Чек-лист:

6 ШАГОВ ДЛЯ УСТРАНЕНИЯ ПОСЛЕДСТВИЙ УТЕЧКИ



В 2022 г. в Закон о персональных данных введена обязанность операторов сообщать уполномоченным органам об инцидентах с персональными данными. Организации обязаны в течение 24 часов сообщать в Роскомнадзор (субъекты КИИ – в НКЦКИ) о случившихся инцидентах, а в течение 72 часов с обнаружения нарушений – отчитаться об итогах внутреннего расследования. Ниже – инструкция, как действовать в случае инцидента, расследовать его и отчитаться регулятору.

SEARCHINFORM
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1 Соберите рабочую группу

Заранее распределите задачи, которые необходимо закрыть при утечке информации, между разными отделами.

Как?

- ИБ- и ИТ-отделы отвечают за устранение утечки, оценку ее масштабов и расследование, готовят отчеты для регулятора и доказательства для представления в контролирующих органах и в суде.
- Бизнес-подразделение, руководство и пиар-отдел: сообщают клиентам об утечке.
- Пиар-отдел: занимается отработкой негатива в СМИ и соцсетях.
- Юристы оценивают и нивелируют правовые риски, ведут коммуникацию в случае проверок, представляют интересы организации в контролирующих органах и в судах.

Зачем?

В экстренной ситуации ответственные отделы помогут быстро предотвратить последствия утечки для компании.

2 Уведомьте регулятора

Всем операторам ПДн необходимо отчитываться об инцидентах в уполномоченные органы. Согласно приказу ФСБ № 77, субъекты КИИ сообщают о нарушениях в НКЦКИ, а операторы, не относящиеся к КИИ – в Роскомнадзор. Финансовые учреждения сообщают об инцидентах в Банк России согласно Стандарту № СТО БР БФБО-1.5-2023.

Как?

- Сообщение в Роскомнадзор подается через форму на портале регулятора, с использованием аутентификации через «Госуслуги». Альтернативный вариант – отправить уведомление на бумаге в территориальное управление Роскомнадзора.
- Субъекты КИИ могут сообщить о нарушениях с ПДн в НКЦКИ или ФинЦЕРТ так же, как и о других инцидентах. Некоторые ИБ-средства позволяют автоматизировать процесс: сформировать и отправить отчет через программный интерфейс приложения (API). Альтернативные варианты – электронная и обычная почта.
- Передавать нужно: сведения о предполагаемых причинах и последствиях события, принимаемых мерах по ликвидации утечки. Современные ИБ-средства позволяют оперативно собрать и выгрузить все нужные для отчета сведения.

Это важно сделать в течение 24 часов с момента обнаружения инцидента!

Зачем?

1. Неуведомление или пропуск сроков для уведомления уполномоченных органов с 2025 года наказываются штрафами: от 1 до 3 млн рублей для бизнеса и от 400 до 800 тыс. рублей для должностных лиц органов власти, учреждений бюджетной и некоммерческой сфер.

2. Содействие регулятору в установлении обстоятельств нарушения, согласно КоАП РФ, является смягчающим обстоятельством.

3 Проведите расследование

Как?

- Оцените масштаб утечки – сколько записей утекло, сколько среди них уникальных, пострадали ли ПДн специальных категорий или биометрия.
- Определите канал утечки: почта, внешние носители, мессенджеры, облака, уязвимости ИТ-инфраструктуры и др.
- Установите, причастен ли сотрудник компании или внешний нарушитель, либо данные утекли не из вашей компании, а, например, от контрагента или ИТ-подрядчика.
- Установите обстоятельства инцидента: была ли это случайная утечка или умышленная и подготовленная акция.
- Уточните, какие меры защиты принимались до, во время и после инцидента, и как они помогли минимизировать ущерб.
- Соберите доказательства – опросите свидетелей, выгрузите данные из системы защиты от утечек информации (DLP), системы аудита и защиты файловых хранилищ (DCAP) и системы управления инцидентами информационной безопасности (SIEM) (скриншоты рабочего стола, архив переписки, аудит операций в файловой системе и т.д.) и др.

Зачем?

1. Расследование поможет увидеть «слабые места» в компании и закрыть их, что даст возможность предотвратить утечку в будущем и смягчить ответственность за действующий инцидент.

2. Данные расследования дадут доказательства, для привлечения к ответственности сотрудника или подрядчика и подтверждения добросовестности вашей организации.

В течение 72 часов передайте регулятору результаты внутреннего расследования: сообщите о виновных, причинах и вреде от инцидента.

4 Предупредите клиентов

Составьте простое и понятное письмо или публикацию с объяснениями и официальными извинениями, без профессиональных ИБ-терминов.

Как?

- Расскажите клиентам, что произошло и в каких масштабах.
- Объясните, какие меры предпринимаете для расследования утечки и как планируете усилить защиту.
- Сообщите, что за утечкой могут последовать фишинг, звонки мошенников, попытки использовать скомпрометированный аккаунт.
- Расскажите, как могут действовать мошенники и посоветуйте, как избежать угрозы с их стороны: сменить пароли, ввести двухфакторную аутентификацию, перепривязать почту и т.д.
- Предложите клиентам, чьи данные пострадали, корпоративные бонусы, скидки или подарки. Это покажет лояльность к клиентам.
- Будьте готовы к запросам клиентов. Одни попросят уточнить статус работы с данными, другие – отзовут согласие на обработку. На запросы необходимо отвечать не позже, чем через 10 рабочих дней с момента их получения, а прекращать обработку ПДн при отзыве согласия – в срок, установленный согласием или не позднее, чем через 30 календарных дней с даты такого отзыва.
- Передайте информацию об утечке в СМИ. Следует придерживаться такой позиции: «Мы допустили ошибку, не скрываем этого, работаем над тем, чтобы устранить последствия и не оступаться впредь».

Зачем?

1. Разослав клиентам предупреждение об утечке, вы дадите им возможность самостоятельно защитить себя и покажет клиентоориентированность вашей организации;

2. Так будет больше шансов сохранить репутацию: вы успеете объяснить ситуацию до того, как информация появится в СМИ.

3. Внимание к клиентам в случае инцидента снизит риск их оттока и обращений с жалобами и требованиями.

5 Устройте профилактику

Как?

- Обучайте сотрудников ИБ-грамотности. Важно освещать темы фишинга, парольной политики, правила блокировки ПК, безопасного логического доступа.
- Наведите порядок в ИТ-инфраструктуре: разграничьте доступ к защищаемым файлам, удалите их дубликаты. Настройте двухфакторную аутентификацию для доступа к ИСПДн, используйте защищенные каналы передачи данных.
- Внедрите технические средства защиты, если их раньше не было. Настройте политики ИБ: в системе аудита и защиты файловых хранилищ (DCAP) – на обнаружение персональных данных, в системе защиты от утечек информации (DLP) – на контроль действий с такими файлами, в системе управления инцидентами ИБ (SIEM) – на поиск уязвимостей и выявление подключений к ИСПДн.
- Введите ответственность за разглашение конфиденциальной информации.

Зачем?

Профилактика снизит риски, что инцидент повторится и покажет, что вы пресекли угрозы дальнейших нарушений.

6 Готовьтесь к суду

Если протокол о нарушении по факту утечки составлен, дело попадет в суд. Помимо этого, в ходе внутреннего расследования вы можете найти признаки преступления. Пострадавшие могут обратиться к вам с исками. Все это – зона совместной ответственности: юристы будут представлять интересы компании, а задача службы ИБ – дать им необходимую доказательную базу.

Как?

- В ходе проверки Роскомнадзора, перед заседанием суда и в его процессе предоставьте письменные и устные пояснения. Покажите отчеты ИБ-систем, расскажите, какие меры вы принимаете для ликвидации последствий и исключения дальнейших рисков, просите об участии в деле ваших ИБ-специалистов как свидетелей. Ссылайтесь на то, что вы изначально принимали меры к предотвращению инцидента, помогли установить его обстоятельства, минимизировали последствия и риски .
- Если вы выяснили, что в утечке виноват внутренний нарушитель, обратитесь в МВД с заявлением о преступлении(ст. 183, 272 или 272.1 УК РФ). Сообщите об этом в Роскомнадзор. Как действовать по такому сценарию, мы рассказали в **памятке**.
- Если инцидент произошел у подрядчика, то по итогам дела вы можете обратиться к нему с иском о компенсации нанесенного вам ущерба. Оцените вред в денежной сумме, подтвердить, что инцидент произошел по вине контрагента, а ваша компания приняла все необходимые меры к защите персональных данных.
- Если к вам обратились с исками пострадавшие граждане, проведите переговоры, предложите мировое соглашение. Если истцы не согласятся, ссылайтесь в суде на принятие мер к минимизации последствий утечки и добровольное раскрытие информации о ней вашим клиентам.

Зачем?

1. Если вы соберете достаточно сведений, чтобы подтвердить факт преступления, причастность нарушителя и добросовестность вашей компании, у организации есть **шансы** избежать наказания или серьезно его снизить.

2. Существует **судебная практика**, подтверждающая возможность возмещения нанесенного подрядчиком ущерба от утечки персональных данных.

SEARCHINFORM
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

«СёрчИнформ» – ведущий российский разработчик средств информационной безопасности. Входит в ассоциации «РУССОФТ» и АПКИТ. Клиенты – более 4000 компаний по всей России и в 20+ странах мира.

В активе команды разработчиков – инструменты, которые позволяют комплексно контролировать источники внутренних угроз на всех уровнях информационной системы компании.

«СёрчИнформ КИБ»

Система защиты информации от утечки (DLP) «СёрчИнформ КИБ» блокирует утечки информации и обнаруживает признаки корпоративного мошенничества: откатов, боковых схем, саботажа, воровства.

«СёрчИнформ Файловый Аудитор»

Система аудита и защиты файловых ресурсов (DCAP) «СёрчИнформ Файловый Аудитор» («СёрчИнформ FileAuditor») классифицирует критичные данные, позволяет управлять доступом к ним и контролирует операции в файловой системе.

«СёрчИнформ Мониторинг безопасности»

Система управления инцидентами ИБ (SIEM) «СёрчИнформ Мониторинг безопасности» («СёрчИнформ SIEM») проводит мониторинг событий безопасности в корпоративной ИТ-инфраструктуре, выявляет сбои оборудования и ПО, признаки внешних атак и опасные действия пользователей.

«Аутсорсинг ИБ»

Сервис информационной безопасности по подписке без трудозатрат со стороны заказчика. ИБ-аналитик возьмет на себя мониторинг и реагирование на них, расследование инцидентов и отчеты перед заказчиком.

«СёрчИнформ КИБ» и другие инструменты внутренней ИБ можно развернуть в облаке. Компания получит защиту по подписке без единовременных затрат на закупку лицензий ПО и оборудования, на котором такой софт должен работать.

Больше аналитики и новостей безопасности читайте на сайте компании searchinform.ru, в телеграм-канале или в MAX.

Белые книги, памятки, чек-листы и результаты исследований можно посмотреть на сайте searchinform.ru в разделе «Практика и аналитика».