

**с•терра®**

*Ваш ориентир в мире безопасности*

# Новинки в линейке С-Терра: обзор новых продуктов и дорожная карта развития на 2026–2027 гг.

Сергей Маненков

Руководитель разработки NGFW ООО «С-Терра СиЭсПи»

Минск, 2026

## Описание

---

ПП«Шлюз BelVPN 4.7» функционирует как в виртуальной среде – наиболее популярных гипервизорах (VMware ESXi, Citrix XenServer, KVM и др.), так и на любых аппаратных платформах поддерживающих ОС Linux

## Сертификация

---

- Соответствует требованиям ТР 2013/027/ВУ (для уровня безопасности 1)

## Основные характеристики

---

- Количество одновременно поддерживаемых VPN туннелей 10/50/1000/неограниченное количество
- Производительность до 10 Гбит/с
- Защита трафика IPsec
- Cisco-like интерфейс

## Описание

КПА «Шлюз BeVPN 4.7» предназначен для защиты информации (сетевое трафика), поступающей в информационную систему и/или выходящей из нее, а также для защиты информационной системы посредством фильтрации потока информации.

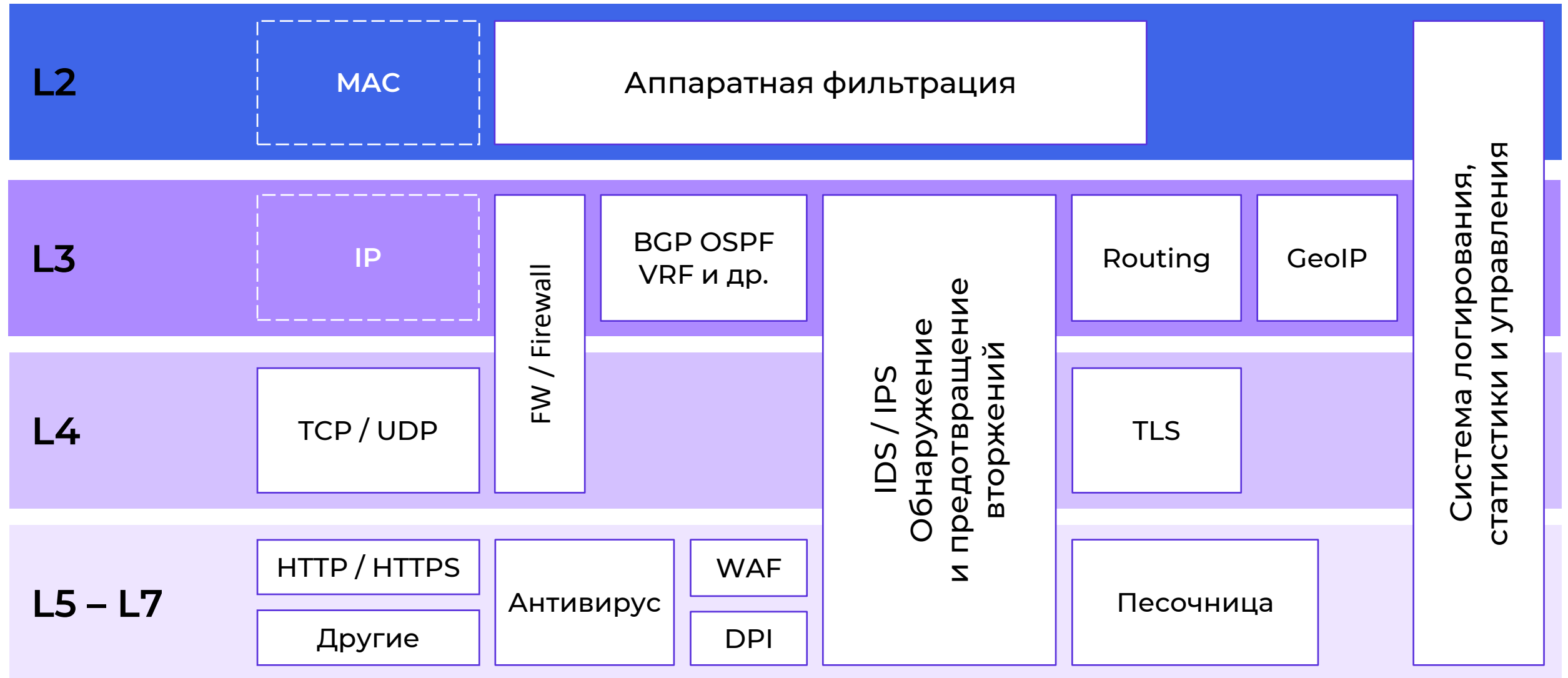
## Сертификация

- Соответствует требованиям ТР 2013/027/ВУ (для уровня безопасности 3)

## Основные характеристики

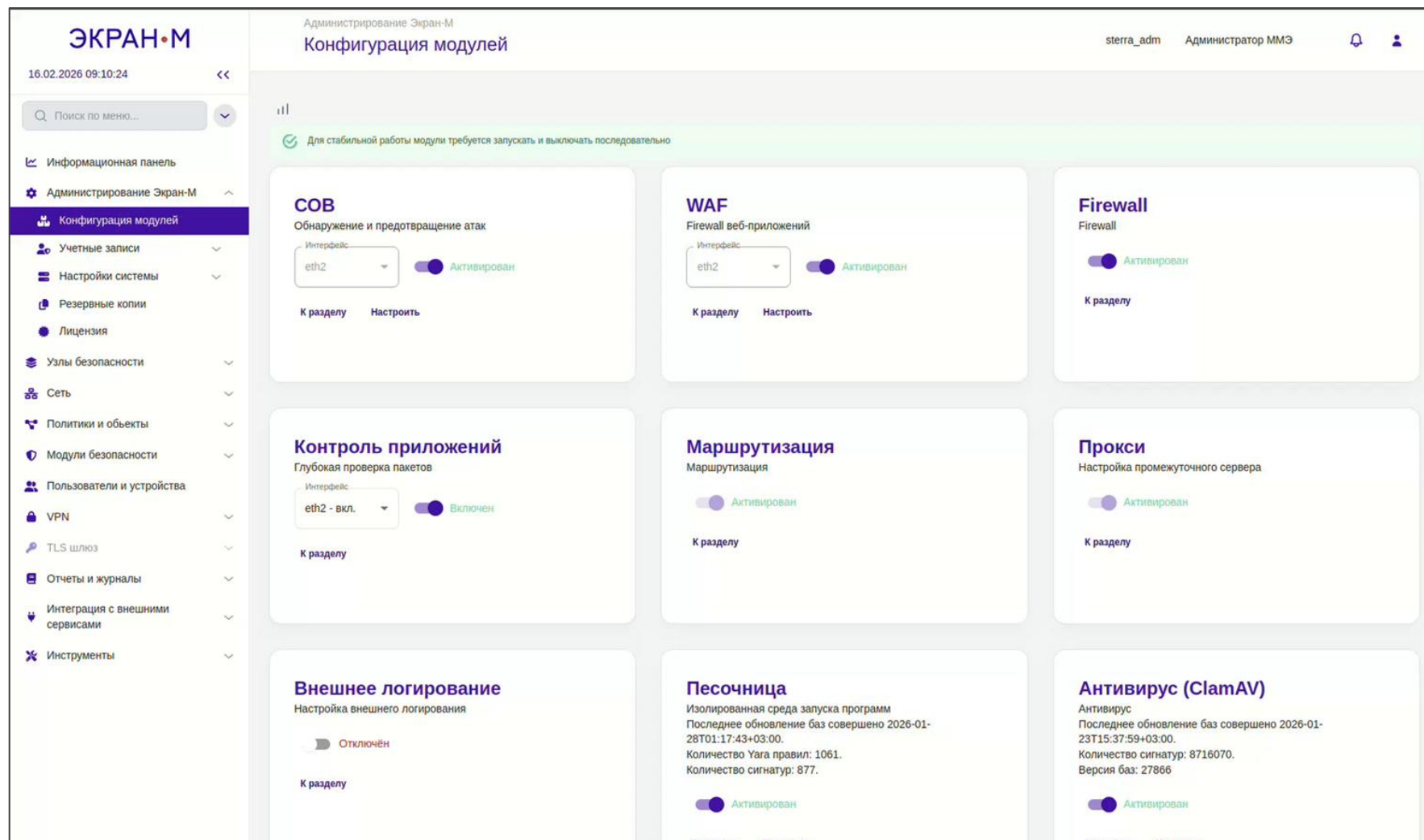
- Количество одновременно поддерживаемых VPN туннелей 10/50/1000/неограниченное количество
- Производительность до 15 Гбит/с
- Защита трафика IPsec
- Cisco-like интерфейс

АРХИТЕКТУРА С-ТЕРРА ЭКРАН-М



# РАБОТА С МОДУЛЯМИ ЭКРАН-М

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



## С-Терра Экран-М 8000



## С-Терра Экран-М 7000



# 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



# ЧТО ПОЛУЧАЕТ РЫНОК

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 <b>96</b> Гбит/с	До <b>38</b> Гбит/с	100 тыс. ACL
FW + IDS / IPS	До <b>24</b> Гбит/с	До <b>12</b> Гбит/с	100 тыс. ACL + 40 тыс.
FW + IDS / IPS + WAF	До <b>10</b> Гбит/с	До <b>6</b> Гбит/с	100 тыс. ACL + 60 тыс.
FW + IDS / IPS + DPI + WAF + Антивирус + Песочница	До <b>5</b> Гбит/с	До <b>3.5</b> Гбит/с	100 тыс. ACL + 150 тыс.

## 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

Правила

sterra sterra

⚠ Будьте осторожны при самостоятельном редактировании правил, некорректные правила могут нарушить работу системы!

Правила | Настройка

Источники ^

Отключение правила по регулярному выражению:   Включить  Расширенный редактор

Название	URI	Последнее обновление	Логин	Категории	Правила
444444	Файл	25.07.2025 12:30:19		2	26
Anomaly	Файл	25.07.2025 12:30:19		1	16
Categories-URL	Файл	25.07.2025 12:30:19		1	8
Dangerous-hyperlink	Файл	25.07.2025 12:30:19		1	13923
Info	Файл	25.07.2025 12:30:19		1	1553

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

<> Редактор регулярных выражений ? ✔ Корректное

Регулярное выражение  
\*sid:3400139:

Введите регулярное выражение (например: \*[a-z0-9\_]{3,16}\$)

Тестовая строка  
\*sid:3400139:

Введите строку для проверки регулярного выражения

Результаты:  
Найдено совпадений: 1

Справка по регулярным выражениям ▾

Включить

# АНАЛИЗ И ОТСЛЕЖИВАНИЕ ИЗМЕНЕНИЙ В КОНФИГУРАЦИИ

## Сравнение правил (DIFF)

ЭКРАН.М Правила sterra\_admin

Изменения успешно получены.

Имя	Тип	Дата/Время	Статус	Действия
Ssl-Blacklist	Файл	12.05.2025 16:19:02	1	9514
S-Terra	Файл	12.05.2025 16:19:02	1	47

**Просмотр изменений** Сбросить изменения

Обновленные правила

SID

Перекл. статус

Выбор	SID	Категория	Сообщение	Статус	Действия
<input type="checkbox"/>	2008119	tftp	ET TFTP Outbound TFTP Error Message	Применено	Отменить Подробнее

Правил на странице: 1 - 1 из 1

Принять изменения

SID	Логин	Сообщение	Изменено
2008117		ET TFTP Outbound TFTP Data Transfer	12.05.2025 16:19:06

**Просмотр и редактирование правила**

Категория: tftp

**Старое правило**

```
alert udp $HOME_NET any -> $EXTERNAL_NET 69 ( msg:"ET TFTP Outbound TFTP Error Message"; content:"|00 05|"; depth:2; byte_test:1,&0x1F0,relative; classtype:policy-violation; reference:url,en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol#TFTP_messages; sid:2008119; rev:3; metadata: created_at 2010_07_30, signature_severity Informational, updated_at 2019_07_26, service tftp;)
```

**Новое правило**

```
alert udp $HOME_NET any -> $EXTERNAL_NET 69 ( msg:"ET TFTP Outbound TFTP Error Message"; content:"|00 05|"; depth:2; classtype:policy-violation; id:2008119; rev:3; metadata: created_at 2010_07_30, signature_severity Informational, updated_at 2019_07_26;)
```

**Редактирование**

```
alert udp $HOME_NET any -> $EXTERNAL_NET 69 ( msg:"ET content:"|00 05|"; depth:2; classtype:policy-violation; sid:2008119; rev:3; metadata: created_at 2010_07_30, signature_severity In )
```

Отмена Сохранить

**ЭКРАН.М**

06.11.2025 15:04:12

Информационная панель

- Конфигурация
- Пользователи
- Мониторинг
- Сервисы
- Правила трафика
- URL фильтрация
- СОВ
- Правила
- Статус
- Настройки
- NAT
- Firewall
- Контроль приложений
- WAF
- Geo IP
- Отчеты и журналы
- Внешние системы
- Песочница

## Правила

srmkv root

⚠ Будьте осторожны при самостоятельном редактировании правил, некорректные правила могут нарушить работу системы!

### Источники

Regex редактор
IDS
Отключен
Применить правила
Добавить

Активных правил: 30958    Всего правил: 30974

Название ↑	URI	Последнее обновление	Логин	Категории	Активные правила	Правила	
Unwanted-elements	Файл	2025-11-06T14:55:50.941487+03:00		9	105	105	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Источников на странице: 5    11 - 11 из 11

### Классы правил

Добавить класс

Название ↑	Описание	Приоритет
------------	----------	-----------

# ПЕСОЧНИЦА

Песочница получает объекты из различных источников, выполняет проверку и выносит вердикт о вредоносности ПО

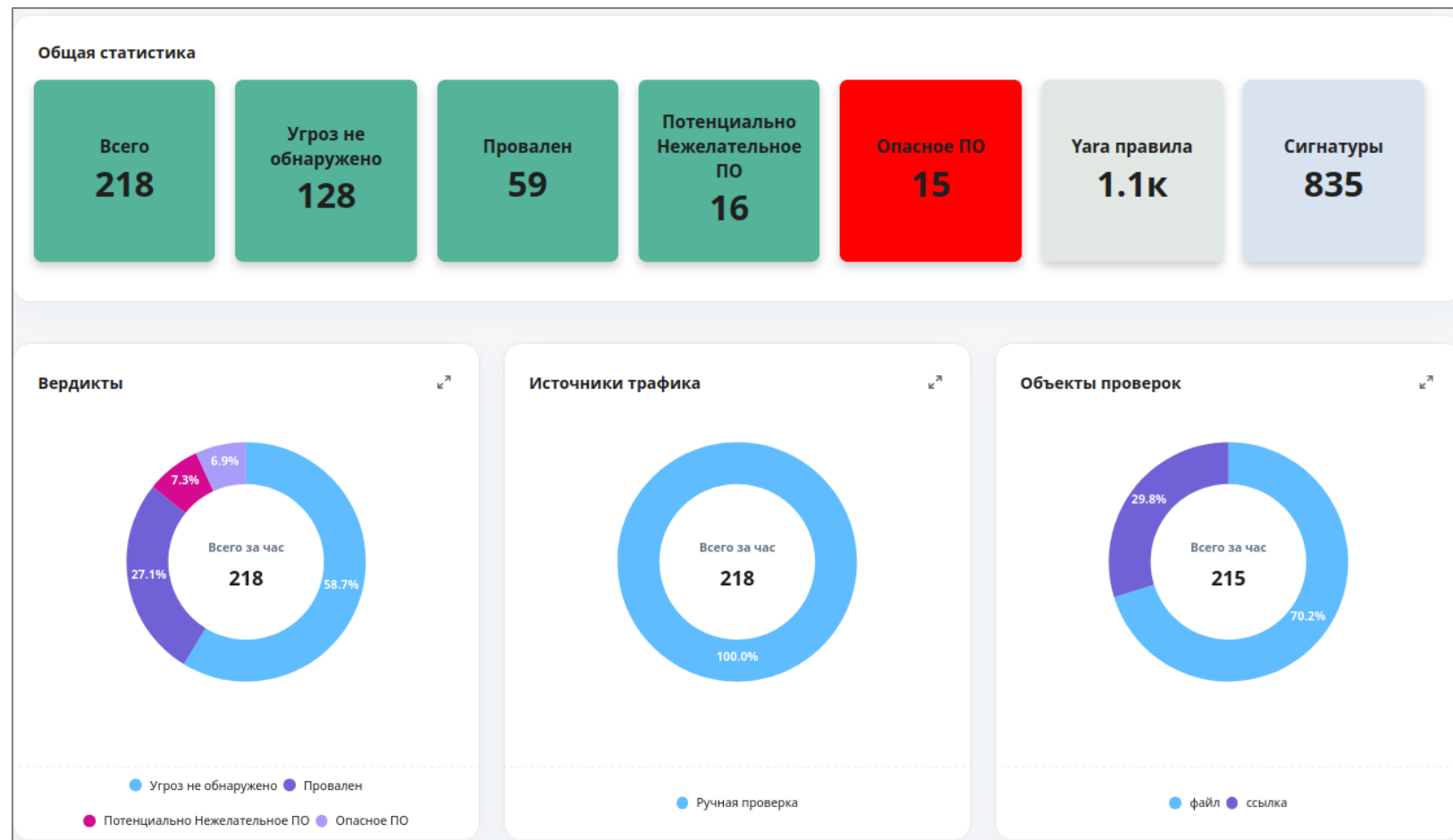


## РАБОТА ПЕСОЧНИЦЫ

- Возможность ручной загрузки объектов с настройкой параметров проверки
- Просмотр журнала анализируемых объектов

Статус проверки	Решение о блокировке	Дата создания ↓	Задание	Вердикт	Источник проверки	Уровень опасности
✓	⚠	2026-03-03T14:08:16+03:00	31ba55e38f0e36371cd3.exe	Опасное ПО	Ручная проверка	10.0 из 10
✓	✓	2026-03-02T23:46:17+03:00	qr ТГ.jpeg	Угроз не обнаружено	Ручная проверка	3.2 из 10
✓	✓	2026-03-02T23:46:12+03:00	qr обычный.png	Угроз не обнаружено	Ручная проверка	2.2 из 10
✓	⚠	2026-03-02T23:36:50+03:00	qr doc.docx	Потенциально Нежелательное ПО	Ручная проверка	5.7 из 10
✓	✓	2026-03-02T23:36:41+03:00	qr ТГ.jpeg	Угроз не обнаружено	Ручная проверка	3.2 из 10

# РАБОТА ПЕСОЧНИЦЫ



Временная статистика событий

Гибкая настройка анализа объектов из сетевого трафика

Точечная проверка пользователей или хостов по IP-адресам

# ПОДРОБНЫЙ АНАЛИЗ В ПЕСОЧНИЦЕ

**О задании**
Добавить сигнатуру в антивирус

Общая информация
Результаты анализа
Анализ угроз

**Решение о блокировке**

⚠ Зablokirовать

**Вердикт**

Опасное ПО

**Уровень опасности**

10.0 из 10

**Статус проверки**

✓ Завершено

<b>Источник для проверки</b>	🔒 Ручная проверка
<b>Время создания сессии</b>	2026-03-01T23:07:48+03:00
<b>Время окончания сессии</b>	2026-03-01T23:08:25+03:00
<b>Время начала анализа</b>	2026-03-01T23:07:48+03:00
<b>Время завершения анализа</b>	2026-03-01T23:08:17+03:00
<b>Продолжительность анализа</b>	29 сек
<b>Роль</b>	Администратор ММЭ
<b>Пользователь</b>	sterra_adm
<b>Режим проверки</b>	Поведенческий анализ

**Типы угроз** ▾

**Файл**

**31ba55e38f0e36371cd3.exe**

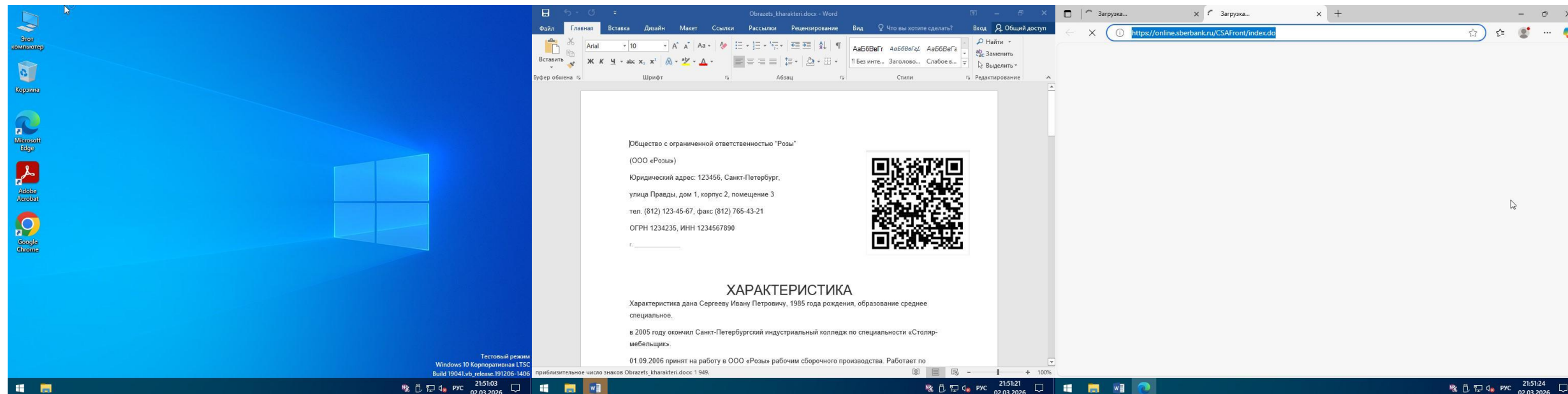
Тип файла	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MIME-тип	application/vnd.microsoft.portable-executable
Формат файла	exe
Размер	213572 bytes
MD5	c9539d1b44440b83c2673361e7225e59
SHA1	1f1e86bb47fa1ef37a2c5dd796e5810b9082eb51
SHA256	31ba55e38f0e36371cd39c8d117617e47261691def9f998262dfe618fca8557

**Загрузка файлов:** Загрузить pcap Загрузить screenshots


- Выявленная сетевая активность
- Возможность загрузить pcap файлы и скриншоты анализа
- Создание антивирусных сигнатур на основе вердикта Песочницы
- Обнаруженные сигнатуры Песочницы с маркерами, описывающие поведение файла в изолированной среде

# ПЕСОЧНИЦА - ПРОВЕРКА ССЫЛОК ИЗ QR-КОДОВ

Песочница обнаруживает QR - коды на изображениях или документах, извлекает содержащиеся в них ссылки и проверяет их



**Настройки**

 Защита зашифрованных файлов работает только в режиме блокировки

Режим работы

Обнаружение

Защита зашифрованных файлов

Фильтры проверки трафика

Проверять все

Проверять конкретных клиентов

Проверять все из конкретной подсети

**Сохранить настройки**

- Блокировка зашифрованных файлов
- Точечная проверка пользователей или хостов по IP адресам
- Анализ объектов в двух режимах работы (Блокировка / Ожидание)

**Поддержка  
аппаратных платформ**

Поддержка работы  
на средних и младших  
платформах ЭКРАН-М

**Поддержка  
отечественных ОС**

Установка на Astra Linux,  
поддержка виртуальных  
сред с Astra Linux

**Динамический обход  
защитных механизмов**

Раскрытие техник  
анти-песочниц  
во время анализа

# ГРУППИРОВКА СОБЫТИЙ РАЗЛИЧНОГО ТИПА ПО ГРУППАМ ПОЛЬЗОВАТЕЛЕЙ

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

### Настройка отображения событий безопасности

Роль:  
sterra

#### События администрирования

Действия администраторов:  Регистрировать события  Уведомлять о событиях

#### События обнаружения компьютерных атак

События безопасности COB:  Регистрировать события  Уведомлять о событиях

#### События сбоев

События сбоев Экран-М:  Регистрировать события  Уведомлять о событиях

#### События обнаружения вредоносного ПО

События безопасности песочницы:  Регистрировать события  Уведомлять о событиях

События безопасности антивируса:  Регистрировать события  Уведомлять о событиях



## Больше, чем вы ждёте

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

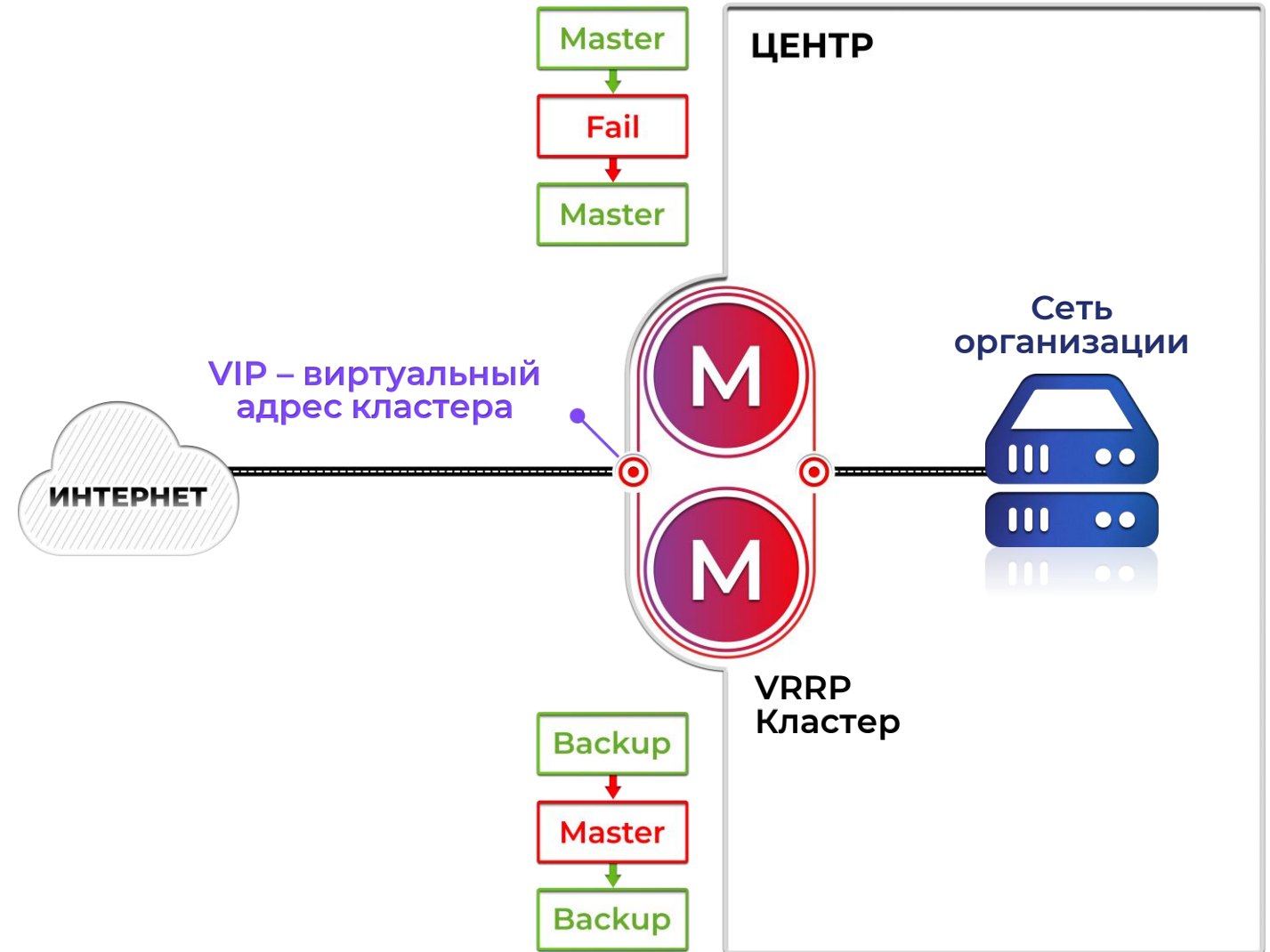
- NAT / PAT  
*(трансляция сетевых адресов и портов)*
- VLAN  
*(802.1Q)*
- VxLAN  
*(Virtual Extensible LAN – виртуализация сети)*
- IPv6  
*(NAT, маршрутизация, правила МЭ)*
- SPAN  
*(порт зеркалирования)*
- Статическая и динамическая маршрутизация  
*(OSPF, BGP)*
- LACP  
*(агрегация каналов)*
-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

## КЛАСТЕР ЭКРАН-М

Отказоустойчивость на базе протокола VRRPv3

### Типы отказов

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

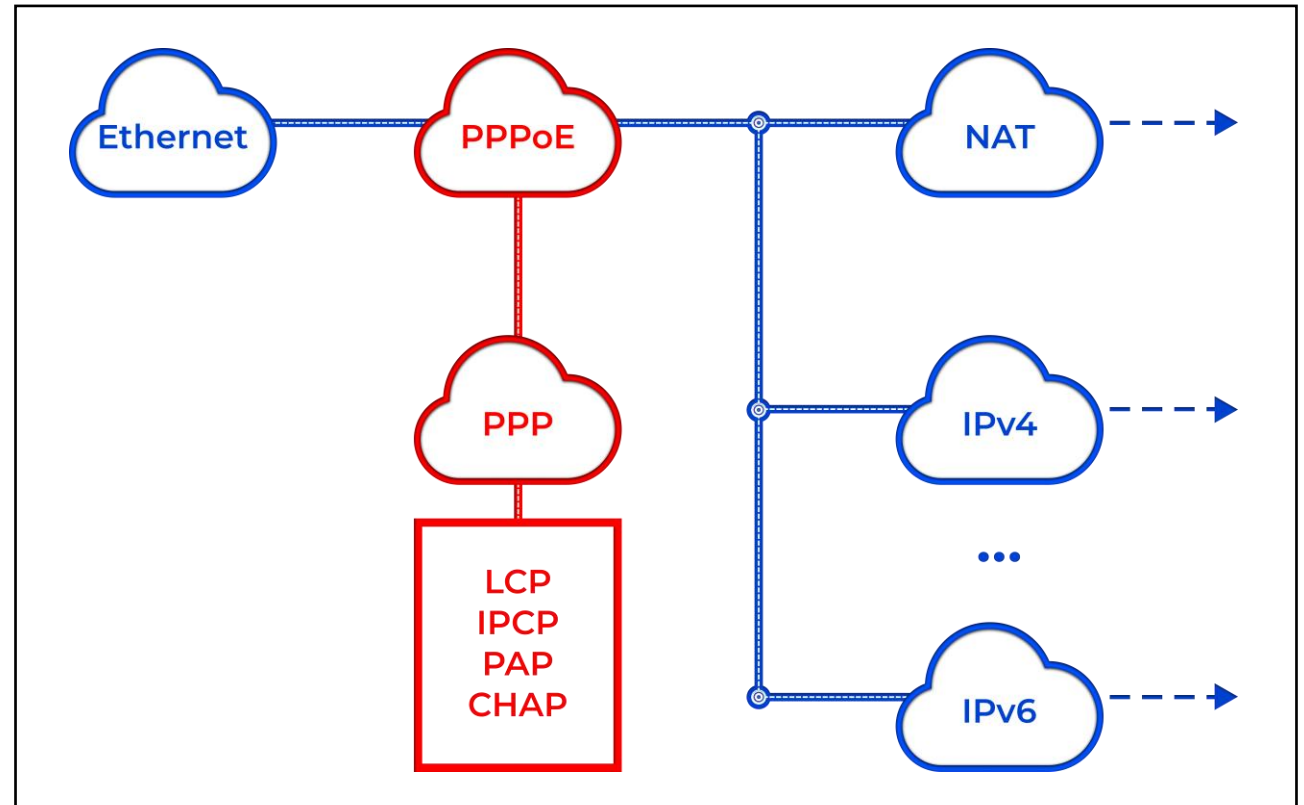


# ПОДДЕРЖКА СОЕДИНЕНИЙ PPPOE

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)
    
```

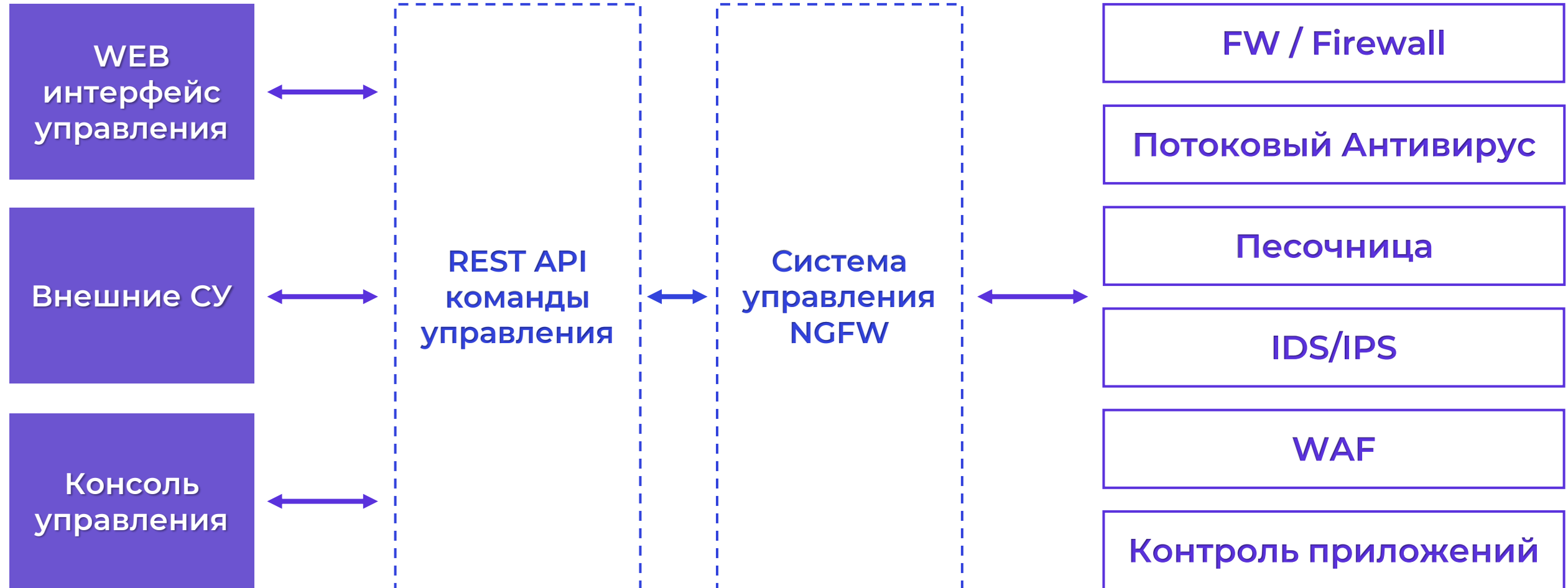


## Управление и эксплуатация

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  
*(управление доступом через DRAG&DROP)*
- Групповое управление подчиненными межсетевыми экранами  
*(централизованное администрирование нескольких устройств из одного интерфейса)*

## Единая система управления



# ОТКРЫТЫЙ REST API — АВТОМАТИЗАЦИЯ И КОНТРОЛЬ

Открытый интерфейс для подключения к вашей инфраструктуре

OS		^
GET	/api/v1/os/disk	∨
GET	/api/v1/version	∨
GET	/api/v1/os/memory	∨
GET	/api/v1/os/cpu	∨
VPP		^
GET	/api/v1/vpp/interfaces	∨
ACL		^
POST	/api/v1/vpp/acl/interfaces/rules	∨
DELETE	/api/v1/vpp/acl/interfaces/rules	∨
POST	/api/v1/vpp/acl/rules	∨
DELETE	/api/v1/vpp/acl/rules	∨

FRR		^
GET	/api/v1/frr/ospf	∨
POST	/api/v1/frr/ospf	∨
DELETE	/api/v1/frr/ospf	∨
BGP		^
POST	/api/v1/frr/bgp	∨
POST	/api/v1/frr/bgp/neighbors	∨
DELETE	/api/v1/frr/bgp/neighbors	∨
EIRGP		^
POST	/api/v1/frr/eigrp	∨
GET	/api/v1/frr/eigrp	∨
POST	/api/v1/frr/eigrp/neighbor	∨
DELETE	/api/v1/frr/eigrp/neighbor	∨

# ГРУППОВОЕ УПРАВЛЕНИЕ ПОДЧИНЕННЫМИ МЕЖСЕТЕВЫМИ ЭКРАНАМИ

Контроль и управление из одного окна

**ЭКРАН.М**

< >

- Информационная панель
- Конфигурация ^
- Модули
- Система
- Подчинённые ПАК
- Резервные копии
- Пользователи ^
- Учетные записи
- Пользователи сети
- Обнаруженные устройства

## Подчинённые ПАК

sterra sterra 🔔 👤

Ваш лицензионный номер для подключения: 1234500890

Название ▼

Поиск 🔍

Добавить группу

Название	Количество	
▼ Без группы	0	
▼ Нижний Новгород	1	✎ 🗑️
▼ Зеленоград	1	✎ 🗑️

Элементов на странице: 5 1 - 3 из 3 < >

# РОЛЕВАЯ МОДЕЛЬ С-ТЕРРА ЭКРАН-М. НАСТРОЙКА РОЛЕЙ

Экран-М обеспечивает возможность управления полномочиями для ролей в ММЭ

**Настройка ролей**

Редактировать  Создать

Роль: Администратор безопасности

Раздел	Чтение	Запись	Изменение	Удаление
Информационная панель	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Пользователи и устройства	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Администрирование Экран-М - Конфигурация модулей	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Администрирование Экран-М - Учетные записи - Администраторы	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Администрирование Экран-М - Учетные записи - Активные сессии	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Администрирование Экран-М - Учетные записи - Сертификаты - TLS-сертификаты	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Администрирование Экран-М - Учетные записи - Сертификаты - SSH	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Администрирование Экран-М - Настройки системы - Система	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Администрирование Экран-М - Настройки системы - SMTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Администрирование Экран-М - Настройки системы - SNMP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Администрирование Экран-М - Настройки системы - Внешнее логирование	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Выход

**Преднастроенные роли по требованиям ММЭУС**

**Гибкая настройка привилегий**

# ВИЗУАЛИЗАЦИЯ ЗОН И РЕЖИМОВ РАБОТЫ ИНТЕРФЕЙСОВ

**ЭКРАН•М**

Информационная панель

Конфигурация

Модули

**Система**

Подчинённые ПАК

Резервные копии

Пользователи

Мониторинг

Сервисы

Правила трафика

Отчеты и журналы

Внешние системы

Песочница

Антивирус (ClamAV)

sterra sterra

## Система

### Зоны интерфейсов

<b>eth1</b>	N/A	Удалить
<b>eth2</b>	40 Gbit/s	Удалить
<b>eth3</b>	40 Gbit/s	Удалить
<b>eth7</b>	1 Gbit/s	Удалить
<b>eth6</b>	10 Gbit/s	Удалить
<b>eth4</b>	1 Gbit/s	Удалить

Перетащите интерфейс сюда

**Нераспределённые зоны**

LAN / WAN

**Экран-М**

WAN

eth0 eth5

LAN

eth1 eth2 eth3

eth7 eth6 eth4

**eth0** N/A

WAF COB DPI

Удалить

**eth5** 10 Gbit/s

Удалить

Перетащите интерфейс сюда

**Нераспределённые интерфейсы**

## 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 таблиц Запрос 1000 эл-ов. За последний месяц

Таблицы | Пересечения | Условия | Группировка | Дополнительно | Имена полей

### Модули

- COB
- Антивирус
- Песочница
- Прокси
- Syslog
- WAF
- Действия администраторов

### Доступные поля

Выбрать все

- Антивирус ▾
- Прокси ▲
- Идентификатор
- Временная метка (эпоха)
- Временная метка (ISO)
- Пользователь
- User Agent
- Код ответа
- Хост
- MAC адрес
- HTTP метод

> <

### Выбранные поля

Выбрать все

- COB ▲
- Идентификатор
- Сигнатура
- ID сигнатуры
- Тип события
- Действие
- IP источника
- IP назначения
- Категория
- Категория серьезности
- Название сервиса

Сохранить Отменить

# ВЫГРУЗКА СОБЫТИЙ В ФОРМАТЕ ГЦМ ГОССОПКА

- NAT
- 🛡️ Firewall ▾
- 🔍 Контроль приложений
- 🛡️ WAF ▾
- 🌐 Geo IP
- 📄 Отчеты и журналы ^
- 📶 Трафик
- ⚙️ Настройка логирования
- 📖 Журнал антивируса
- 📖 Журнал песочницы
- 👤 События безопасности
- 👤 Действия администраторов
- ➔ Журнал авторизации
- 🛡️ ГЦМ ГосСОПКА
- 🔗 Конструктор отчетов
- 📄 Syslog
- 🌐 Внешние системы ▾
- 📖 Песочница

## ГЦМ ГосСОПКА

sterra
sterra
🔔
👤

Время начала  
07/07/2025, 05:51 PM

Время конца  
07/08/2025, 05:51 PM

Выборка  
1000

Отобразить

ID Модуля  
40

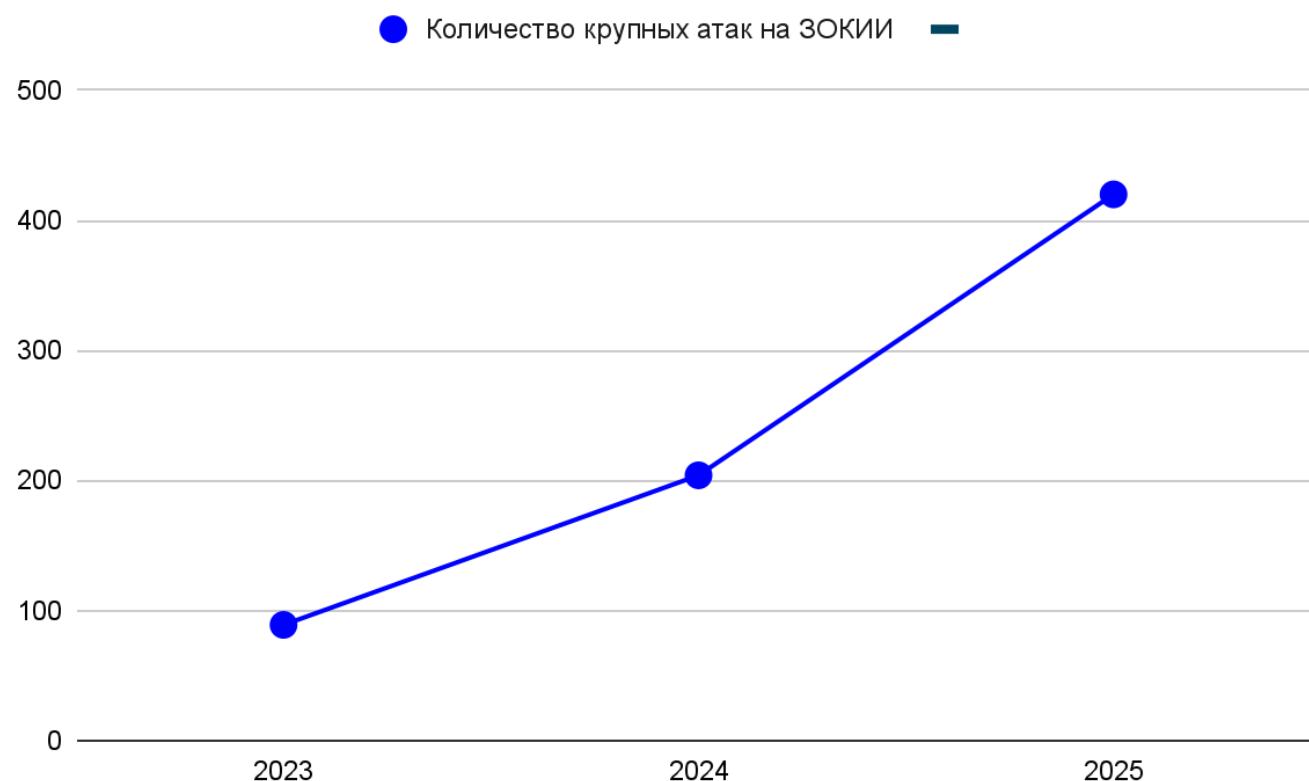
Тип сообщения ▾

Поиск 🔍

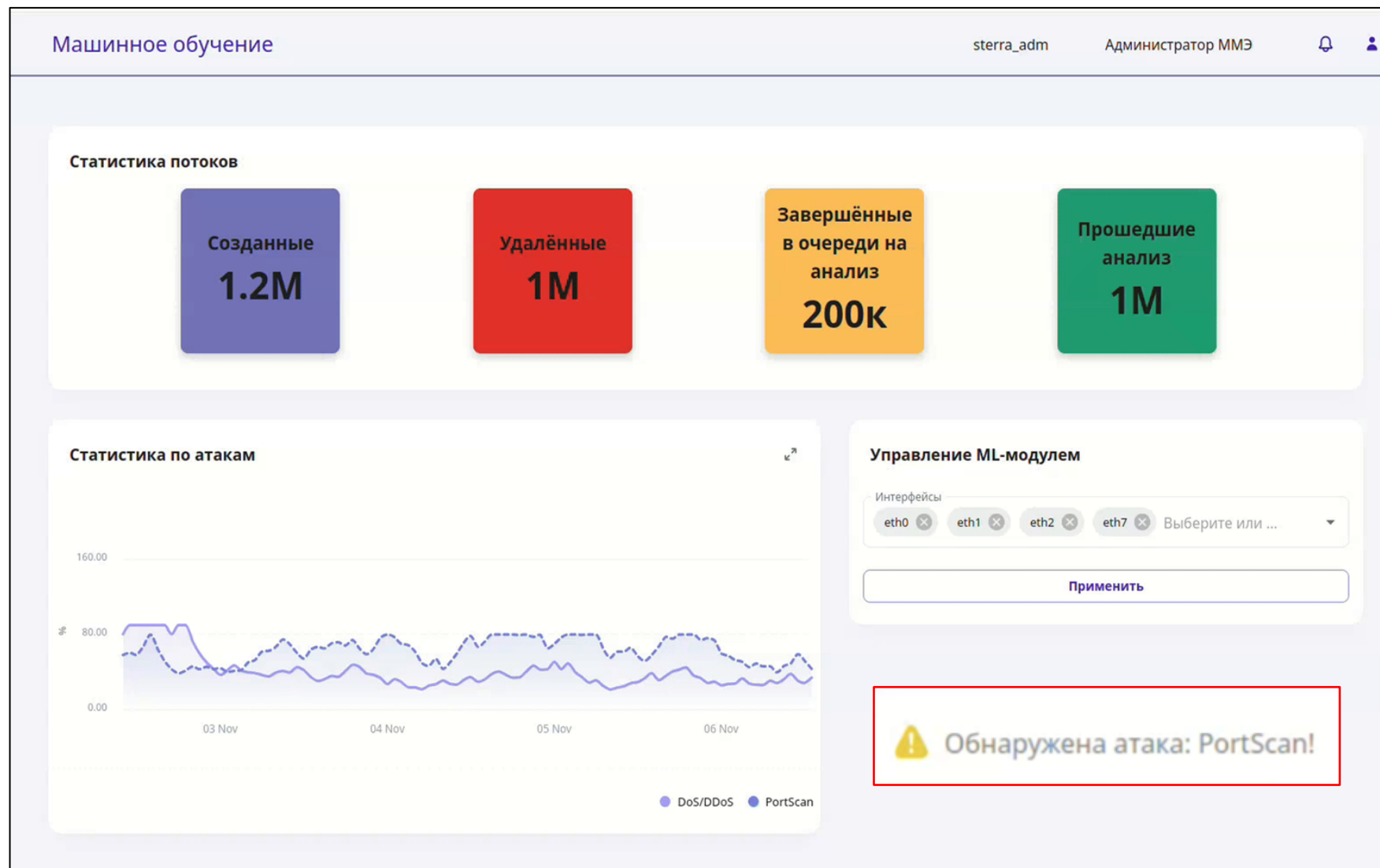
Скачать

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

## АТАКИ С ИСПОЛЬЗОВАНИЕМ AI АССИСТЕНТОВ



- Использование легитимных учётных записей (valid accounts) - ~31 % случаев.
- Фишинг и эксплуатация публичных приложений - ~26 % каждое.
- Внедрение инфостилеров (infostealers) выросло на 84 % в 2025 году по сравнению с 2024 показателем.
- Атаки становятся **более целенаправленными и технологически сложными**: AI-инструменты, инфостилеры, легитимные учётные записи используются активнее.



- Поддержка работы на нескольких интерфейсах
- Отображение уровня нормы
- Оповещение администраторов

Модули безопасности

## Машинное обучение

sterra\_admin    Администратор ММЭ

Управление    **Настройка**

### Исключения ^

IP    Поиск Q    RE\*    **Добавить**

IP ↑	Направление	Исключенных TCP сессий	Получено	
16.0.165.233	Источник	<b>Включен</b>	4	<input checked="" type="checkbox"/> <a href="#">Изменить</a> <a href="#">Удалить</a>
48.0.101.11	Назначение	<b>Включен</b>	7	<input checked="" type="checkbox"/> <a href="#">Изменить</a> <a href="#">Удалить</a>

Элементов на странице: 5    1 - 2 из 2

### События безопасности ^

Временная метка (эпоха)    Поиск Q    RE\*

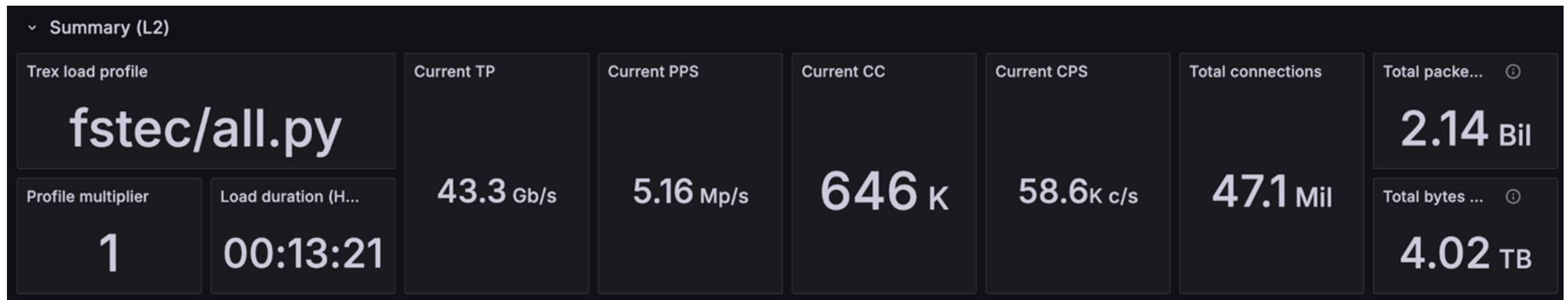
**Обнаружена атака: PortScan!**

Временная метка (эпоха)	Временная метка (ISO)	Тип атаки	Вероятность атаки	Интерфейс	Источник	Назначение	Порт источника	Порт назначения	Протокол
1770909746	2026-02-12T15:22:26.000Z	PortScan	0.647118	4	<a href="#">192.4.0.99</a>	<a href="#">192.4.0.1</a>	50956	4550	6
1770909746	2026-02-12T15:22:26.000Z	PortScan	0.607341	4	<a href="#">192.4.0.99</a>	<a href="#">192.4.0.1</a>	50956	5800	6
1770909746	2026-02-12T15:22:26.000Z	PortScan	0.62933	4	<a href="#">192.4.0.99</a>	<a href="#">192.4.0.1</a>	50956	49152	6
1770909746	2026-02-12T15:22:26.000Z	PortScan	0.643438	4	<a href="#">192.4.0.99</a>	<a href="#">192.4.0.1</a>	50956	139	6
1770909746	2026-02-12T15:22:26.000Z	PortScan	0.644534	4	<a href="#">192.4.0.99</a>	<a href="#">192.4.0.1</a>	50956	1046	6

Элементов на странице: 5    1 - 5 из 20

- Журнал исключений IP-адресов
- Оповещение администраторов
- События безопасности

- Оптимизированный для высокой производительности
- Защита от Zero-days атак



# USERNETCHECK - МОДУЛЬ ПОЛЬЗОВАТЕЛЕЙ СЕТИ

The screenshot displays the 'Пользователи сети' (Network Users) configuration page. It includes a sidebar with navigation options like 'Информационная панель', 'Конфигурация', and 'Пользователи'. The main content area features a notification 'Правила успешно удалены', tabs for 'Правила сети', 'Коннектор', and 'Пользователи сети', and several configuration sections: 'Включение модулей' (with 'Включение DPI' and 'Включение фильтрации пользователей' dropdowns), 'Настройки' (with 'Политика по умолчанию' set to 'Запретить' and a 'Сохранить' button), 'Правила фильтрации' (with a search bar and a table header including 'idx', 'Политика', 'Пользователи', 'Группы', 'Протоколы', and 'Расписание'), and 'Действия администраторов' (with a search bar and a 'Очистить действия администраторов' button).

- Добавлен статус «Онлайн»
- Добавлена поддержка IPv6
- Добавлена настройка политики по умолчанию
- Добавление возможности проверки пользователя антивирусом и песочницей
- Выбор идентификации для конкретного пользователя

# USERNETCHECK - МОДУЛЬ ПОЛЬЗОВАТЕЛЕЙ СЕТИ

## Расширенная статистика по пользователю

The screenshot displays the 'Пользователи сети' (Network Users) section of the USERNETCHECK interface. It features a sidebar with navigation options like 'Информационная панель', 'Конфигурация', 'Пользователи', and 'Учетные записи'. The main content area is divided into two sections: a table of network users and a section for authorization events.

Имя	Группы	MAC	Проверяется по MAC	IP	Проверяется по IP	Песочница	Антивирус	Онлайн
1		00:00:00:00:00:00	✗	103.239.44.147	✓	Выключен	Выключен	✗
user1		00:00:00:00:00:00	✗	dd44:124e:e324:2432:4324:2213:1dad:adad	✓	Выключен	Выключен	✗

Below the table, there is a section for 'События авторизации пользователей сети' (Network User Authorization Events). This section currently shows 'Нет данных' (No data) and includes search and filter options.

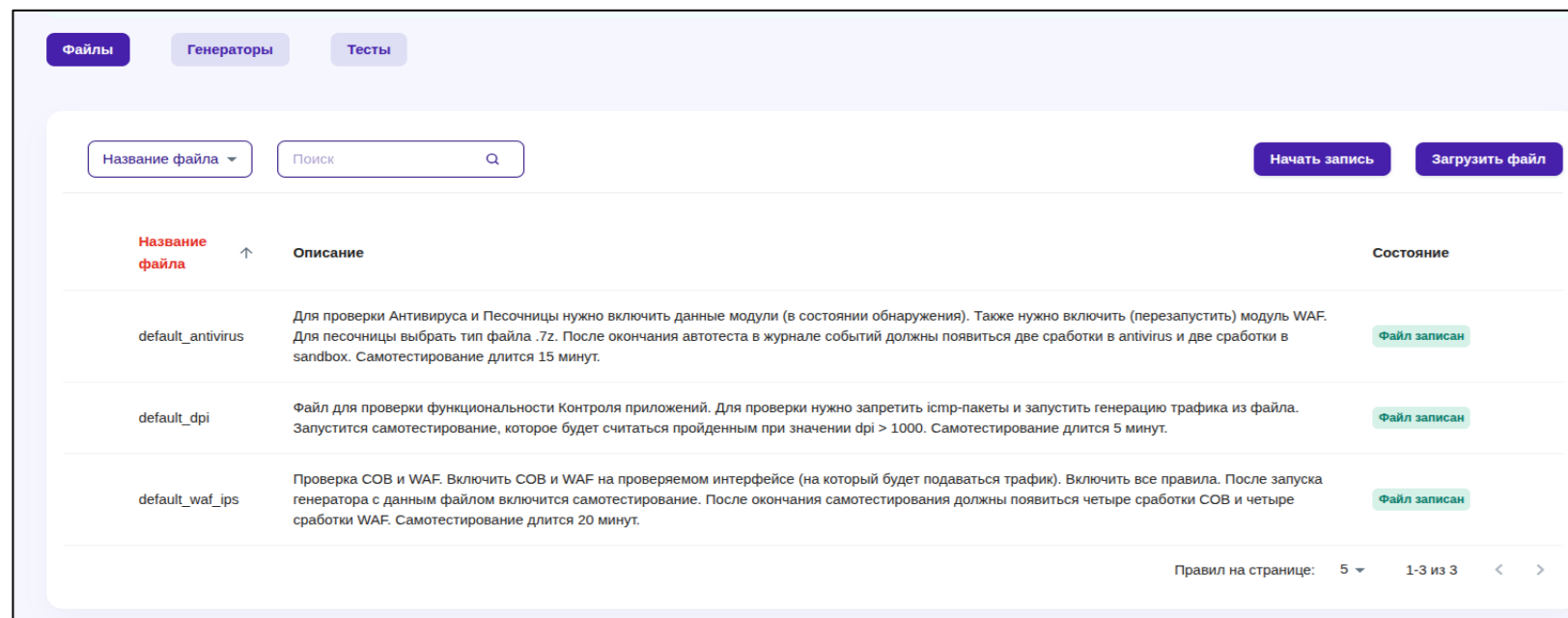
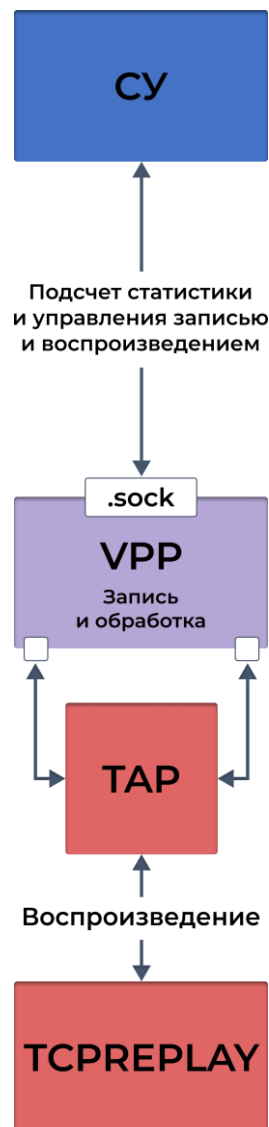
## WAF

- Топ атак (WAF)
- Топ IP, атакуемых пользователем
- Топ IP, атакующих пользователя
- Все сработки на пользователя

## СОВ

- Топ сигнатур
- Топ атакующих пользователя
- Топ атакуемых пользователем
- Все сработки по пользователю
- История авторизации

# МОДУЛЬ САМОТЕСТИРОВАНИЯ



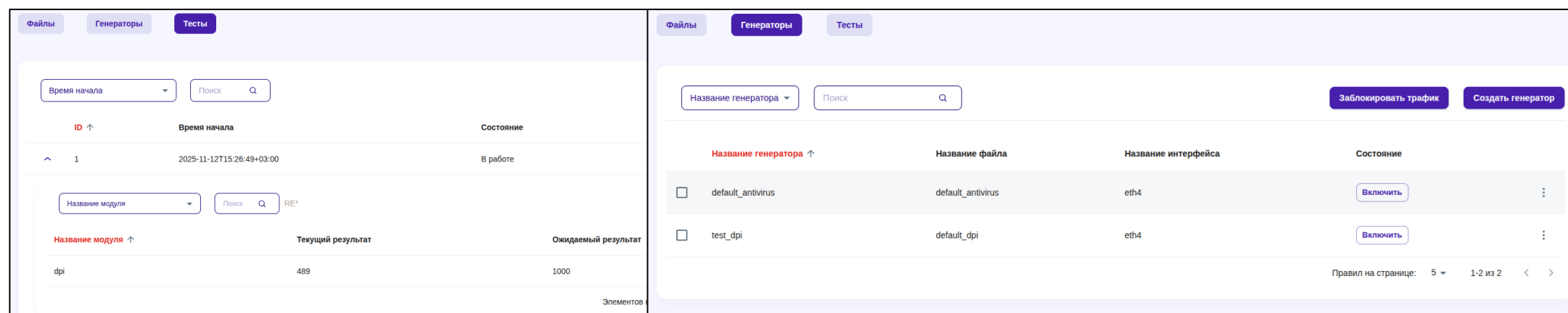
## Функции модуля

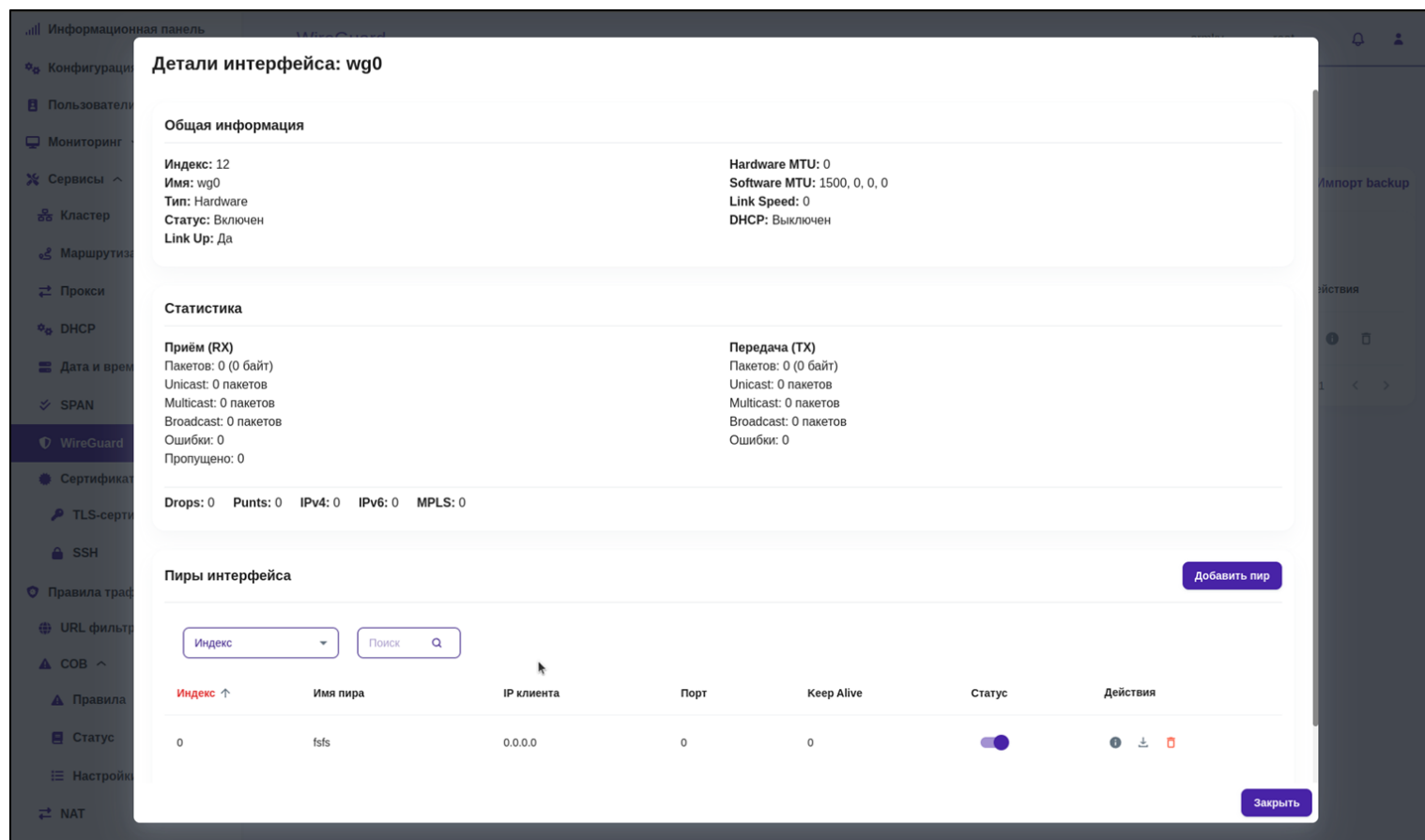
1. Готовые сценарии для тестирования:

- DPI
- WAF и COB
- Антивирус и песок

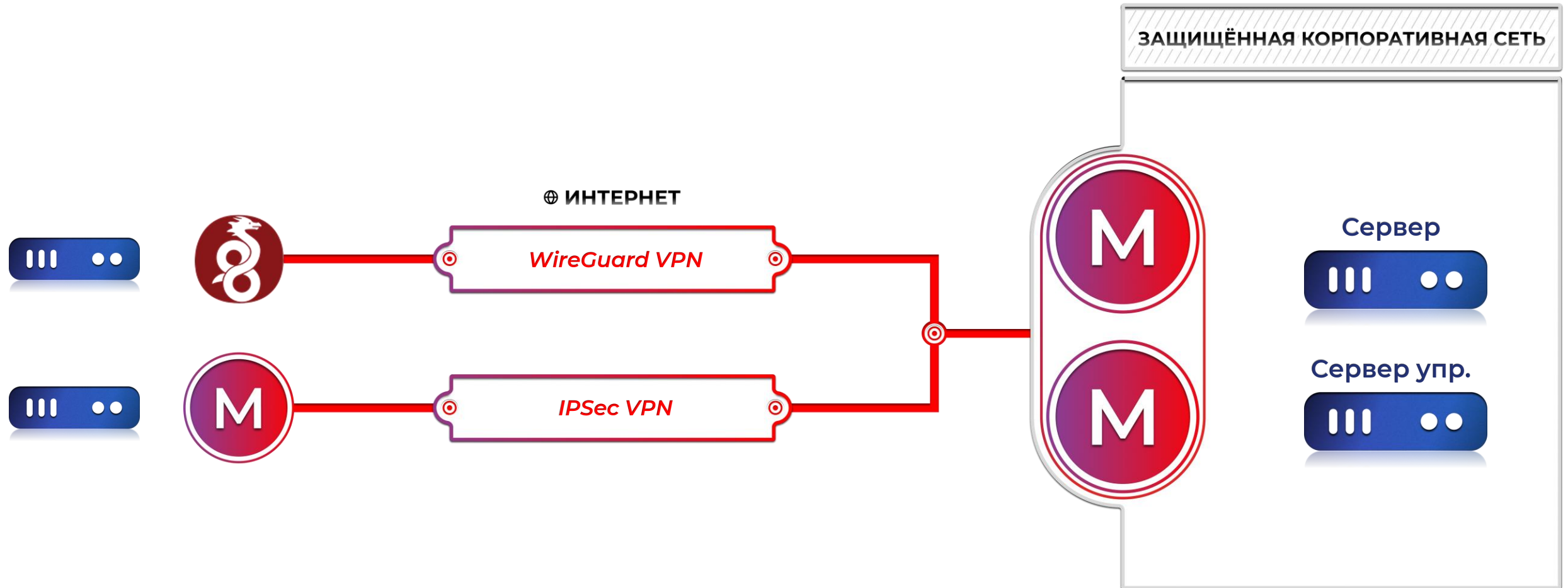
2. PCAP файлы:

- Запись
- Воспроизведение

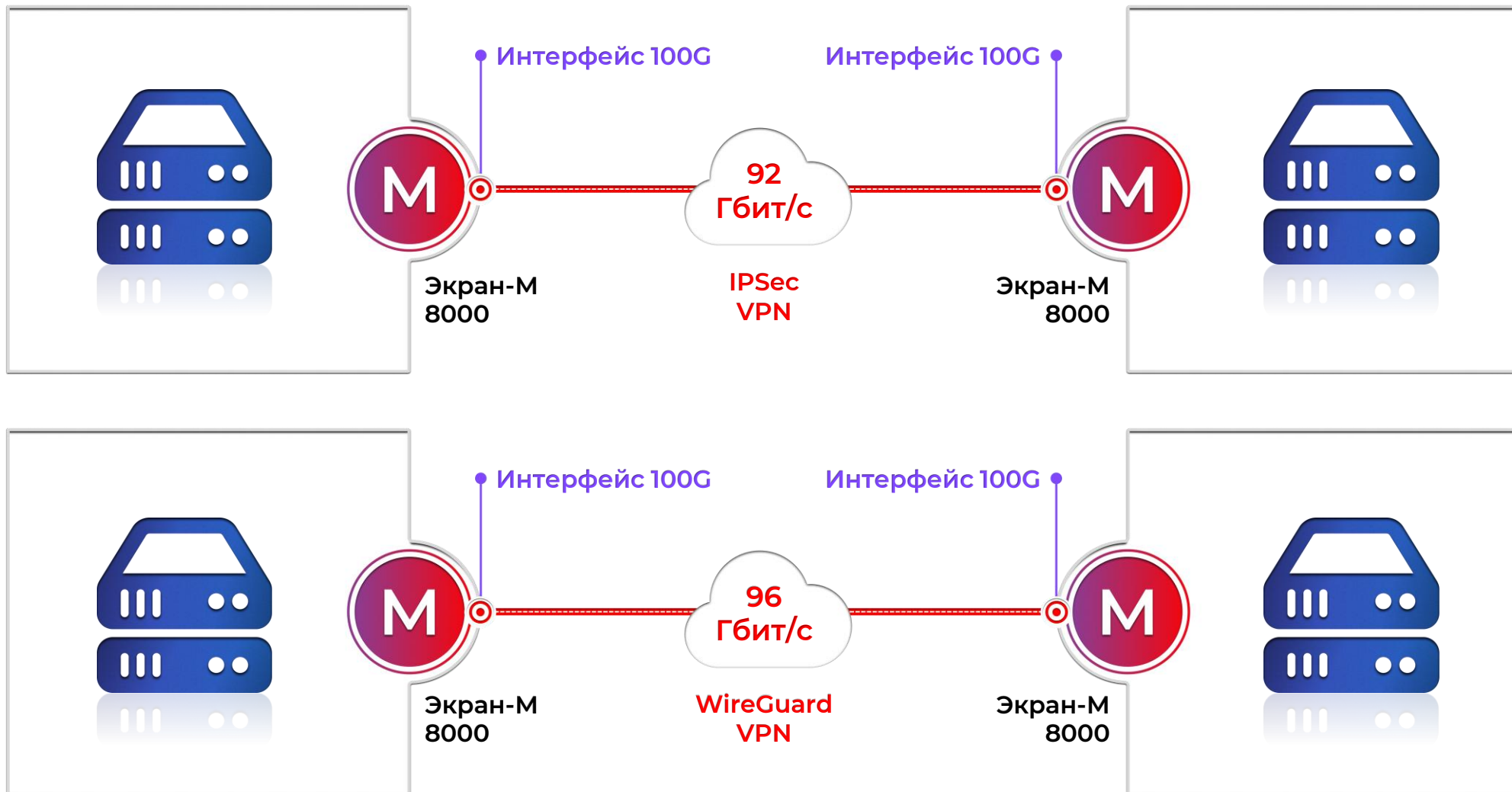




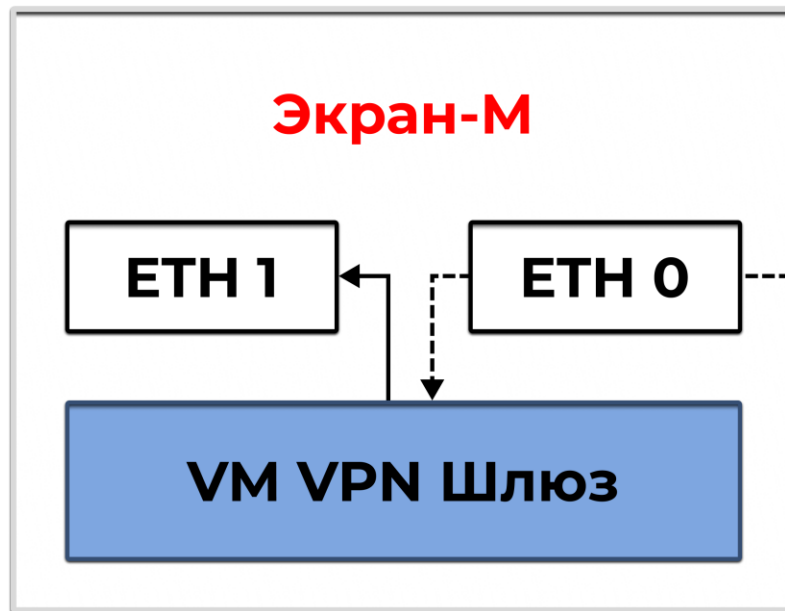
- Реализован как пользовательский плагин
- Шифрует трафик в fast-path без обходов через ядро
- Низкие задержки и высокая пропускная способность ~ равна скорости порта
- Богатая сервис-цепочка: NAT44/NAT66, ACL/ABF (policy-routing), QoS/traffic-policing, VRF/VRF-leak, IDPS, WAF, DPI — всё на одном dataplane



IPSec VPN и WireGuard VPN



### Удаленный офис



### Центральный офис



----- VPN ГОСТ  
———— Нешифрованный трафик

**ЭКРАН.М**

06.11.2025 23:37:55

- Информационная панель
- Конфигурация
- Пользователи
- Мониторинг
- Сервисы
- Правила трафика
- Отчеты и журналы
- Внешние системы
- Песочница
- Антивирус (ClamAV)
- Тестирование
- S-Console

sterra\_admin    Администратор ММЭ

### WireGuard

Интерфейсы WireGuard ^

Индекс:     Поиск:

Индекс ↑	Имя	Статус	Тип	MTU	RX Пакеты	TX Пакеты	Действия
25	wg0	Включен	Hardware	0	0	0	
26	wg1	Включен	Hardware	0	0	0	

Элементов на странице: 5    1 - 2 из 2    < >

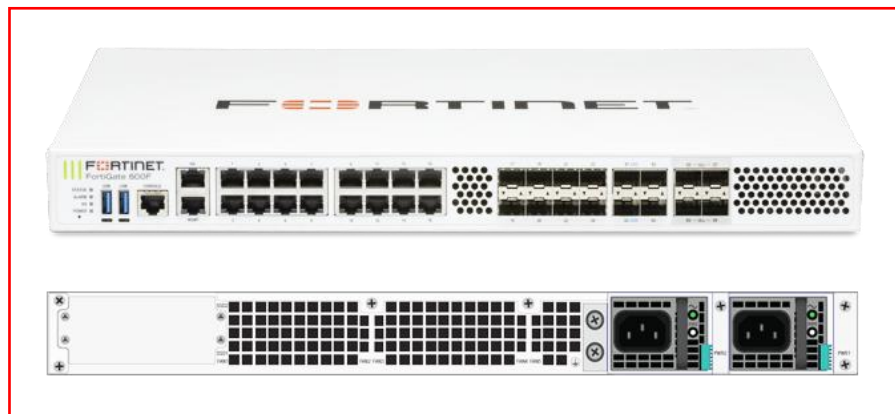
Добавить интерфейс    Экспорт backup    Импорт backup

# 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

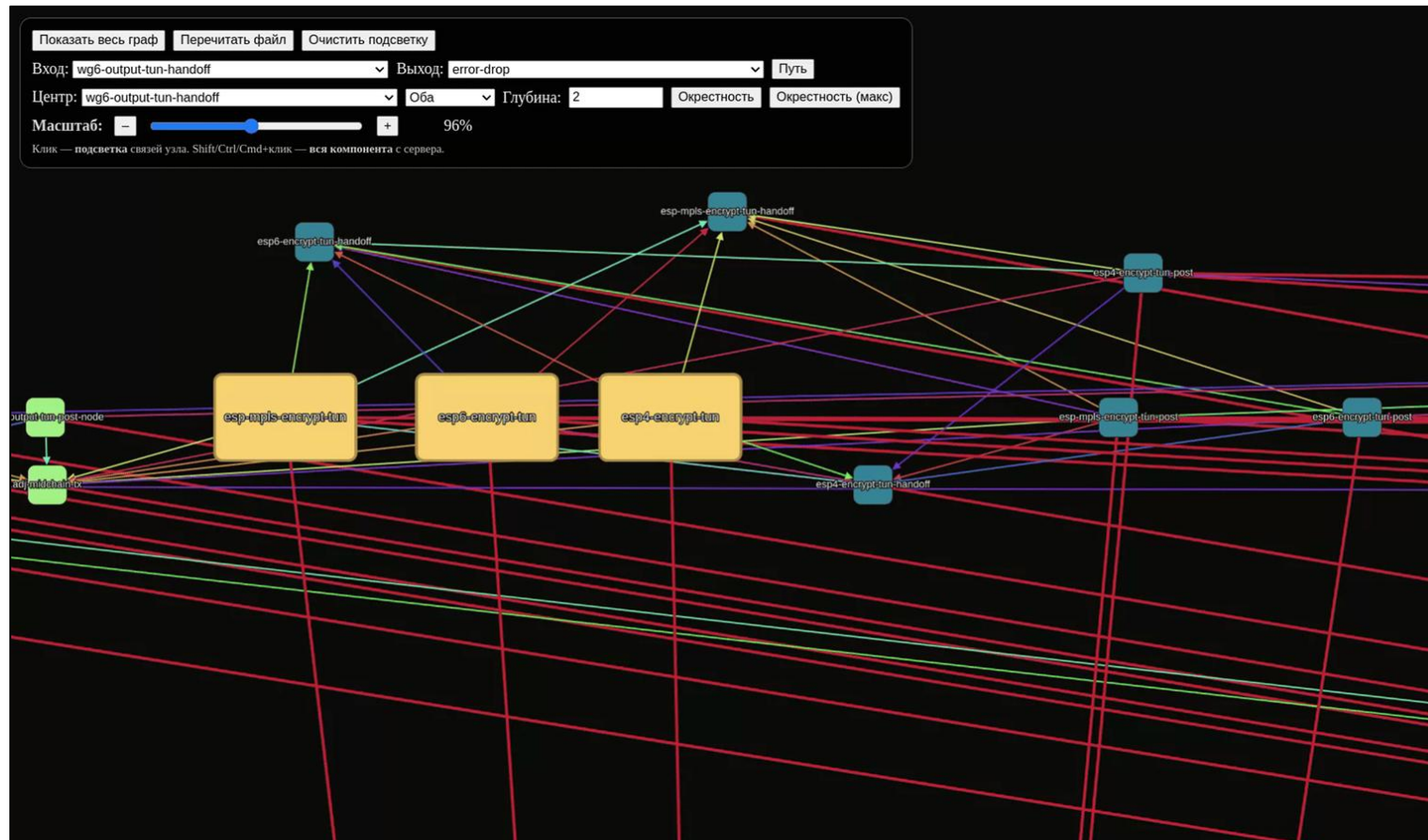


Перенос

## Экран-М



# ИНТЕРАКТИВНЫЕ СЕРВИС PACKET FLOW



- Просмотр связей
- Упрощение написания документации
- Построение прохождения пакета от А графа к Б, или общему drop графу

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

ДОРОЖНАЯ КАРТА РАЗВИТИЯ НА 2026-2027 гг.

**Июль 2026**

Сертификация  
Экран-М 2.0  
в Испытательной  
Лаборатории  
С-Терра БЕЛ на  
соответствие ТР  
2013/027/EU

**Март 2027**

- Разработка (КПА/ПП) Шлюз BelVPN 5.0 с IKEv2

**Получение  
сертификата  
соответствия ТР  
2013/027/EU**

**Март 2026**

- Сертификация  
продуктов (КПА/ПП)  
BELVPN 4.7

**Ноябрь 2026**

- Сертификация на  
соответствие ТР 2013/027/EU
- ПП «BelVPN Client - L 4.7»
- ПП «BelVPN Client - A 4.7»
- ПП «BelVPN Client - W 4.7»

**Сентябрь 2027**

- Встраивание белорусской криптографии в Экран-М

## ОТДЕЛ ПО РАБОТЕ С КЛИЕНТАМИ

---



**info@s-terra.by**

Общие вопросы по партнёрской политике и развитию бизнеса с «С-Терра»

## ОТДЕЛ КЛИЕНТСКОГО СЕРВИСА

---



**service@s-terra.by**

Техническая поддержка по купленному оборудованию

**с•терра®**

*Ваш ориентир в мире безопасности*

**СПАСИБО  
ЗА ВНИМАНИЕ!**

Минск, 2026