

Чек-лист 2

Реагирование на утечку ПД

Чтобы избежать штрафов за утечку, придется доказать сперва Роскомнадзору, а затем и суду, что хотя утечка и произошла в этом нет вашей вины. Почему? Потому что всё, что можно и нужно было сделать для предотвращения утечки и минимизации ее последствий, вы своевременно и в полном объеме сделали.

Есть две группы доказательств, которые необходимо собрать:

- (1) доказательства рутинных privacy-процедур по предотвращению утечек и
- (2) доказательства надлежащего реагирования на утечку для минимизации ее последствий.

Ниже чек-лист с примерами доказательств второй группы, а [здесь](#) – первой.

Контроль

Артефакт и уровень соответствия

Зона ответственности

Остановка утечки

- Приказ/распоряжение о принятии экстренных мер (отключение / консервация системы / сервера, вкл. компоненты горизонтального перемещения / повышения привилегий злоумышленника, сброс паролей и т.д.)
- Архив собранных логов всех системных компонентов на всех уровнях за период инцидента с метками времени
- Отчеты SIEM/SOC/NAC/WAF о срабатывании автоматических правил блокировки / изоляции

- ИБ
- ИТ

Мониторинг и противодействие публикациям утекших данных

- Скриншоты / выписки найденных утечек на открытых площадках, отчет о результатах мониторинга утечек
- Отправленные требования владельцу / админу ресурса о снятии данных с публикации
- Подтверждение удаления / снятия данных с публикации

- ИБ
- Legal

Контроль

Артефакт и уровень соответствия

Зона ответственности

Создание рабочей группы и оценка инцидента

- Фиксация даты и времени обнаружения инцидента (служебная записка, email отчет и др.)
- Отчет с оценкой нарушения прав субъектов ПД, причинами инцидента, атрибутами скомпрометированных ПД
- Документирование создания рабочей группы
- «Карта воздействия» сценариев злоупотребления данными (моделирование доп. рисков, определение финансового урона)

- Руководство
- DPO
- ИБ
- Legal

Работа с контрагентами (если применимо)

- Уведомление контрагента об инциденте с требованием проверки (тикет, email и др.)
- Акт о выявленных нарушениях договора (NDA, SLA по ИБ, поручение) с приложением доказательств
- Расторжение договора и/или претензия о компенсации убытков / неустойке по договору
- Заключение договора с резервным вендором
- Направление вовлеченным поставщикам и партнерам писем о компрометации данных с целью принятия мер реагирования
- Киберфорензик отчет по системе контрагента

- DPO
- Legal
- Бизнес-подразделения
- ИБ

Уведомление регулятора*

- Зарегистрированные отправленные уведомления (24 / 72 часа)
- Актуализация ранее поданного уведомления (новые сведения, объем ПД и др.)

- Руководство
- DPO
- ИБ

* В случае нарушения прав субъектов ПД оператор подает уведомление регулятору о возникшей утечке. При этом необходимо учитывать особенности регулирования в зависимости от типа деятельности, например, кредитные организации дополнительно обязаны уведомить Банк России.

Контроль

Артефакт и уровень соответствия

Зона ответственности

Информирование
субъектов ПД
(если применимо)

- Уведомление субъектов ПД (с логами рассылки, шаблонами и др.)
- Публичное размещение пресс-релиза (PR-коммюнике) на официальном сайте
- Усиление первой линии для обработки запросов субъектов (скрипты чат-бота, горячая линия и т.д.)
- Журналирование обращений / жалоб субъектов
- Утвержденная программа поддержки субъектов (партнерские программы, льготы, компенсации)
- Доказательства добровольной компенсации пострадавшим из-за утечки

- DPO
- PR/Коммуникации
- Legal

Преследование
нарушителя

- Отчет с версией инцидента (вкл. потенциально виновных) в утечке правомерно собранных ПД
- Заявление в полицию: регистрация в КУСП (Книга учета сообщений о происшествиях)
- Постановление о возбуждении уголовного дела
- Распоряжение о применении дисциплинарного взыскания для внутреннего нарушителя

- Legal
- Руководство (при поддержке ИБ)

Исправление

- Досье инцидента: хронология, действия, решения, коммуникации, RCA, исправления, профилактики
- Утвержденная дорожная карта исправлений (RACI, сроки, ресурсы, приоритеты)
- Отчет о выполнении дорожной карты исправлений
- Отчеты пентестов на исправленных системах (внутренний и внешний)
- Подтверждение повышения осведомленности привилегированных и простых пользователей (отчеты о тренингах, результаты тестирования и т.д.)

- Координатор рабочей группы (DPO/ИБ)
- Legal
- Бизнес-подразделения

Не является результатом оказания юридических услуг. Если необходима консультация, мы рады помочь.



Артем Дмитриев
Управляющий партнер

artem.dmitriev@comply.ru
t.me/artydmritriev
+7 (961) 806 27-76

Comply.

Comply.ru
info@comply.ru
t.me/comply_ru