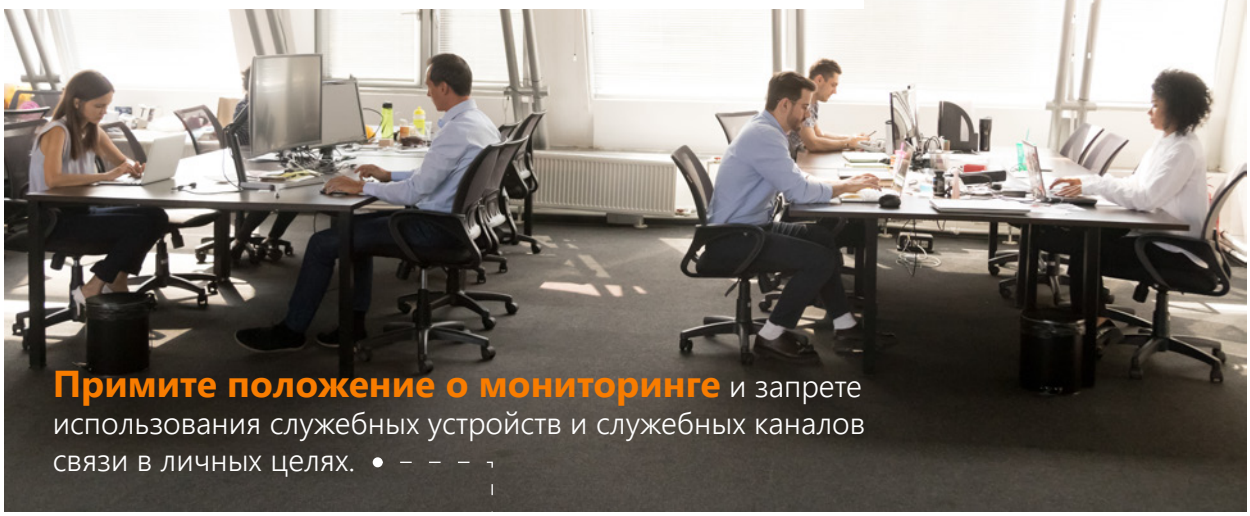
Документально закрепите правила и ознакомьте с ними сотрудников под роспись. Без закреплённых требований привлечь работника к ответственности будет проблематично.»

Включите положения о коммерческой тайне в трудовые договоры и договоры с вашими контрагентами. Подпишите соглашения о неразглашении.

В нём нужно указать, что сотрудник обязан сохранять коммерческую тайну, а также принимает ответственность, которая наступит при нарушении: например, по **ст. 183 УК РФ или пп. «в» п. 6 ч. 1 ст. 81 ТК РФ**. Иногда уже на уровне NDA прописывают наказания для сотрудников за разглашение тех или иных сведений.

2. Уведомьте работников о возможном мониторинге

Зачем? Так работник не сможет оспорить контроль под предлогом того, что работодатель «вмешивается в частную жизнь». Сотрудники будут знать, что информация на их компьютерах просматривается, а работодатель не нарушит права работников, даже если они решат хранить на рабочем месте личные данные.



Как? **Примите положение о мониторинге** и запрете использования служебных устройств и служебных каналов связи в личных целях.

Укажите, зачем это делается: например, чтобы исполнить требования регулятора, следить за соблюдением трудового распорядка, сохранностью имущества компании (рабочих ПК).

Ознакомьте с ним работников и получите согласие под роспись. Со всеми в штате такую бумагу нужно подписать индивидуально.

3. Соберите согласия сотрудников на обработку их персональных данных

Зачем? Использование DLP-систем прямо не предусмотрено трудовым законодательством, поэтому сбор данных о работнике с помощью таких систем возможен только с его согласия.

Как? В документе должны быть прописаны способы сбора данных, сведения о сроках их хранения, информация о том, кому они могут передаваться. Учитывайте правила, как должны быть оформлены согласия – сверьтесь с законом и требованиями РКН. В частности, учитывайте, что одно согласие может содержать только одну цель обработки персональных данных.

Вадим Перевалов – преподаватель Moscow Digital School:

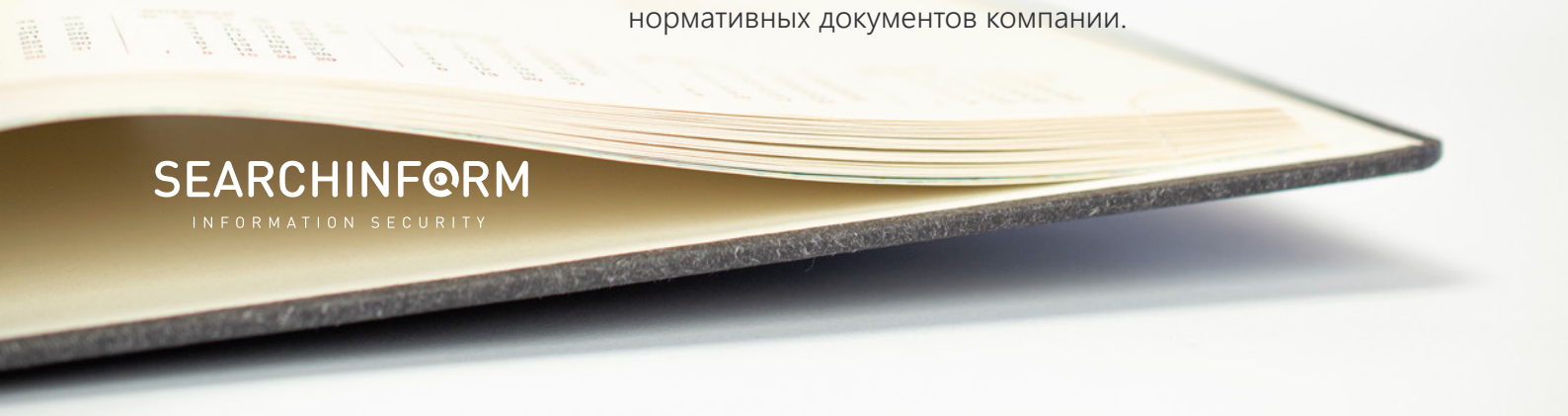
Moscow Digital School

Хранение переписки можно обосновать необходимостью соблюдать требования «Пакета Яровой». Это применимо в отношении собственных коммуникативных сервисов (онлайн-мессенджеров, электронных серверов, почты) и инструментов обмена файлами через Интернет. Компания может сослаться на Ст. 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

Документ не позволит компании полностью обосновать использование накопленных данных, но и не даст возможности сотрудникам требовать удаления любой информации, собранной во время рабочего процесса.

Итого: шпаргалка по необходимым документам

- Положение о коммерческой тайне.
- Положение о персональных данных.
- Документ об ознакомлении и согласии работника с положениями о коммерческой тайне и персональных данных и обязательстве не допускать их разглашения.
- Пункт об охране и недопущении работником разглашения конфиденциальной информации и персональных данных в трудовом договоре.
- Положение об обработке и защите информации и использовании средств мониторинга.
- Уведомление работника о применении в компании технологий мониторинга, в том числе ПО для предотвращения утечек конфиденциальной информации.
- Инструкция по работе с конфиденциальной информацией.
- Документы, содержащие положения и процедуры информационной безопасности.
- Инструкции для работников по использованию информационных систем, сервисов и средств защиты информации.
- Положение о привлечении работника к ответственности за нарушение им локальных нормативных документов компании.



SEARCHINFORM
INFORMATION SECURITY

Как законно наказать нарушителя?

Итак, все положения приняты, в компании действует режим защиты информации, а DLP-система следит за его соблюдением. В рамках мониторинга обнаруживается попытка слива чувствительных данных. Пора в суд?

Ещё нет. Инцидент предстоит зафиксировать и расследовать по всем правилам, чтобы законно применять дисциплинарные меры.

Вот пошаговая инструкция, как вести разбирательство:

1. Установить факт инцидента или подозрения в том, что инцидент произошёл.
2. Создать комиссию по расследованию инцидента. Перечень лиц, обязанных участвовать в проведении служебной проверки, законом не установлен. Как правило, этим занимается служба безопасности или отдел кадров. В состав комиссии также часто включают юристов, экономистов, бухгалтеров, членов профсоюзной организации.
3. Провести внутреннее расследование. По его итогам установить размер причинённого ущерба и обстоятельства инцидента. В расследование может входить опрос свидетелей, проверка письменной документации работника, данные DLP-системы (скриншоты рабочего стола, архив переписки, аудит операций в файловой системе и т.д.).
4. Подготовить акт о результатах работы комиссии. В него должна войти вся информация о расследовании, собранные доказательства и выводы членов комиссии с личными подписями.
5. Ознакомить сотрудника с результатами работы комиссии.
6. Потребовать от сотрудника письменного объяснения. А в случае отказа предоставить объяснение – составить и подписать акт об этом.
7. Потребовать у сотрудника возмещения ущерба.
8. При отказе обратиться в правоохранительные органы или суд.

Когда расследование доказывает вину сотрудника, компания может наказать инсайдера одним из следующих способов:

SEARCHINFORM
INFORMATION SECURITY

⟶ Уволить

Трудовой кодекс полностью на стороне работодателя: если работник нарушает закон, его можно уволить по статье с указанием причины в трудовой книжке:

«Трудовой договор может быть расторгнут работодателем в случае разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника» (***Ст. 81 п. 6 пп. «В» ТК РФ***).

⟶ Обязать возместить ущерб

Привлечь сотрудника к такой ответственности можно по ТК или ГК РФ.

Статьи 232, 233, 238-250 ТК РФ говорят о том, что работник несёт материальную ответственность перед работодателем, если в результате его действий компания понесла ущерб. Однако предстоит провести служебную проверку, в рамках которой установить размер ущерба, причины его возникновения, доказать вину работника и взять с него объяснительную. Всё это можно сделать в рамках первичного расследования инцидента – главное пошагово задокументировать всю процедуру.

Елена Мышливец – эксперт Moscow Digital School:

Moscow Digital School

Важно учитывать и пределы материальной ответственности. Как правило, за причинённый ущерб работник несёт ответственность в пределах своего среднего месячного заработка (242 ТК РФ). Но есть варианты, когда сотрудника можно обязать полностью компенсировать компании убытки.

В частности, материальная ответственность в полном размере причинённого ущерба возлагается (ст. 243 ТК РФ) в случае умышленного причинения ущерба, разглашения сведений, составляющих охраняемую законом тайну. Также материальная ответственность в полном размере может быть установлена трудовым договором, заключаемым с заместителями руководителя организации, главным бухгалтером.

Помните, что по ТК РФ с работника можно взыскать только действительный материальный ущерб (т.е. фактическую стоимость украденной информации и/или её носителя). Недополученную прибыль – например, если из-за утечки вы потеряли конкурентное преимущество или упустили клиентов – таким образом возместить нельзя.

Однако если сотрудник разгласил секрет производства (это не то же, что коммерческая тайна, а отдельный вид интеллектуальной собственности) и его вина доказана, компания может подать гражданский иск на возмещение вреда (по п. 1 ст. 1472 ГК РФ). Такой процесс предусматривает компенсацию в том числе недополученной прибыли и репутационных потерь.

→ Привлечь к уголовной ответственности

Разглашение информации, составляющей коммерческую тайну (а также налоговую, банковскую и некоторые другие виды тайн), карается по ст. 183 УК РФ. Но не всякий инцидент может считаться нарушением закона – соответственно, за него нельзя наказать в суде.

Сделать это можно, если:

1. **Сведения, которые разгласил работник, по действующему законодательству относятся к конфиденциальным:** это информация из вашего перечня КТ, персональные или иные защищённые законом данные, не входящие в перечень.

2. **Факт незаконного сбора или разглашения комтайны действительно имел место.** Например, если сотрудник просто скопировал документ с грифом «КТ» на флешку, это не разглашение данных – максимум нарушение внутренних нормативов, если использование флешек в компании запрещено.

   Но если тот же документ сотрудник попытался отправить внешнему адресату по электронной почте, или даже обсуждал такую возможность с третьим лицом – это разглашение комтайны, которое карается по ст. 183 УК РФ.

SEARCHINFORM
INFORMATION SECURITY

3. **Работник имел доступ к закрытой информации по долгу службы.** Он включён в перечень лиц, допущенных к работе с КТ, его трудовой договор и/или должностные инструкции содержат соответствующие пункты.

4. **Сотрудник письменно обязался не разглашать конфиденциальные сведения.** Соответствующие договорённости закреплены в NDA, положении о конфиденциальности или в трудовом договоре.

И ещё пара важных пунктов, которые могут повлиять на успех разбирательства:

Доказательства нарушения должны быть собраны в соответствии с законом.	В суде не примут за доказательства данные, полученные путём взлома личного почтового ящика сотрудника, его страницы в соцсетях и телефона или с помощью скрытой прослушки. Подойдут только легальные инструменты, использование которых закреплено в локальных нормативных актах компании (например, в политике безопасности).
Работник должен был быть уведомлён о факте контроля со стороны работодателя.	Это необходимое условие: в противном случае работодатель не сможет обосновать, каким образом ему стало известно о факте разглашения, и предъявить доказательства. А у виновника слива появится лазейка, чтобы не просто избежать наказания, но и выступить с ответным иском.

Чтобы инициировать разбирательство по уголовной статье, с материалами служебного расследования нужно обратиться в полицию. Собранная фактура облегчит работу следственным органам – чем качественнее проделана работа, тем выше вероятность, что уголовное дело будет возбуждено и дойдёт до суда. Но будьте готовы, что полиция может инициировать новые проверки и разбирательства, вплоть до того, чтобы наблюдать за инсайдером «в поле» и в конечном итоге поймать с поличным.

Кроме того, могут потребоваться дополнительные подтверждения ваших доказательств.

Например, у компании могут запросить разъяснения, как именно работает система, с помощью которой собраны улики, и какую функцию выполняет. Например, что Active Directory действительно разграничивает права пользователей и они просто не видят – или не могут открыть – папку с конфиденциальными сведениями, если не имеют права с ними работать.

С подготовкой справки о принципе работы контролирующего ПО может помочь вендор. На крайний случай подойдёт краткое описание решения с указанием сертификатов (сгодится даже маркетинговая брошюра).

В уголовном деле доказательства, собранные с помощью DLP, могут учитываться, но не могут считаться исчерпывающими. Большую роль для следствия в рамках уголовно-процессуального кодекса имеют показания потерпевших, свидетелей, заключения и показания экспертов и специалистов, вещественные доказательства – например, изъятые у инсайдеров флешки с украденной клиентской базой или деньги, полученные за неё от конкурентов.

Итого: шпаргалка по необходимым документам

- **Докладная записка** на имя руководителя компании от лица, обнаружившего инцидент.
- **Приказ** о создании комиссии для служебного расследования, составленный руководителем.
- **Уведомление** на имя работника, допустившего инцидент, о необходимости предоставить письменные объяснения.
- **Объяснительная** от работника, допустившего инцидент, с подробным описанием обстоятельств.
- **Акт об отказе**, если работник не соглашается предоставить письменные объяснения.
- **Акт о результатах работы комиссии** с указанием всех выявленных обстоятельств по факту инцидента. С ним нужно под роспись ознакомить сотрудника!
- **Акт об отказе**, если сотрудник не соглашается знакомиться или расписываться в ознакомлении с результатами расследования комиссии.

В случае выявления вины работника, компания принимает решение и составляет:

- **Приказ** о наложении дисциплинарного взыскания (замечание, выговор).
- **Приказ** о прекращении трудовой деятельности.
- **Акт об отказе**, если работник не соглашается под роспись ознакомиться с приказом.

Желательно получить **обязательство о неразглашении** информации, ставшей известной в ходе проведения служебного расследования и участия в нём, от всех членов комиссии, свидетелей и работника, допустившего инцидент.

SEARCHINFORM
INFORMATION SECURITY

Как использовать данные DLP-системы в суде?

Мы собрали истории клиентов «СёрчИнформ», которые наглядно показывают, как использование DLP-системы в комплексе с юридическими документами помогают выиграть судебные дела против нарушителей.

Кейс:

Слив клиентской базы Ст. 183 УК РФ

Что произошло: DLP-система обнаружила, что сотрудница в рабочее время общается по почте с представителем конкурентной фирмы. Сотрудник СБ написал докладную записку об инциденте и запросил расследование.

Как расследовали:

Анализ переписки показал, что сотрудница зарабатывала на клиентской базе компании, в которой работала. Её задача заключалась в том, чтобы переводить клиентов фирмы к конкурентам. Для полноты расследования «подняли» записи телефонных разговоров с клиентами, где сотрудница вводила собеседника в заблуждение относительно доступных ему условий обслуживания и затем прямо рекомендовала сотрудничать с компанией конкурента. Полученные сведения о клиентах, включая условия договоров с ними, она передавала конкурентам, тем самым разгласив информацию, составляющую КТ.

Для расследования инцидента собрали комиссию из трех человек: представителя СБ, отдела кадров и юриста. Сотрудницу попросили написать объяснительную, но она отказалась. Был составлен акт об отказе, комиссия начала расследование. В расследовании использовались данные, полученные DLP-системой. Комиссия также рассмотрела все документы, подписанные сотрудницей при заключении контракта: согласие на мониторинг, согласие с принятым в компании положением о КТ, NDA.

Итого: **Обвинительный приговор, лишение свободы на 3 года условно.**

Кейс:

Слив переписки руководителя

Ст. 183 УК РФ

Что произошло: Компания с помощью DLP-системы обнаружила, что один из сотрудников втайне просматривает почтовый ящик начальника управления.

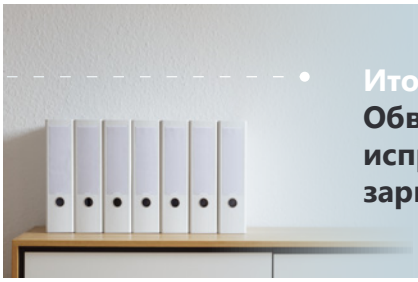
Как расследовали:

Подробный анализ показал, что часть писем пересылается конкурентам. В отправлениях содержались цены и условия контрактов с партнерами, результаты анализа рынка, детали стратегии по продвижению продукции за рубеж. Согласно принятому в компании положению о конфиденциальности, эти сведения составляли коммерческую тайну.

Внутреннее расследование показало, что сотрудник занимался этим на протяжении двух лет. В результате конкуренты получили преимущество, а компания стала фиксировать отток клиентов, потеряла рынки сбыта, понесла финансовый и репутационный ущерб. Нарушителя уволили за грубое нарушение трудовых обязанностей на основании п. «в» ч. 6 ст. 81 ТК РФ (разглашение охраняемой законом коммерческой тайны). Затем на инсайдера подали в суд.

В качестве доказательств в суде представили распечатки писем конкуренту из почтового ящика, который принадлежал обвиняемому. К ним прилагалось подтверждение из DLP о том, что во всех случаях доступ к этому ящику осуществлялся с использованием учётной записи сотрудника.

Также предъявили заявку обвиняемого на право использования электронной почты, где он под подпись предупреждался об ответственности за несанкционированную отправку в Интернет конфиденциальных сведений. А заодно соглашался с проведением контроля содержимого его электронной почты специальными программно-техническими средствами. Наконец, представили объяснительную: в ней инсайдер писал, что передавал конфиденциальные данные, потому что рассчитывал получить у конкурентов должность с большей зарплатой.



Итого:
Обвинительный приговор, 1 год 9 месяцев исправительных работ с удержанием 15% зарплаты в доход государства.

SEARCHINFORM
INFORMATION SECURITY

Кейс:

Иск после увольнения за утечку

Ст. 81 п. 6 пп. «В» ТК РФ

Что произошло: Компания уволила сотрудника за попытку слива информации, как это предусмотрено Трудовым кодексом. Работник обратился с иском в суд к работодателю о признании увольнения незаконным на том основании, что не согласен с выводами служебной проверки. Добивался восстановления на работе и взыскания невыплаченной премии.

Как расследовали:

В суде пришлось восстанавливать хронологию изначального инцидента. Тогда сотрудник службы безопасности через модуль контроля съёмных устройств в DLP-системе обнаружил передачу файлов на посторонний гаджет. При этом в компании было запрещено использование USB-портов. Дальнейший анализ показал, что в копируемых файлах содержалась информация, попадающая под гриф «секретно».

Нарушитель уже попадал в поле зрения службы ИБ и входил в группу особого контроля, поэтому его заподозрили в передаче конфиденциальных данных третьим лицам. В объяснительной работник не назвал объективной причины, зачем ему нужна была информация. Работодатель не выплатил премию и уволил нарушителя с работы.

Сотрудник счёл, что компания не доказала, что он действительно собирался сливать информацию на сторону, и поэтому оспорил заключения служебного расследования. Однако не учёл главного: он был знаком с принятой в компании политикой безопасности и запрете на флешки, в чём добровольно расписывался. Кроме того, в положении о коммерческой тайне, с которым он также был ознакомлен, прямо указывалось, что файлы с грифом «секретно» нельзя копировать. Наличие этих документов помогло работодателю обосновать факт нарушения, а данные из DLP – доказать факт копирования конфиденциальной информации на съёмный диск.

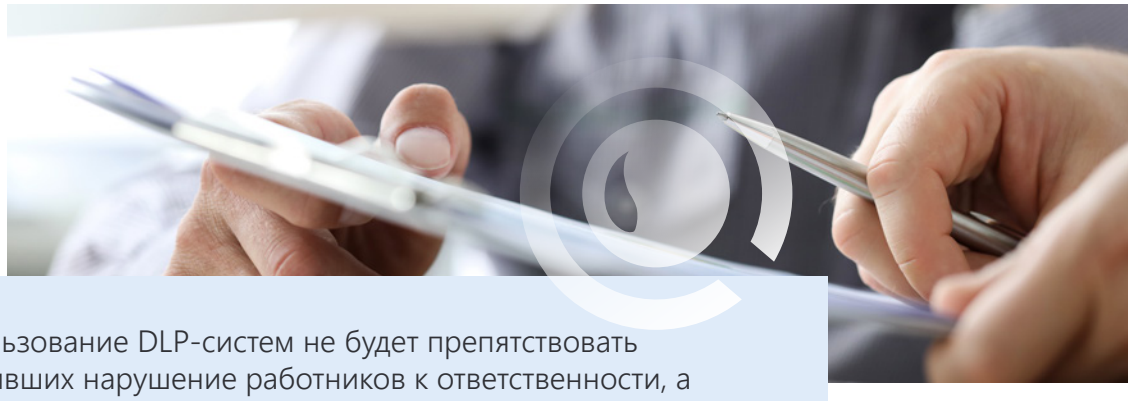
Итого: Суд отказал работнику в исковых требованиях в полном объёме.

Что в итоге?

Закрепим:

Использовать DLP – законно. Чтобы применить данные о нарушениях в суде, нужно помнить о следующих нюансах:

- для использования системы важно правильно оформить внутренние документы организации на самом первом этапе внедрения DLP-систем (самый важный из них – информированное согласие сотрудника на мониторинг);
- следует сразу установить режим конфиденциальности данных (КТ и других тайн, ПДн);
- результаты служебных расследований должны быть оформлены по всем правилам (акты, объяснительные, приказы).



Таким образом, использование DLP-систем не будет препятствовать привлечению допустивших нарушение работников к ответственности, а наоборот поспособствует в суде. Однако следует соблюдать все правила оформления результатов служебных расследований, ведь именно такие, не связанные с DLP-системой ошибки чаще всего мешают успешному привлечению виновных к ответственности.