

Управление инцидентами

Выжимка практики. Что это, как устроено, чем меряется и где ломается

Практика «Управление инцидентами» (INC)

<https://itsm4u.ru/spravochnik/inc/>

Зачем практика

Инцидент — незапланированное прерывание услуги или снижение качества её работы по сравнению с согласованным уровнем.

Практика управления инцидентами существует ради одного: **сократить время, в течение которого услуга работает не так, как договорились**. Не найти виноватого и не докопаться до причины — причина остаётся за расследованием проблем, — а вернуть работу.

Из этой узкой цели следует всё остальное устройство практики. Восстановить работу можно обходным путём, не понимая причины, и это будет правильно. Отсюда же главный конфликт, в который упирается каждая вторая служба поддержки: **быстро восстановить и разобраться в причине — разные задачи, и смешивать их в одном процессе вредно**.

> Скорость восстановления — это не про инструмент. Это про то, назначен ли > владелец инцидента в каждый момент времени.

Когда практика работает

Практика считается работающей не по наличию регламента, а по трём вещам, которые получаются или не получаются.

Сбой находят раньше, чем о нём сообщат. Проверяемый признак: известна доля инцидентов, пришедших от средств наблюдения, а не от людей, и она растёт. Пока эта доля не считается, о раннем обнаружении говорить не о чем.

Работу восстанавливают быстро и тем способом, который потом можно повторить. Проверяемый признак: способ решения записан в самой записи, а не остался в голове того, кто чинил. Быстро, но неповторяемо — это не результат практики, это удача конкретного инженера.

Подход к восстановлению пересматривают. Проверяемый признак: после критичных инцидентов проходит разбор, и его выводы доходят до изменений в процессе, в моделях инцидентов или в средствах наблюдения. Разбор, который заканчивается протоколом, третьему признаку не соответствует.

По каждому можно ответить «да» или «нет», не открывая регламент.

Что входит и что рядом

Половина споров про управление инцидентами — это спор о границе.

Входит в практику	Рядом, но это другая практика
Обнаружение и регистрация сбоя	Наблюдение за состоянием систем

Входит в практику	Рядом, но это другая практика
Классификация, оценка влияния и срочности	Приём и сопровождение обращений
Диагностика и поиск способа восстановить работу	Расследование причин
Восстановление, в том числе обходным путём	Внесение изменений
Ведение записи и хода диагностики	Оформление решения в базу знаний
Оповещение о ходе восстановления	Договорённости о сроках
Разбор после решения	Доведение выводов до изменений
Отсев обращений, которые сбоем не являются	Исполнение самих запросов

Отдельно про две границы, которые чаще всего стирают.

Инцидент и проблема. Практика не обязана находить причину. Её задача – вернуть работу. Смешение даёт узнаваемый эффект: инженер держит заявку открытой, пока не поймёт, что случилось, а пользователь всё это время сидит без услуги.

Инцидент и непрерывность. Отказ, при котором обычного восстановления не хватает, перестаёт быть инцидентом. Критерий перехода задаётся заранее: решать его в момент аварии – значит не решить вовсе.

Как это устроено

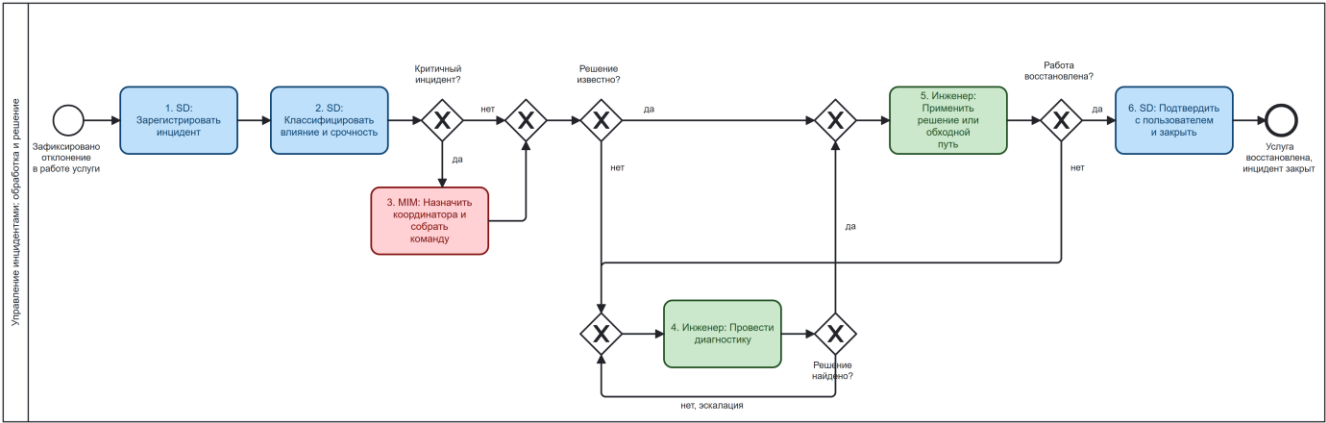


Схема процесса управления инцидентами. Нумерация шагов совпадает с таблицей ниже. Исходник для правок – [раздел «Как это работает» на сайте](#)

Обнаружение показано не шагом, а стартовым событием: сигнал может прийти и от средств наблюдения, и от пользователя, и от инженера, но дальше поток один.

Три возврата на схеме важнее прямого хода. Диагностика не сработала – эскалация. Решение применили, а работа не восстановилась – обратно в диагностику. Именно эти петли съедают время, и именно они не описаны в большинстве регламентов.

Владелец инцидента должен быть в каждый момент времени. Владение может передаваться по ходу, но не должно исчезать. Инцидент без владельца – это инцидент, о котором все думают, что им занимается кто-то другой.

Чем меряется

Здесь четыре показателя из девяти – те, с которых имеет смысл начинать.

Что меряем	Зачем	Чем искажается
Доля инцидентов, обнаруженных средствами наблюдения	Отделяет зрелую эксплуатацию от реактивной	Растёт от шумных срабатываний, которые инцидентами не являются
Доля решённых первой линией	Качество классификации и базы знаний	Улучшается закрытием сложных случаев «по истечении времени»
Доля восстановленных в срок	Выполняются ли обещания	Паузой «ожидание» без причины; переводом инцидентов в запросы
Удовлетворённость тех, кого сбой задел	Противовес остальным: при слишком быстром закрытии те растут, а эта падает	Портится частыми опросами

У показателя должно быть два числа, а не одно. Целевое значение и значение, при котором пора вмешиваться. Цель показывает, куда идём, порог – когда переставать наблюдать и начинать действовать.

Ни один показатель нельзя делать целевым в одиночку. Требование «закрывать 95% в срок» получают не ускорением работы, а переклассификацией: инциденты начинают заводиться как запросы, срок по которым мягче. Формально выполнено, реально стало хуже.

Где ломается

Два из шести узнаваемых мест. Остальные разобраны на странице практики.

Инциденты не доходят до системы. Часть решается в мессенджерах и коридорах и в записи не попадает. Проверяется просто: возьмите рабочие чаты поддержки за неделю и посчитайте, сколько раз там что-то починили, не заведя записи. Даже грубый счёт обычно даёт десятки – и тогда показатели надёжности отражают дисциплину регистрации, а не работу систем.

Обходные решения копят и превращаются в технический долг. Долг этот измеримый, а не образный, и считается тремя числами: сколько обходных решений применяется сейчас, сколько раз каждое применено за период и сколько времени прошло с первого применения. Обходное решение, живущее полгода и применённое сорок раз, – это уже не временная мера, а незадокументированная часть услуги.

Где вы сейчас

Пять уровней зрелости. Здесь два из пяти — чтобы было видно, как устроена шкала. Разница между уровнями не в том, есть ли документ, а в том, что происходит в понедельник утром.

Уровень 2 — повторяемый. Привычки сложились, но нигде не записаны. Все обращения попадают в одно место. У инцидента есть ответственный. Инцидент отличают от запроса хотя бы на словах, и это отличие одинаково понимают на первой линии.

Уровень 3 — определённый. Порядок описан и применяется. Приоритет назначается по правилу, а не по тому, кто громче попросил. Новый сотрудник может работать по написанному без наставника. Ход диагностики фиксируется по мере работы. Есть отдельный порядок для критичных инцидентов.

Уровни 4 и 5, полный перечень признаков и вопросы для самооценки — на странице практики. Самооценка проходится за десять минут и считается в браузере: никуда ничего не отправляется.

Что нужно собрать, чтобы это заработало

Карта документов практики. Каждый вырастает из своего раздела разбора.

Слой	Документы
Порядок работы	Регламент управления инцидентами
Правила	Перечень услуг и критичность · Матрица приоритетов и сроки · Классификатор · Матрица эскалации и оповещения
Рабочие формы	Карточка инцидента · Модель инцидента · Порядок при критичном инциденте · Форма разбора · Реестр обходных решений
Роли и договорённости	Роли и матрица ответственности · Согласование понятий с подрядчиком
Измерение	Паспорта показателей · Форма отчёта
Ввод в действие	Приказ и план-график

Порядок сборки важнее состава: сначала услуги, потом приоритеты, потом настройка системы, и только четвёртым — регламент. Регламент, написанный первым, ссылается на то, чего ещё нет, и через две недели переписывается наполовину.

На чём это основано

Свод	Раздел
ITIL 4	Отдельное практическое руководство Incident Management
COBIT 2019	Цель DSS02 «Управление запросами на обслуживание и инцидентами»
ISO/IEC 20000-1	Требования к управлению инцидентами и запросами
MOF 4.0	SMF-функция «Обслуживание заказчиков» на этапе «Эксплуатация»

Разбор опирается на тринадцать источников, включая процессное руководство Стейнберга, описание процесса Fermilab как пример настоящего внедрённого регламента и книгу Брукса о показателях. Полный список со ссылками — на странице практики.

Дальше

Разбор целиком — с таблицей шагов, перечнем полей записи, разбором автоматизации по активностям, полными критериями зрелости и всеми шестью местами, где практика ломается, — открыт и лежит на странице практики.

Комплект документов для внедрения — там же.

Где почитать подробнее

Этот документ вырос из разбора практики. Там же — схема в исходнике, критерии зрелости с вопросами самооценки и материалы по теме.

- [Зачем эта практика](#)
- [Когда практика работает](#)
- [Что входит и что рядом](#)
- [Как это работает](#)
- [Как измерять](#)
- [Критерии зрелости](#)
- [Где ломается чаще всего](#)

Практика целиком: <https://itsm4u.ru/spravochnik/inc/>