Nevel

БЕЗОПАСНОСТЬ

Реагирование на инциденты

Локализация, доказательства, роли, восстановление и уведомление Роскомнадзора в предусмотренных законом случаях.

Облако / В контуре

https://docs.nevel.sh/security/incidents/

Процедура применяется к подозрению на несанкционированный доступ, раскрытие данных, нарушение маршрута, компрометацию ключа и отказ защитного компонента. Её результат — остановить дальнейшее воздействие, установить затронутую область, сохранить доказательства, выполнить необходимые уведомления и безопасно вернуть сервис в работу.

Технический сигнал и подтверждённый инцидент различаются. Срабатывание статистического порога требует разбора; оно не доказывает утечку. Одновременно отсутствие оповещения не отменяет сообщение пользователя, уведомление провайдера или обнаруженную в журнале передачу. Каналы первичного обнаружения описаны в мониторинге.

Роли и готовность до события

Организация назначает координатора инцидента и заместителя, специалиста ИБ, технического исполнителя и ответственного за персональные данные. Координатор ведёт общую временную шкалу; ИБ оценивает воздействие и доказательства; технический исполнитель меняет доступ и маршруты; уполномоченное лицо принимает юридические решения и направляет необходимые уведомления.

В облаке Nevel расследует собственные компоненты и предоставляет заказчику относящиеся к нему факты. Заказчик проверяет своих пользователей, интеграции, устройства и основания обработки. В on-prem технические действия с установленной платформой выполняет эксплуатационная команда заказчика в пределах распределения работ; доступ поддержки Nevel предоставляется по действующим полномочиям. Если запрос использовал внешний разрешённый маршрут, расследование включает соответствующего российского провайдера, self-hosted инфраструктуру Nevel или глобальную цепочку API. Само размещение Platform у заказчика не исключает внешнего получателя. Передача диагностического архива не становится разрешённой только потому, что возник инцидент.

Контактный лист хранится вне единственного потенциально недоступного сервиса. В нём указаны основной и резервный канал, ответственный за получение, порядок работы вне обычного графика и адрес защищённого обмена материалами. Срок реакции поддержки и срок уведомления органа власти имеют разные основания. Условие одного клиентского договора нельзя автоматически применять ко всем установкам.

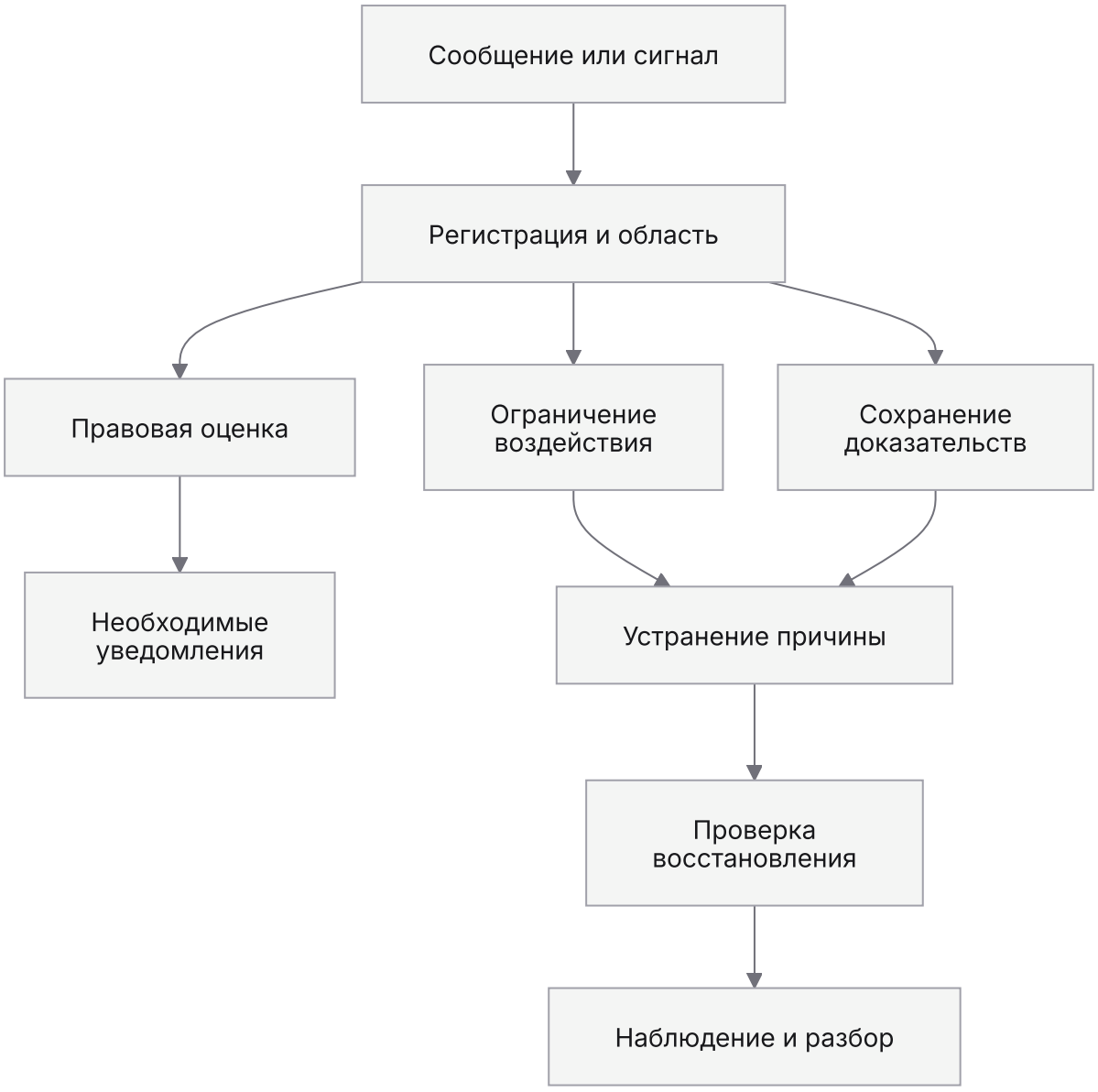
Первые действия

1. **Зарегистрировать событие.** Присвоить номер, сохранить время первого сообщения, время предполагаемой операции и источник. Не заменять раннюю отметку временем открытия задачи инженером.
2. **Установить область.** Определить организацию, пользователей, ключи, файлы, модели и интервал. Проверить, затронуты ли другие пространства, не раскрывая заказчику чужие данные.
3. **Остановить продолжение.** Отозвать подозрительный ключ или сессию, отключить скомпрометированное подключение, запретить конкретный маршрут либо ограничить затронутую функцию.
4. **Зафиксировать состояние.** Сохранить доступные журналы, версии политик, настройки маршрута, сетевые события и подтверждения выполненных действий.
5. **Оценивать последствия параллельно.** Не ждать полного восстановления, чтобы привлечь ответственного за персональные данные и запустить необходимые уведомления.

Ограничение выбирается по механизму угрозы. Для утечки одного ключа первичным действием служит отзыв этого ключа и проверка его обращений. При ошибке общей политики недостаточно отключить одного пользователя: блокируется опасный маршрут для всей затронутой категории. Если DLP недоступен, восстановление доступности не должно включать обход обязательной проверки. Границы допустимого переключения определены в архитектуре и сетевой защите.

СХЕМА 1

Реагирование на инцидент



Что доказывать в расследовании

Ключевой вопрос для модельного запроса — прошли ли данные границу получателя. Отказ после отправки не означает, что передача не состоялась; блокировка до исходящего вызова имеет другой характер. Восстановление цепочки идёт от идентификатора операции через проверку прав, формирование контекста, решение Guardrail, исходящий вызов и обработку ответа.

Материал	Что устанавливает	Как ограничить раскрытие
Журналы запроса и маршрута	Время, участника, получателя, стадию и результат	Выгружать относящиеся к событию записи

Материал	Что устанавливает	Как ограничить раскрытие
Версия политики	Правило, действовавшее при операции	Сохранять версию и изменения, не заменять текущей конфигурацией
Журнал ключа и доступа	Полномочия и действия предполагаемого участника	Использовать идентификатор ключа, не его секрет
Сетевые события	Фактическое соединение с получателем	Учитывать NAT, прокси и временные метки
Сведения об объекте	Затронутые категории и объём	Начать с метаданных; содержание открывать по необходимости
Действия реагирования	Кто и когда ограничил или восстановил работу	Фиксировать каждое изменение и его результат

Доказательства сохраняются в ограниченном хранилище с учётом доступа и целостности. Для экспортированного файла фиксируются источник, время выгрузки, исполнитель и контрольная сумма. Рабочая копия отделяется от сохранённого экземпляра. Это рекомендуемая организация расследования, а не заявление о наличии у каждой установки отдельной криминалистической системы.

Нельзя очищать аудит ради уменьшения числа ошибок на панели. С другой стороны, инцидент не разрешает бессрочно собирать все тела запросов. Объём и срок сохранения материалов определяются расследованием и применимыми основаниями; обычные правила описаны в хранении данных.

Когда действуют 24 и 72 часа

Часть 3.1 статьи 21 152-ФЗ относится к установленному факту неправомерной или случайной передачи, предоставления, распространения либо доступа к персональным данным, повлёкшему нарушение прав субъектов. Обязанность уведомить Роскомнадзор возложена на оператора. Отсчёт связан с выявлением такого инцидента оператором, регулятором или иным заинтересованным лицом. Официальный текст 152-ФЗ, статья 21.

Срок от выявления	Содержание уведомления
В течение 24 часов	Инцидент, предполагаемые причины и вред, принятые меры, уполномоченное контактное лицо
В течение 72 часов	Результаты внутреннего расследования; сведения о лицах, действия которых стали причиной, при наличии

Оба срока идут от одного момента: это не 24 часа плюс ещё 72. Норма задаёт часы, не рабочие дни. Например, от отметки 10:00 во вторник пределы наступают в 10:00 среды и пятницы. Полного установления причины не требуется для первичного сообщения: закон прямо предусматривает предполагаемые причины и вред. Пункты 1–2 части 3.1 статьи 21.

Поручение обработки должно предусматривать уведомление оператора о таких случаях. Nevel, действуя по поручению заказчика, передаёт сведения оператору; это не означает автоматического представительства перед регулятором. Роли определяются для конкретных данных и операций. Статья 6, часть 3.

Практически в карточке следует вести три отдельные отметки: когда произошло действие, когда выявлен указанный законом инцидент и когда команда получила сообщение. Разница между ними объясняется фактами. Открытие внутреннего расследования не используется для произвольного переноса начала отсчёта. Другие отраслевые обязанности рассматриваются отдельно по карте требований РФ.

Подготовка и передача уведомления

Порядок взаимодействия установлен приказом Роскомнадзора № 187 от 14.11.2022. Первичное сообщение включает сведения об операторе, дате и времени выявления, характеристиках затронутых данных и числе записей, предполагаемых причинах и вреде, принятых мерах и контактном лице. Дополнительное отражает результаты расследования и уточнённые меры. Официальная публикация приказа № 187.

Приказ допускает бумажное и электронное направление. Электронная специализированная форма используется после авторизации через ЕСИА; уведомление подписывается электронной подписью согласно установленному порядку. Для дополнительного электронного сообщения сохраняются номер и ключ первичного уведомления. Они позволяют связать материалы одного события и не предназначены для публичного размещения. Приказ № 187, порядок взаимодействия.

Внутренний пакет готовится так, чтобы уполномоченный сотрудник мог заполнить форму без повторного опроса инженеров. Подтверждённые факты отделяются от гипотез, неизвестное обозначается явно. Число запросов не подменяет число записей или субъектов. Копия направленного сообщения, время отправки и подтверждение получения сохраняются в деле инцидента. Рабочую доступность учётной записи и способ подписания проверяют заранее, а не в последние минуты срока.

Возврат в работу и приёмка процедуры

Возврат начинается после устранения механизма нарушения: отзыва старого ключа, исправления прав или политики, проверки затронутого получателя. Контрольный запрос должен подтвердить разрешённое действие, а отрицательный тест — запрет повторения опасного сценария. Для восстановления из копии применяются проверки эксплуатации и DR.

Учебная проверка включает утечку тестового ключа, ошибку маршрута и ложный сигнал DLP. Команда должна найти действие по идентификатору, ограничить нужную область, собрать обезличенный пакет, определить применимость уведомления и рассчитать сроки. Уведомление в учебном сценарии готовится как черновик, без отправки вымышленного события регулятору.

Закрытие фиксирует причину, масштаб, временную шкалу, принятые меры и владельцев оставшихся действий. Успешный повторный запрос сам по себе не закрывает расследование. Нормативная справка на 8 сентября 2026 года и версии применимых актов приведены в разделе о 152-ФЗ; сроки и порядок действий определяются действующими требованиями.