Чек-лист:

5 ШАГОВ к легальному контролю с системой защиты от утечек информации (DLP)

SEARCHINFORM
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Системы защиты от утечек информации (DLP) незаменимы в вопросах защиты от утечек информации, предотвращения корпоративного мошенничества и других нарушений, которые допускают работники. Чтобы не создавать рисков для организации, контроль не должен нарушать требований закона. Собрали чек-лист по юридическому оформлению внедрения систем защиты от утечек информации (DLP).

1 Организуйте режим защиты конфиденциальной информации

Как?

- Установите, с какой конфиденциальной информацией работает ваша организация и определите категории этих данных (информация для служебного пользования, персональные данные, сведения, составляющие коммерческую, банковскую, налоговую, врачебную, налоговую, адвокатскую тайну).
- Разработайте внутренние документы о защите информации:
  - Положение о работе с персональными данными – для любых организаций;
  - Положение о коммерческой тайне – для бизнеса;
  - Положение о работе со служебной информацией ограниченного распространения – для госсектора;
  - Положения о работе с конфиденциальной информацией – в случаях, если обрабатываются защищаемые сведения иных видов.

В этих документах определите, кто имеет к доступ к конфиденциальной информации, кто отвечает за ее безопасность, порядок ее маркировки, обязанности сотрудников при работе с этой информацией, меры ответственности за нарушения, права организации в части защиты информации. Перечень сведений, относящихся к защищаемым категориям, отразите в приложениях к документам.

- Включите пункты о неразглашении конфиденциальной информации и соблюдении режима ее защиты в трудовые договоры сотрудников. Отразите положения о конфиденциальности в договорах с вашими контрагентами.
- Промаркируйте носители конфиденциальной информации грифами «Коммерческая тайна», «Для служебного пользования», «Конфиденциально» или иными. Найти и промаркировать конфиденциальные файлы в электронном формате поможет система аудита и защиты файловых хранилищ (DCAP)
- Ознакомьте работников под роспись с документами о защите информации, подпишите актуализированные договоры и соглашения с сотрудниками и контрагентами.

Зачем?

- Без документального оформления защиты информации проблематично доказать статус конфиденциальности сведений, принятие мер к их безопасности, подтвердить факты нарушений.
- Обеспечение режима защиты информации – это правовое основание для внедрения технических ИБ-средств.

2 Установите правила открытого контроля

Как?

- Отразите в правилах внутреннего распорядка и должностных инструкциях сотрудников:
  - Запрет на использование корпоративных устройств, средств коммуникации, информационных систем, аккаунтов и учетных записей в целях, не связанных с исполнением должностных обязанностей;
  - Право организации осуществлять, в т.ч. с помощью технических средств защиты от утечек, контроль соблюдения работниками правил о работе с защищаемой информацией и использования сотрудниками корпоративных устройств, средств коммуникации, информационных систем, аккаунтов и учетных записей.
- Ознакомьте всех сотрудников под роспись с актуализированными правилами внутреннего распорядка и должностными инструкциями.

Зачем?

- Это исключит риски, связанные с получением сведений о частной жизни работника.
- Это позволит привлекать сотрудников к ответственности за нецелевое использование ИТ-ресурсов работодателя.

3 Соберите согласия сотрудников на обработку их персональных данных

Как?

- В согласиях об обработке персональных данных сотрудников и политике обработки персональных данных в организации отразите дополнительные цели работы с персональными данными: выполнение мероприятий по защите информации и контроль выполнения работниками трудовых функций.
- В этих документах должны быть прописаны способы сбора персональных данных, сроки их хранения, порядок их защиты, передачи, актуализации, уничтожения, определен ответственный за обработку этих данных.
  При оформлении согласий на обработку персональных данных и политики обработки сверяйтесь с требованиями ФЗ № 152 и предписаниями Роскомнадзора.

Зачем?

- Защита информации в целом и контроль сотрудников, в том числе, с использованием системы защиты от утечек информации (DLP), требуют обработки персональных данных работников. Однако, такие случаи не подпадают под возможность получения этих данных без согласия сотрудников.

4 Закрепите за работниками их учетные записи

Как?

- Отразите во внутренних документах организации, каким образом учетные записи закрепляются за конкретными работниками. При необходимости разработайте отдельный приказ или положение об учетных записях работников. Обяжите сотрудников сохранять в тайне служебные учетные данные, не передавать их никому, не применять корпоративные учетные записи в личных целях и не дублировать комбинации «логин-пароль» от рабочих аккаунтов в личных учетных записях.

Зачем?

- В случае спора придется доказать, что инцидент был допущен при использовании учетной записи конкретного работника и обосновать, как этот аккаунт связан с сотрудников.
- Это позволит пресекать нарушения, связанные с передачей служебных учетных записей и их нежелательным использованием.

5 Официально введите систему защиты от утечек информации (DLP) в эксплуатацию

Как?

- Разработайте и примите приказ о вводе в эксплуатацию системы защиты от утечек информации (DLP). Отразите в приказе:
  - Цели внедрения системы защиты от утечек информации (DLP): выполнение требований по защите персональных данных, защита коммерческой тайны, обеспечение конфиденциальности служебной информации ограниченного распространения, контроль выполнения правил внутреннего распорядка;
  - Устройства, на которых устанавливаются компоненты систему защиты от утечек информации (DLP);
  - Состав, права и обязанности лиц, ответственных за установку, обслуживание, эксплуатацию системы защиты от утечек информации (DLP), а также имеющих доступ к показателям и отчетам системы защиты от утечек информации;
  - Условия о неразглашении информации из системы защиты от утечек информации (DLP), случаи, в которых эта информация может использоваться: взаимодействие с контролирующими органами (РКН, ФСТЭК, ФСБ), предоставление в правоохранительные органы или суды, проведение служебных проверок.
  - Дату ввода системы защиты от утечек информации (DLP) в эксплуатацию.
- Ознакомьте с приказом сотрудников организации, причастных к работе с системой защиты от утечек информации (DLP).

Зачем?

- Приказ о вводе системы защиты от утечек информации (DLP) в эксплуатацию позволит зафиксировать законные цели использования системы, конфиденциальность полученной с ее помощью информации, пределы использования системы и ее отчетов, а также момент внедрения контроля в организации.

Легитимный контроль позволяет организациям не только избежать рисков при использовании системы защиты от утечек информации (DLP), но и успешно использовать показатели этих систем для защиты своих интересов в судах и правоохранительных органах.

*Дополнительно делимся памятками о том, как ввести в организации режим **коммерческой тайны** и как **привлечь** ИБ-нарушителей к дисциплинарной ответственности.*

Подробнее о практике использования системы защиты от утечек информации (DLP) читайте в разделе «Практика и аналитика» на сайте searchinform.ru