

РЕГЛАМЕНТ РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

что происходит с момента сбоя до записи в протоколе недели

редакция от 07.09.2026

1. Что считается инцидентом

- 1.1. Критичный. Остановлена работа заказчика. Не работает запись пациентов или приём заявок, сайт, телефония, учётная система, касса. Сюда же утечка данных и подозрение на взлом.
- 1.2. Обычный. Система работает с ошибками или медленно, приём и выдача не остановлены.
- 1.3. Класс инцидента определяет дежурный при подтверждении обращения и сообщает его заказчику.

2. Как сообщить

- 2.1. Любым каналом из графика дежурства. Telegram @tech_ash_it, телефон +7 (499) 113-71-05, почта info@protocol-it.ru.
- 2.2. Что написать. Что не работает, с какого времени, кого касается (один сотрудник, филиал, все), снимок экрана, если есть. На снимке не должно быть данных пациентов, клиентов и заёмщиков.
- 2.3. Сбои, которые видит мониторинг, дежурный берёт в работу без обращения и сам сообщает заказчику.

3. Сроки

Шаг	Критичный	Обычный
Подтверждение получения и класс инцидента	1 час в рабочее время	1 час в рабочее время
Приступаем к работе	4 часа в рабочее время	срок называется в ответе
Сообщение заказчику о ходе работ	каждые 2 часа до восстановления	по завершении
Разбор письменно	акт в течение 3 рабочих дней	строка в протоколе недели

Вне рабочего времени сроки считаются с 9:00 следующего рабочего дня. Для заказчиков с круглосуточным режимом сроки записаны в договоре сопровождения.

4. Кто

- 4.1. Дежурный по графику принимает обращение, определяет класс и назначает исполнителя.
- 4.2. Критичный инцидент ведёт ИТ-директор проекта или руководитель сопровождения. Второй исполнитель подключается сразу и ведёт журнал.
- 4.3. Со стороны заказчика нужен ответственный, который принимает решения о простое и подтверждает восстановление. Его контакт записан в договоре.

5. Ход работ

- 5.1. Подтвердить. Дежурный отвечает заказчику, называет класс инцидента и время следующего сообщения.
- 5.2. Оценить. Что именно не работает, сколько людей затронуто, есть ли риск данных.

- 5.3. Обойти. Пока идёт восстановление, работа заказчика продолжается по обходной схеме. Для клиники бумажная форма записи у стойки, для финансовой компании приём заявок по телефону с внесением после подъёма, переадресация номеров на мобильные по списку.
- 5.4. Восстановить. По плану восстановления заказчика, из проверенной копии, на резервном сервере или на том же после починки.
- 5.5. Проверить вместе с заказчиком. Сверка по контрольным числам, подтверждение ответственного, закрытие инцидента с записью времени.

6. Утечка или подозрение на взлом

- 6.1. Затронутая система изолируется от сети, доступы, которые могли быть скомпрометированы, отзываются немедленно.
- 6.2. Заказчик уведомляется немедленно, не позднее часа с момента обнаружения.
- 6.3. Заказчик как оператор персональных данных уведомляет Роскомнадзор в течение 24 часов о факте и в течение 72 часов о результатах разбора, по части 3.1 статьи 21 Федерального закона № 152-ФЗ. Мы готовим проект уведомления и описание инцидента.
- 6.4. Финансовая организация уведомляет Банк России в порядке и сроки, установленные для её вида, проект уведомления готовим мы.
- 6.4.1. Если заказчик — субъект критической информационной инфраструктуры (клиника или финансовая компания — юридическое лицо), он без промедления информирует НКЦКИ о компьютерном инциденте в порядке и сроки, установленные ФСБ России (пункт 1 части 2 статьи 9 Федерального закона № 187-ФЗ). Проект сообщения готовим мы. Уведомление об утечке через портал Роскомнадзора по пункту 6.3 информирование ГосСОПКА об этой утечке уже закрывает.
- 6.5. Выкуп вымогателям не обсуждается. Восстановление идёт из проверенной копии на чистое оборудование.

7. После инцидента

- 7.1. Каждый инцидент попадает в протокол недели. Причина, что сделано, сколько заняло, что меняем, чтобы не повторилось.
- 7.2. По критичному инциденту в течение 3 рабочих дней составляется акт с временем обнаружения, временем восстановления и потерянными данными.
- 7.3. Если инцидент показал разрыв в плане восстановления, план пересматривается, следующие учения проверяют исправление.

ИТ-директор проекта

(подпись)

С. Михайлов

Действующий документ компании «Протокол», protocol-it.ru. Передаётся заказчику при подписании договора, пересматривается после каждого критичного инцидента.