С•терра®

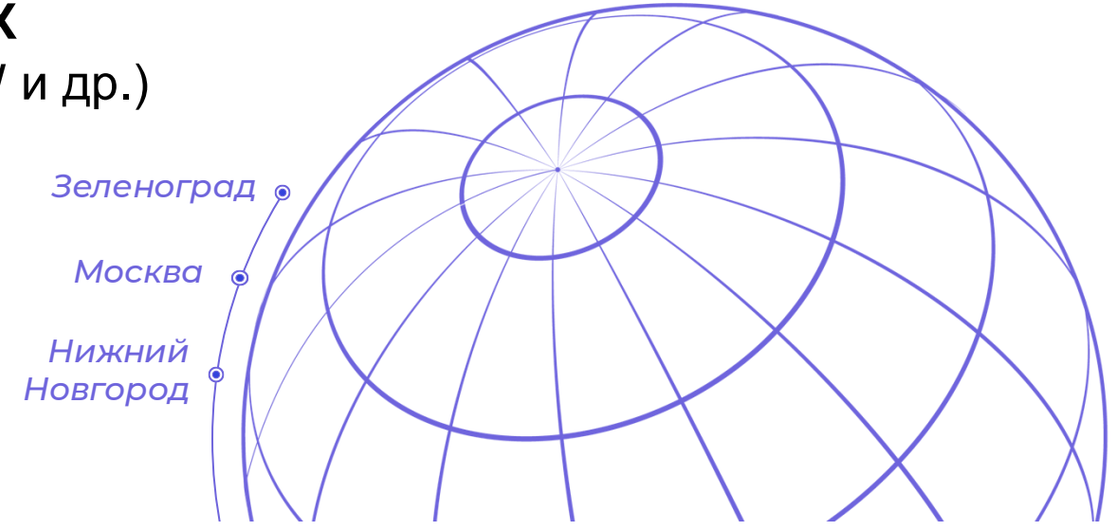
Ваш ориентир в мире безопасности

С-ТЕРРА ЭКРАН-М

Москва, 2025

Разработка и производство **СЕРТИФИЦИРОВАННЫХ** средств защиты каналов связи (VPN, FW, TLS, NGFW и др.)

КРИПТОГРАФИЧЕСКАЯ защита информации.
Лицензиаты ***ФСБ*** России и ***ФСТЭК*** России



2003	2006	2008	2010	2012	2014	2017	2020	2025
Основание компании	Разработки с Cisco NME-RVPN	Версия 3.0	Версия 3.1	Версия 3.11	Версия 4.1	Версия 4.2	Версия 4.3	**Экран-М**

НАМ ДОВЕРЯЮТ

[Органы власти]

Безопасная цифровая среда для управления, устойчивости и доверия

Федеральное дорожное агентство РОСАВТОДОР

[Производство и ТЭК]

ИБ-решения для непрерывной работы и защиты стратегической инфраструктуры

Газпром нефть · Роснефть · Россети · СИБУР · АО «СО ЕЭС»

[Финансовые организации]

Защита фин.сервисов, клиентских данных и критичных операций

ВТБ · Банк России · РоссельхозБанк · ГАЗПРОМБАНК

[Операторы связи]

Надёжность и контроль в сетях с миллионами подключений.

МТС · Ростелеком

ЧТО МЫ ПРЕДЛАГАЕМ РЫНКУ И ЧЕМ МЫ ЛУЧШЕ

ЭКРАН·М ногофункциональный одульный ежсетевой

С-Терра Экран М - многофункциональный межсетевой экран уровня сети

[Архитектура]

- Разработана с нуля в 2023–2024 г.
- Создавалась под требования ФСТЭК

[Сертификация]

- ФСТЭК по профилю защиты многофункциональных межсетевых экранов уровня сети четвертого класса защиты
- Российская разработка под ОС Astra Linux

[Модульность]

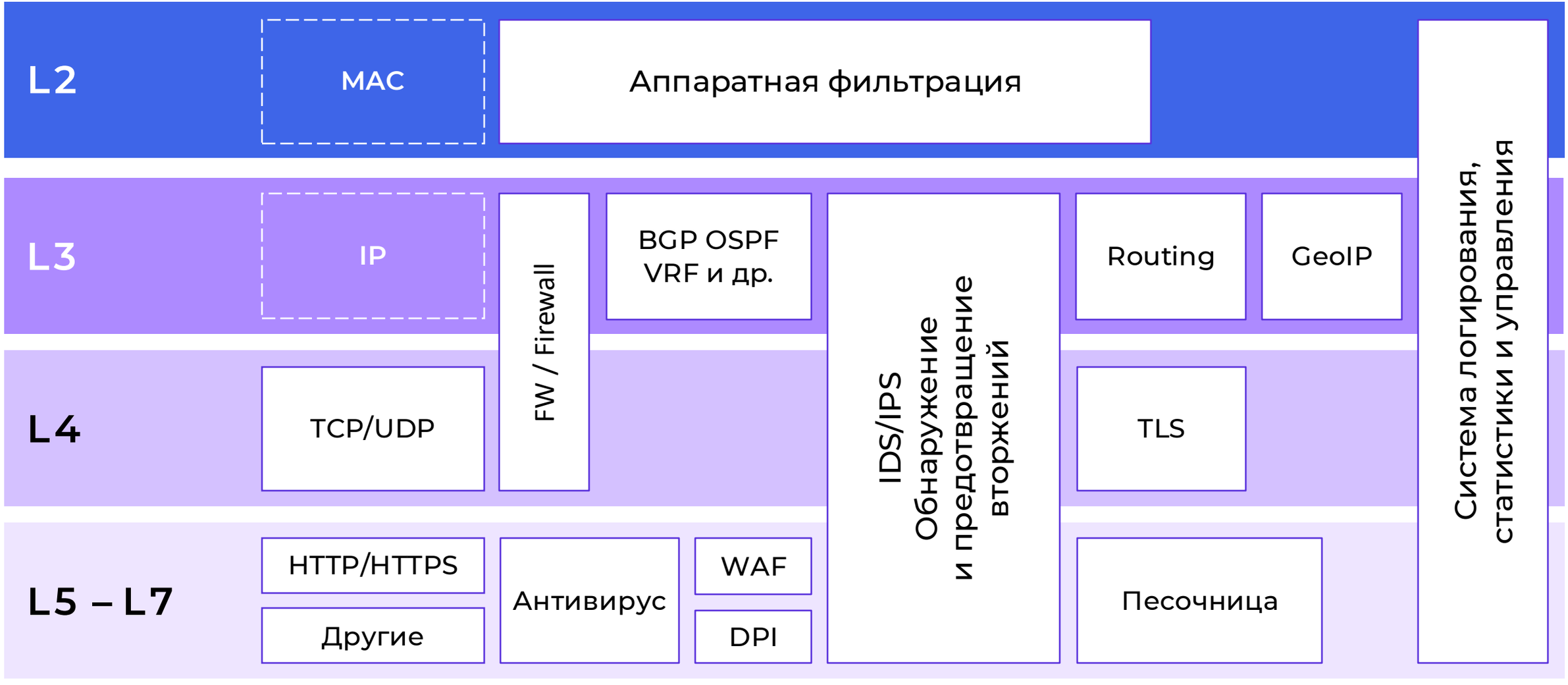
- Интеграция с внешними системами
- Гибкое изменение состава модулей

[Опыт]

- Существующие решения С-Терра
- Экспертиза и компетенции компании с более чем 21 летним опытом работы на рынке ИБ

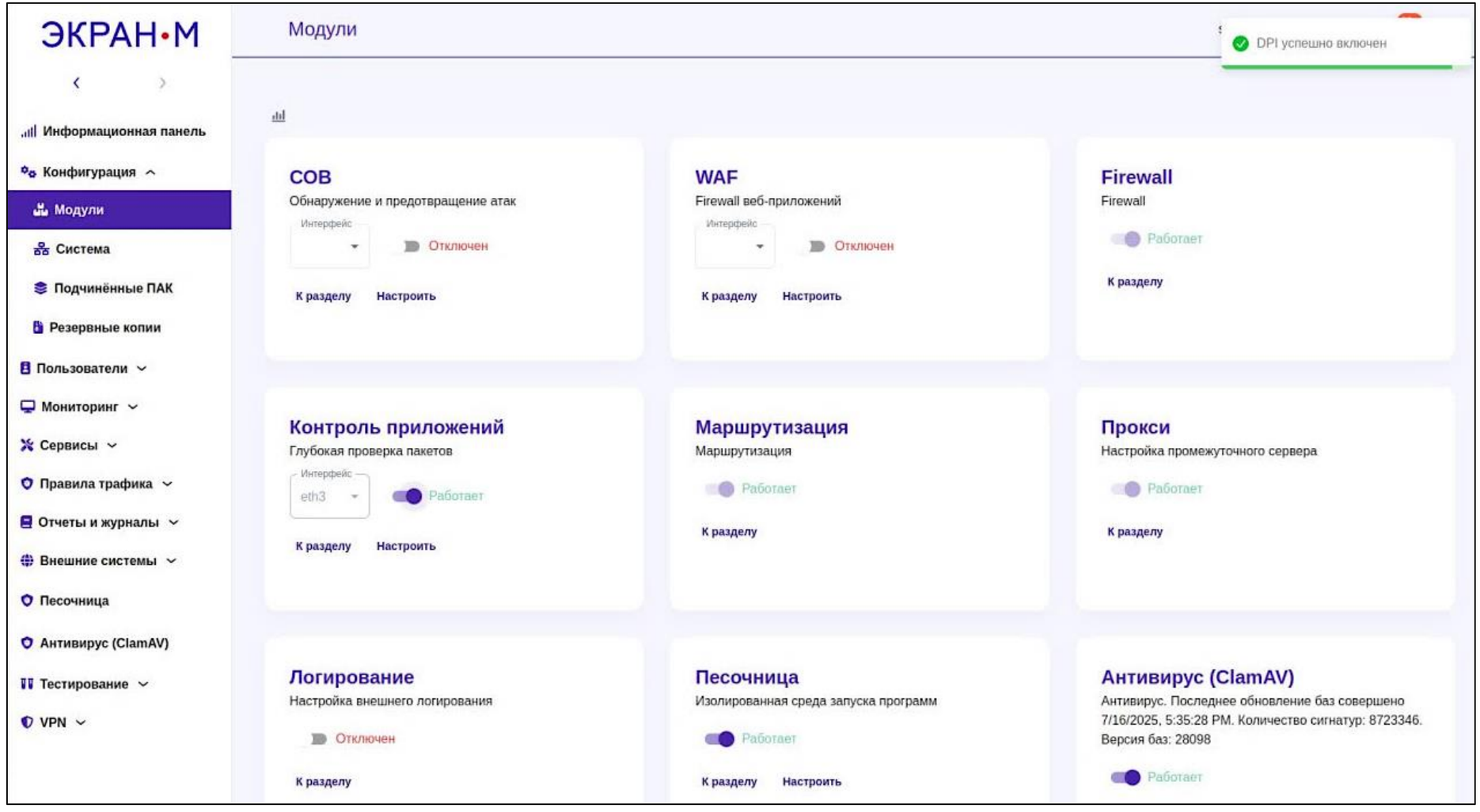
АРХИТЕКТУРА С-ТЕРРА ЭКРАН-М

ЭКРАН·М многофункциональный модульный межсетевой



РАБОТА С МОДУЛЯМИ ЭКРАН-М

Firewall, IPS, Контроль приложений, Антивирус, WAF, Песочница и другие



МОДИФИКАЦИИ С-ТЕРРА ЭКРАН-М

[С-Терра Экран-М 8000]

[С-Терра Экран-М 7000]

ЧТО ПОЛУЧАЕТ РЫНОК

ЭКРАН·М ногофункциональный модульный межсетевой

В декабре 2024 года стартовала сертификация Экран-М на соответствие требованиям к ММЭ уровня сети во ФСТЭК РФ

2024
Протестировано ЦБ РФ

2025
Проверено ФСТЭК РФ

- Обработка трафика вынесена за пределы ядра в пользовательское пространство. Взаимодействие с сетевой картой напрямую
- Технологии DPDK и VPP

Пропускная способность в режиме **FW + Stateful + NAT + IPS + Антивирус** для **Экран М 8000 – до 24 Гбит/с**
*Согласно тестам Инфосистемы Джет

Режим работы	Пропускная способность на один порт		Количество правил
	Экран-М 8000	Экран-М 7000	
FW + Stateful	До **96** Гбит/с	До **38** Гбит/с	100 тыс. ACL
FW + IDS/IPS	До **24** Гбит/с	До **12** Гбит/с	100 тыс. ACL + 40 тыс.
FW + IDS/IPS + WAF	До **10** Гбит/с	До **6** Гбит/с	100 тыс. ACL + 60 тыс.
FW + IDS/IPS + DPI + WAF + Антивирус + Песочница	До **5** Гбит/с	До **3.5** Гбит/с	100 тыс. ACL + 150 тыс.

В ПЛАНАХ — РАСШИРЕНИЕ ЛИНЕЙКИ ДЛЯ ЭКРАН-М

Модификации Экран-М на младших и средних аппаратных платформах

[С-Терра Экран-М 100]

[С-Терра Экран-М 1000]

[С-Терра Экран-М 3000]

[С-Терра Экран-М 7000]

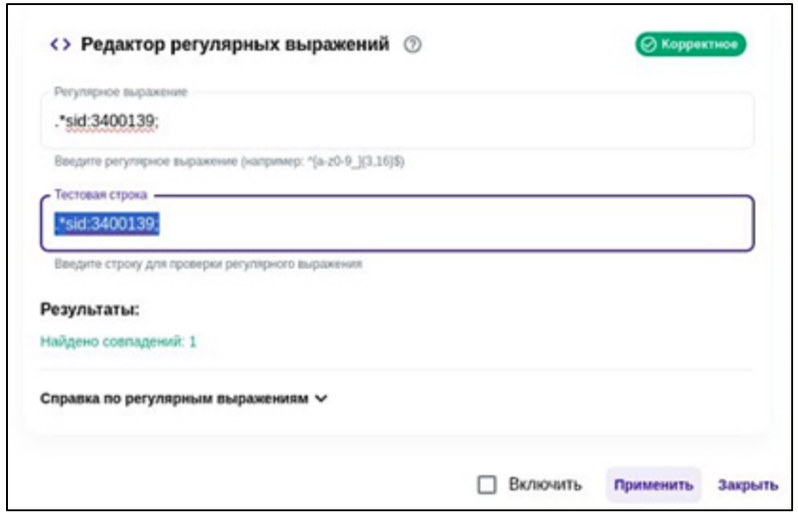
[Информационная безопасность]

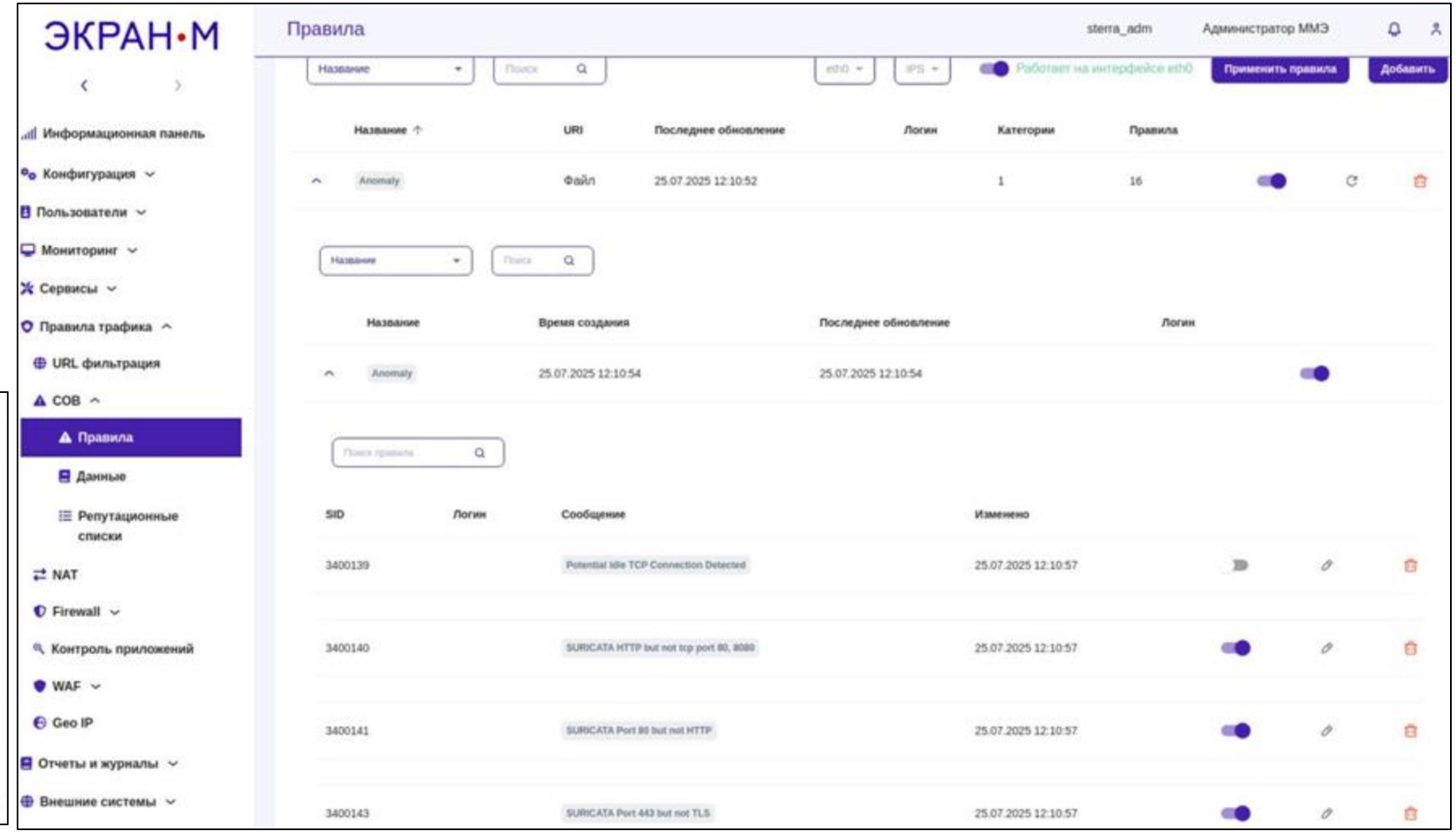
IPS и IDS / URL-фильтрация / GeoIP / Прокси-сервер / Расширенный DNS-анализ / Интеграция с MS AD

- VPN
  (IPsec IKEv2 без ГОСТ, WireGuard)
- Антивирус и Песочница
  (изолированная среда анализа с контролем поведения объектов)
- Интеграция с внешними системами по REST API
  (включая автоматизацию реакции на инциденты, прямая интеграция с Гарда DLP)
- Межсетевой экран
  (Firewall, в т.ч. stateful фильтрация)
- Определение категории сайта конкретного запроса
  (категории фильтрации)
- Группировка событий различного типа, сгенерированных в рамках одной сессии
  (межсетевое экранирование, защита от угроз, контроль передачи файлов, URL-фильтрация, времени сессий)

РАБОТА С СИГНАТУРАМИ ПРИ ПОМОЩИ РЕГУЛЯРНЫХ ВЫРАЖЕНИЙ

В примере выполняется поиск и отключение совпадений по SID (signature ID)





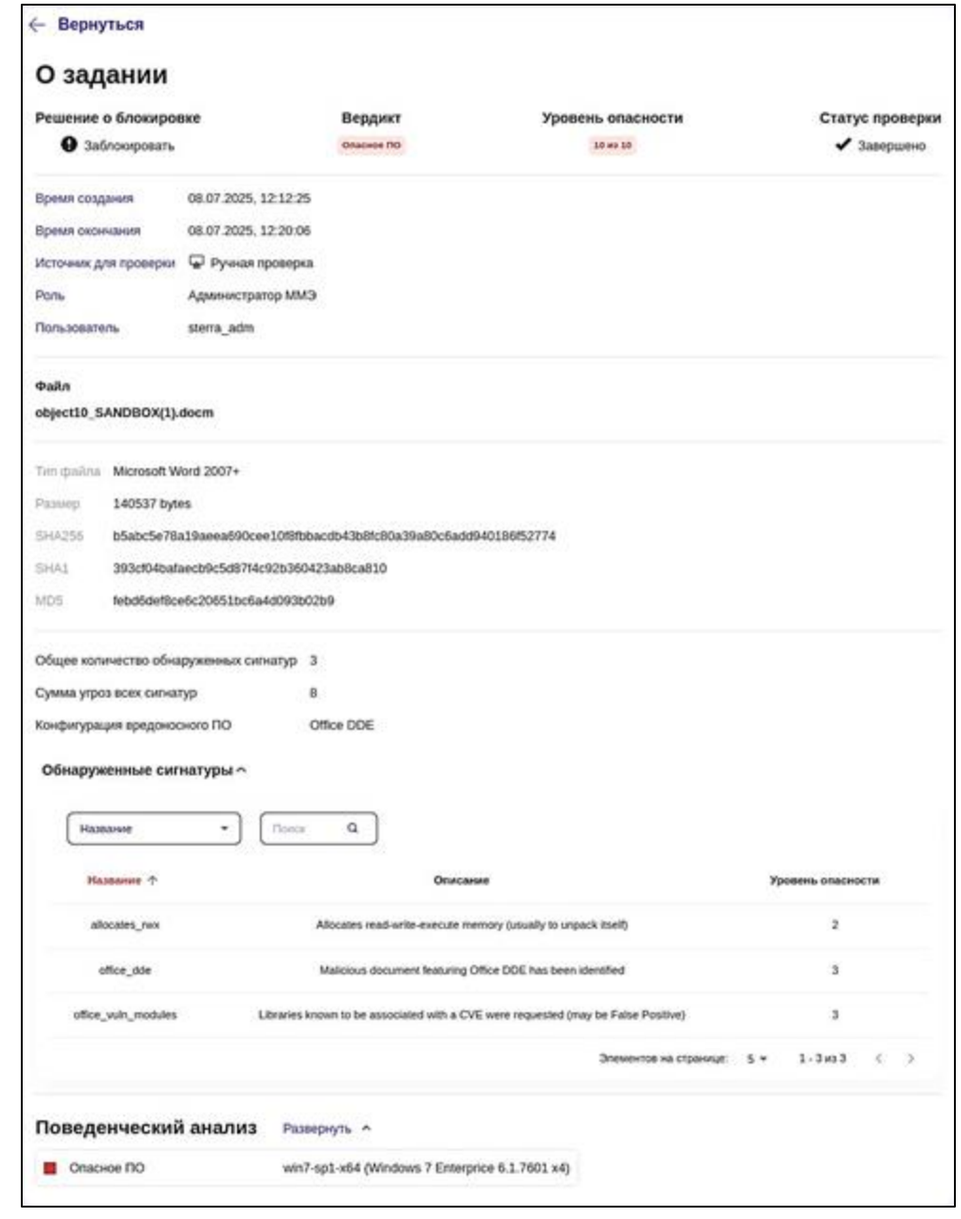
РАБОТА ПЕСОЧНИЦЫ И АНТИВИРУСА

[Песочница]

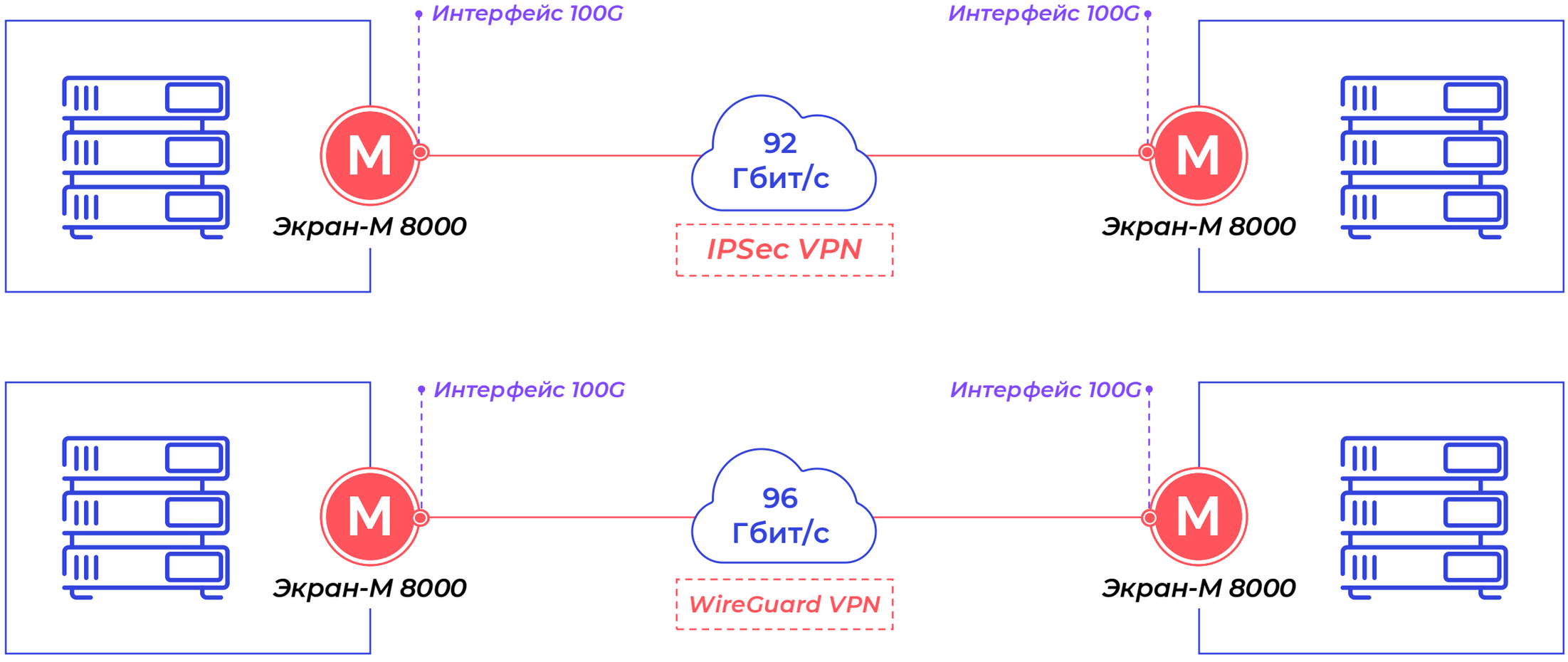
- Отчёт содержит подробную статистику по срабатываниям сигнатур
- Настройка работы песочницы по пользователям или хостам
- Поддерживается работа на всех аппаратных платформах линейки

[Антивирус]

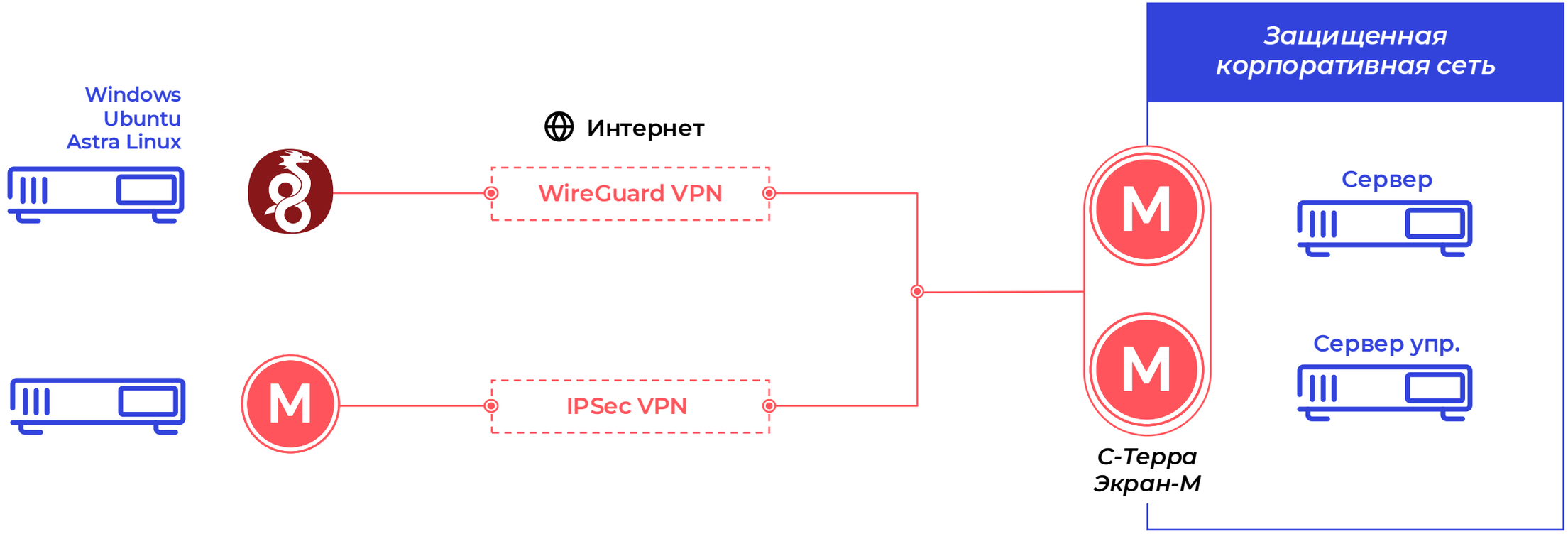
- Поддержка блокировки зашифрованных файлов
- Поддерживается работа на всех аппаратных платформах линейки
- Настройка антивируса для точечной проверки пользователей или хостов по IP / MAC адресам



IPSec VPN и WireGuard VPN

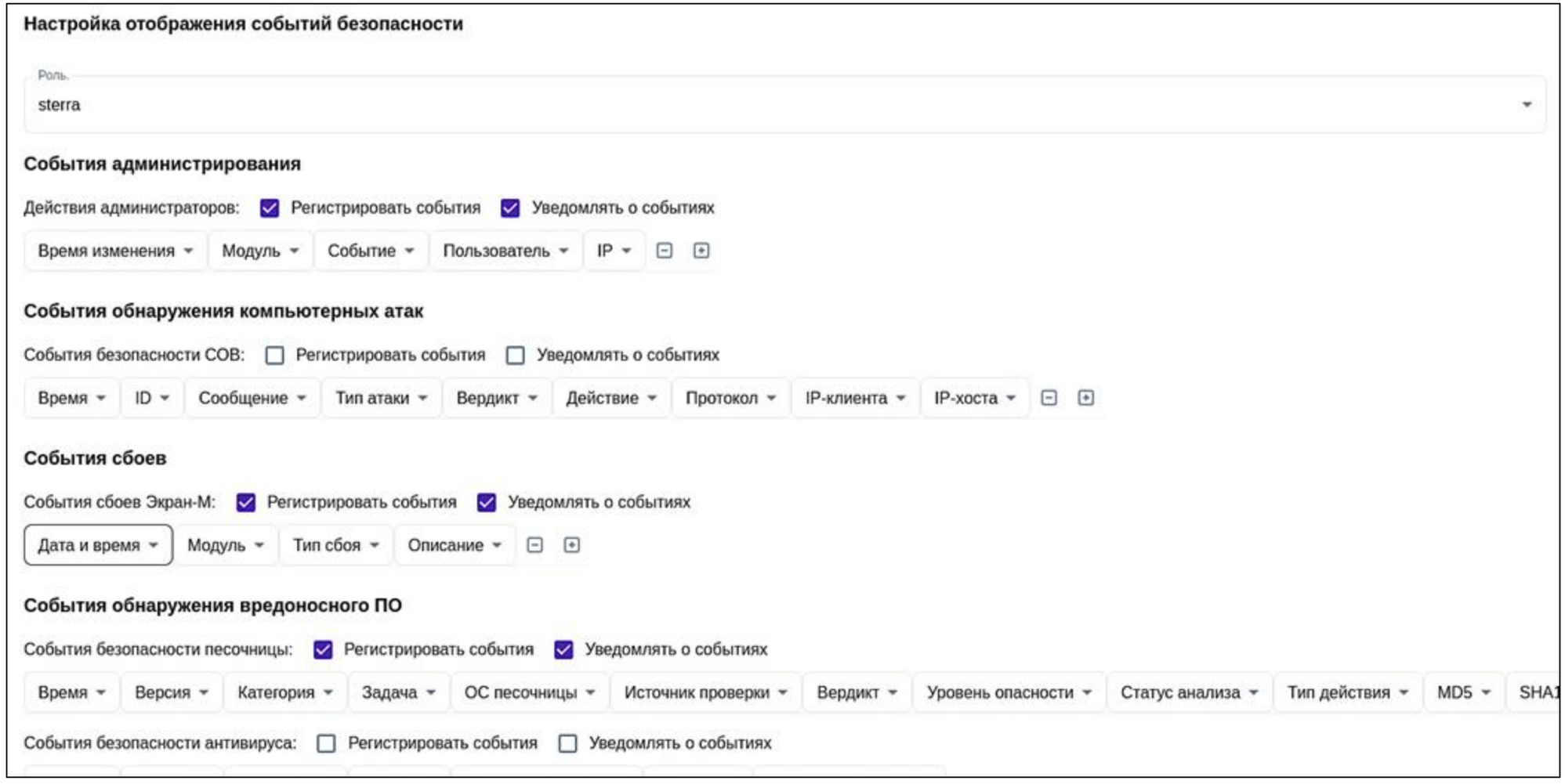


WIREGUARD ЭКРАН-М КЛИЕНТ



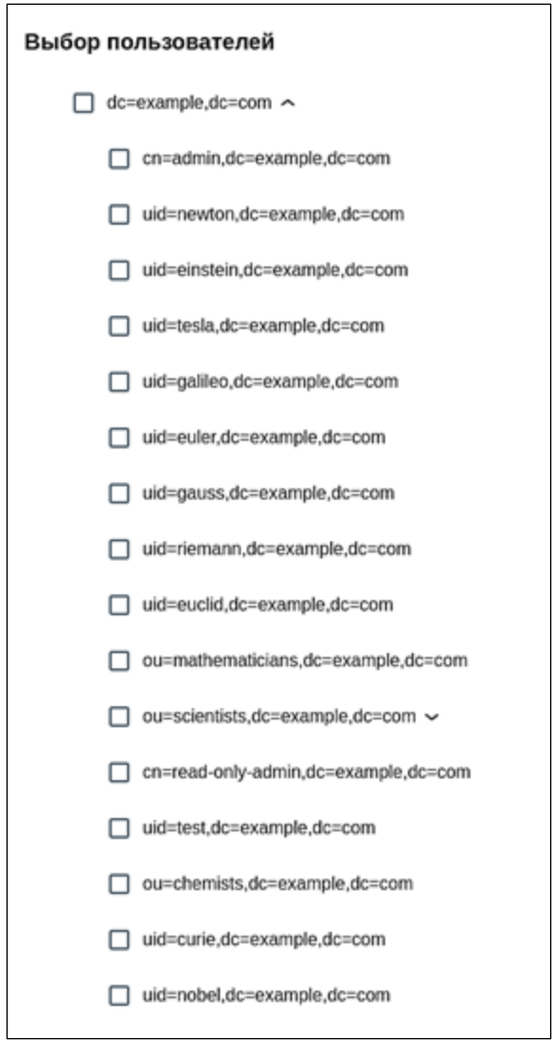
ГРУППИРОВКА СОБЫТИЙ РАЗЛИЧНОГО ТИПА ПО ГРУППАМ ПОЛЬЗОВАТЕЛЕЙ

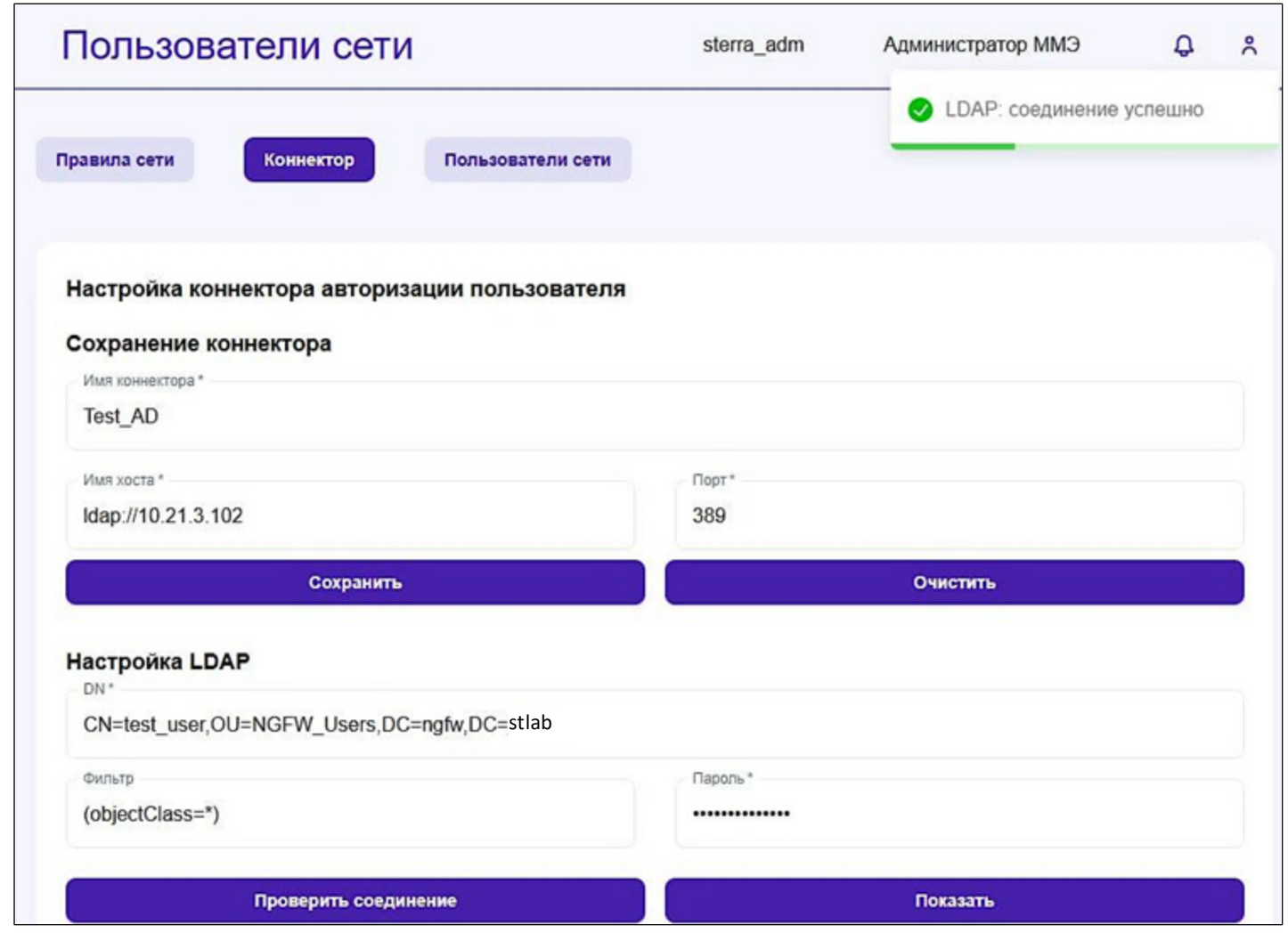
События сбоев, события администрирования, обнаружения компьютерных атак, обнаружения вредоносного ПО



ИНТЕГРАЦИЯ С MICROSOFT ACTIVE DIRECTORY ДЛЯ ПОЛИТИК БЕЗОПАСНОСТИ

Применение политик безопасности на основе групп и пользователей





[Больше, чем вы ждёте]

SMTP / NTP-клиент / DHCP (сервер и relay) / PPPoE

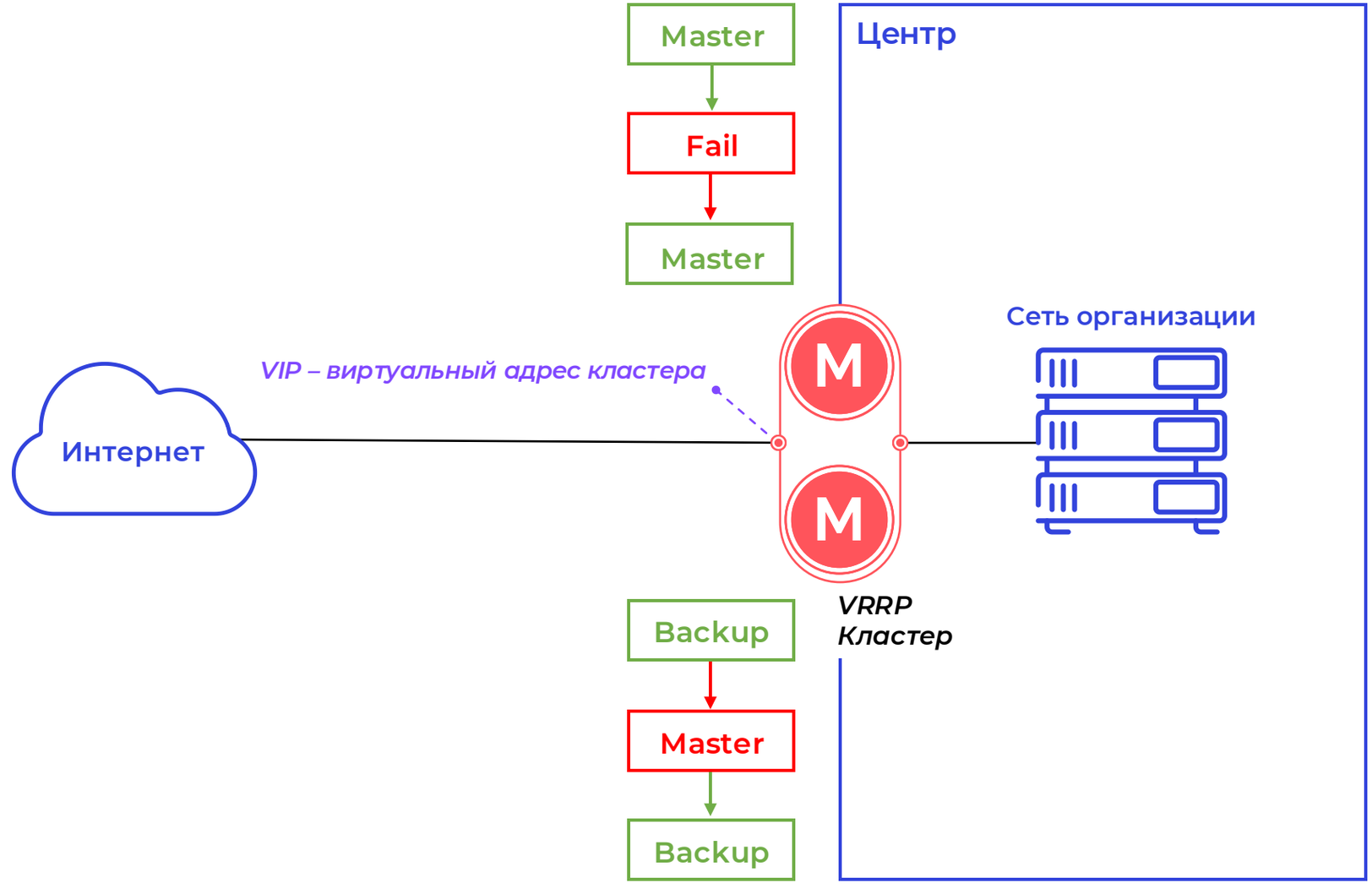
- NAT / PAT
  (трансляция сетевых адресов и портов)
- VLAN
  (802.1Q)
- VxLAN
  (Virtual Extensible LAN – виртуализация сети)
- IPv6
  (NAT, маршрутизация, правила МЭ)
- SPAN
  (порт зеркалирования)
- Статическая и динамическая маршрутизация
  (OSPF, BGP)
- LACP
  (агрегация каналов)
- Кластеризация
  (отказоустойчивость на базе VRRPv3)

КЛАСТЕР ЭКРАН-М

Отказоустойчивость на базе протокола VRRPv3

[Типы отказов]

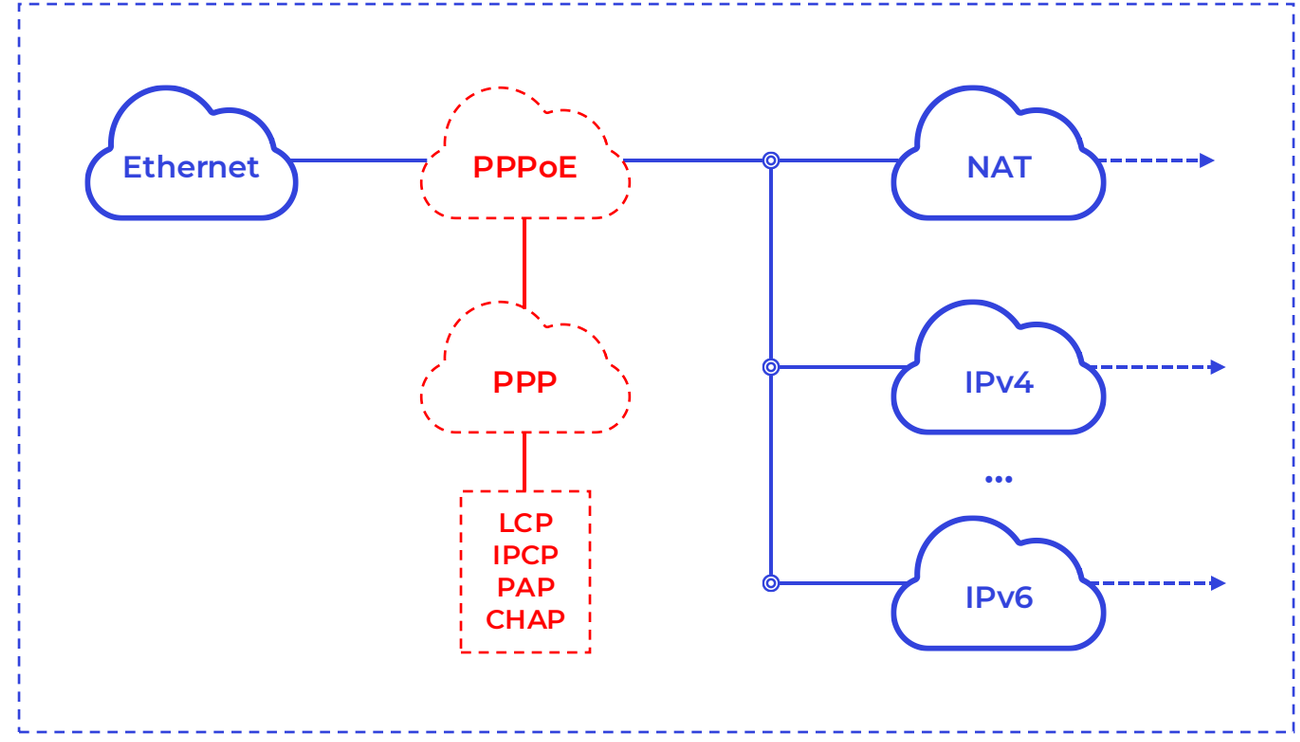
- Отключение питания
- Выход из строя аппаратной платформы
- Отказ сетевого интерфейса
- Отказ порта на коммутационном оборудовании



ПОДДЕРЖКА СОЕДИНЕНИЙ PPPOE

Point-to-Point Protocol over Ethernet - прямое подключение к провайдеру

```
show pppoe client session
  state:         11111
  session_id:    19
  sw_if_index:   vpp0
  LCP id:        7
  AUTH id:       0
  IPCP id:       3
  MRU:           1492
  Auth method:   CHAP
  Magic number: 0x327b23c6
  our_ip:        47.1.1.118
  peer_ip:       47.1.1.6
  dns1:          8.8.8.8
  dns2:          8.8.4.4
  cookie_len:    20
  cookie:        edc08bf80fcf949a660df456aab24d3cd1670000
  username:      test
  password:      test
  provider:      pppoe
-- more -- (2-18/18)
```



[Управление и эксплуатация]

Анализ и отслеживание изменений конфигурации / Создание пользователей и настройка ролей

- Структура управления

  (единая система с Web-интерфейсом, консолью и REST API для контроля всех функций Экран-М)

- Автоматизация и контроль

  (открытый REST API для интеграции с внешними системами и автоматизации управления)

- Автоматические скрипты переноса настроек из других вендоров

  (импорт настроек из решений других вендоров без ручной переработки)

- Простая настройка ACL

  (управление доступом через DRAG&DROP)

- Визуализация зон и режимов работы интерфейсов

  (наглядное отображение связей между зонами безопасности и сетевыми интерфейсами)

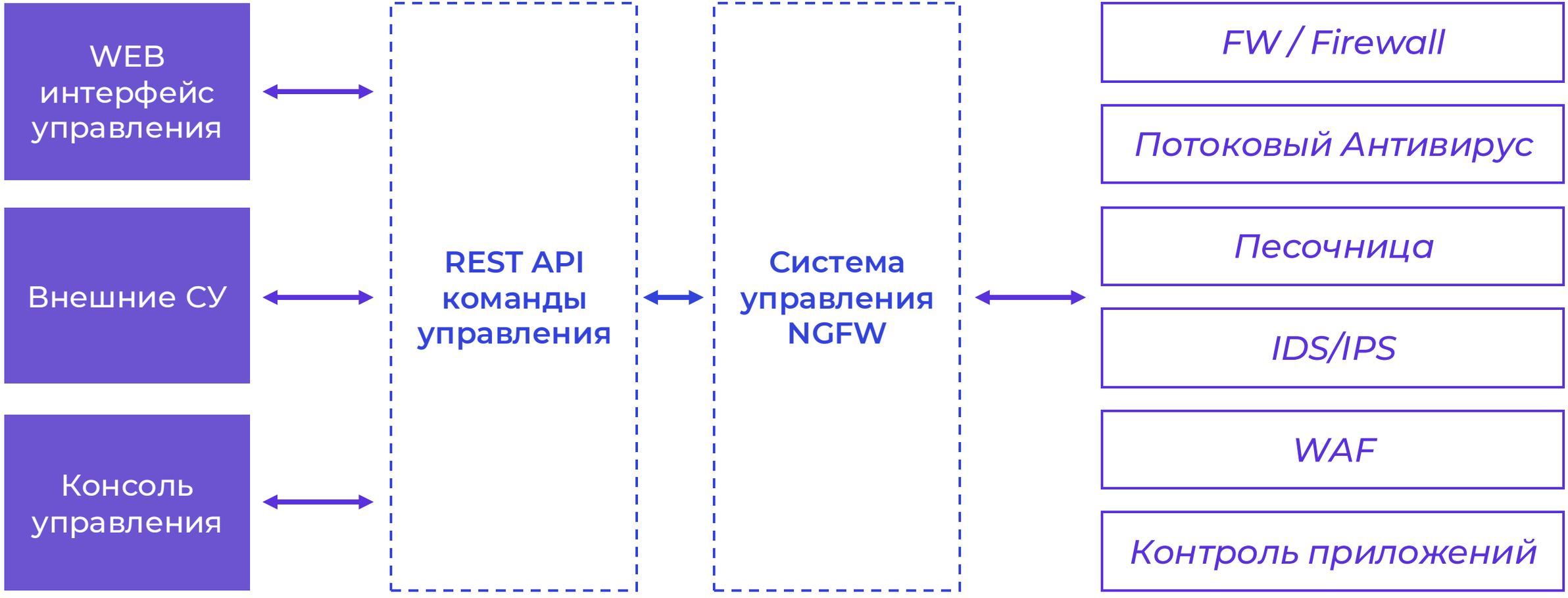
- Групповое управление подчиненными межсетевыми экранами

  (централизованное администрирование нескольких устройств из одного интерфейса)

СТРУКТУРА УПРАВЛЕНИЯ С-ТЕРРА ЭКРАН-М

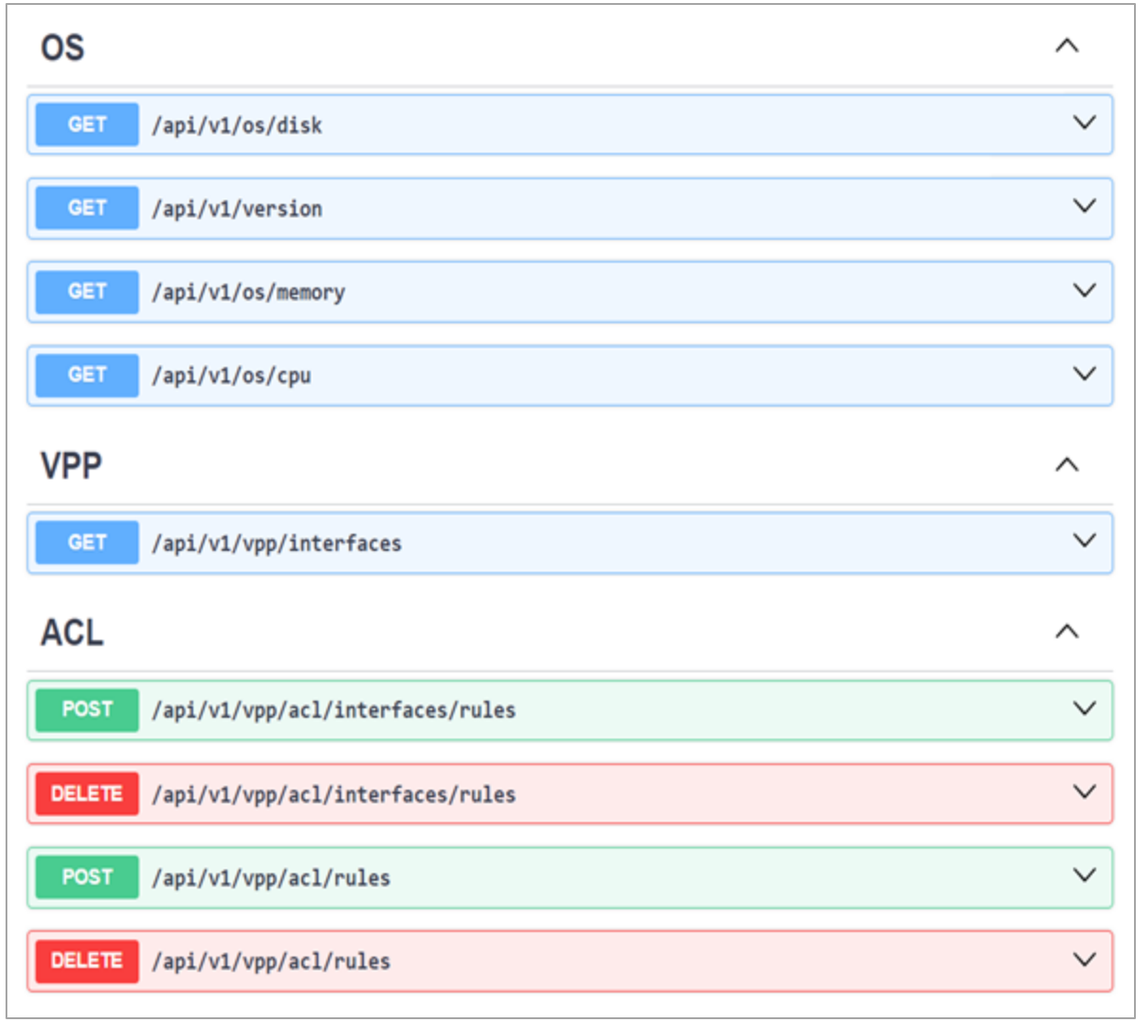
ЭКРАН·М ногофункциональный модульный межсетевой

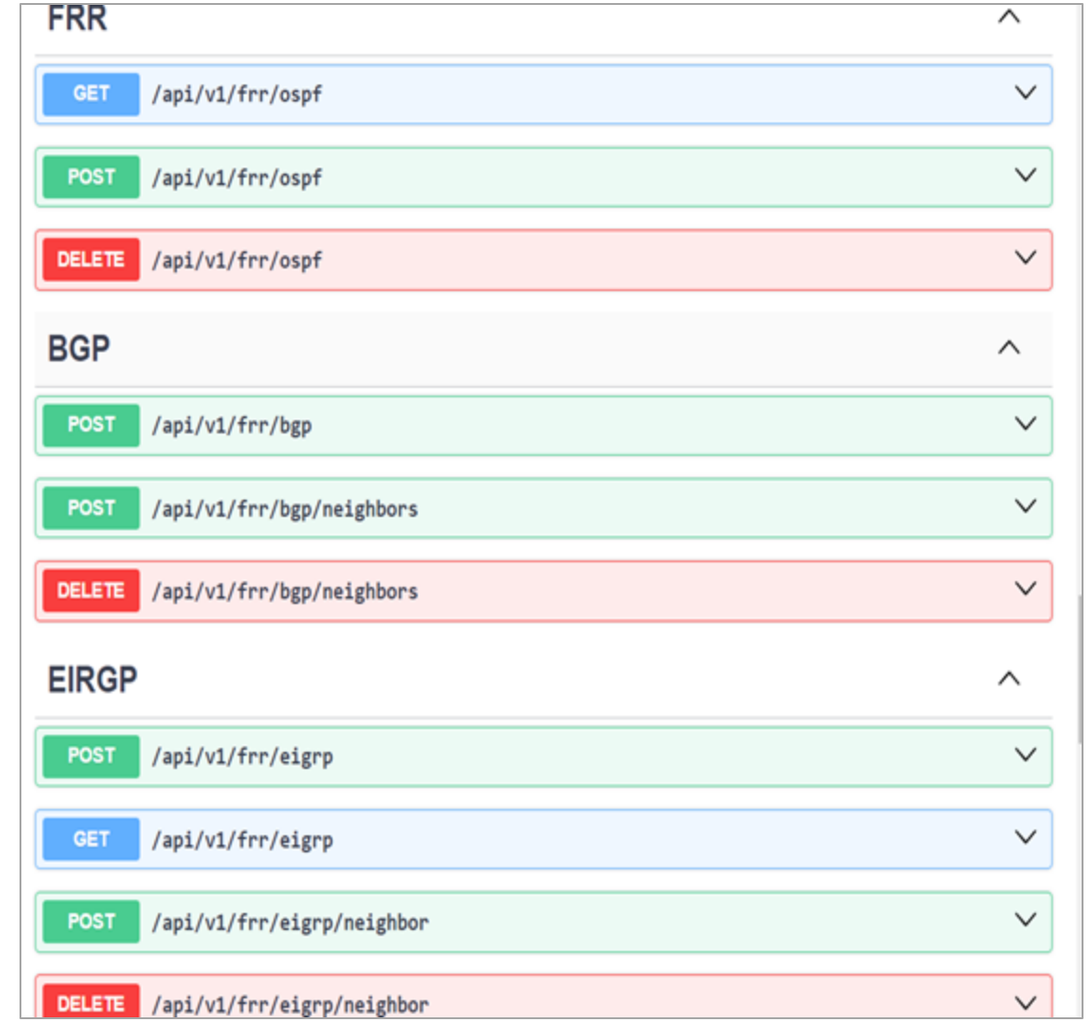
Единая система управления



ОТКРЫТЫЙ REST API — АВТОМАТИЗАЦИЯ И КОНТРОЛЬ

Открытый интерфейс для подключения к вашей инфраструктуре

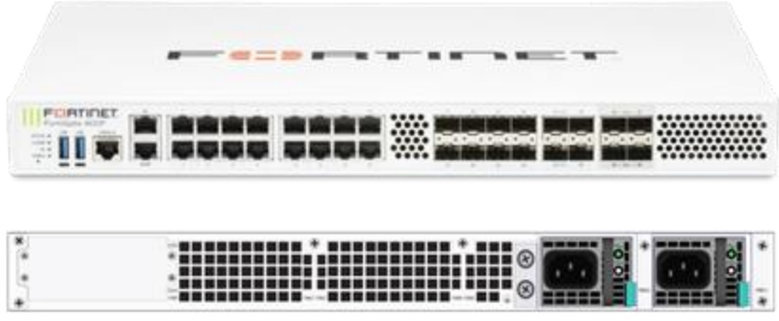




АВТОМАТИЧЕСКИЕ СКРИПТЫ ПЕРЕНОСА КОНФИГУРАЦИИ

Возможность переноса настроек с оборудования других вендоров (FW + NAT).
Подбор конкретной аппаратной платформы С-Терра осуществляется с учётом требований проекта.

[FortiNet]



Перенос

[Экран-М]

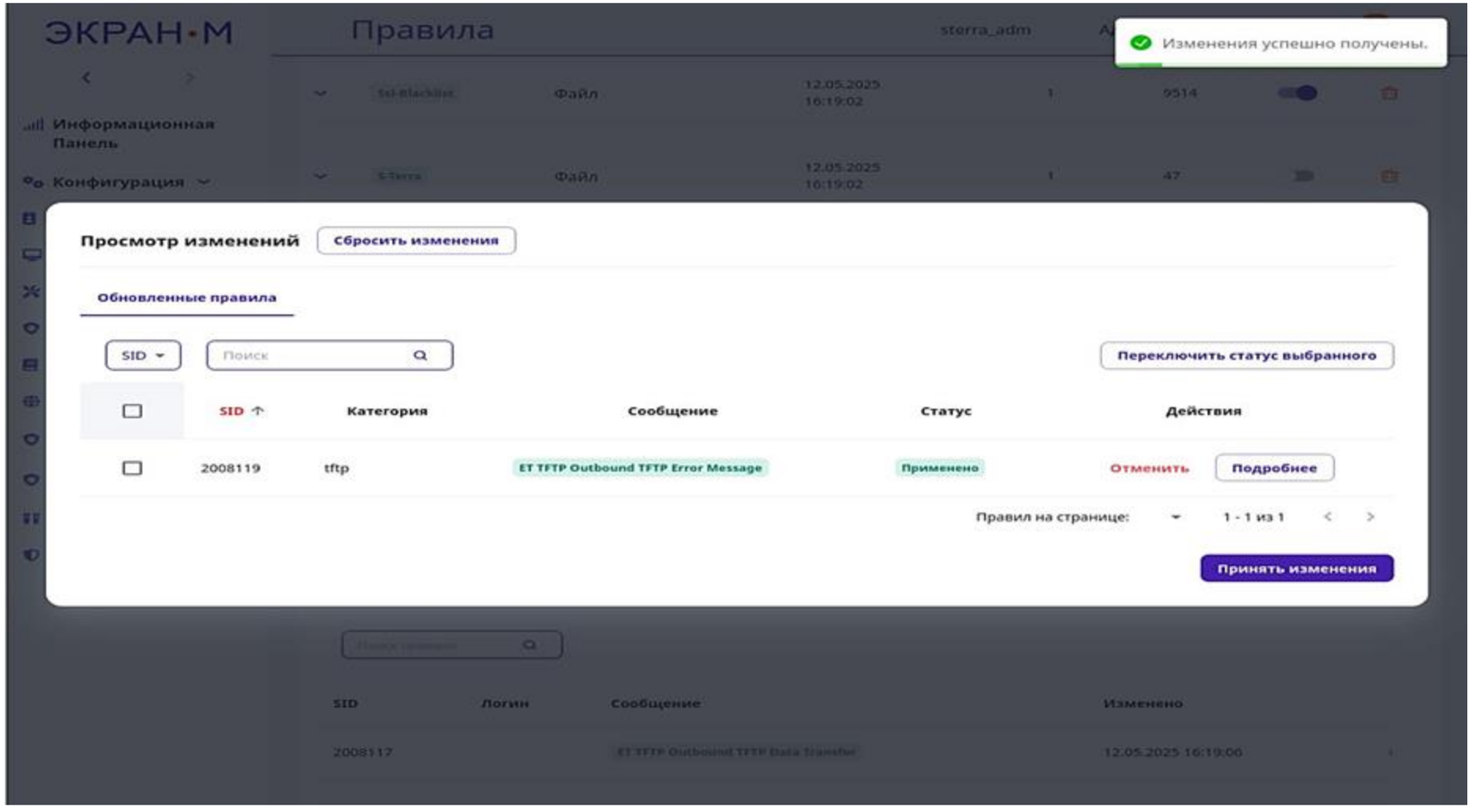
[Check Point]

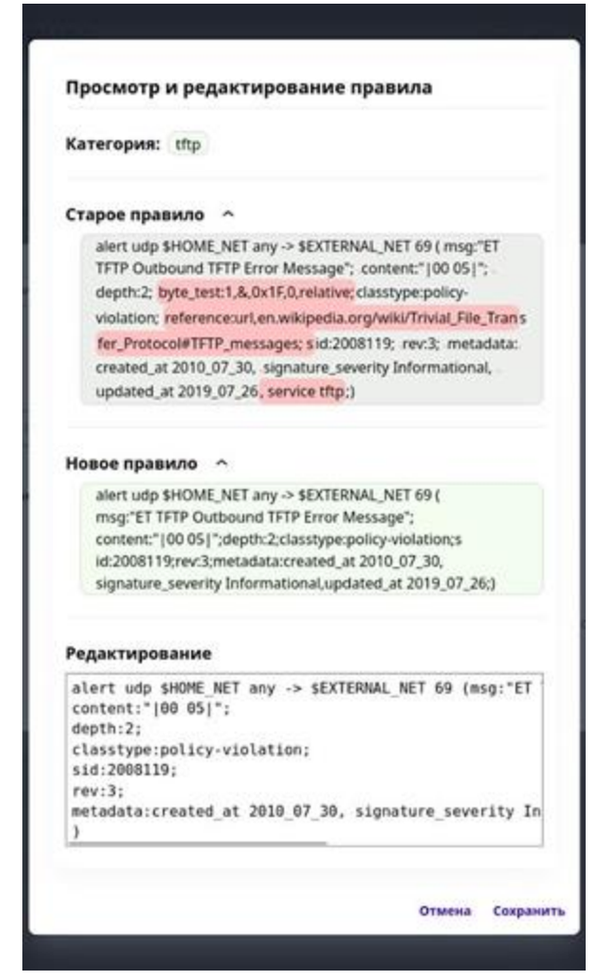
Перенос

[Экран-М]

АНАЛИЗ И ОТСЛЕЖИВАНИЕ ИЗМЕНЕНИЙ В КОНФИГУРАЦИИ

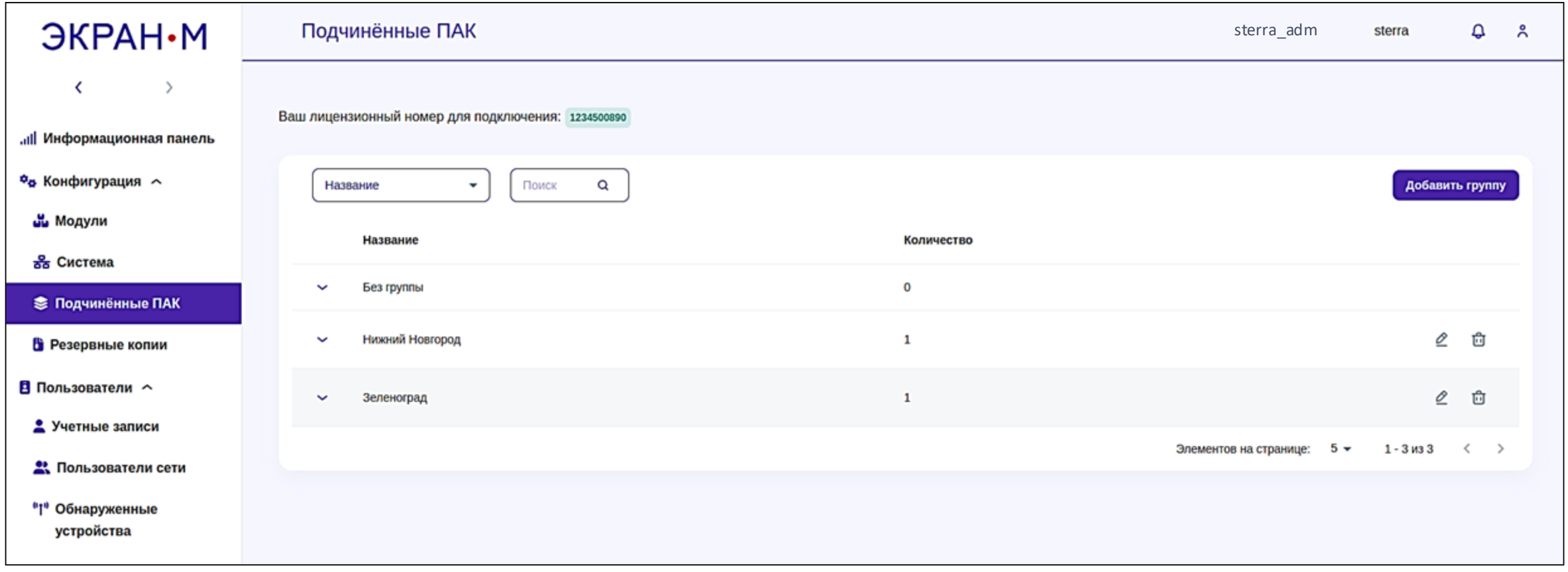
Сравнение правил (DIFF)





ГРУППОВОЕ УПРАВЛЕНИЕ ПОДЧИНЕННЫМИ МЕЖСЕТЕВЫМИ ЭКРАНАМИ

Контроль и управление из одного окна



РОЛЕВАЯ МОДЕЛЬ С-ТЕРРА ЭКРАН-М. СОЗДАНИЕ ПОЛЬЗОВАТЕЛЯ

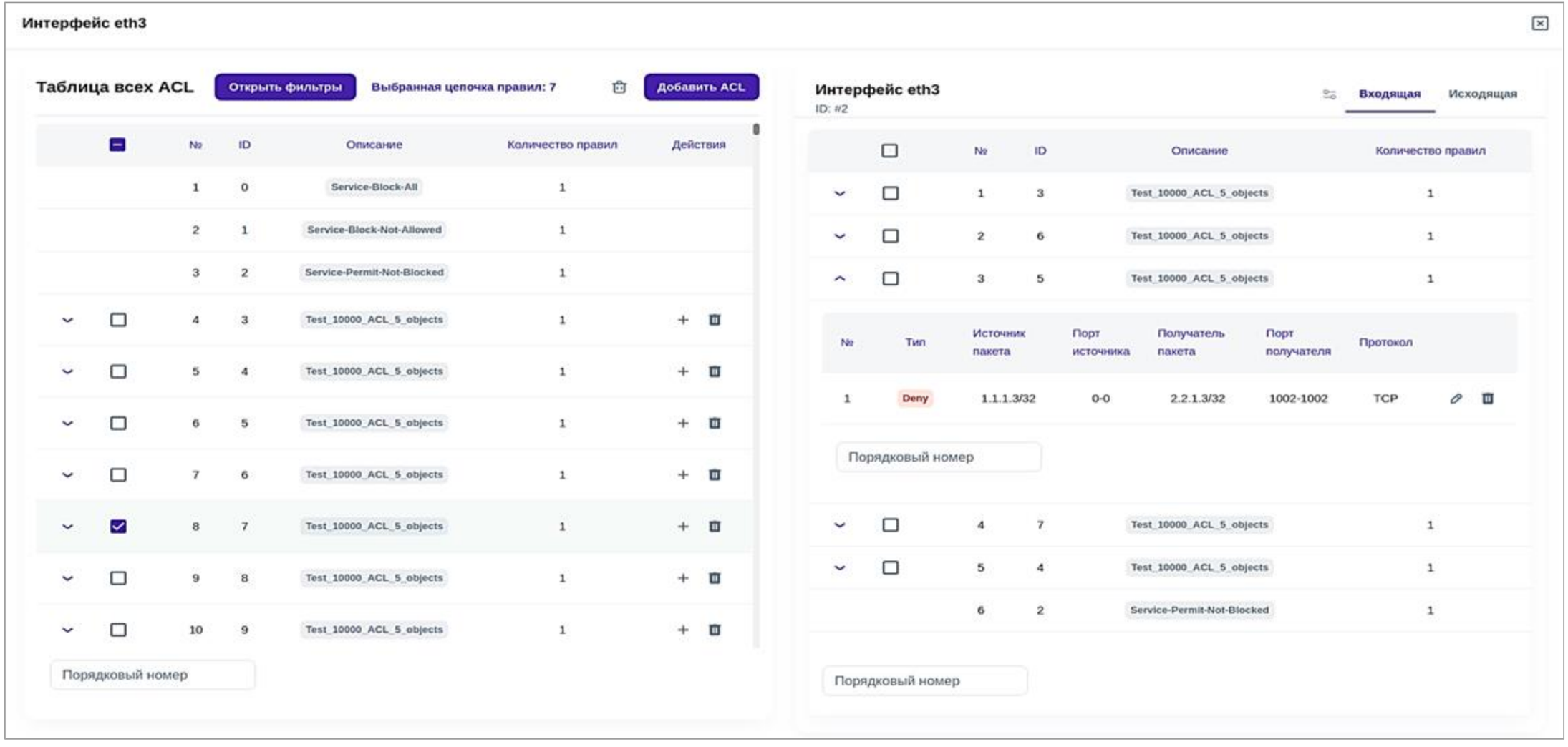
Экран-М обеспечивает возможность определения полномочий для пользователей ММЭ в пределах назначенных им ролей

РОЛЕВАЯ МОДЕЛЬ С-ТЕРРА ЭКРАН-М. НАСТРОЙКА РОЛЕЙ

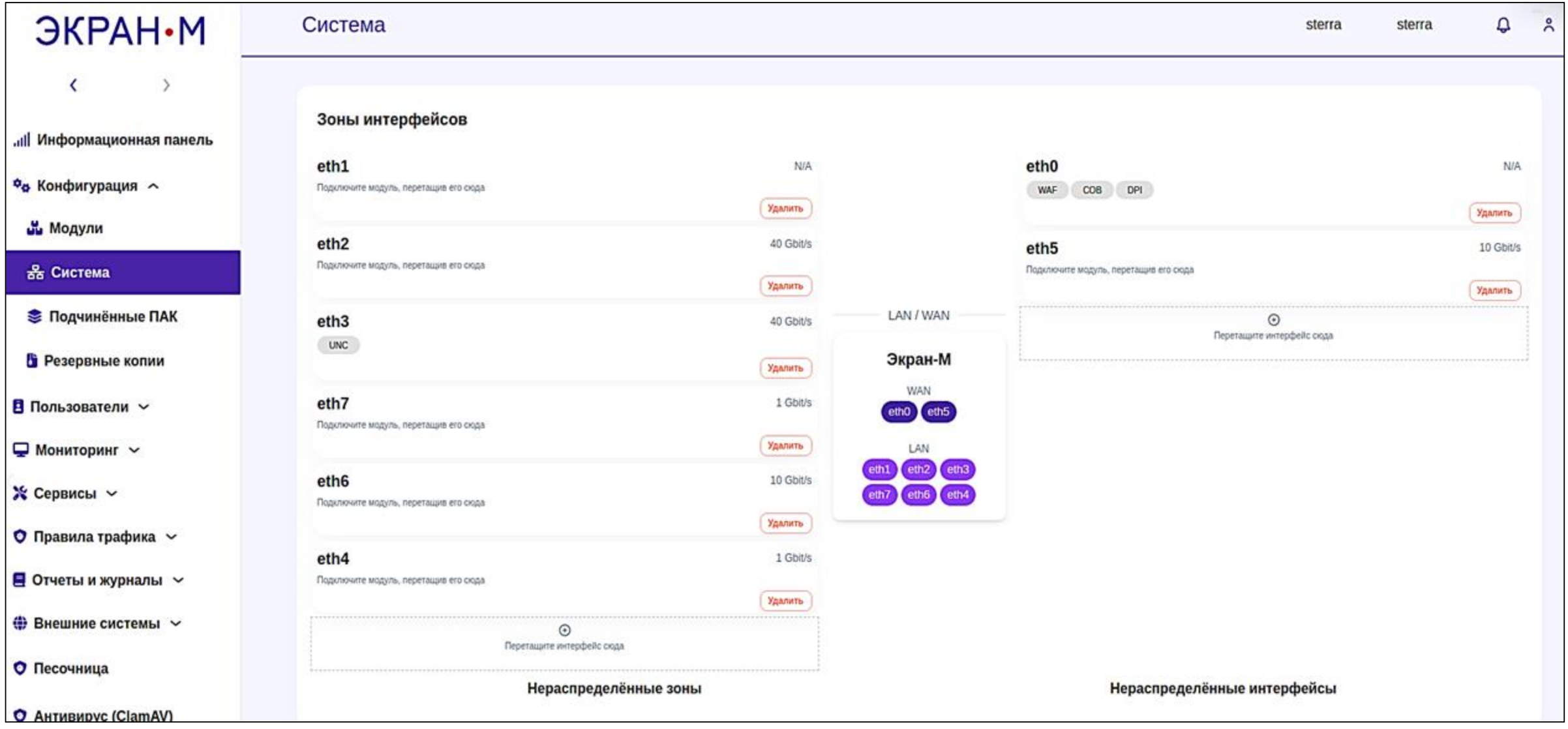
Экран-М обеспечивает возможность управления полномочиями для ролей в ММЭ

ПРОСТАЯ НАСТРОЙКА ACL — УПРАВЛЕНИЕ ДОСТУПОМ ЧЕРЕЗ DRAG&DROP

Настройка ACL без скриптов, консоли. Наглядно и удобно



ВИЗУАЛИЗАЦИЯ ЗОН И РЕЖИМОВ РАБОТЫ ИНТЕРФЕЙСОВ

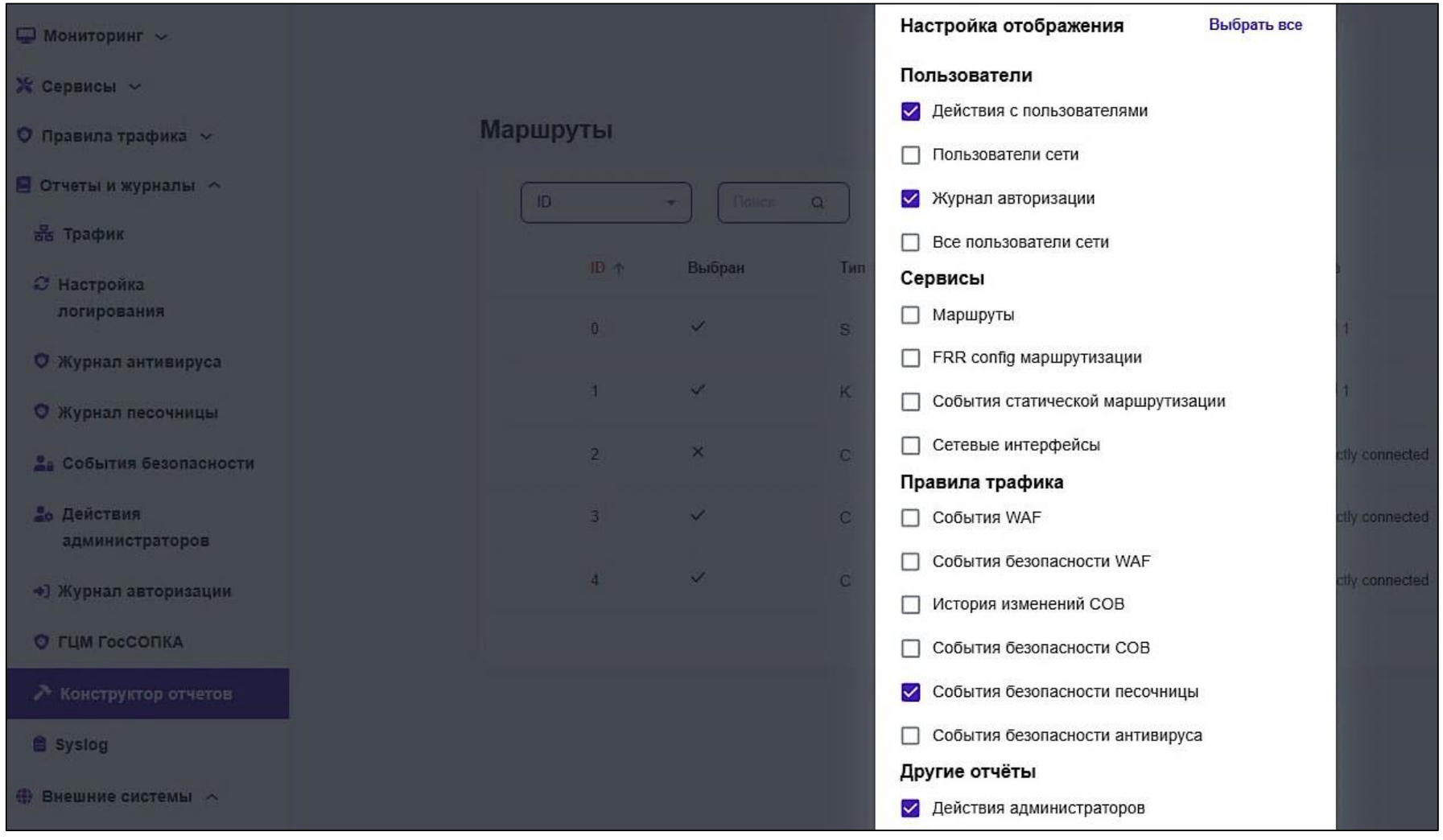


[События, отчёты и контроль]

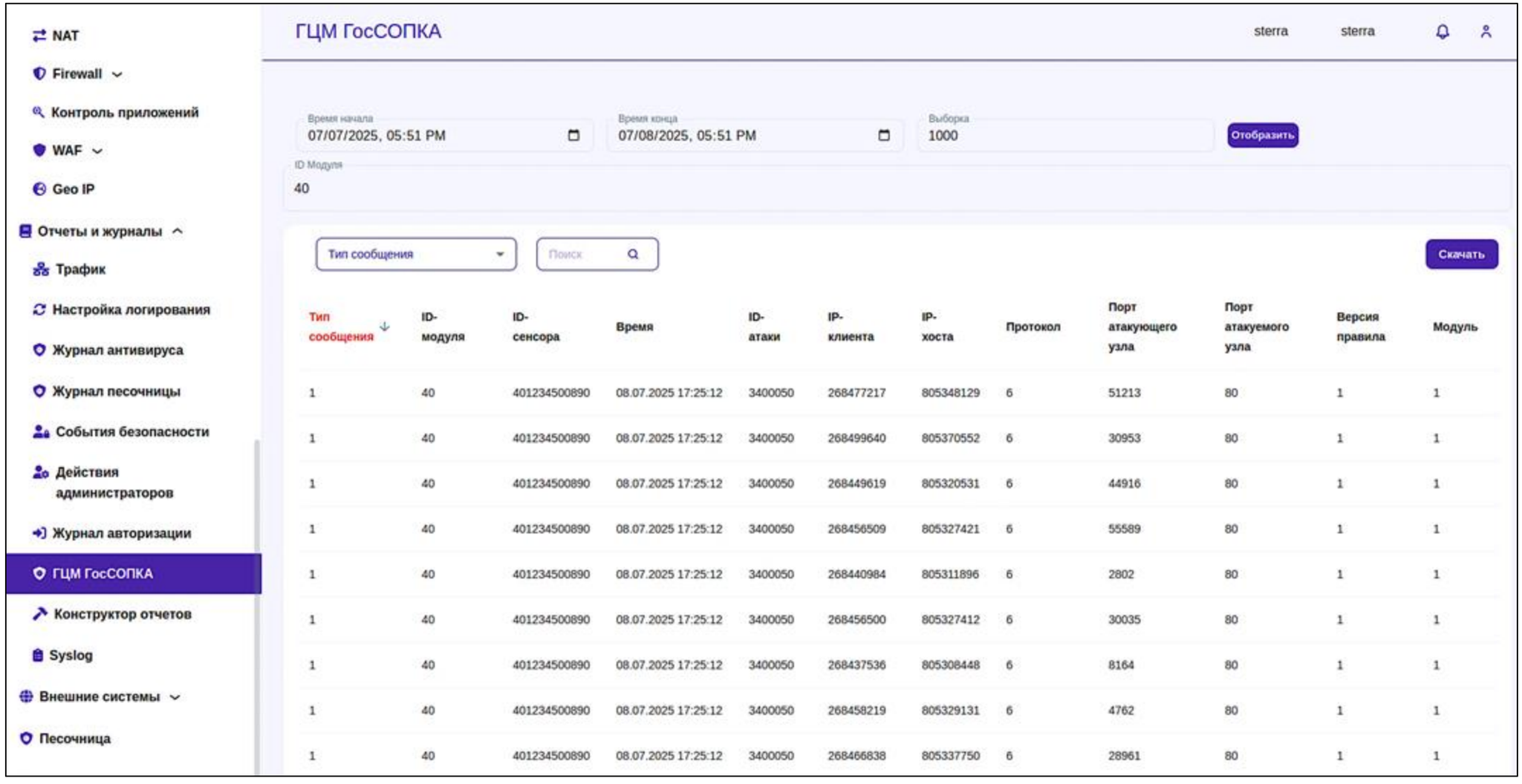
Всё, что нужно для анализа инцидентов и отчётности по безопасности

- Конструктор отчётов
  (создание настраиваемых отчётов по событиям, трафику и инцидентам)
- Подробное логирование событий безопасности
  (все действия фиксируются на устройстве для анализа и формирования отчётов)
- Совместимость с внешними системами
  (передача событий REST API)
- Гибкий экспорт событий безопасности
  (CSV, JSON)
- Поддержка стандартов экспортируемых форматов
  (включая выгрузку в формате ГЦМ для взаимодействия с ГосСОПКА)
- Поиск и фильтрация по событиям в интерфейсе
  (быстрый доступ к нужной информации)

КОНСТРУКТОР ОТЧЁТОВ. СОЗДАНИЕ НАСТРАИВАЕМЫХ ОТЧЁТОВ ПО СОБЫТИЯМ



ВЫГРУЗКА СОБЫТИЙ В ФОРМАТЕ ГЦМ ГОССОПКА



Тип сообщения	ID-модуля	ID-сенсора	Время	ID-атаки	IP-клиента	IP-хоста	Протокол	Порт атакующего узла	Порт атакуемого узла	Версия правила	Модуль
1	40	401234500890	08.07.2025 17:25:12	3400050	268477217	805348129	6	51213	80	1	1
1	40	401234500890	08.07.2025 17:25:12	3400050	268499640	805370552	6	30953	80	1	1
1	40	401234500890	08.07.2025 17:25:12	3400050	268449619	805320531	6	44916	80	1	1
1	40	401234500890	08.07.2025 17:25:12	3400050	268456509	805327421	6	55589	80	1	1
1	40	401234500890	08.07.2025 17:25:12	3400050	268440984	805311896	6	2802	80	1	1
1	40	401234500890	08.07.2025 17:25:12	3400050	268456500	805327412	6	30035	80	1	1
1	40	401234500890	08.07.2025 17:25:12	3400050	268437536	805308448	6	8164	80	1	1
1	40	401234500890	08.07.2025 17:25:12	3400050	268458219	805329131	6	4762	80	1	1
1	40	401234500890	08.07.2025 17:25:12	3400050	268466838	805337750	6	28961	80	1	1

Разработка нового релиза Экран-М с расширенным функционалом

[Экран-М новые релизы в разработке]

→→→

[Защита]

Многофункциональный межсетевой экран уровня сети вместе с ГОСТ-шифрованием

Расширенная функциональность

Сделаем на одном устройстве

- *NGFW*
- *WAF*
- *DPI*
- *IDS / IPS*
- *Sandbox*
- *ГОСТ VPN*

[Преимущества подхода]

- Многофункциональный межсетевой экран
- Поддержка ГОСТ-шифрования
- Экономия на закупках и обслуживании
- Упрощение архитектуры сети

С-ТЕРРА ЭКРАН-М. ПУТЬ РАЗВИТИЯ ПРОДУКТА С 2025 ГОДА

ЭКРАН·М ногофункциональный модульный межсетевой

Март

- Начло испытаний Экран-М 1.0 в Испытательной Лаборатории ФСТЭК

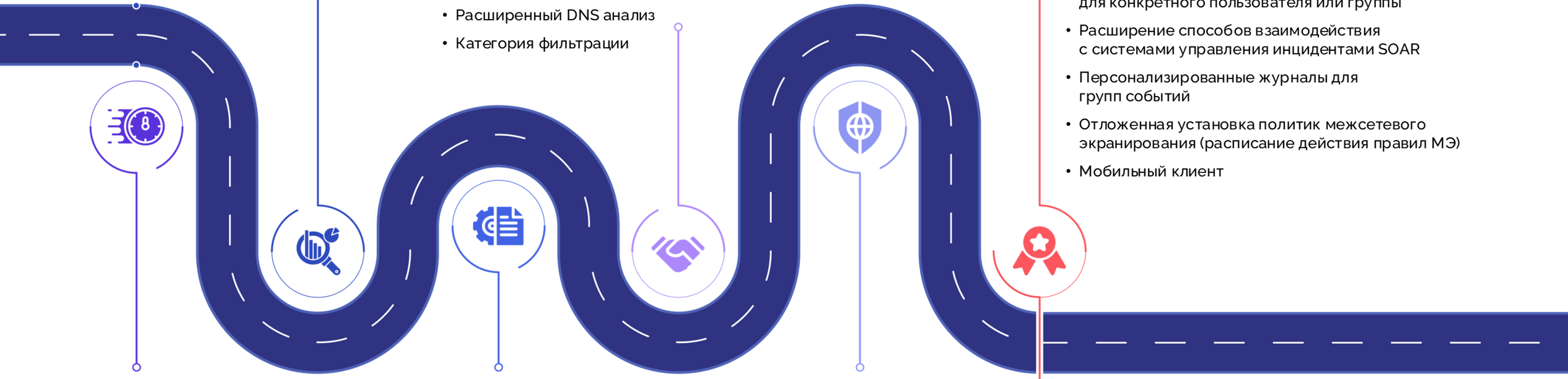
Июль

- Расширение линейки аппаратных платформ
- Управление трафиком на уровне пользователей
- Автоматизация реакций на инциденты через API
- Скрипты переноса
- Расписание действия правил МЭ
- Расширенный DNS анализ
- Категория фильтрации

Дальнейшее развитие продукта

Разработка и выпуск новых релизов Экран-М

- Расшифровка и инспекция трафика SSL/TLS путем подмены сертификата
- Реализация управления скоростью трафика для конкретного пользователя или группы
- Расширение способов взаимодействия с системами управления инцидентами SOAR
- Персонализированные журналы для групп событий
- Отложенная установка политик межсетевого экранирования (расписание действия правил МЭ)
- Мобильный клиент



Февраль

- SNMP мониторинг
- Увеличение производительности

Май

- PPPOE
- Реализация полной инспекции трафика SSL / TLS

Сентябрь

- Завершение сертификации Экран-М 1.0

- Поддержка передачи статистики по протоколу NetFlow во внешние системы
- Виртуальные контексты с раздельными ресурсами, таблицами маршрутизации и политиками фильтрации

К КОМУ ОБРАЩАТЬСЯ?

[Отдел по работе с партнёрами]

partner@s-terra.ru

Сотрудничество с С-Терра - развитие партнёрской сети и совместных инициатив

[Отдел по работе с клиентами]

sales@s-terra.ru

Коммерческие условия и приобретение продукции

[Отдел технического консалтинга]

presale@s-terra.ru

Технические консультации при выборе решения и в процессе пилотирования

[Отдел клиентского сервиса]

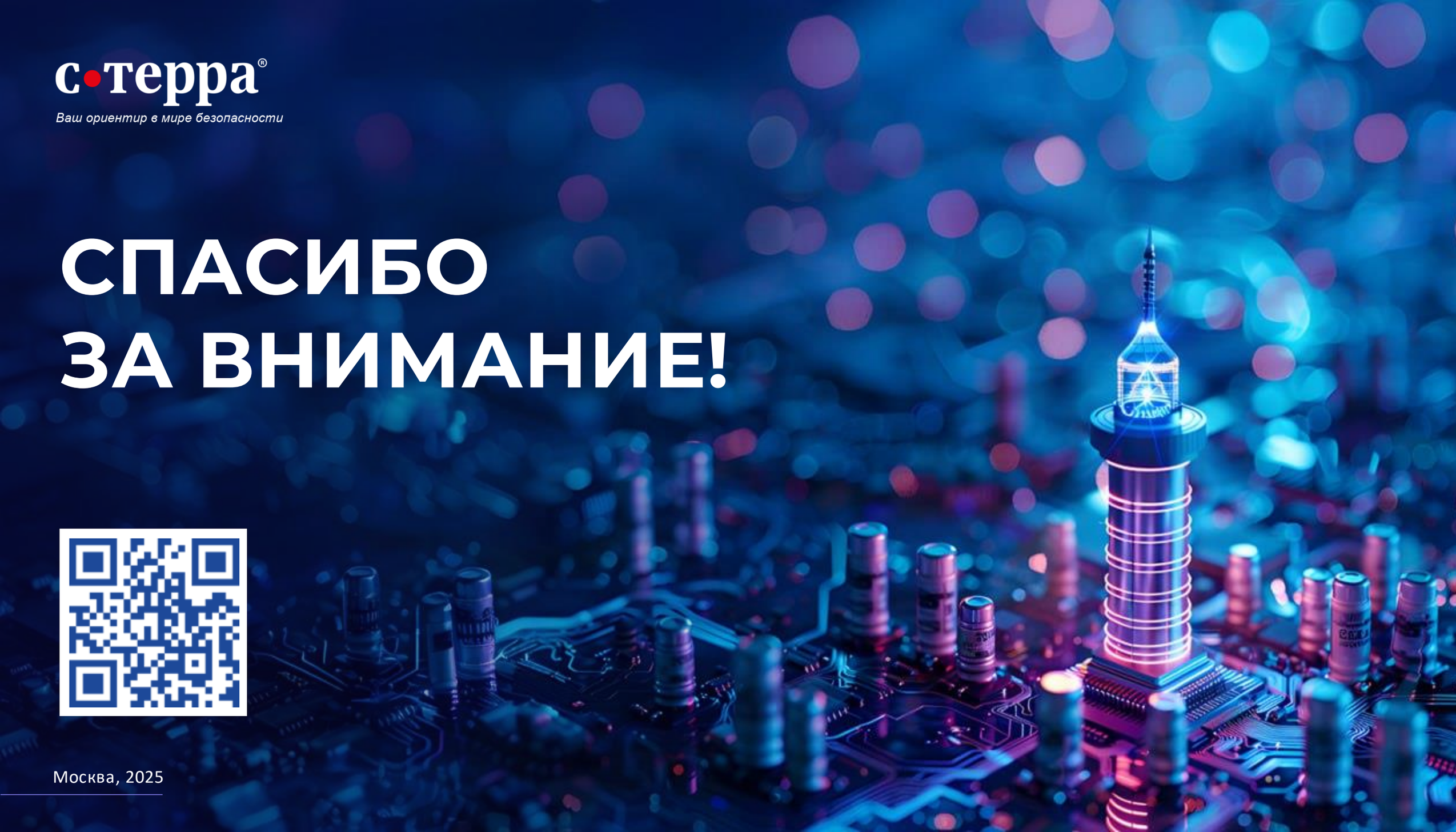
support@s-terra.ru

Техническая поддержка по приобретённым решениям и платформам

С•Терра®

Ваш ориентир в мире безопасности

СПАСИБО ЗА ВНИМАНИЕ!



Москва, 2025