Чек-лист:

5 ШАГОВ для внедрения режима коммерческой тайны



Зачем?

Внедрение режима коммерческой тайны (КТ) – не только право обладателя информации, согласно 98-ФЗ, но и насущная необходимость. Например, без него инсайдера не привлечь к ответственности в суде, если произойдет утечка. Как показывает судебная практика, даже если в компании есть СЗИ и они детально зафиксировали «слив», при отсутствии режима КТ сложно доказать ценность утекших сведений и вину сотрудника.

Как?

1 Определите, какая информация является конфиденциальной

Обычно это любая производственная, техническая, экономическая, организационная и другая информация, которая имеет или может иметь коммерческую ценность. Например: ноу-хау, планы развития, метод изготовления продукта, результаты переговоров, клиентские базы и т.п.

Согласно 98-ФЗ «О коммерческой тайне» КТ не могут составлять учредительные документы, данные о числе работников, системе оплаты труда, производственном травматизме и т.д.

Сведения, составляющие КТ, могут быть раскрыты в рамках взаимодействия вашей компании с органами власти, однако такое раскрытие не освобождает любых лиц, кому эта информация была передана, от обязанностей по защите КТ.

2 Создайте Положение о коммерческой тайне

В Положении прописывается:

- порядок обращения и передачи конфиденциальных данных
- методы контроля за выполнением этого порядка
- перечень лиц, имеющих к ним доступ, и пределы такого доступа
- перечень мер защиты КТ
- порядок отнесения информации к КТ
- ответственность за нарушения.

Перечень сведений, составляющих КТ, прописывается в приложении к Положению.

Положение должно быть введено в действие приказом руководителя компании, все сотрудники, в т.ч. работающие удаленно, должны подтвердить ознакомление с ним под подпись.

SEARCHINFORM
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

3 Промаркируйте конфиденциальные данные грифом «КТ»

Это необходимо, чтобы разработать систему учета лиц, которым был предоставлен доступ к КТ. Порядок маркировки и образец грифа отражаются в Положении о КТ. Маркировка не только дисциплинирует, но и помогает доказать конфиденциальность сведений, если произойдет утечка, а также установить виновника инцидента.

Если данные хранятся в электронной форме, могут возникнуть сложности с их маркировкой. Помогут технические средства – например, системы аудита и защиты файловых хранилищ (DCAP), которые присваивают документам цифровые метки в зависимости от их содержания. Систему можно настроить так, чтобы она автоматически расставила грифы на критичные файлы в соответствии с принятым в компании Положением о КТ. Порядок такого учета, возможность и порядок применения СЗИ также должны быть прописаны в Положении.

Маркировке подлежат все документы в бумажном и электронном виде. Во втором случае – также носители информации, включая флешки, диски и т.п.

98-ФЗ не содержит указаний по способу нанесения грифа. Это может быть штамп, наклейка, включение грифа в фирменный бланк и т.п. Главное требование: маркировка должна ясно указывать, что информация на носителе относится к коммерческой тайне и принадлежит конкретному владельцу.

4 Возьмите обязательство о неразглашении у всех, имеющих доступ к КТ

Обязательство следует сразу включать в трудовой договор с новыми сотрудниками, или оформить как дополнительный документ с уже текущими.

С контрагентами нужно заключить соглашение о неразглашении (NDA). В него следует включить обязательство партнера по обеспечению конфиденциальности и защиты получаемых данных. Соглашение о неразглашении конфиденциальной информации (NDA) можно включить в договор или подписать отдельно.

В обязательствах сотрудников и соглашении о неразглашении конфиденциальной информации (NDA) нужно указать, что они обязаны сохранять коммерческую тайну, а также несут ответственность за нарушения с переданными им сведениями, составляющими КТ.

5 Обеспечьте контроль и защиту

Чтобы этого добиться, нужно:

- Хранить бумажные документы с КТ в защищенных хранилищах (например, сейфах или отдельных помещениях), а выдавать только при предъявлении документов, подтверждающих уровень доступа.
- В электронных хранилищах использовать технические средства разграничения доступа и управления правами пользователей, а также мониторинга за соблюдением правил оборота КТ.

Системы аудита и защиты файловых хранилищ (DCAP) помогут разметить КТ в «цифре», организовать места безопасного хранения таких данных, ограничить доступ к ним сотрудников и задать правила их обработки. Например, если регламентом запрещено изменение документов с грифом «КТ», можно запретить открывать их в текстовых редакторах.

Системы защиты от утечек информации (DLP) позволят контролировать, как соблюдаются регламенты работы с КТ, обнаружат попытки получить к ней несанкционированный доступ и защитят от утечек этих данных по всем цифровым каналам: в почте, мессенджерах, звонках, распечатке, даже фото на смартфон.

Организациям с техническими средствами защиты намного проще доказать, что был нарушен режим коммерческой тайны. Также системы помогают обосновать в суде, что компании был нанесен ущерб, а информация с грифом КТ действительно была разглашена. Но для этого внедрение СЗИ должно быть оформлено юридически правильно. Здесь делились памяткой, как это сделать.