

Первые пятнадцать минут

Памятка дежурного при критичном инциденте. На стену

Порядок действий

Когда	Что делаете
0–2 мин	Убеждаетесь, что сбой реальный: проверяете сами, а не по одному звонку
2–3 мин	Признаёте инцидент критичным, если подходит хоть один признак. Не подходит — работаете обычным порядком
3–5 мин	Назначаете координатора. Если никого — координатор вы, и тогда вы не чините
5–8 мин	Открываете канал взаимодействия. Собираете тех, кто нужен по симптомам, а не по оргструктуре
8–12 мин	Отправляете первичное оповещение. Пишете, что не работает и когда следующее сообщение
12–15 мин	Начинаете вести хронологию: время, событие, кто сообщил

Дальше — по порядку работы при критичном инциденте.

Признаки критичного

Хватает **одного**:

- недоступна услуга первого уровня критичности;
- остановлено обслуживание клиентов;
- затронуты больше работников, чем установленный порог;
- под угрозой срок обязательств перед регулятором или контрагентом;
- нужна одновременная работа нескольких команд;
- инцидент Р1 не восстановлен в установленный срок;
- есть признаки нарушения информационной безопасности.

Что сказать в первом сообщении

> Зафиксирован сбой: **что именно не работает, словами пользователя**. > Затронуты: кто. Начало: время. > Работы ведутся. Обходной способ работы: есть такой-то / отсутствует. > Следующее сообщение в **время**.

Причину не называете. Первая версия причины неверна почти всегда, а разосланная наружу живёт дольше самой аварии.

Срок не выдумываете. «Пока не определено, следующее сообщение через полчаса» — честно и работает. Названный и не выдержанный срок дороже его отсутствия.

Три вещи, которые сломают всё

Вы чините сами. Через двадцать минут вы перестаёте и чинить, и руководить: вас отвлекают каждые три минуты. Координатор не чинит — в этом его работа.

Хронологию пишете потом. Потом не напишете: люди помнят события не в том порядке, в каком те происходили. Разбор по восстановленной по памяти хронологии даёт неверные выводы.

Инженеры отвечают на вопросы о сроках. Все вопросы — к вам. Ради этого канал и открывали.

Когда это уже не инцидент

Если восстановление штатными средствами невозможно и нужен переход на резервную площадку, резервные каналы или ручные процедуры — это работа по плану непрерывности, и решение принимает не дежурный.

Критерий перехода записан заранее. Найдите его до аварии, а не во время.

Перед тем как разойтись

- разослать завершающее оповещение;
- закрыть канал взаимодействия;
- **назначить дату разбора** — пока все ещё здесь;
- передать хронологию тому, кто проводит разбор.

Инцидент закрыт после разбора, а не после восстановления.

Телефоны

Список оповещения и контакты — в матрице эскалации. Проверьте, что он у вас под рукой **сейчас**, а не когда понадобится.