ЧЕК-ЛИСТ:

КАК НАКАЗАТЬ ИНСАЙДЕРА ЗА СЛИВ ПДн



30 мая вступят в силу изменения в ст. 13.11 КоАП, которые увеличат штрафы за инциденты с персональными данными до 150 раз. Наказание за первую утечку может достигнуть 15 млн рублей, за повторную — до 3 % от оборота компании. **Но если доказано, что за утечкой стоит инсайдер, ему грозит уголовное наказание по статье 272.1 УК РФ, а компания сможет избежать штрафа.**

Как его вычислить и привлечь к ответственности? Разбираемся по шагам.

0 ПРИНЯТЬ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Технические меры:

Навести порядок в хранении персональных данных и коммерческой тайны.

Система аудита и защиты файловых хранилищ (DCAP):

- Какие файлы из общего массива — конфиденциальные, какие содержат ПДн;
- Где хранятся такие данные;
- Какие сотрудники имеют к ним доступ.

Система защиты от утечек информации (DLP):

Как ПДн перемещаются в периметре организации и за его пределы.

Система управления инцидентами информационной безопасности (SIEM):

- Как администраторы распределяют права доступа к местам хранения ПДн и КТ.
- Состояние и доступность файловых хранилищ, где содержатся ПДн и КТ.

Организационные меры:

Внедрить **Политику обработки персональных данных.** Вот рекомендации регулятора, как это сделать.

Внедрить **Режим коммерческой тайны.** Подробная инструкция здесь.

Совокупность этих средств минимизирует риск инцидента с ПДн и покажет, что организация принимала меры защиты персональных данных.

Легитимизировать внедрение СЗИ.

Подробная инструкция здесь.

Принять **Положение о служебном расследовании.** Оно должно содержать указания:

- на каком основании можно начинать расследование,
- в какие сроки оно должно проходить,
- какие решения можно принять по итогам.

1 ЗАФИКСИРОВАТЬ НАРУШЕНИЕ

Технические меры:

Зафиксировать факт утечки ПДн.

- **Система аудита и защиты файловых хранилищ (DCAP)** покажет факт неправомерного доступа к данным, если у сотрудника не было на это прав.
- **Система защиты от утечек информации (DLP)** отобразит, как инсайдер украл данные: отправил письмом, загрузил в интернет, скопировал на флешку, сфотографировал и т. д.
- **Система управления инцидентами информационной безопасности (SIEM)** сообщит, если данные украли хакеры извне, воспользовавшись уязвимостью.

Об обнаружении инцидента с утечкой ПДн необходимо отчитаться в Роскомнадзор в течение 24 часов.

Организационные меры

Составить **служебную записку руководству** от сотрудника или руководителя службы ИБ о факте утечки. В ней указать:

- **На каком устройстве, как и когда выявили нарушение.**

Если утечку зафиксировали в СЗИ, нужно приложить скриншоты инцидента или отчеты системы об этом.

- **Какие меры уже приняты.**

Например, описать, что попытку слива заблокировала система защиты от утечек информации (DLP). Даже если данные не покинули компанию, это нарушение и требует расследования.

На основании записки руководителю нужно принять **Приказ о проведении служебного расследования.**

2 УСТАНОВИТЬ ОБСТОЯТЕЛЬСТВА ИНЦИДЕНТА

Выяснить:	Поможет:
Время и место инцидента	
Разобраться, где и когда произошла утечка: в офисе компании или у сотрудника на удаленке, в рабочие или нерабочие часы и т. д.	**СЗИ**, они ведут запись событий: • дату и время инцидента, • идентификатор ПК, где он произошел, • учетную запись, активную в момент происшествия, • сетевой адрес (IP) подключения к корпоративной сети и др. **Система защиты от утечек информации (DLP)** и **система управления инцидентами информационной безопасности (SIEM)** отображают местоположение ПК сотрудников на интерактивной карте. **Система защиты от утечек информации** ведет съемку с веб-камеры сотрудника – по снимкам можно убедиться, в офисе он или нет.
Какие данные пострадали?	
Сопоставить утекшие данные с файлами компании, учитывая все возможные дубликаты и редакции.	**Система аудита и защиты файловых хранилищ (DCAP)** найдет все копии файла в любых хранилищах. Даже если файл скопировали, а потом изменили, система распознает его как дубликат в прошлом.
Что с ними произошло?	
Восстановить историю обращений к местам хранения пострадавших файлов, выявить кто, в каком объеме, в каких программах работал с ними.	**Система аудита и защиты файловых хранилищ (DCAP)** отобразит, кто и как открывал, копировал и перемещал пострадавшие файлы в последнее время.
Установить факт неправомерного выноса данных: выгрузку в личное облако, на личный носитель информации, пересылку в почте или мессенджере, фото с экрана.	**Система защиты от утечек информации (DLP)** покажет: • Как данные выгружались на устройства пользователей из корпоративных хранилищ и бизнес-систем. • Производилась ли их выгрузка в интернет, передача, фотографирование.
Выяснить, не было ли признаков хакерской атаки.	**Система управления инцидентами информационной безопасности (SIEM)** проанализирует: • Есть ли в ИТ-инфраструктуре компании уязвимости, которыми могли воспользоваться хакеры. • Возникали ли в ПО или на оборудовании компании инциденты ИБ или потенциально опасные события.
Как задокументировать?	
Собрать **суммарный отчет по инциденту.**	Служба ИБ должна указать: • объем пострадавших данных, • какие конкретно ПДн раскрыты, • оценку возможного вреда, • результаты предварительного внутреннего расследования.



3 УСТАНОВИТЬ ЛИЧНОСТЬ И ВИНУ ИНСАЙДЕРА

Выяснить:	Поможет:
Кто работал с ПДн	
Восстановить историю работы на рабочей станции, где хранились пострадавшие файлы.	**Система аудита и защиты файловых хранилищ (DCAP)** покажет: • На каком ПК работали с ПДн. • Имя пользователя (учетной записи), который это делал. • Какие операции совершались с пострадавшими файлами. **Система защиты от утечек информации (DLP)** прояснит: • Использовал ли учетку ее владелец, или под ней авторизовался другой пользователь.
Уполномочен ли сотрудник работать с ПДн	
Провести ревизию должностных инструкций и трудовых договоров с подозреваемым сотрудником.	В документации сотрудника выяснится: • Подтверждал ли он ознакомление с локальными актами по ИБ личной подписью.
Проверить фактическое распределение прав пользователя в ИТ-системах в соответствии с его должностными полномочиями.	**Система аудита и защиты файловых хранилищ (DCAP)** отобразит, были ли разрешены эти действия подозреваемому.
Был ли у нарушителя мотив	
Проанализировать активность и продуктивность, круг общения вероятного нарушителя за 1–2 недели до инцидента.	**Система защиты от утечек информации (DLP)** покажет: • Какое ПО сотрудник использовал и какие сайты посещал, не совершал ли действий, не связанных с рабочими обязанностями. • Имел ли подозреваемый конфликты с коллегами или проблемы, мешающие работе, например, долги или зависимости. • Общался ли подозреваемый с конкурентами, уволенными сотрудниками или заказчиками «пробива».
Оценить вероятность, что сотрудник подвергался социальной инженерии.	**Система защиты от утечек информации (DLP)** выявит: • Получал ли сотрудник фишинговые письма, сообщения или звонки. • Посещал ли сотрудник фишинговые сайты. **Система управления инцидентами информационной безопасности (SIEM)** подтвердит факты обращений сотрудника к ресурсам, имеющим идентификаторы компрометации ФинЦЕРТ.
Как задокументировать?	
Получить **письменные объяснения** сотрудника по факту инцидента.	Если сотрудник не представляет объяснения в течение двух дней, компания должна составить об этом акт.
Подготовить **акт служебного расследования.**	Приобщить к нему: • докладную записку руководителя ИБ, • выгрузки СЗИ, • пояснения ИБ-специалистов, • объяснительную записку нарушителя.

Важно предоставить в РКН отчет об итогах расследования инцидента с ПДн в течение 72 часов.

Виновник должен быть ознакомлен с актом.

Если внутреннее расследование выявило умышленный «слив» данных:



- Отразить в акте служебного расследования наличие противоправных действий нарушителя и решение о передаче материалов расследования в правоохранительные органы.
- Выполнить требования Роскомнадзора: направить уведомление об инциденте, указать в качестве причины умышленные действия сотрудника.
- Подготовить и подать заявление в орган МВД по месту нахождения организации. Приложить к нему все материалы служебного расследования, политику обработки персданных, должностную инструкцию работника, приказ о введении в эксплуатацию ИБ-средств.
- Контролировать возбуждение уголовного дела: быть на связи с МВД, получить копию постановления о возбуждении уголовного дела. При проведении следственных действий поручить ИБ-специалистам показать сотрудникам полиции отчеты СЗИ и дать по ним комментарии.
- Если дело об административном правонарушении уже возбуждено – обжаловать, ссылаясь на наличие признаков преступления.



Технические средства защиты надежнее всего фиксируют факты нарушений обработки ПДн. Также СЗИ ускоряют расследование таких инцидентов, позволяя уложиться в отведенные регулятором сроки. А собранные в системах доказательства принимаются в суде. Главное – система аудита и защиты файловых хранилищ (DCAP), система защиты от утечек информации (DLP) и система управления инцидентами информационной безопасности (SIEM) минимизируют риски нарушений и ущерб от них. В том числе их применение служит смягчающим обстоятельством, если за инцидент отвечает компания – с ними повторная утечка ПДн обойдется организации в 10 раз дешевле.