

PIR-XXX: Краткое название инцидента

Заполняйте наблюдаемые факты отдельно от гипотез. Точное время, ссылки на доказательства и владельцы действий важнее красивого пересказа.

Severity	P1 / P2 / P3	Статус	открыт / восстановлен / закрыт
Начало воздействия	YYYY-MM-DD HH:MM TZ	Обнаружен	YYYY-MM-DD HH:MM TZ
Сервис восстановлен	YYYY-MM-DD HH:MM TZ	Владелец	
Затронутые системы		Рабочий тред	

Краткое описание

Что произошло и как это заметили.

Влияние

Кого затронуло, масштаб, продолжительность, финансовое или операционное влияние.

Хронология и восстановление

Время	Событие	Доказательство
YYYY-MM-DD HH:MM		
YYYY-MM-DD HH:MM		
YYYY-MM-DD HH:MM		
YYYY-MM-DD HH:MM		
YYYY-MM-DD HH:MM		
YYYY-MM-DD HH:MM		
YYYY-MM-DD HH:MM		
YYYY-MM-DD HH:MM		

Восстановление

Что восстановило работу, как это подтверждено и остались ли временные ограничения.

Причина и RCA

Пять вопросов - ориентир, а не обязательная квота. Для каждого ответа укажите доказательство. Остановитесь, когда причина стала проверяемой и на неё можно воздействовать.

Шаг	Почему это произошло?	Ответ	Доказательство
1	Почему возник пользовательский симптом?		
2	Почему возникла непосредственная техническая причина?		
3	Почему система это допустила?		
4	Почему защита или процесс не сработали?		
5	Почему это условие существовало организационно или архитектурно?		
Итог	Корневая причина		

Итог RCA

Подтверждённая причина, способ проверки, отвергнутые гипотезы и ссылка на подробный RCA.

Действия и закрытие

Действия после инцидента

Действие	Владелец	Трекер	Срок	Статус

Закрытие

- ☐ Сервис восстановлен и это проверено
- ☐ Основная причина подтверждена доказательствами
- ☐ Предотвращающие действия заведены в трекере
- ☐ Для каждого действия указаны владелец и срок
- ☐ Команда разобрала PIR