

МОНИТОРИНГ И ОЧЕРЕДЬ ЗАЯВОК

Правила обработки автоалертов мониторинга

Когда событие мониторинга остаётся событием, когда становится заявкой и как распознать «волну» однотипных обращений.

Визард-АйТи · служба сопровождения · 4 сентября 2026 г. · страница-источник: <https://wizardit.ru/blog/alerty-monitoringa-zabivayut-ochered-zayavok-it-podderzhki>

Система мониторинга следит за серверами и рабочими станциями и сообщает об отклонениях: не обновился антивирус, заполнился диск, не отвечает сервис. Такое сообщение — автоалерт. Когда он попадает в очередь заявок, он выглядит как обращение, но заявителя-человека у него нет. В кейсе, из которого взяты эти правила, таких «заявок» оказалось 92 из 1 297 — каждая четырнадцатая. Правила разводят три разные проблемы: куда должны попадать такие сообщения, как найти их общую причину и что делать, когда один сбой порождает волну обращений от людей.

Событие	Запись в системе мониторинга: что, где и когда отклонилось от нормы. Событие может закрыться само, когда всё восстановилось.
Задача / заявка	Работа для инженера с исполнителем и сроком. Появляется только тогда, когда нужно действие человека.
Инцидент	Сбой, который затронул нескольких пользователей или критичную систему. Один инцидент может объединять десятки событий и обращений.
Порог	Условие, при котором событие становится задачей: например, три повтора на одной станции за неделю. Пороги задаются в правилах мониторинга и согласуются под конкретную инфраструктуру.
Первая и вторая линии	Первая линия принимает обращения и решает типовые вопросы; вторая — инженеры по серверам, сети и 1С, которые разбирают причины и меняют инфраструктуру.
Дежурный	Инженер, который в данный момент отвечает за приём событий и обращений.

Правило 1. Событие живёт в мониторинге, а не в очереди заявок

- Событие мониторинга регистрируется в контуре мониторинга, а не в очереди заявок.
- Оно закрывается автоматически при восстановлении: станция обновилась — событие закрыто, без участия инженера.
- События делятся на **информационные** (фиксируются, не требуют действия) и **требующие действия** (создают задачу по правилу повторяемости).

Правило 2. Заявка — только по правилу повторяемости

Условие	Что создаётся	Кто разбирает
Одинокое событие, восстановилось само	Ничего: событие закрыто автоматически	—

Условие	Что создаётся	Кто разбирает
N повторов на одной станции за период (порог согласуется, ориентир — 3 за неделю)	Одна заявка на станцию с историей событий	Первая линия
Однотипный сбой на многих станциях одновременно	Один инцидент с классом по числу затронутых рабочих мест	Вторая линия, руководитель группы в курсе
Серия однотипных событий за месяц и дольше	Задача на разбор корневой причины	Вторая линия, результат — изменение в инфраструктуре

Правило 3. Серия — это один дефект

74 однотипных сбоя обновления антивируса за семь месяцев — не 74 независимых случая, а признак одной неисправности в том, как устроено обновление антивируса на станциях. Такую серию нельзя закрывать по одной: она получает одну инженерную задачу, у которой есть ответственный, предположение о причине и условие закрытия — события больше не повторяются.

Правило 4. Регламент «волны»

Что такое волна

Любой сбой, затрагивающий много рабочих мест, — сеть, почта, сервер 1С — за минуты порождает десятки однотипных обращений от людей. Если обрабатывать каждое отдельно, очередь забивается, а реальная причина остаётся без владельца.

- 1. Распознать.** На приёме должно быть достаточно людей, чтобы за минуты увидеть, что обращения однотипны. Признаки: одинаковые формулировки, один сервис, разные пользователи, короткий интервал.
- 2. Связать.** Все обращения привязываются к одному инциденту; пользователи получают один и тот же статус, а не персональный ответ на каждую заявку.
- 3. Классифицировать.** Класс инцидента — по числу затронутых пользователей и критичности сервиса, а не по тону первого обращения.
- 4. Закрывать волну одним действием.** После восстановления все связанные обращения закрываются с общей причиной; из оценки качества они считаются как один инцидент.

Как считать эффект

Число автоуведомлений в очереди × среднее время на заявку. В кейсе: $92 \times 24,3$ минуты ≈ 37 часов за семь месяцев ≈ 64 часа в год — около восьми рабочих дней инженера, ушедших на ручное закрытие событий, которые могли закрыться сами. Плюс чистая статистика обратной связи: у автоматики нет оценок, и она искажает покрытие.

Материал из аналитической записки по потоку заявок службы сопровождения группы компаний (обезличенная версия). Разбор, контекст и другие файлы: <https://wizardit.ru/blog/alerty-monitoringa-zabivayut-ochered-zayavok-it-podderzhki>. Визард-АйТи, 2026.