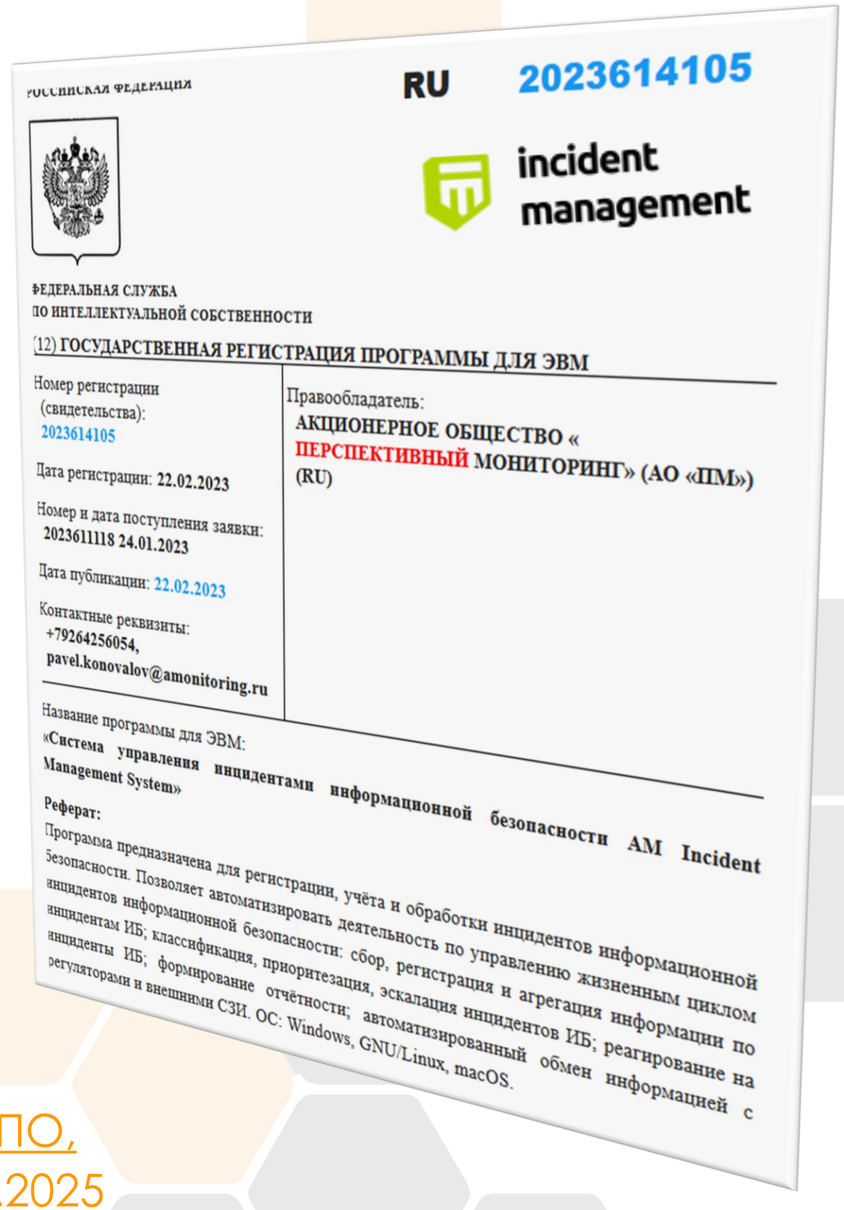
AM IMS 3.0: Управление инцидентами информационной безопасности

Артём Савчук
Технический директор
«Перспективный мониторинг»

БОЛЬШОЙ МОСКОВСКИЙ ТЕХНО ФЕСТ infotecs

AM Incident Management System

Система управления инцидентами является «службой одного окна» для всех специалистов, задействованных в процессе управления инцидентами ИБ, удобной как для работников Центра мониторинга, так и для специалистов Заказчика.



РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU 2023614105

incident management

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства): 2023614105

Дата регистрации: 22.02.2023

Номер и дата поступления заявки: 2023611118 24.01.2023

Дата публикации: 22.02.2023

Контактные реквизиты: +79264256054, pavel.konovalov@amonitoring.ru

Правообладатель: АКЦИОНЕРНОЕ ОБЩЕСТВО «ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ» (АО «ПМ») (RU)

Название программы для ЭВМ: «Система управления инцидентами информационной безопасности AM Incident Management System»

Реферат:
Программа предназначена для регистрации, учёта и обработки инцидентов информационной безопасности. Позволяет автоматизировать деятельность по управлению жизненным циклом инцидентов информационной безопасности: сбор, регистрация и агрегация информации по инцидентам ИБ; классификация, приоритезация, эскалация инцидентов ИБ; реагирование на инциденты ИБ; формирование отчётности; автоматизированный обмен информацией с регуляторами и внешними СЗИ. ОС: Windows, GNU/Linux, macOS.

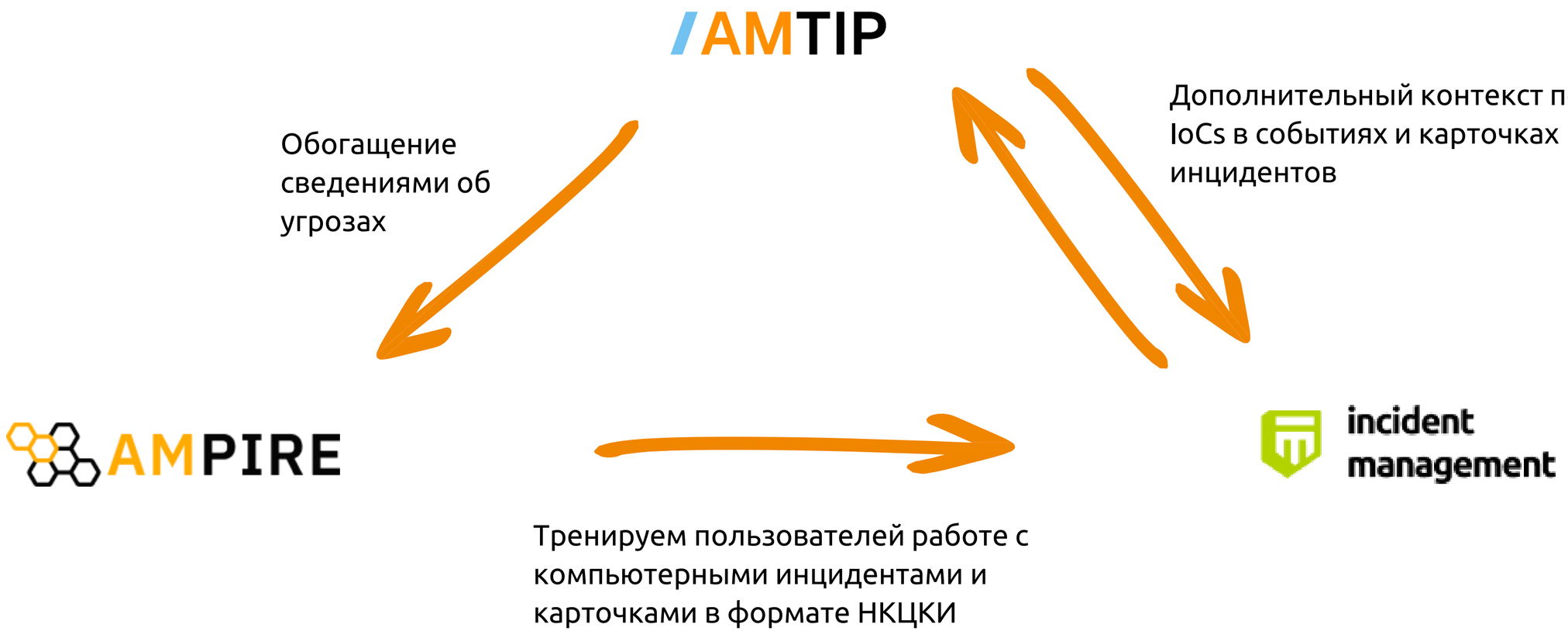
Включено в реестр отечественного ПО, реестровая запись №29485 от 29.08.2025

Возможности

AM Incident Management System

- Управление инцидентами ИБ
- Учёт ИТ-активов
- Формирование отчётности
- Интеграция с ГосСОПКА
- Обмен информацией об угрозах ИБ
- Построение статистических графиков, дашбордов
- Работа с организациями и филиалами
- Оперативное оповещение по e-mail, telegram, sms

Экосистема продуктов ПМ



Управление инцидентами ИБ*

AM IMS применяется:

- **На этапе планирования и подготовки** - для формализации политик ИБ, информирования пользователей;

- **На этапе использования** – для создания, оповещения, расследования и реагирования на инциденты ИБ;

- **На этапе анализа** – для обобщения, анализа и систематизации информации об инцидентах ИБ;

- **На этапе улучшения** – для уточнения результатов и улучшения системы менеджмента инцидентов ИБ.

* - ГОСТ Р ИСО/МЭК ТО 18044-2007

Управление КИ

для субъектов ГосСОПКА

ГОСТ Р 59710-2022 регулирует управление КИ для:

- субъектов ГосСОПКА, осуществляющих управление КИ в отношении собственных информационных ресурсов;

- центров ГосСОПКА, в зону ответственности которых входят информационные ресурсы других субъектов ГосСОПКА.

Соответствие IM требованиям

ГОСТ Р 59710-2022

Требование	AM IMS	Примечание
Организация деятельности по управлению КИ		
Разработка политики управления КИ	**Помогает**	Раздел «Документация» позволяет сформировать базу знаний на основе ПИБ Компании.
Разработка плана реагирования на КИ		
Определение подразделения, ответственного за управление КИ	**Помогает**	При создании пользователя задается соответствующая ему роль в системе
Организация взаимодействия с подразделениями внутри организации и с внешними организациями	**Позволяет**	Диспетчеризация внутри системы + API
Материально-техническое оснащение подразделения, ответственного за управление КИ	**Не позволяет**	
Организовать обучение и информирование в части управления КИ	AMPIRE	Может быть реализовано на киберполигоне Ampire
Проведение тренировок по отработке мероприятий плана реагирования на КИ		
Обнаружение и регистрация КИ		
Регистрация признаков возможного возникновения компьютерных инцидентов	**Позволяет**	В разделе «Инциденты» возможно создавать карточки КИ и КА, при закрытии инцидента указывается признак True/False positive
Подтверждение компьютерных инцидентов	**Позволяет**	

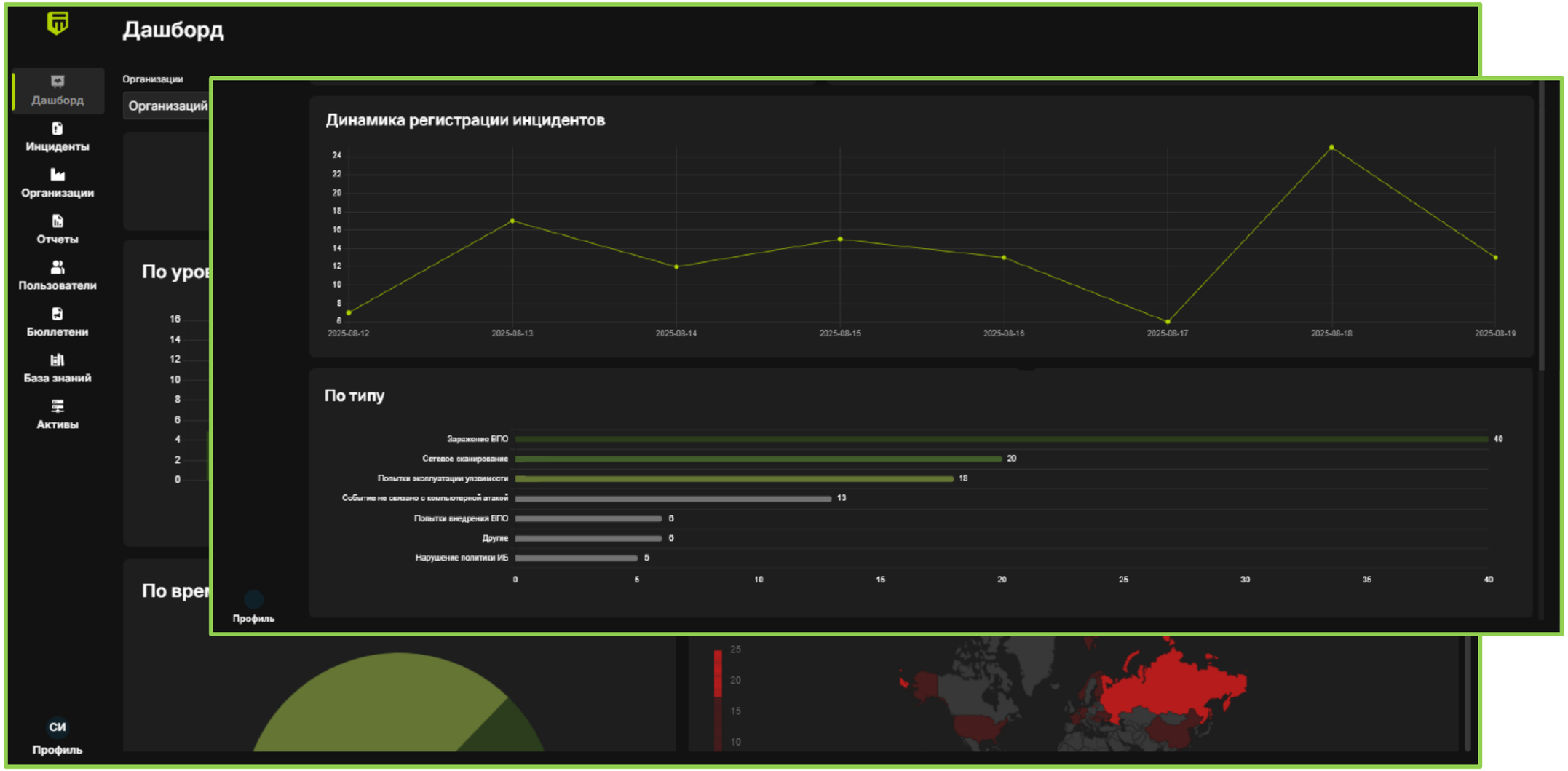
Соответствие IM требованиям

ГОСТ Р 59710-2022

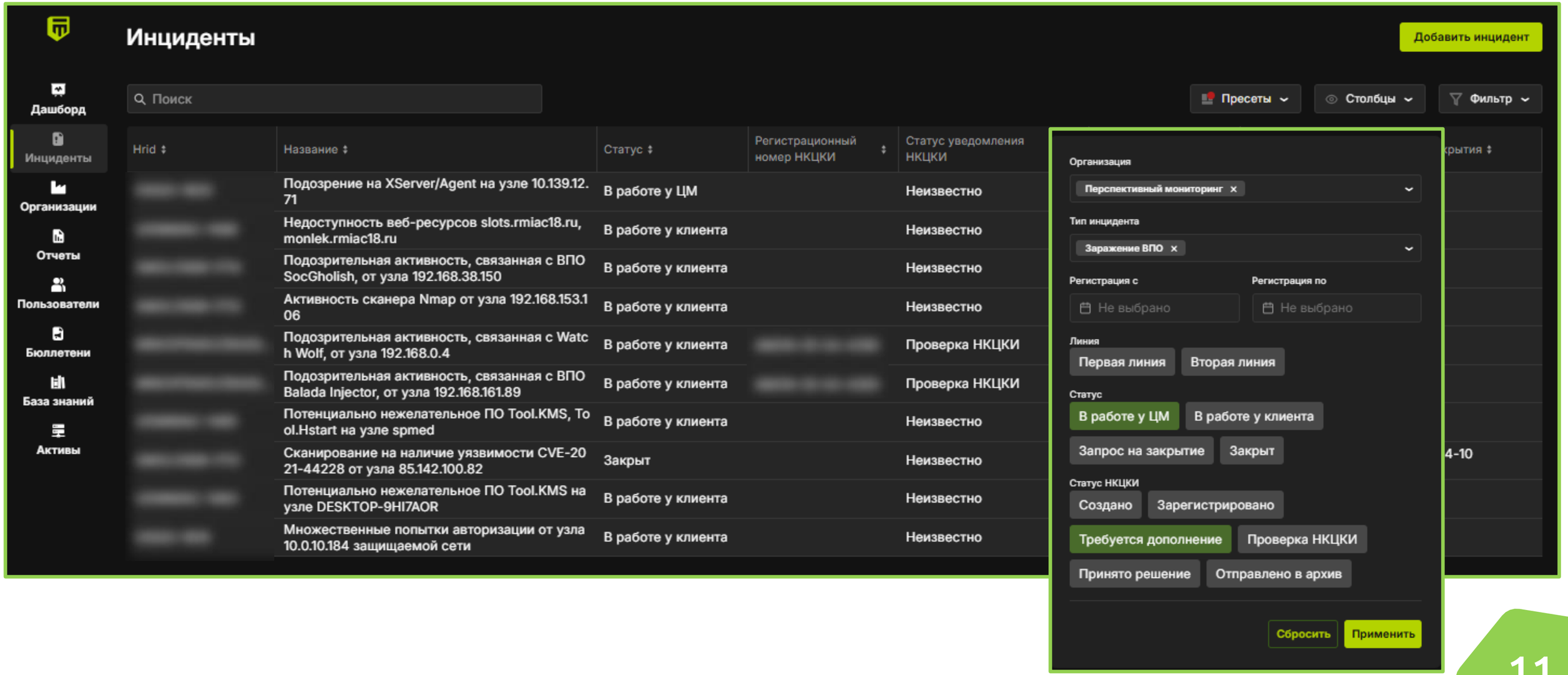
Требование	AM IMS	Примечание
Реагирование на компьютерные инциденты		
Определение вовлеченных в КИ элементов информационной инфраструктуры	**Позволяет**	Раздел «Активы» позволяет вести учет ИТ-активов организации
Выявление последствий КИ	**Позволяет**	Функция «Проверка активности» позволяет проверить полноту реагирования
Ликвидация последствий КИ	**Помогает**	Выполняется вне ИС по указанным в карточке КИ/КА шагам (runbooks)
Локализация КИ		
Закрытие КИ	**Позволяет**	Обработанные инциденты Переходят в статус «Закрыт»
Фиксация материалов, связанных с возникновением компьютерного инцидента	**Позволяет**	Вкладка «Файлы» в карточке КИ позволяет крепить цифровые следы
Установление причин и условий возникновения компьютерного инцидента	**Позволяет**	Вкладка «События» и история карточки КИ
Анализ результатов деятельности по управлению КИ		
Приобретение и накопление опыта по результатам управления КИ	**Позволяет**	В разделе «Документация» возможно добавлять статьи с разбором кейсов
Разработка рекомендаций по устранению в ИР причин и условий возникновения КИ	**Помогает**	Карточки КИ/КА, извлечение уроков, playbooks для аналогичных кейсов
Оценка результатов и эффективности реагирования на КИ	**Позволяет**	«Дашборд» позволяет просматривать статистику и SLA по зарегистрированным инцидентам

Построение статистических графиков, дашбордов

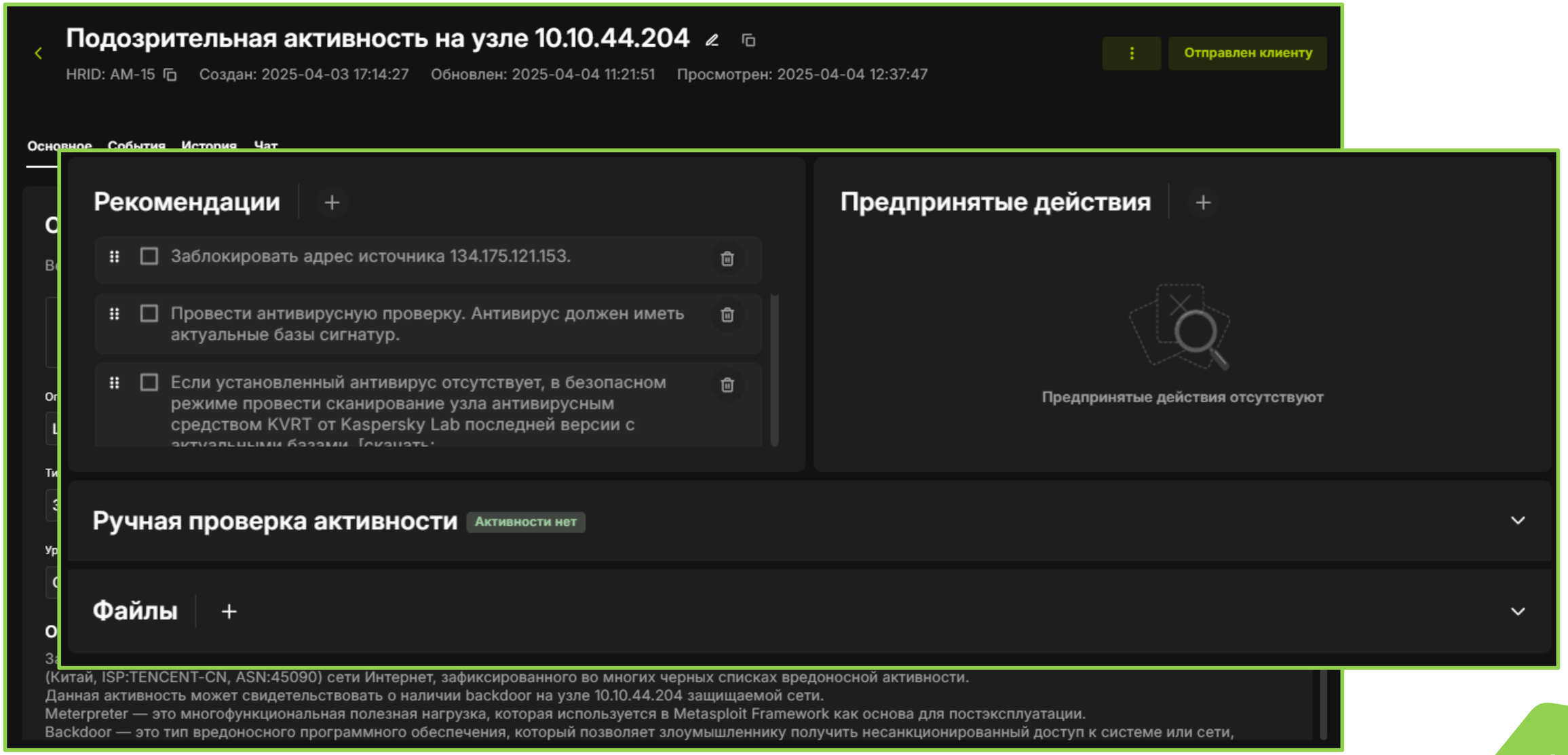
Построение статистических графиков, дашбордов



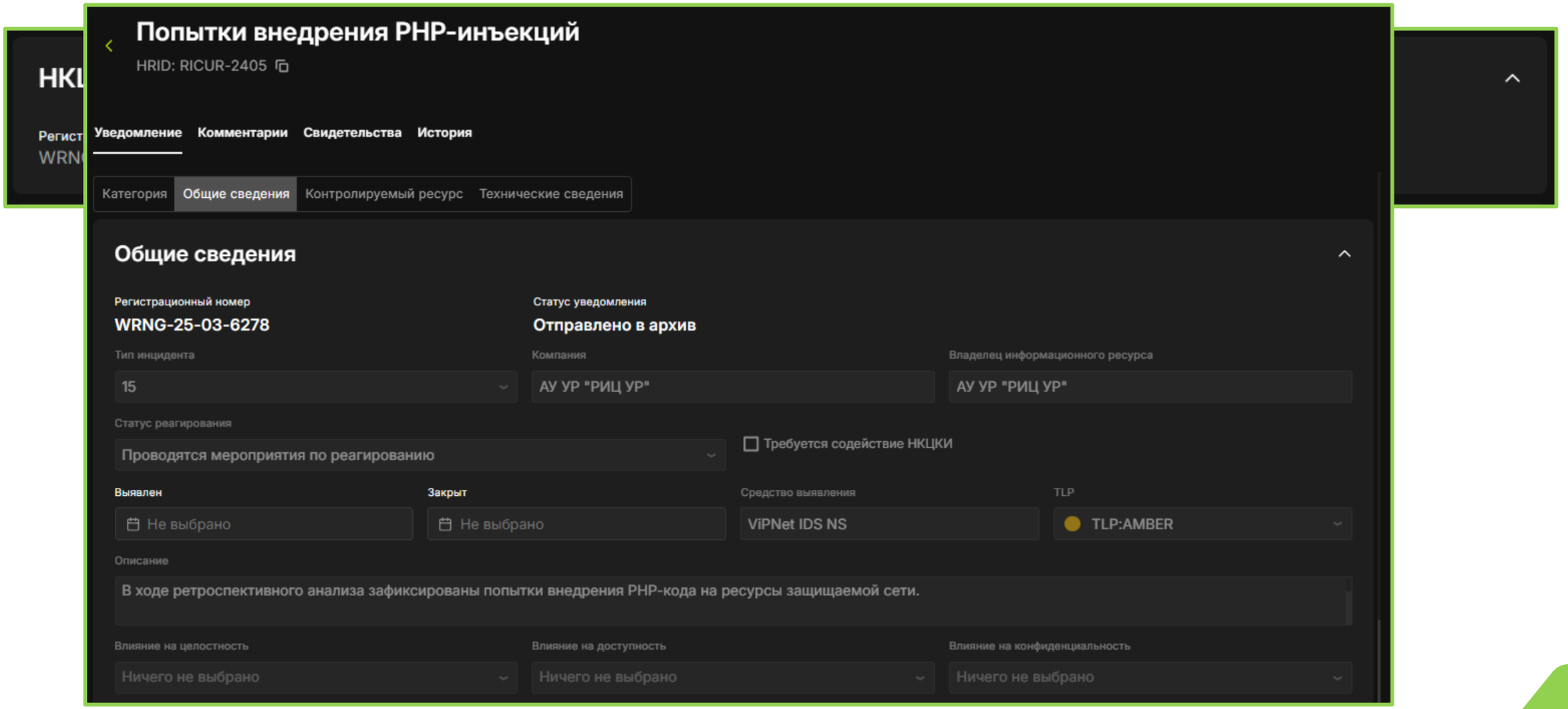
Управление инцидентами ИБ
Раздел «Инциденты»



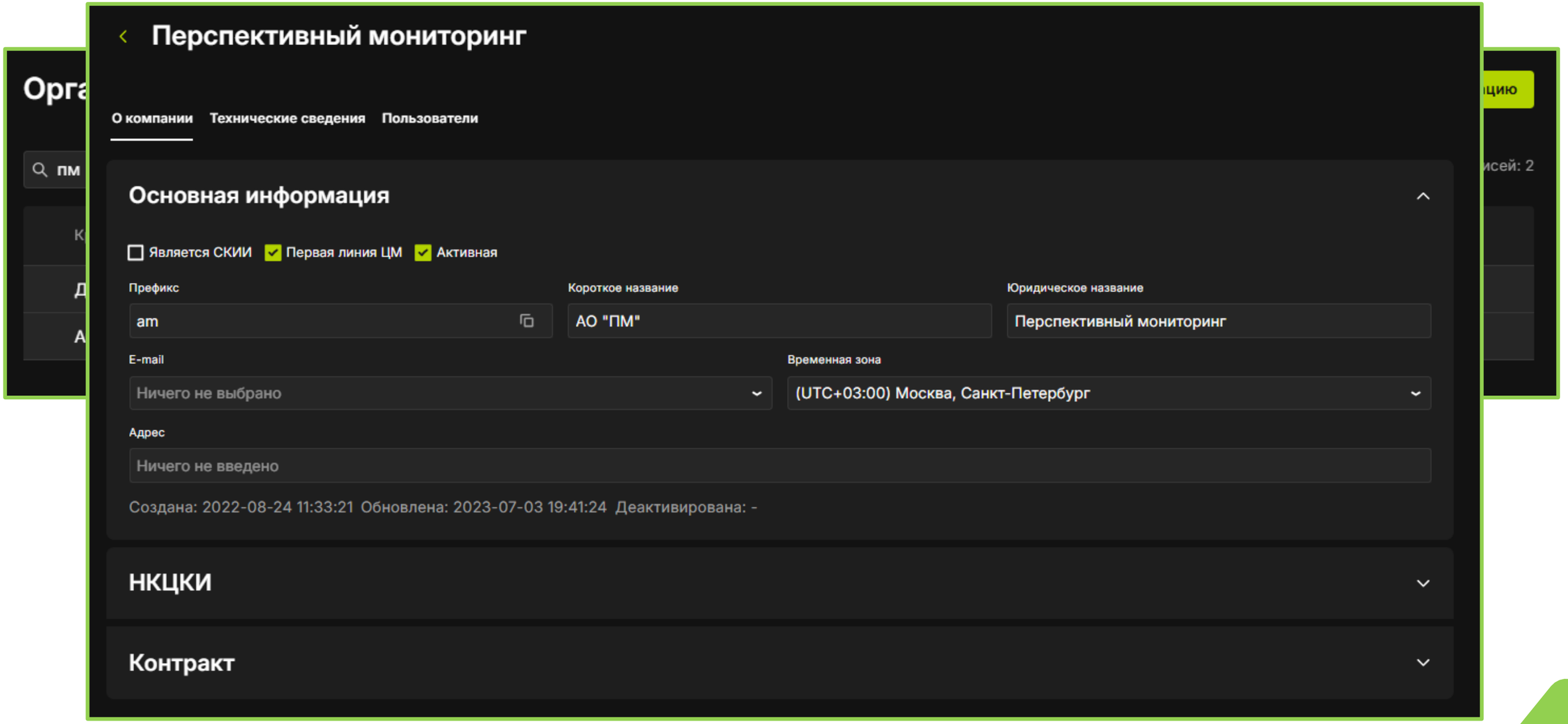
Управление инцидентами ИБ
Карточка КИ/КА



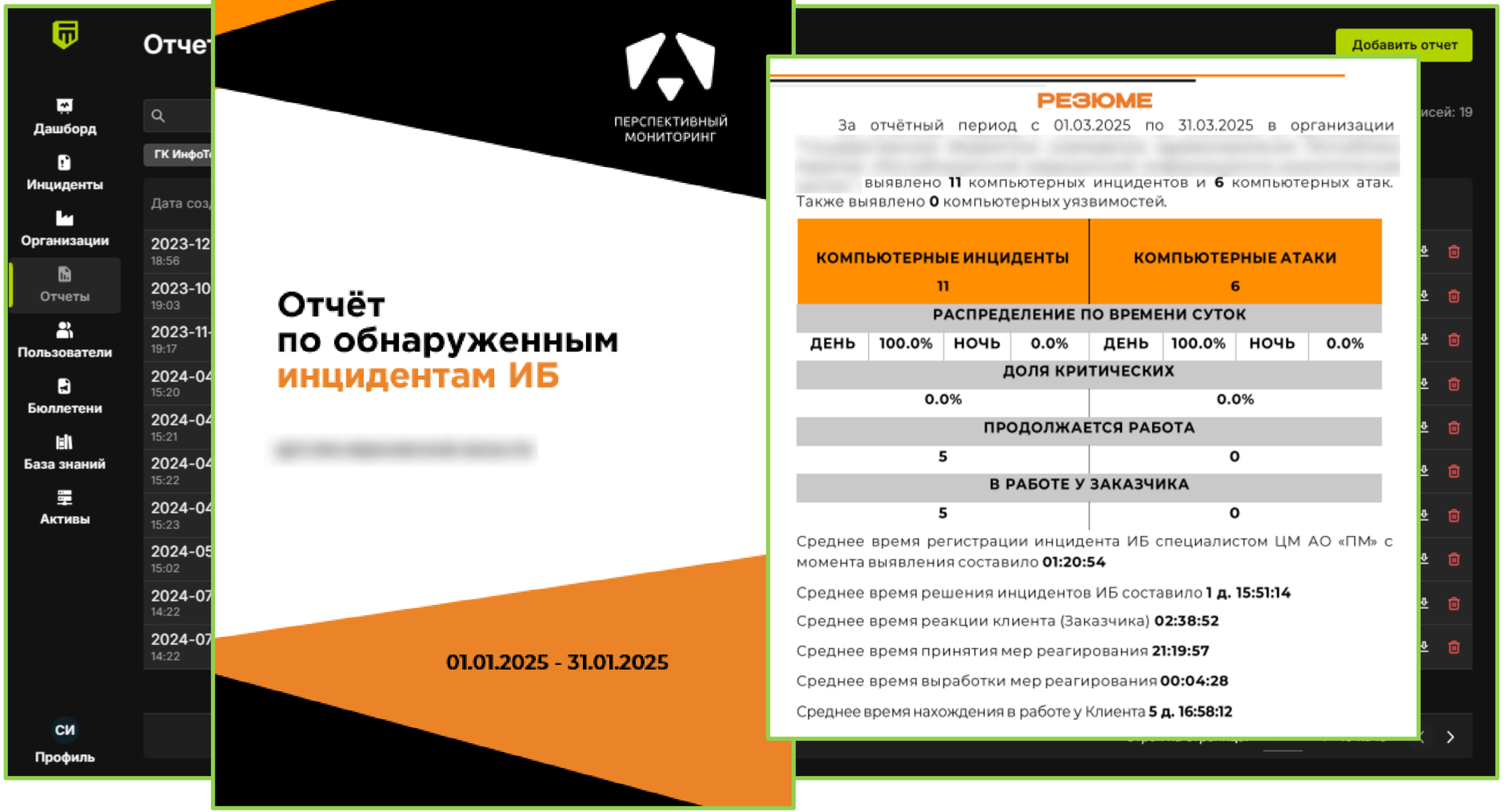
Интеграция с ЛК ГосСОПКА



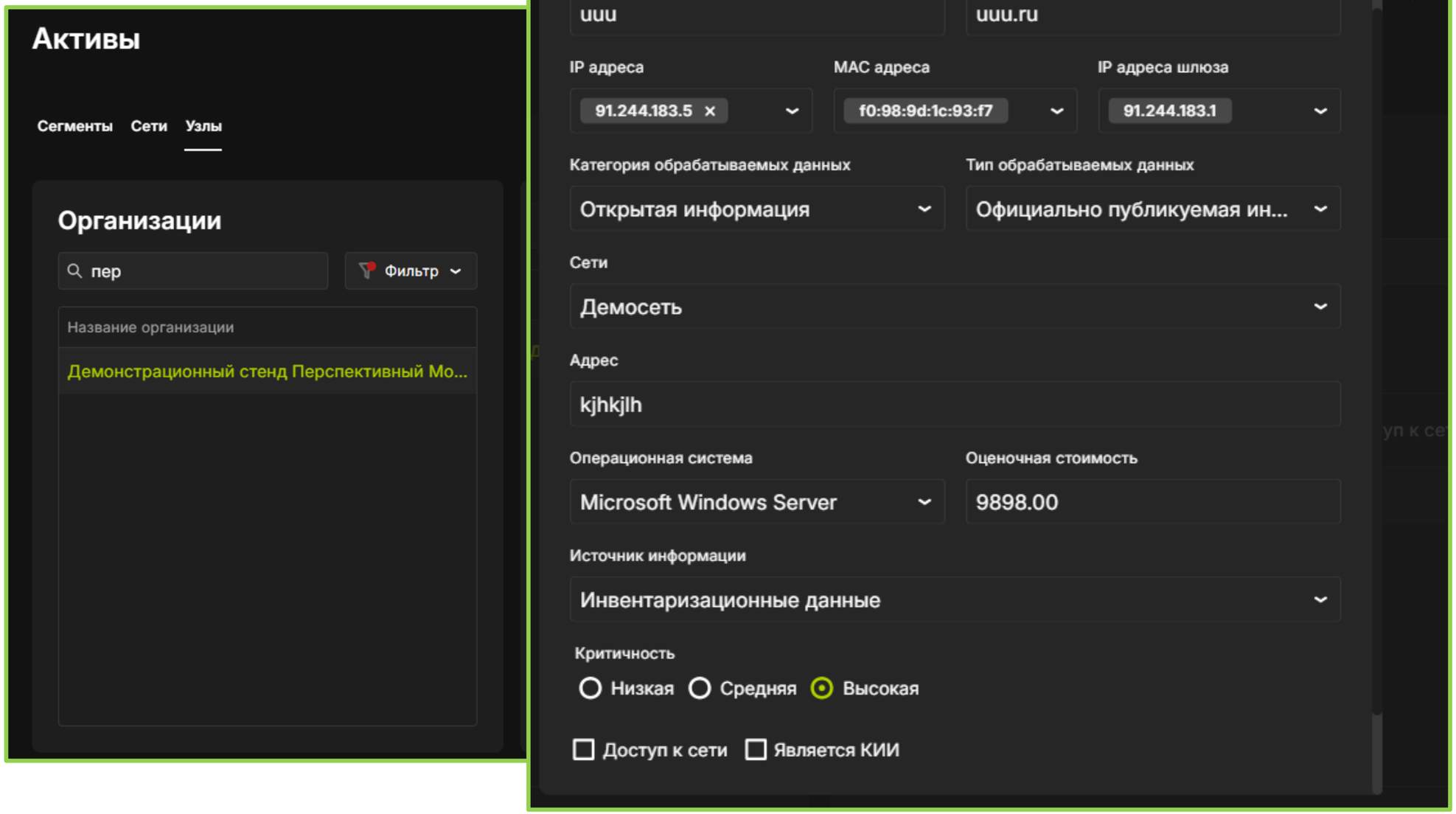
Работа с организациями и филиалами



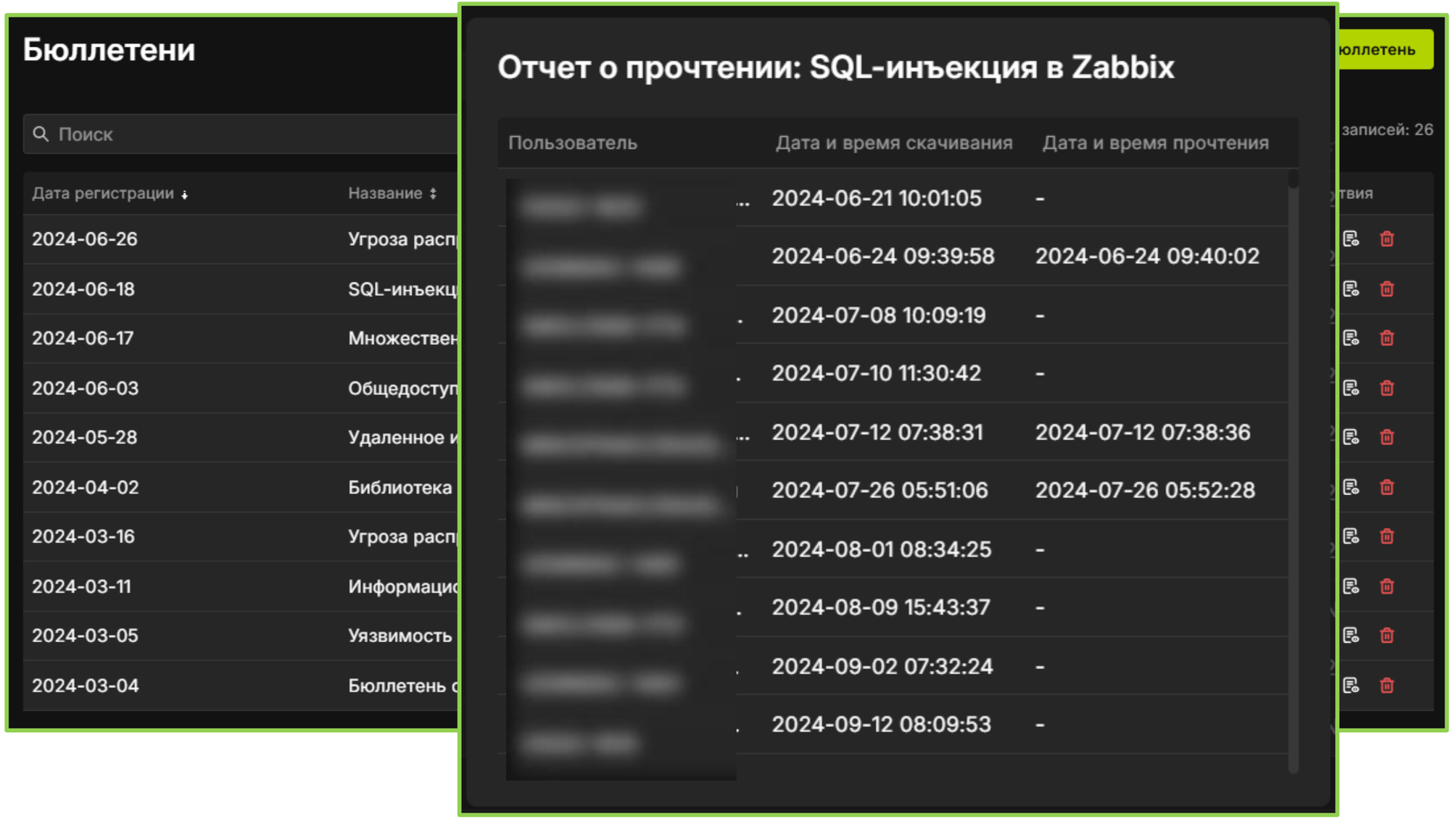
Формирование отчётности



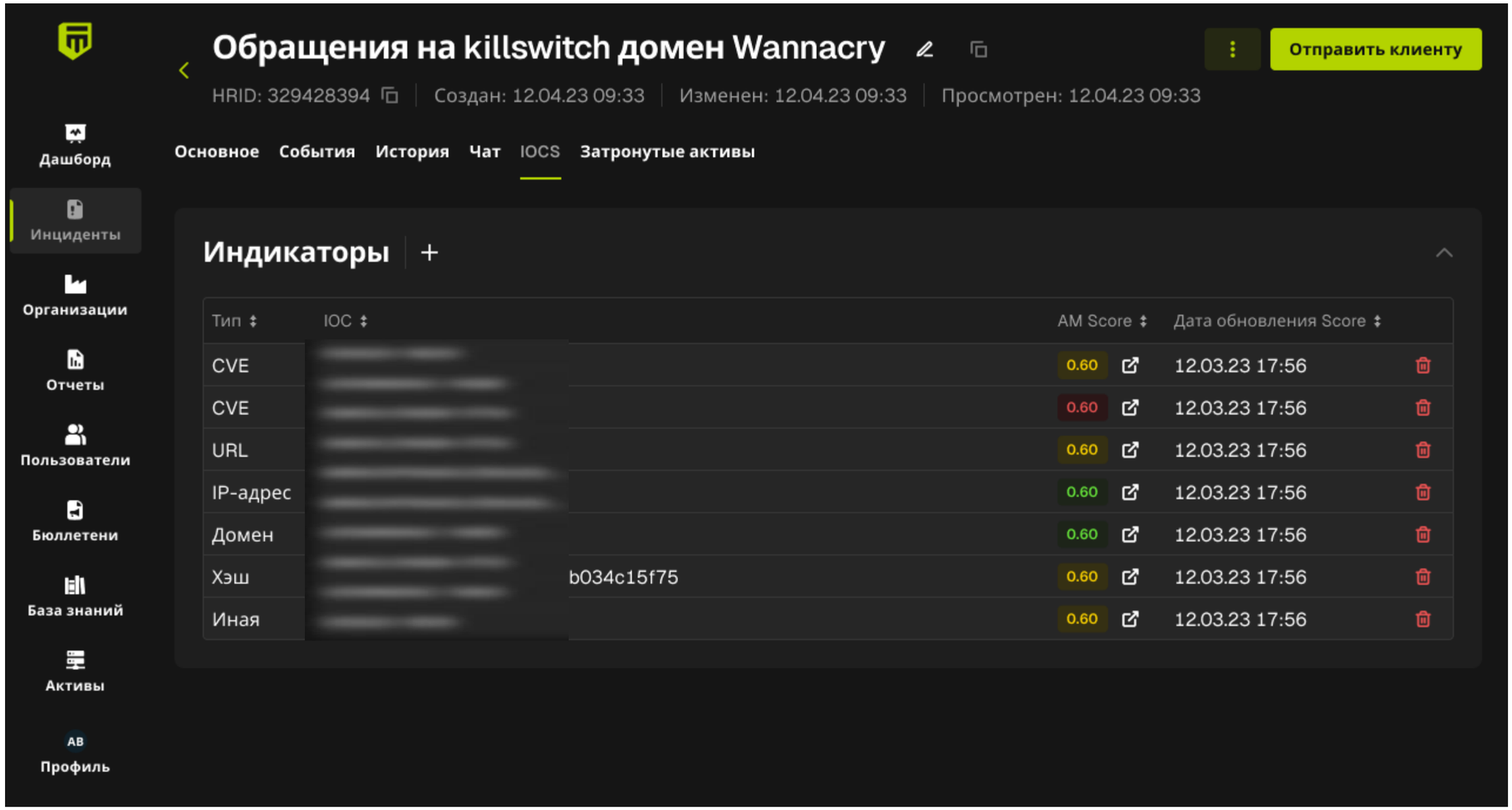
Учёт ИТ-активов



Обмен информацией об угрозах ИБ
Бюллетени



Обмен информацией об угрозах ИБ с /AMTIP



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

t.me/pm_public

@AMonitoring

amtip.ru

Артём Савчук

Технический директор

+7 (495) 737-61-97

info@amonitoring.ru

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA
NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ
GLOBAL DIGITAL SPACE
CISOCLUB
РУТОКЕН КОМПАНИЯ АКТИВ
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ
АВАНГАРД
ARinteg
АТБ ЭЛЕКТРОНИКА
infotecs {/-cademy}
merlion
УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС