

Инцидент менеджмент

Выявление и устранение непредвиденных ситуаций

Что такое инцидент? 🔥

Мы определяем инцидент как событие, которое приводит к нарушению или снижению качества работы сервиса и требует незамедлительных действий.

Устранение инцидентов 🧑🚒

Инцидент считается устраненным, когда затронутый сервис возобновляет работу в обычном режиме.

Это подразумевает выполнение лишь тех задач, которые необходимы для восстановления всех функциональных возможностей.

Разбор инцидента 🤔

Разбор инцидента выполняется после его устранения и включает выяснение основной причины инцидента и планирование действий (шагов) для ее устранения, чтобы не допустить повторных инцидентов.

Когда создать инцидент?

Если какой-то сервис* не работает уже 1 минуту,
и вы попробовали CTRL+SHIFT+R

Сервис – в широком смысле слова функционал сайта, приложения
или элемент инфраструктуры.

Как создать инцидент? 

Тикет с типом Ошибка и приоритетом Неотложный
появляется в Инцидентах через 1 минуту

Классификация инцидентов 🚒👉

- Неотложные – ошибки в работе инфраструктуры для проектов
- Срочные – ошибки внутри самого сайта (приложения)

Это сделано для разделения зон ответственности группы эксплуатации и команды проекта.

Устранение срочных ошибок в приложениях 🤖

Для срочных ошибок программных проектов есть возможность сделать детальный разбор случившегося.

В список попадают срочные ошибки, которые были исправлены и выпущены – есть версия исправления у тикета.

Может это всё-таки не инцидент? ☐

Изменение приоритета инцидента доступно руководителям проектов и ведущим программистам.

Не заматайте “сор под ковёр” – потом может быть еще больнее. 🔥

1. Обнаружение

Мы должны узнавать о проблемах раньше, чем клиенты

2. Реагирование

Реагируй быстро, собери всех, кто тебе может потребоваться в чате (портала) и Дискорде

Координируй действия исполнителей других информационных систем (1С и проч.), если требуется

Извести руководителей ИТ служб, если авария достаточно серьезная.

Если портал не доступен, то в чате дискорда.

3. Восстановление

Проблемы случаются, их надо устранять максимально быстро

4. Выводы

Никакого поиска виновных, мы улучшаем работу отдела

5. Улучшения 😇

Никогда не допускайте повторения инцидентов

Контрольные временные точки

1. **Время возникновения** – реальная дата возникновения, даже если релиз был несколько дней назад.
2. **Время оповещение** – когда мы о нем узнали из автоматического тикета или из средств коммуникаций.
3. **Начало устранения** – время, когда мы непосредственно начали работы по восстановлению работоспособности.
4. **Окончание устранения** – приложение или системы работают как обычно (на момент возникновения аварии).

Влияние инцидента или ошибки 🤖

1. Доступность сайта или его сервиса – мы не можем взаимодействовать с сайтом или его частью в принципе.
2. Скорость работы – есть замедление скорости работы выше оговорённого предела – обычно 2 секунды.
3. Достоверность данных – приложение отображает ошибочные данные с точки зрения бизнес-логики внутри приложения.
4. Актуальность данных – в приложении ошибочные данные (не)полученные из другой системы.
5. Безопасность проекта – выявлена уязвимость в работе или настройках.

Обнаружение инцидента

- Мониторинг
- Клиент
- Сотрудник компании
- Сотрудник ИНТ
- Директор ГК

Критические сбои должен выявлять мониторинг.

Затрагиваемые группы пользователей и влияние на них

Какая группа пользователей могла наблюдать ошибку или проблему.

Процент влияние на пользователей оценивается приблизительно исходя из потенциального охвата.

- до 5%
- до 20%
- свыше 20%

Причины возникновения 🙄

1. Сбой аппаратной части
2. Ошибка настройки инфраструктуры
3. Ошибка в приложении – неверно написан код и он прошел приёмочный тест.
4. Сбой DNS
5. Проблема с каналом связи
6. Технические работы по плану
7. Человеческая ошибка – случайно выполненные действия
8. Злонамеренные действия – внешняя атака

Симптомы события. Что наблюдали пользователи? 🙄

Опишите, как проблема или ошибка выглядела у пользователей.

Что работало не должным образом? 🚧

Предшествующие события, катализатор проявления – укажите, что не работало или могло послужить катализатором проявления.

Укажите номер тикета, если работы или релиз по нему послужили катализатором возникновения этой ошибки.

Тикет, приведший к проблемам 📄

Ссылка на тикет в Ютреке, работы по которому вызвали эти последствия.

Если работ не было, и это воздействие внешнего фактора, то это поле заполняется номером текущего тикета инцидента.

Основная причина. Используйте "Метод 5 почему".

Выясните изначальную первопричину, которая вызвала эту ошибку или проблему – чтобы ее устранение позволило никогда не допустить повторения.

Действия по ликвидации и восстановлению работоспособности

Опишите все действия, которые потребовались и были предприняты для возвращения сервиса в работоспособное состояние.

Улучшить, чтобы не допустить повторения ☐

- Инфраструктуру развёртывания приложений
- Код приложения и (или) его тестирование
- Мониторинг
- Регламентную инструкцию, обучение сотрудника

Критерий улучшений для инцидентов

1. Время безаварийной работы MTBF увеличивается
1. Интервалы $MTT(A, R, D)$ уменьшаются (время обнаружения TTA, время диагностики TTD и время на устранение TTR)
1. Количество инцидентов и их величина уменьшается со временем для проекта

Изменения и улучшения процесса

1. Следить за своевременностью заполнения отчетов по срочным ошибкам приложений – ответственные архитекторы (ведущие программисты)
2. Осмысленно прорабатывать и предлагать шаги для предотвращения повторов аналогичных ошибок – старшие программисты и команда
3. Руководителям или архитекторам (ведущим программистам) еженедельно утверждать готовые отчеты
4. Командами на еженедельной рестроспективе анализировать готовые отчеты:
 - осмыслять тикеты первопричины, которые вызвали эти ошибки
 - выбирать шаги, которые будут реализованы на следующей неделе, чтобы не было повторов

Практика устранения инцидентов



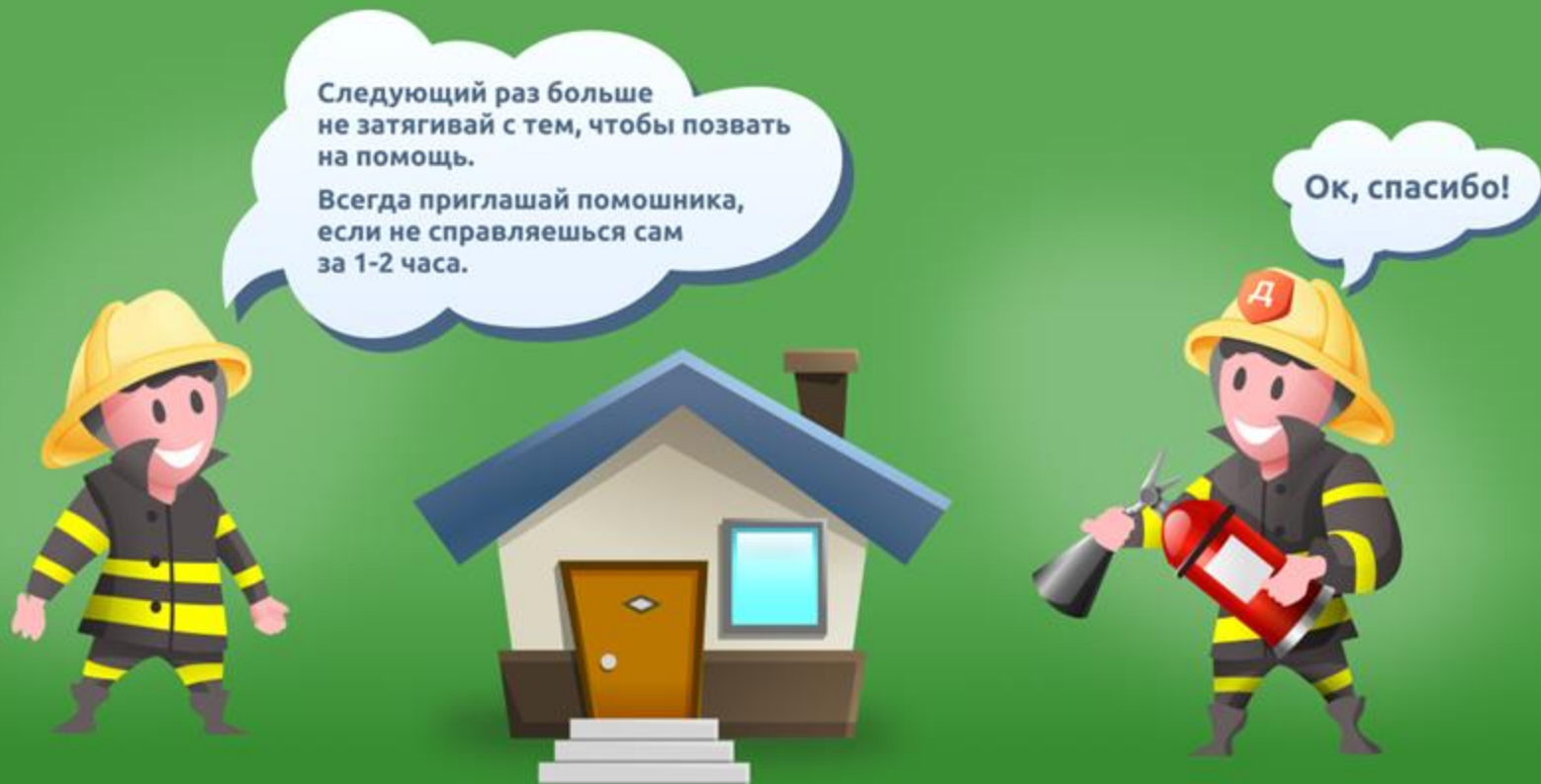
Не пытайтесь бороться в одиночку со сложностями



Вызывайте подмогу, если требуется



“Дружные вороны гуся съедают”



Спасибо за внимание

Остались ли вопросы?