

АльфаИнциденты: Автоматизация центра мониторинга и реагирования

- **Алексей Федотов**
Менеджер продукта «АльфаИнциденты»
- **Александр Кирий**
Руководитель центра мониторинга SOCRAT





Время вебинара ~50 мин



Обменивайтесь сообщениями
во вкладке «Чат»



Запись вебинара направим всем
участникам на указанный
при регистрации e-mail
в течение 2-3 рабочих дней



Задавайте вопросы во вкладке
«Вопросы»



**Среди заданных вами вопросов, каждый
Эксперт выберет лучший, на его взгляд, вопрос,
и мы наградим 2-х авторов фирменным мерчем!**



Системный интегратор в сфере
информационной безопасности
и импортозамещения
информационных технологий

80+

регионов
внедрения

4000+

реализованных
проектов



Входим в ГК «Кейсистемс»



Лицензиат ФСТЭК России

Лицензиат ФСБ России

SOCRAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

SOCRAT – ЭТО ЦЕНТР МОНИТОРИНГА КСБ-СОФТ

Режим работы **24x7**

Инвентаризация

Анализ Уязвимостей

Тестирование на проникновение

Корпоративный
центр **ГосСОПКА** (класс А)

Пакетная система предоставления
услуг (выбор только необходимого)



Российская ИТ-компания,
разработчик экосистемы
приложений «Альфа»



Входим в ГК «Кейсистемс»



Лицензиат ФСТЭК России

Лицензиат ФСБ России

Автоматизированное реагирование

Реагирование в один клик с помощью агента

Реестр инцидентов ИБ

Создание карточки инцидента на основе своего шаблона или в формате НКЦКИ. Выгрузка в формате csv.

Сценарии реагирования (Playbook)

Гибкий конструктор и набор действий под каждый тип инцидента

Оперативные оповещения

Почта, телеграм, SIP телефония

Интеграция с ГосСОПКА

Интеграция с SIEM-системами

Отчетная документация

Карта сети

Чем помогает **Альфа** Инциденты?

Взаимодействие между

- ИТ и ИБ (при внутреннем мониторинге)
- операторы SOC и заказчик (при внешнем мониторинге)

Стандартизация отчетной документации

- Карточка инцидента с рекомендациями для заказчика\ИБ
- Карточка инцидента для отправки в НКЦКИ

Контекст инцидента

- Карта активов (инвентаризационная информация)
- Фиксация изменений инфраструктуры

* **Контроль** и метрики

- Соответствие требованиям регулятора по времени реакции на инцидент
- Оценка скорости реакции SOC

Соответствие требованиям НПА



Приказ ФСТЭК России № 117.
Вступает в силу 01 марта 2026 г.

Методические рекомендации ФСТЭК России по проведению:

- Анализа защищенности;
- Тестирования на проникновение

Распространяется на:

Государственные органы,
государственные унитарные предприятия,
государственные учреждения



Приказы ФСБ России:

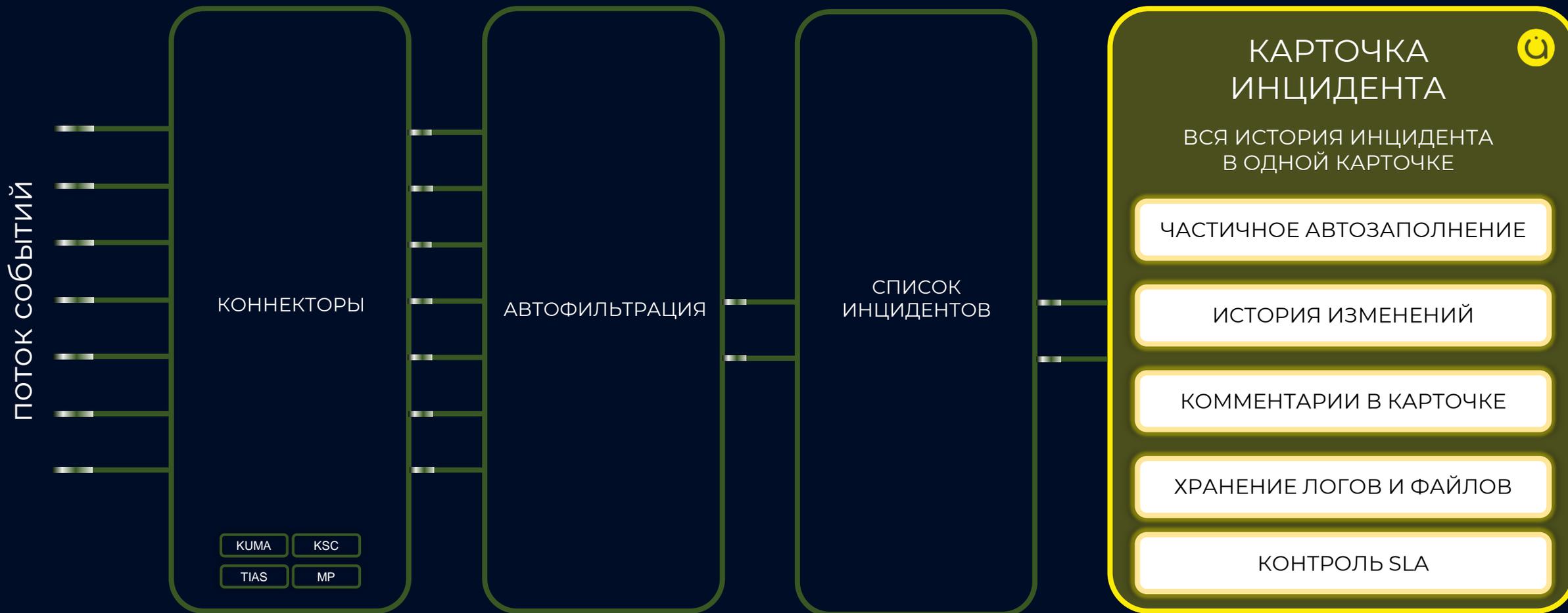
- № 539
- № 540
- № 546
- № 547
- № 548
- № 553
- № 554

Распространяется на:

Государственные органы, государственные
унитарные предприятия, государственные
учреждения

+ субъекты КИИ (ОКИИ\ЗОКИИ)

Кейс 1. Единое окно аналитика



Кейс №2. Повышение эффективности обработки событий ИБ

Взаимодействие команды ИТ и ИБ в карточке инцидента.
Отслеживание статусов по изменениям инцидента и его контроль

1 Все общение по инциденту
прямо в карточке

2 Отслеживайте
историю изменений

The screenshot shows a web interface for incident management. At the top, there are navigation tabs: "Детали", "История", "Файлы", "Комментарии", and "Сценарии реагирования". Below the tabs, there are playback controls and buttons for "Сохранить изменения" and "Сохранить как". The main section is titled "Данные инцидента" and contains several fields:

- Organization: ООО
- Category of incident: Не указано
- Type of incident: Не указано
- Name: Заражение ВПО
- Level: Критический
- Status: Требуется действия пользователя
- Support line: Линия 1
- Registration time: 02/09/2025 20:16:11
- Description: Внешний хост 185.196.220.250 инициирует подозрительный HTTP-запрос на внутренний хост 192.168.7.95. Запрос содержит в URI специфичный для вредоносного ПО OwlProxy паттерн "z?ra=".

МОДУЛЬ РАБОТЫ С ЗАДАЧАМИ



СБОР И ОБРАБОТКА ОБРАЩЕНИЙ –
ПОМОЖЕМ НЕ ПОТЕРЯТЬ ЗАДАЧУ
И ДОВЕСТИ ЕЕ ДО КОНЦА

ВНУТРЕННИЙ ЧАТ ПО КАЖДОМУ КА И КИ

КОНТРОЛЬ СТАТУСА КА И КИ

ОСТАВЛЯЙТЕ РЕКОМЕНДАЦИИ

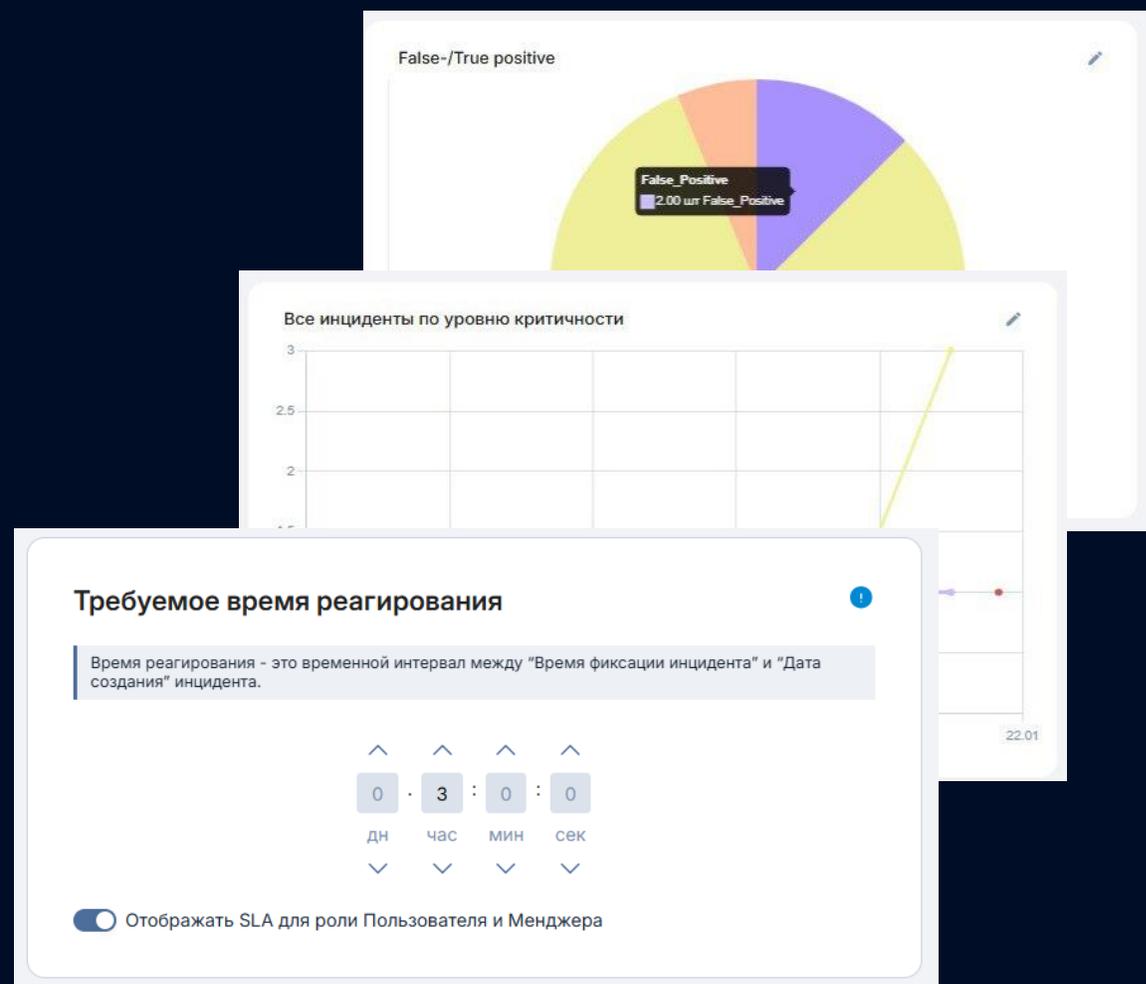
РАССТАВЛЯЙТЕ ПРИОРИТЕТЫ

ОПЕРАТИВНОЕ ОПОВЕЩЕНИЕ

Кейс №3. Контроль работы аналитиков и метрики

Визуализируйте данные в формате графиков или диаграмм за счет создания дашбордов под свои цели и задачи

Задайте пороговое значение времени реагирования на инцидент и контролируйте SLA

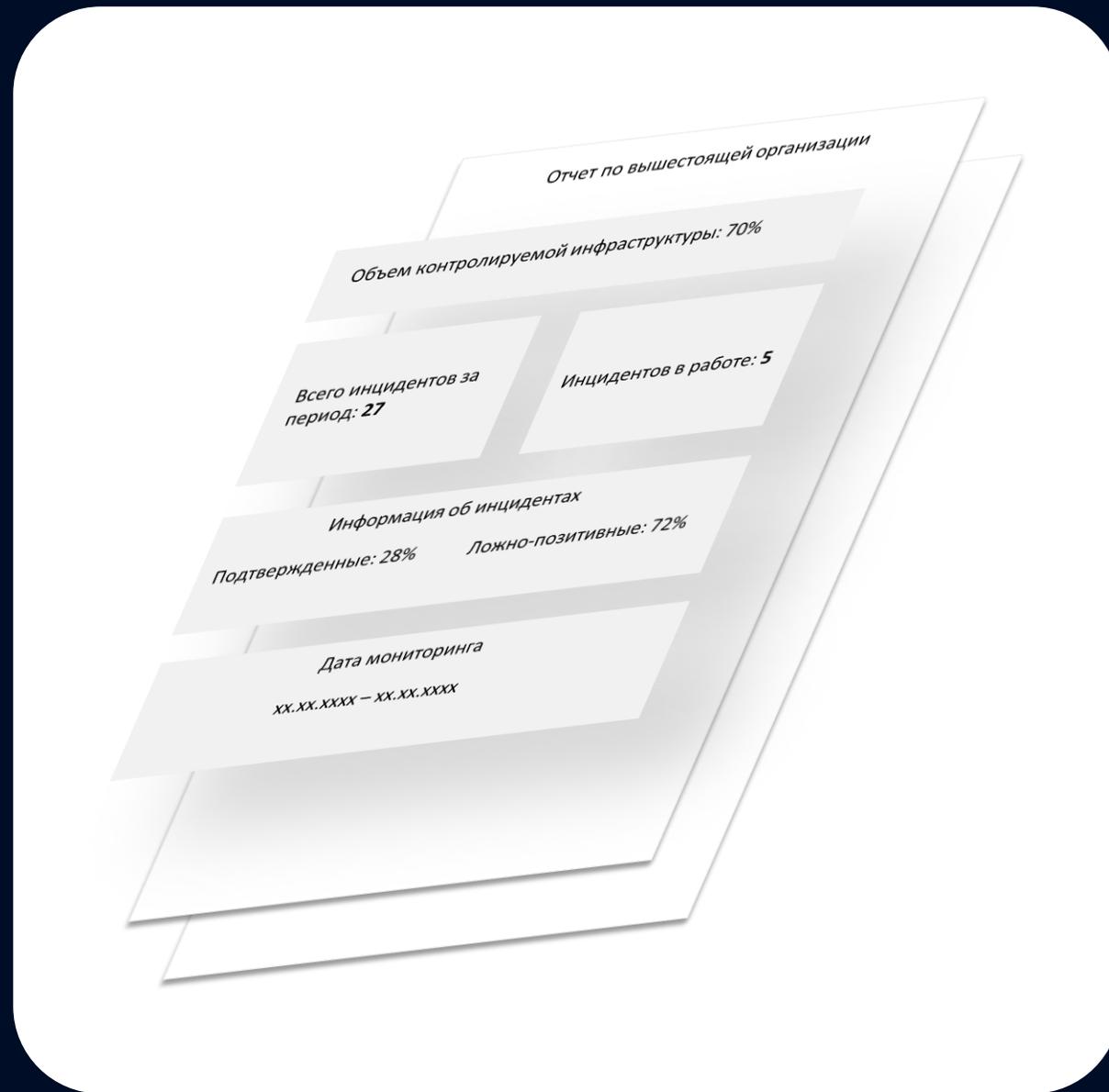


Кейс №3. Контроль работы аналитиков и метрики

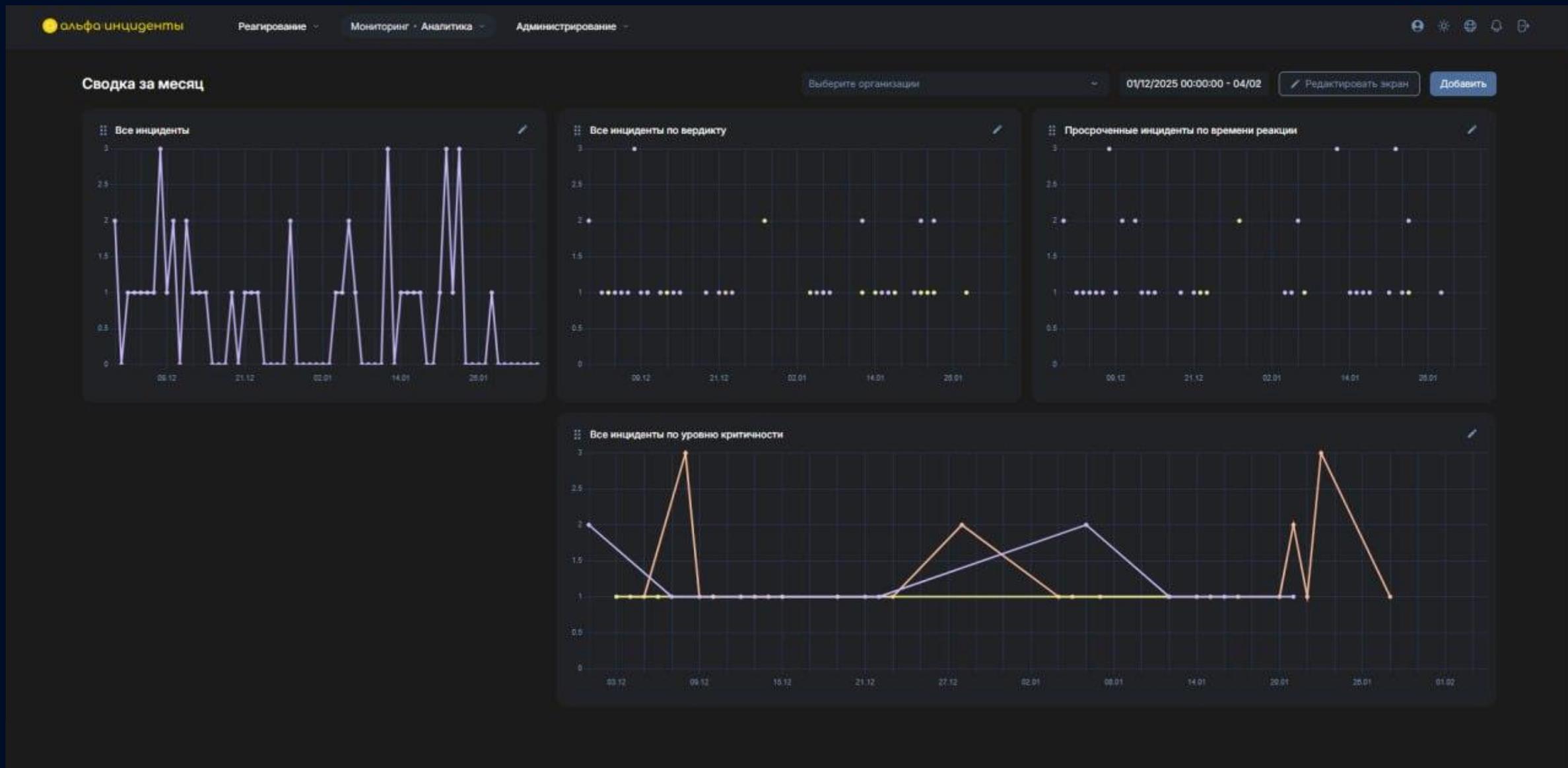
Отчетная документация по управлению инцидентами в соответствии с актуальными требованиями по ИБ, в том числе по 117 приказу ФСТЭК России.



Единый формат отчетной документации для всех уровней организации



Кейс №3. Контроль работы аналитиков и метрики



Кейс №3. Контроль работы аналитиков и метрики



Кейс №4. Соответствие требованиям НКЦКИ



ГОССОПКА

ПОМОЖЕМ ВЫПОЛНИТЬ ТРЕБОВАНИЯ
ЗАКОНОДАТЕЛЬСТВА

ИНФОРМИРОВАНИЕ ОБ КА И КИ

ПОЛУЧЕНИЕ БЮЛЛЕТЕНЕЙ

ФИКСИРУЙТЕ СООБЩЕНИЯ

Несанкционированное разглашение информации Требуются действия пользователя Критический Рег.номер: 6

Дата создания: 29.01.2026, 08:51:30 Дата изменения: 29.01.2026, 09:05:45 Время регистрации: 29.01.2026, 08:18:43 Время реагирования: 0.00:32:47.580 Создатель: alfa (alfa) Адаптер: АльфаИнциденты

[Детали](#) [История](#) [Файлы](#) [Комментарии](#) [Сценарии реагирования](#) Сохранить изменения Сохранить как

Данные инцидента Отправить уведомление в ГосСОПКА

НКЦКИ

- Общая информация
- Общие сведения о контролируемом ресурсе
- Местоположение контролируемого ресурса
- Сведения об утечке персональных данных
- Технические сведения об атакованном ресурсе
- Технические сведения о вредоносной системе

Данные инцидента

Организация: ООО "SOCRAT"

Категория инцидента: Компьютерный инцидент Тип инцидента: Несанкционированное разглашение информации

Название: Несанкционированное разглашение информации

Уровень: Критический Статус: Требуются действия пользователя Линия поддержки: Линия 1

Время регистрации: 29/01/2026 08:18:43

Описание

Кейс №5. Сценарии реагирования и автореагирование

Пошаговые сценарии реагирования на типовые инциденты кибербезопасности

30

Типовых сценариев
на платформе (соотв. Нкцки)

Создавайте свои сценарии
или адаптируйте существующие
с помощью встроенного конструктора



На каждом шаге:

Фиксируйте логи/файлы

Оставляйте примечания

Отправляйте уведомления

Назначайте автоматизацию

ПОШАГОВОЕ ВЫПОЛНЕНИЕ СЦЕНАРИЯ С УКАЗАНИЕМ РОЛИ И ИНСТРУМЕНТОВ

№	Шаги	Ответственный	Инструмент / Автоматизация
⋮ 1.1	Стратегия резервного копирования	Пользователь ×	Офлайн-резервирование × Система резервного копирования × Не указано
⋮ 1.2	Защита конечных устройств	Пользователь ×	EDR × EPP × Не указано

Кейс №5. Сценарии реагирования и автореагирование

Автоматизируйте процесс реагирования на инциденты ИБ с помощью агентов

Через карту сети

В сценарии реагирования

На основе автофильтрации

Поддержка популярных ОС

Windows

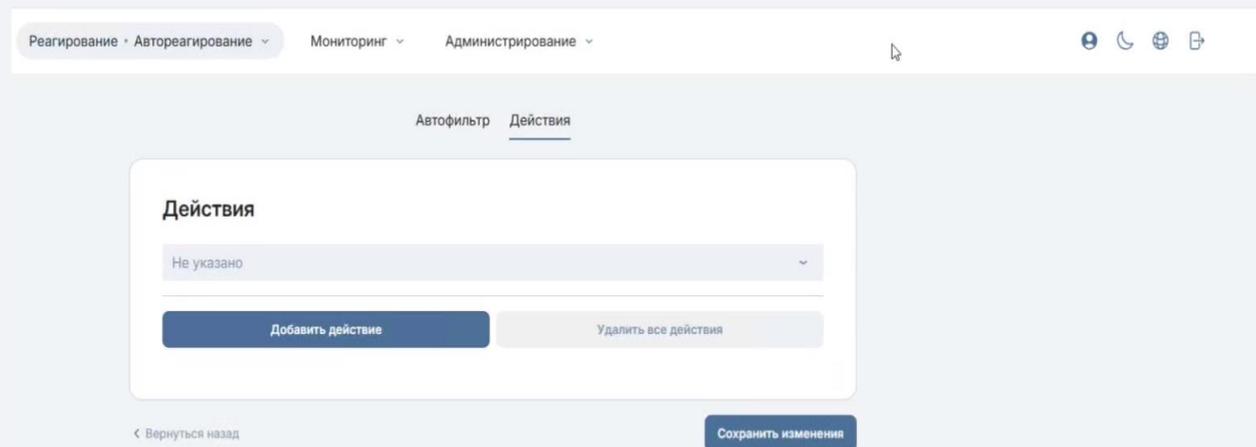
MacOS

Linux Ubuntu

Alt Linux

Astra Linux

RedOS



СЛОЖНЫЕ ФУНКЦИИ В ПРОСТОМ ИНСТРУМЕНТЕ

ЗАПОЛНЕНИЕ КАРТОЧКИ
ИНЦИДЕНТА, МИН



ГосСОПКА

ОТПРАВКА УВЕДОМЛЕНИЙ,
ПРИЕМ БЮЛЛЕТЕНЕЙ
И СООБЩЕНИЙ

ОТЧЕТЫ

ПО ИНЦИДЕНТАМ И ИХ
ПОШАГОВОЙ ЛИКВИДАЦИИ

АВТОРЕАГИРОВАНИЕ

НА ПОТОК СОБЫТИЙ
ИЛИ В СЦЕНАРИИ
РЕАГИРОВАНИЯ

НА ОСНОВЕ АГЕНТОВ

ЗАДАВАЙТЕ ПРАВИЛА
ЧЕРЕЗ КОНСТРУКТОР

ОТПРАВЛЯЙТЕ УВЕДОМЛЕНИЯ
ПОЛЬЗОВАТЕЛЯМ

Реагирование · Автореагирование ▾

СЦЕНАРИИ РЕАГИРОВАНИЕ

ПОДКЛЮЧЕНИЕ
АВТОМАТИЗИРОВАННЫХ
ДЕЙСТВИЙ

30 ТИПОВЫХ СЦЕНАРИЕВ
(НКЦКИ) УЖЕ НА ПЛАТФОРМЕ

НАСТРОЙКА И АДАПТАЦИЯ
ЧЕРЕЗ КОНСТРУКТОР

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ ИНЦИДЕНТАМИ

МОНИТОРИНГ, РЕАГИРОВАНИЕ, УПРАВЛЕНИЕ
ИНЦИДЕНТОМ ИБ В ОДНОЙ ПЛАТФОРМЕ



ДАШБОРДЫ



ВИЗУАЛИЗИРУЙТЕ
ДАННЫЕ ЧЕРЕЗ ГРАФИКИ
ИЛИ ДИАГРАММЫ

ОТ РАЗРАБОТЧИКА ЭКОСИСТЕМЫ АЛЬФА



ПОПРОБУЙТЕ АЛЬФА|ИНЦИДЕНТЫ В РАМКАХ ПИЛОТА

ДОСТУП К ПРОДУКТУ НА 1 МЕСЯЦ

