КСБ-СОФТ

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!

КСБ-СОФТ

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

Корпоративный центр ГосСОПКА (класс А)

Инвентаризация

Анализ Уязвимостей

Тестирование на проникновение

Пакетная система предоставления услуг (выбор только необходимого)

НПЦ КСБ

Российская ИТ-компания,
разработчик экосистемы
приложений «Альфа»

Входим в ГК «Кейсистемс»

Лицензиат ФСТЭК России

Лицензиат ФСБ России

альфа|инциденты

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 АльфаИнциденты?

Взаимодействие между

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

Контекст инцидента

- Карта активов (инвентаризационная информация)
- Фиксация изменений инфраструктуры

Стандартизация отчетной документации

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

*** 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:

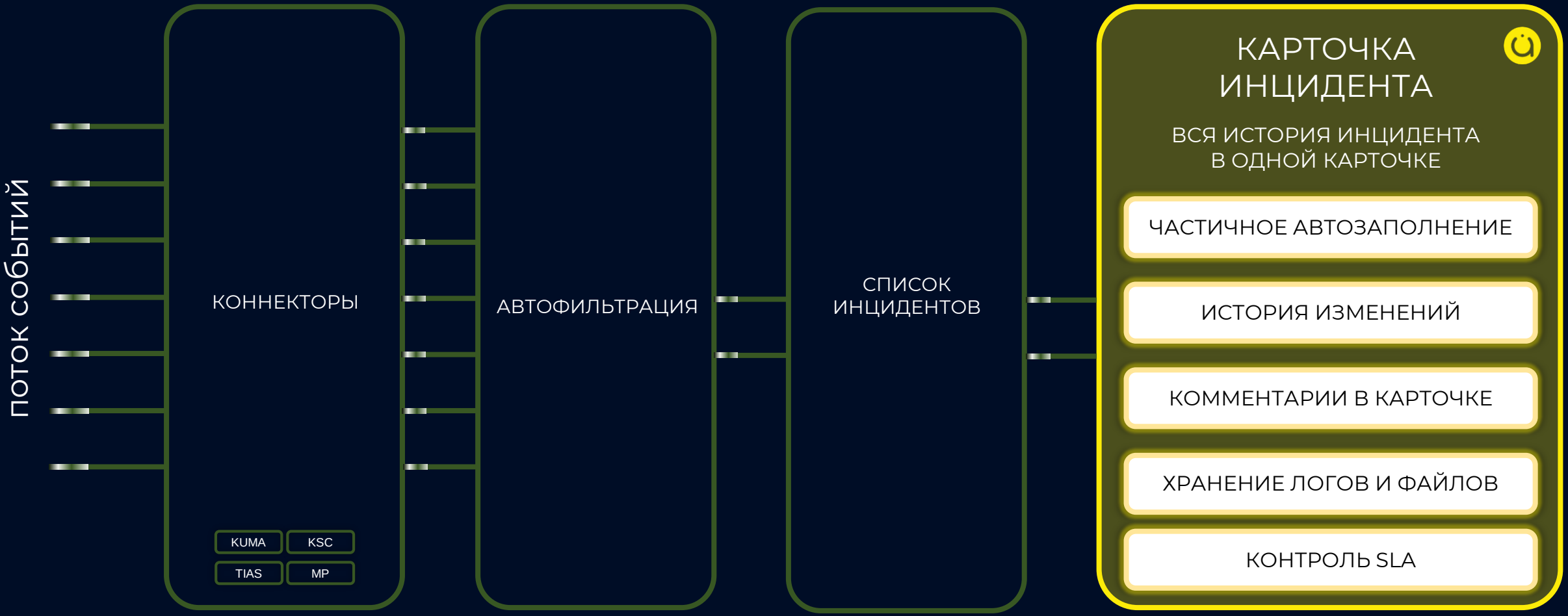
- № 539
- № 540
- № 546
- № 547
- № 548
- № 553
- № 554

Распространяется на:

Государственные органы, государственные унитарные предприятия, государственные учреждения

+ субъекты КИИ (ОКИИ\ЗОКИИ)

Кейс 1. Единое окно аналитика

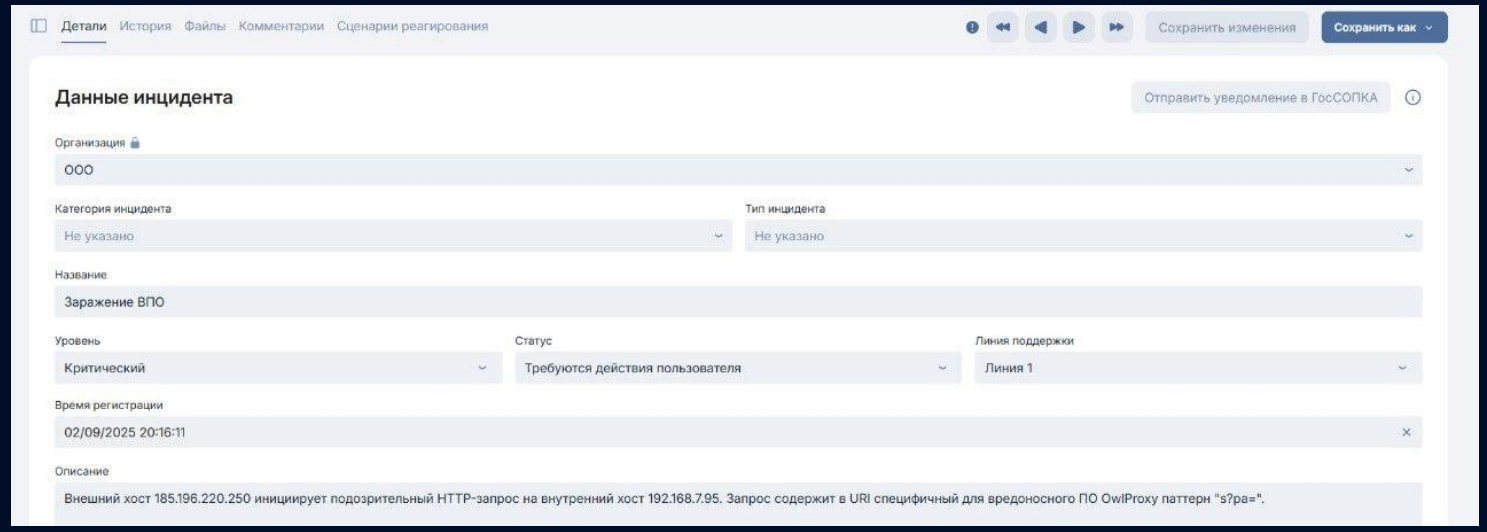


Кейс №2. Повышение эффективности отработки событий ИБ

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



МОДУЛЬ РАБОТЫ С ЗАДАЧАМИ

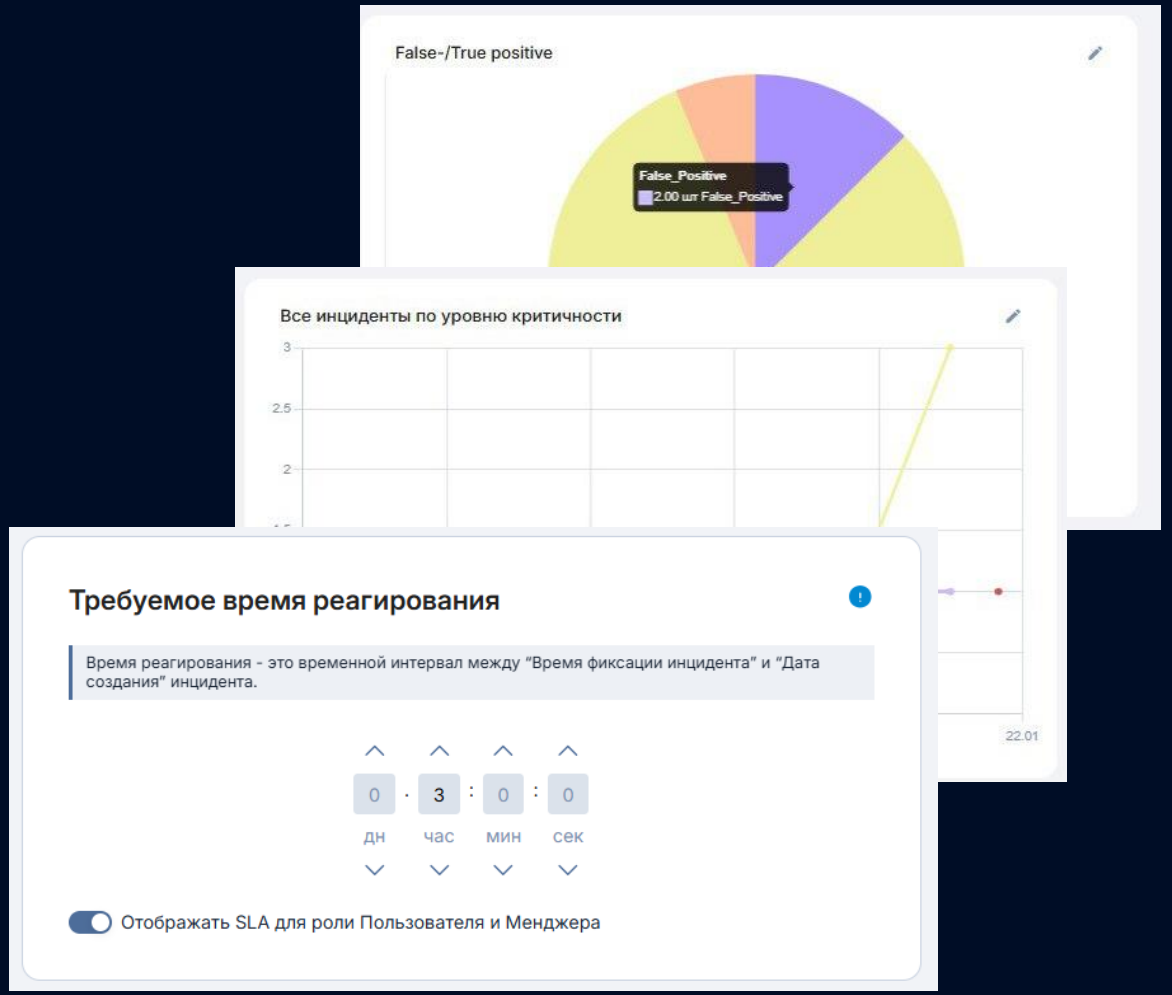
СБОР И ОБРАБОТКА ОБРАЩЕНИЙ – ПОМОЖЕМ НЕ ПОТЕРЯТЬ ЗАДАЧУ И ДОВЕСТИ ЕЕ ДО КОНЦА

- 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

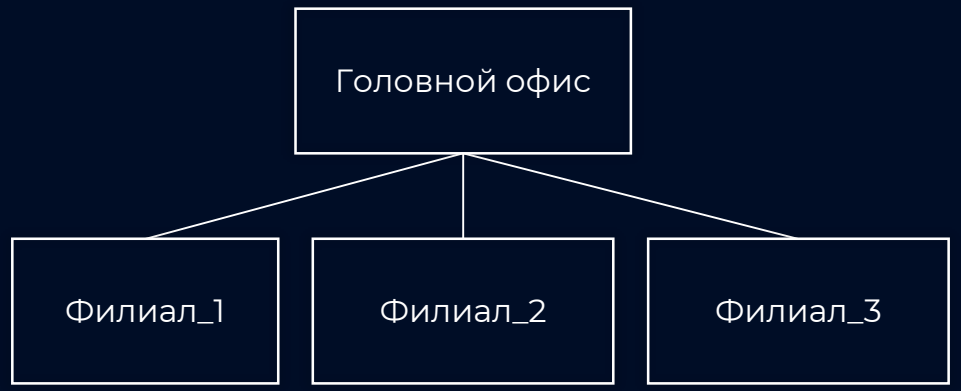
Визуализируйте данные в формате графиков или диаграмм за счет создания дашбордов под свои цели и задачи

Задайте пороговое значение времени реагирования на инцидент и контролируйте SLA

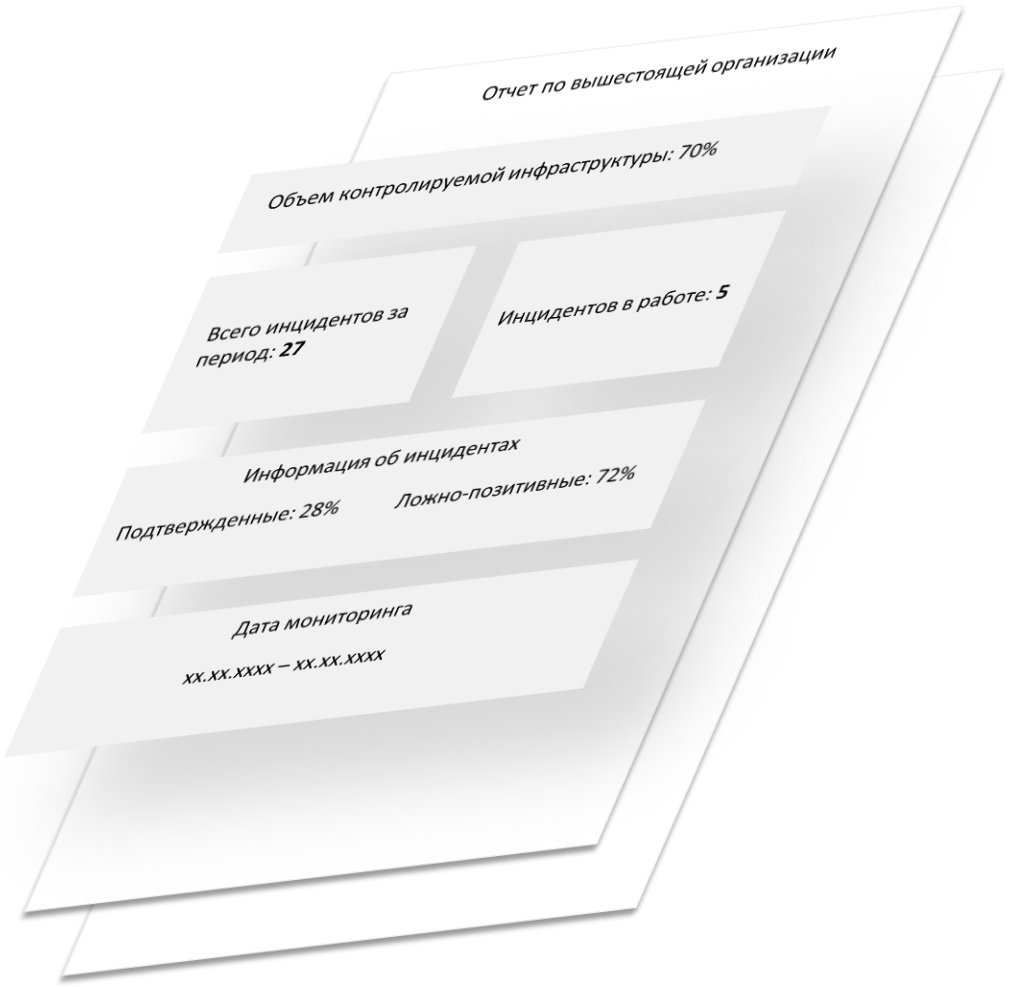


Кейс №3. Контроль работы аналитиков и метрики

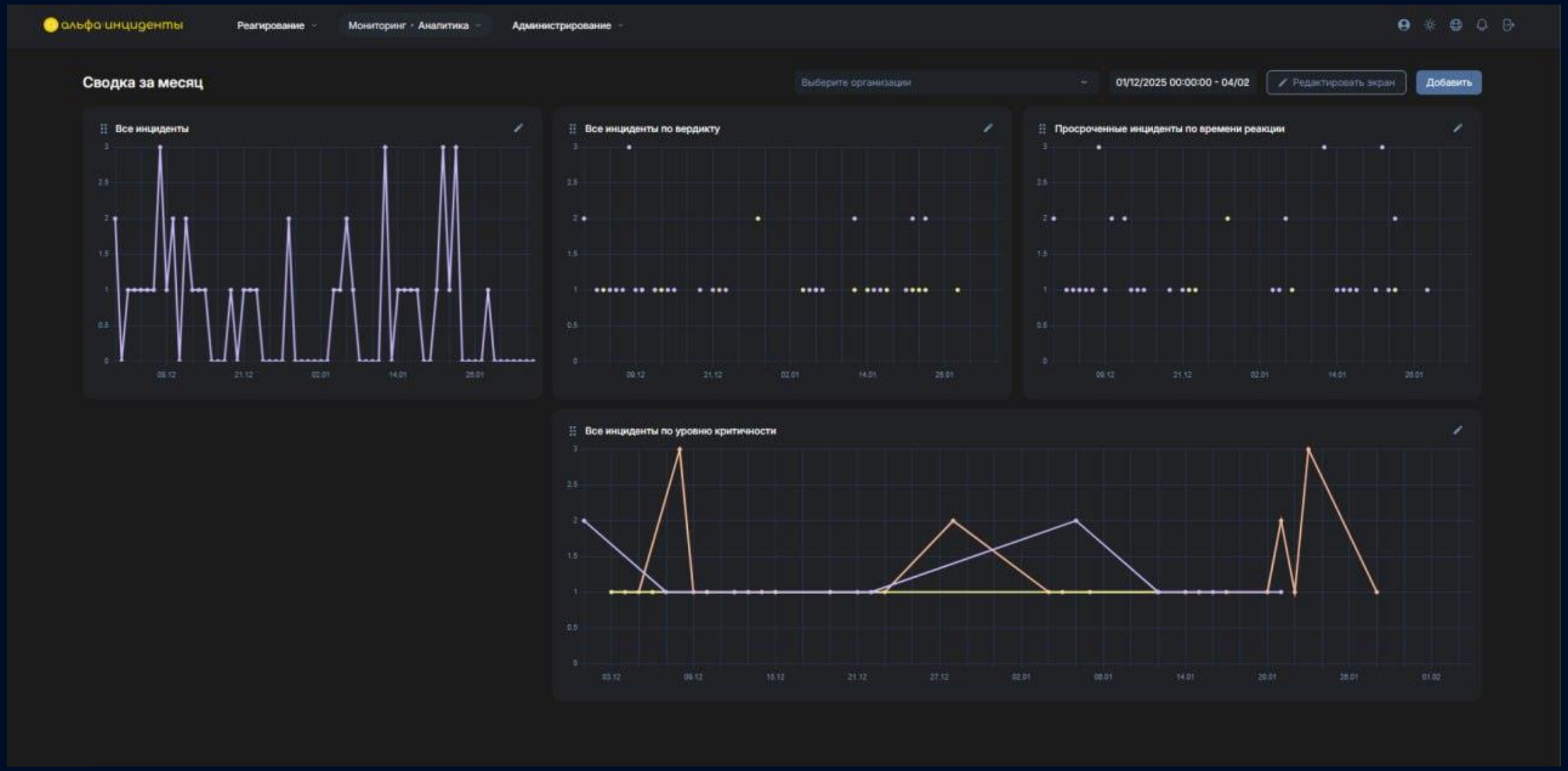
Отчетная документация по управлению инцидентами в соответствии с актуальными требованиями по ИБ, в том числе по 117 приказу ФСТЭК России.



Единый формат отчетной документации для всех уровней организации



Кейс №3. Контроль работы аналитиков и метрики



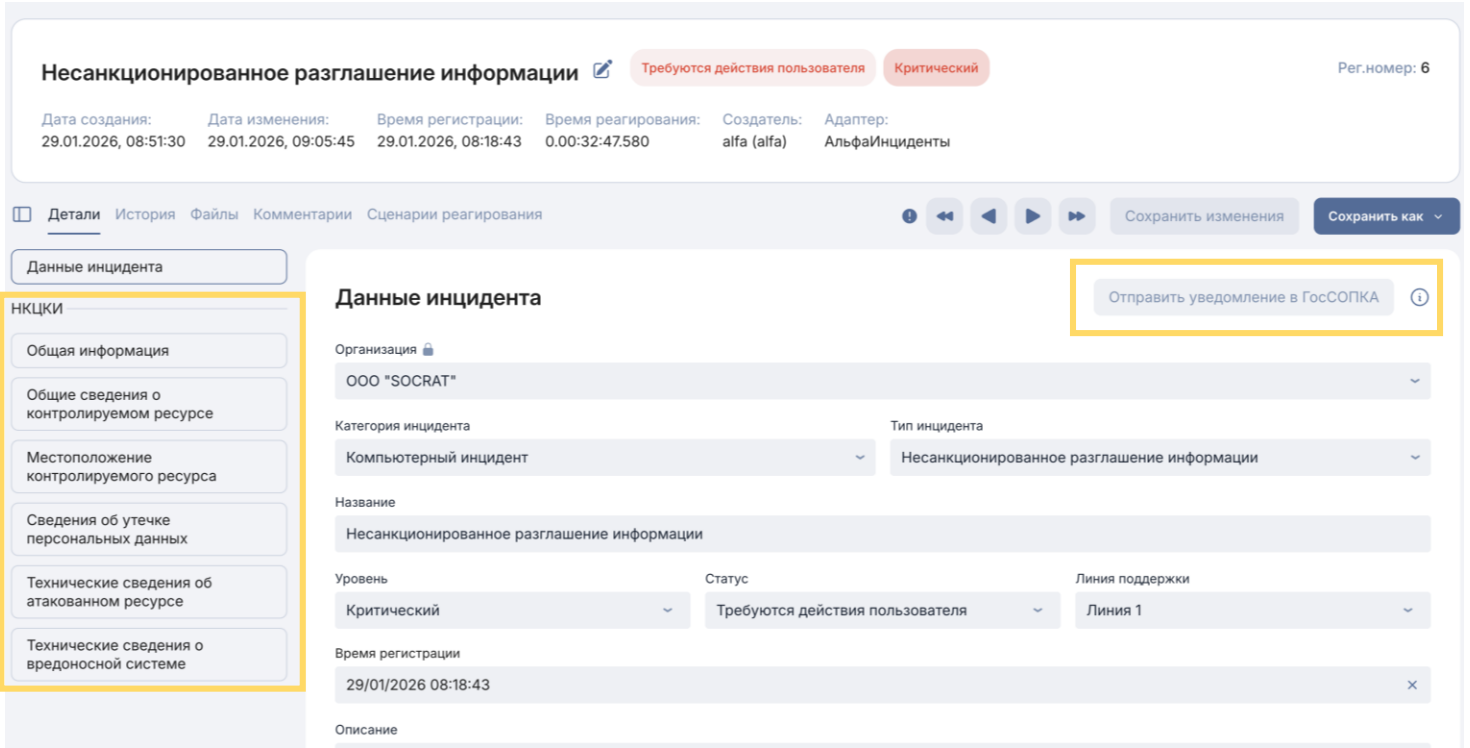
Кейс №3. Контроль работы аналитиков и метрики

Кейс №4. Соответствие требованиям НКЦКИ

ГОССОПКА

ПОМОЖЕМ ВЫПОЛНИТЬ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

- ИНФОРМИРОВАНИЕ ОБ КА И КИ
- ПОЛУЧЕНИЕ БЮЛЛЕТЕНЕЙ
- ФИКСИРУЙТЕ СООБЩЕНИЯ



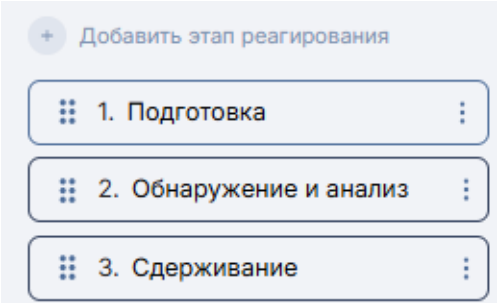
Кейс №5. Сценарии реагирования и автореагирование

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

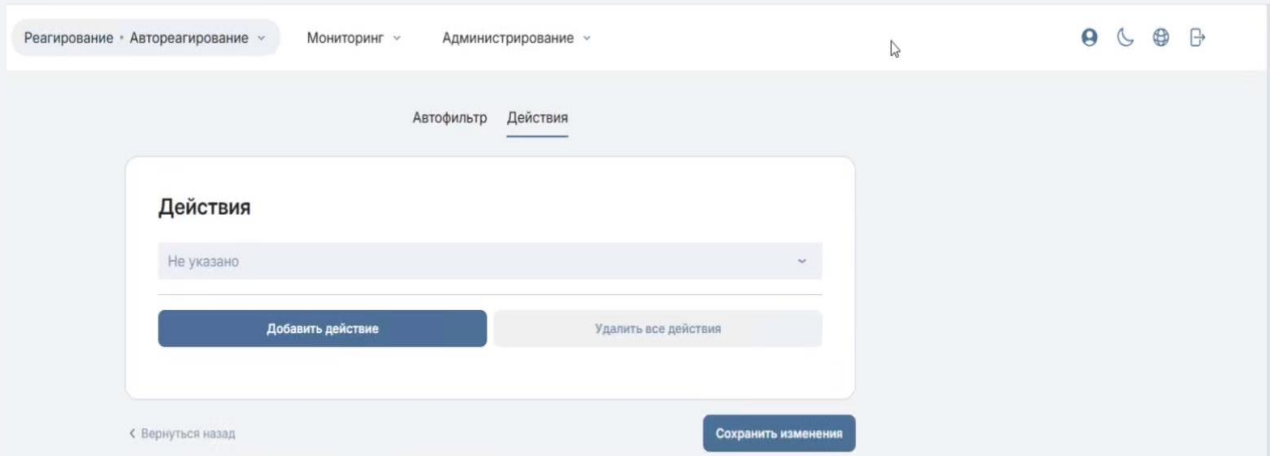
Через карту сети

В сценарии реагирования

На основе автофильтрации

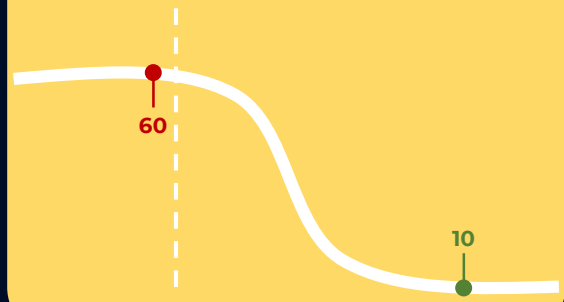
Поддержка популярных ОС

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

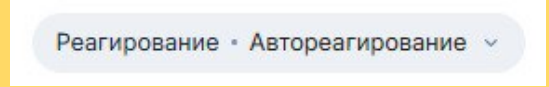
АВТОРЕАГИРОВАНИЕ

НА ПОТОК СОБЫТИЙ ИЛИ В СЦЕНАРИИ РЕАГИРОВАНИЯ

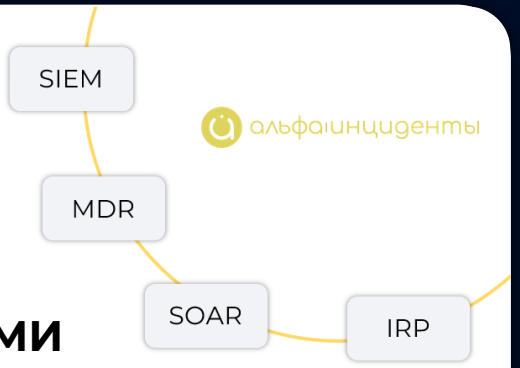
НА ОСНОВЕ АГЕНТОВ

ЗАДАВАЙТЕ ПРАВИЛА ЧЕРЕЗ КОНСТРУКТОР

ОТПРАВЛЯЙТЕ УВЕДОМЛЕНИЯ ПОЛЬЗОВАТЕЛЯМ



ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ ИНЦИДЕНТАМИ



МОНИТОРИНГ, РЕАГИРОВАНИЕ, УПРАВЛЕНИЕ ИНЦИДЕНТОМ ИБ В ОДНОЙ ПЛАТФОРМЕ

СЦЕНАРИИ РЕАГИРОВАНИЕ

ПОДКЛЮЧЕНИЕ АВТОМАТИЗИРОВАННЫХ ДЕЙСТВИЙ

30 ТИПОВЫХ СЦЕНАРИЕВ (НКЦКИ) УЖЕ НА ПЛАТФОРМЕ

НАСТРОЙКА И АДАПТАЦИЯ ЧЕРЕЗ КОНСТРУКТОР

ДАШБОРДЫ

ВИЗУАЛИЗИРУЙТЕ ДАННЫЕ ЧЕРЕЗ ГРАФИКИ ИЛИ ДИАГРАММЫ

ОТ РАЗРАБОТЧИКА ЭКОСИСТЕМЫ АЛЬФА

ПОПРОБУЙТЕ АЛЬФА|ИНЦИДЕНТЫ В РАМКАХ ПИЛОТА

ДОСТУП К ПРОДУКТУ НА 1 МЕСЯЦ