

АО «Сайбер ОК»
г. Москва, 2026 год

Описание функциональных характеристик программного обеспечения

«PentOps»

АННОТАЦИЯ

Настоящий документ предназначен для описания функциональных характеристик программного обеспечения «PentOPS» (далее — Система) в части базовых функциональностей и модулей:

- сканирование и сбор информации о сетевом периметре;
- хранение данных с результатами сканирования;
- хранение справочных данных;
- веб-интерфейс Системы.

ОГЛАВЛЕНИЕ

Аннотация	2
Оглавление.....	3
1 Термины и определения	4
2 Цели, назначение и области использования системы	5
3 Основные технические решения.....	6
3.1 Решения по структуре и архитектуре	6
3.2 Функциональные характеристики реализованных интерфейсов Системы .	8
3.2.1 Сбор данных и сканирование.....	8
3.2.2 Хранение данных	8
3.2.3 Функции веб-интерфейса лицензированного пользователя	9
3.2.4 Функции веб-интерфейса администратора Системы	13
3.3 Общие сведения по программно-аппаратному обеспечению Системы	12
ПРИЛОЖЕНИЕ А. Каталог основных пользовательских интерфейсов Системы.....	13

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Таблица 1. Термины и определения

№	Термин/Сокращение	Определение/Расшифровка
1.	ИБ	Информационная безопасность
2.	Интернет Актив	Аппаратные и программы решения, доступные из Интернет по IP или FQDN.
3.	Веб-интерфейс	Графический интерфейс пользователя
4.	РРПО	Реестр российского программного обеспечения
5.	Application Programming Interface (API)	Механизм, обеспечивающий интеграционное взаимодействие внутри компонентов системы, а также с внешними приложениями и системы
6.	Computer Emergency Response Teams (CERT)	Группа экспертов по компьютерной безопасности, занимающаяся сбором информации об инцидентах, их классификацией и нейтрализацией
7.	External Attack Surface Management (EASM)	Решения класса контроля поверхности атак внешнего периметра
8.	Fully Qualified Domain Name (FQDN)	Полностью определённое имя домена, то есть не имеющее неоднозначностей в определении
9.	Managed Security Service Providers (MSSP)	Внешняя компания (провайдер), являющаяся поставщиком услуг управляемой безопасности

2 ЦЕЛИ, НАЗНАЧЕНИЕ И ОБЛАСТИ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ

Цели создания и области применения Системы:

- централизованное планирование и проведение работ по тестированию на проникновение во внешнем периметре заказчика;
- автоматизированная оркестрация и параллельный запуск инструментов определения внешнего сетевого периметра, инвентаризации сетевых сервисов и выявления угроз информационной безопасности на периметре заказчика;
- централизованный сбор, нормализации и хранения результатов работ (артефактов, доказательной базы, отчётов сканеров) с привязкой к активам и проектам;
- управление проектами пентеста, ролями исполнителей, score-документами и взаимодействий с заказчиками;
- формирование итоговых отчётов (DOCX) по результатам тестирования с привязкой находок к стандартам OWASP, MITRE ATT&CK, PTES и методическим документам ФСТЭК России;
- ведение базы знаний об активах (организации, домены, IP-адреса, FQDN, сети, хосты, сервисы, веб-сайты, идентичности, секреты) с историей состояния.

Внедрение и использование Системы позволит обеспечить выполнение следующих задач:

- поиск, фильтрация, просмотр актуальных данных о состоянии сетевых объектов организации-заказчика с точки зрения наличия угроз информационной безопасности в приложениях и системах;
- оценка уровня защищённости сетевого периметра организации-заказчика.

Система предназначена для следующих ключевых пользователей:

- **Администратор Системы** — сотрудник оператора Системы, обладающий неограниченными полномочиями по действиям в Системе (добавление/блокировка/настройка пользователей Системы, настройка и запуск задач по сбору данных, добавление/редактирование организаций и хостов, настройка справочников);
- **Пользователь-заказчик** — пользователь, имеющий полномочия для просмотра данных связанных с организацией, которую он представляет;
- **Пользователь-эксперт** — пользователь участвующий в сопровождении и подготовке данных о результатах инвентаризации и выявленных угрозах для специалистов организации заказчика.

3 ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

3.1 Решения по структуре и архитектуре

Система разработана на базе архитектуры клиент-серверного веб-приложения, поддерживает технологию тонкого веб-клиента для доступа к сервисам серверной части Системы.

Система состоит из серверной части и веб-интерфейсов (см. Рисунок 1):

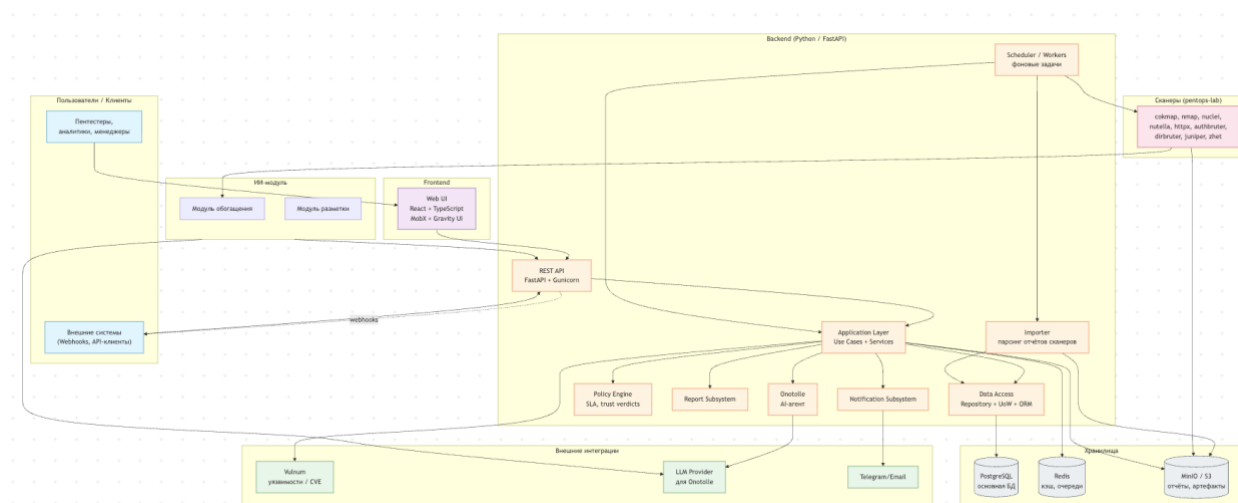


Рисунок 1. Архитектура Системы

Система включает компоненты:

- **Подсистема сканирования сетевого периметра** – совокупность компонент для планирования и реализации распределенного сканирования. Обеспечивает получение данных об узлах, баннерах, приложениях и уязвимостях. Реализованы различные режимы сбора данных, включая получение данных из внешних систем-источников.
- **Хранилище данных** – совокупность технических средств, обеспечивающих хранение промежуточных, полных и исторических данных с результатами сканирования, а также справочных данных Системы.
- **Подсистема ИИ** – подсистема, обеспечивающая обогащение и очистку сигналов о выявленных в ходе сканирования уязвимостей сетевого периметра.
- **Подсистема планирования** – модуль системы, который обеспечивает фоновое выполнение задач согласно указанному расписанию.
- **Подсистема оповещения** – совокупность модулей, которые обеспечивают доставку сообщений о событиях в сервисе по различным информационным каналам до конечных пользователей.

- **Подсистема отчетов** – совокупность модулей, которые обеспечивают генерацию отчетных материалов о состоянии сетевого периметра.
- **Подсистема политик** – модуль ядра системы, обеспечивает настройку правил, изменяющих штатное поведение системы.
- **Пользовательский веб-интерфейс** – набор веб-страниц и логики их демонстрации, обеспечивающих доступ со стороны всех типов пользователей к функционалу Системы.

3.2 Описание функциональные характеристик Системы

3.2.1 Сбор данных и сканирование

Сбор данных и сканирование реализуются с целью сбора и агрегации данных об активах сетевого периметра заказчика и выявления актуальных угроз информационной безопасности.

Для запуска сканирования пользователю системы предоставляется инструмент для создания и редактирования конфигураций сканирования, в котором он может определить периоды, сетевые диапазоны, интенсивность и глубину проверок.

Процесс комплексного сканирования реализован поэтапно:

1. обнаружение портов, разделение портов на TCP и UDP, идентификация жизнеспособности хоста (есть открытые порты), для UDP портов на данном этапе должны собираться данные о приложениях и версиях;
2. сбор с TCP портов данных (включая, но не ограничиваясь):
 - операционная система;
 - протокол уровня L7;
 - баннеры;
 - приложения (с версиями или без);
 - другое.
3. сбор информации о веб-ресурсах
 - Код ответа;
 - Favicon;
 - Скриншот сайта;
 - Заголовок;
 - Перечень технологий.
4. сканирование уязвимостей по типу сервиса:
 - Сбор информации об угрозах на базе пассивных проверок на основе баннеров сервисов;
 - Сбор информации об угрозах на базе активных проверок на основе информации о типе сервиса;
 - Эnumерация ресурсов на выявленных сервисах;
 - Подбор аутентификационной информации на выявленные сервисы;
 - Неформализованный поиск угроз на основе агентских инструментов с использованием больших языковых моделей.

3.2.2 Хранение данных

Хранение данных сканирований и данных справочников осуществляется в хранилище данных Системы. В Системе хранятся следующие виды данных:

- все данные, собранные по сетевым объектам (сервисам, хостам и веб-сайтам) в результате сканирований;
- данные об активах сетевого периметра организации;
- данные о потенциальных и подтвержденных угрозах информационной безопасности сетевого периметра;
- справочные данные по нерекомендованным сервисам, whois и geo-информации;
- производные данные о состоянии сетевого периметра (графики, индексы безопасности).

3.2.3 Функции веб-интерфейса лицензированного пользователя

Веб-интерфейс включает пользовательские интерфейсы Системы, предназначенные для поиска, фильтрации, просмотра и анализа информации, накопленной в Системе в результате сканирований.

Веб-интерфейс обеспечивает выполнение следующих задач:

- вывод статистических данных;
- поиск в результатах сканирования по заданным параметрам.
- Работа с инструментами отчетности, конфигурации сканирования и правил политик SLA и доверенных сервисов.

Основные разделы веб-интерфейса:

- Страница авторизации;
- Страница администрирования системы
- Страница списка проектов
- Страница дашборда проекта
- Страница календаря проекта
- Страница конфигуратора отчетов
- Страница управления активами проекта
- Страница объектов – сервисы, хосты, веб-сайты, сертификаты
- Страница угроз проекта
- Страница задач экспертов
- Страница настроек параметров сканирования.

3.2.3.1 Авторизация в веб-интерфейсе

Авторизация в Веб-интерфейсе должна осуществляться после ввода логина и пароля на странице авторизации и нажатии на кнопку «Войти».

В случае, если у пользователя подключена двухфакторная аутентификация на базе TOTP производится запрос на дополнительный код подтверждения.

После авторизации в Веб-интерфейсе должен осуществляться переход к главной странице со списком проектов доступных для пользователя.

3.2.3.2 Страница администрирования системы

Раздел администрирования системы доступен только пользователям с ролью администратора системы. Раздел позволяет:

- Проводить диагностику состояния подсистем
- Управление пользователями системы и назначения ролей на проекты
- Ведения словаря nereкомендуемых сервисов
- Просмотр журнала аудита
- Управления PAT-токенами всех пользователей

3.2.3.3 Страница списка проектов

Раздел позволяет просмотреть список всех проектов, к которым у пользователя есть доступ. Отображаются избранные проекты, последние просмотренные. По каждому проекту демонстрируется краткая сводка в виде индекса безопасности проекта и распределения угроз по уровню критичности.

3.2.3.4 Страница дашборда проекта

Раздел дашборда проекта содержит сводную информацию о состоянии сетевого периметра организации. Основными элементами этого раздела является индекс безопасности, распределение актуальных угроз по уровню критичности, по типам и состоянию. Отображаются последние угрозы, последние закрытые угрозы, угрозы у которых подходит к концу время устранения. Отображаются топ 5 уязвимых хостов и веб-ресурсов.

3.2.3.5 Страница календаря проекта

Раздел календаря проекта(ов) позволяет отобразить все события организации в сервисе PentOPS в календарном представлении. Пользователь может изучить периоды сканирования, время фиксации угроз, окончания доменных имен и сертификатов в срезах дневного, недельного, месячного и годового представления.

3.2.3.6 Страница конфигуратора отчетов

Раздел конфигурации отчетных материалов позволяет сконструировать необходимый отчет в офисном формате, указывая какие блоки информации должен этот отчет включать. Для удобства пользователя предоставляются predetermined форматы отчетов.

3.2.3.7 Страница управления активами проекта

Раздел управления активами позволяет пользователю определить основные активы сетевого периметра, которые подлежат инвентаризации и анализу на безопасность. Пользователю предоставляется инструменты для работы с такими активами как:

- Доменное имя

- Поддомен
- Сеть
- IP-адрес

Поддерживаются адреса как v4 так и v6 нотации. Система поддерживает региональные доменные имена в punny-code.

3.2.3.8 Страницы объектов проекта

Система предоставляет инструменты для инспектирования результатов инвентаризации сетевого периметра в виде списков сервисов, хостов и веб-ресурсов. Типовой раздел предоставляет инструменты группировки, фильтрации, получения детальной информации и карточки инвентаризационного объекта. Состояние фильтров и группировок запоминается для пользователя. Пользователь имеет возможность выгрузки объектов системы в *xlsx* или *csv* формате согласно примененным фильтрам. Для повышения ориентированности во времени – пользователю предоставляется инструмент для работы с временными срезами, где он может выбрать только объекты актуальные на указанный диапазон времени.

3.2.3.9 Страница угроз проекта

Для получения перечня угроз информационной безопасности сетевому периметру пользователю предоставляется раздел “Угрозы”. Пользователю предоставляется штатный механизм фильтрации и группировки угроз. У угроз есть жизненный цикл, который может управляться пользователем:

- Новая
- Исправленная
- Актуальная
- Повторно-обнаруженная
- Ложное срабатывание
- Риск принят

Для удобства угрозы имеют разные типы:

- Уязвимость
- Устаревшее ПО
- Мiskonфигурация
- Раскрытие информации

В качестве оценки критичности угрозы используется шкала со следующими значениями:

- Шторм (максимальная критичность, угроза несет максимальные риски для организации, подлежит немедленному устранению)
- Критическая

- Высокая
- Средняя
- Низкая
- Инфо

Угрозы могут быть определены крайние сроки для устранения. Правила расчета крайних сроков устранения указываются в разделе политик. Правила могут полагаться на уровень критичности, тип угрозы и сетевые атрибуты объекта, где угроза была выявлена.

3.2.3.10 Страница задач экспертов

Внутренний раздел для пользователей экспертов, где происходит подготовка всех кандидатов в угрозы для публикации заказчику. Инструменты позволяют насытить находки и уязвимости сопровождающей информацией и подтвердить реальность и актуальность выявленных уязвимостей.

3.2.3.11 Страница настроек параметров сканирования

Предоставляет пользователю возможность указать периоды и глубину, с которой будет производиться сканирование сетевого периметра. Пользователь может определить те модули, которые будут задействованы в процессах инвентаризации сетевых сервисов и инструменты, которые будут использоваться для активного анализа защищенности сетевого периметра.

3.3 Общие сведения по программно-аппаратному обеспечению Системы

Модули Системы реализованы на базе операционной системы семейства Linux.

СУБД удовлетворяет требованиям импортозамещения.

Версии всего используемого системного программного обеспечения удовлетворяют требованиям информационной безопасности согласно классу защищенности Системы.

При создании Системы использовалось российское программное обеспечение и программные решения, построенные на базе свободного программного обеспечения.

ПРИЛОЖЕНИЕ А. Каталог основных пользовательских интерфейсов Системы

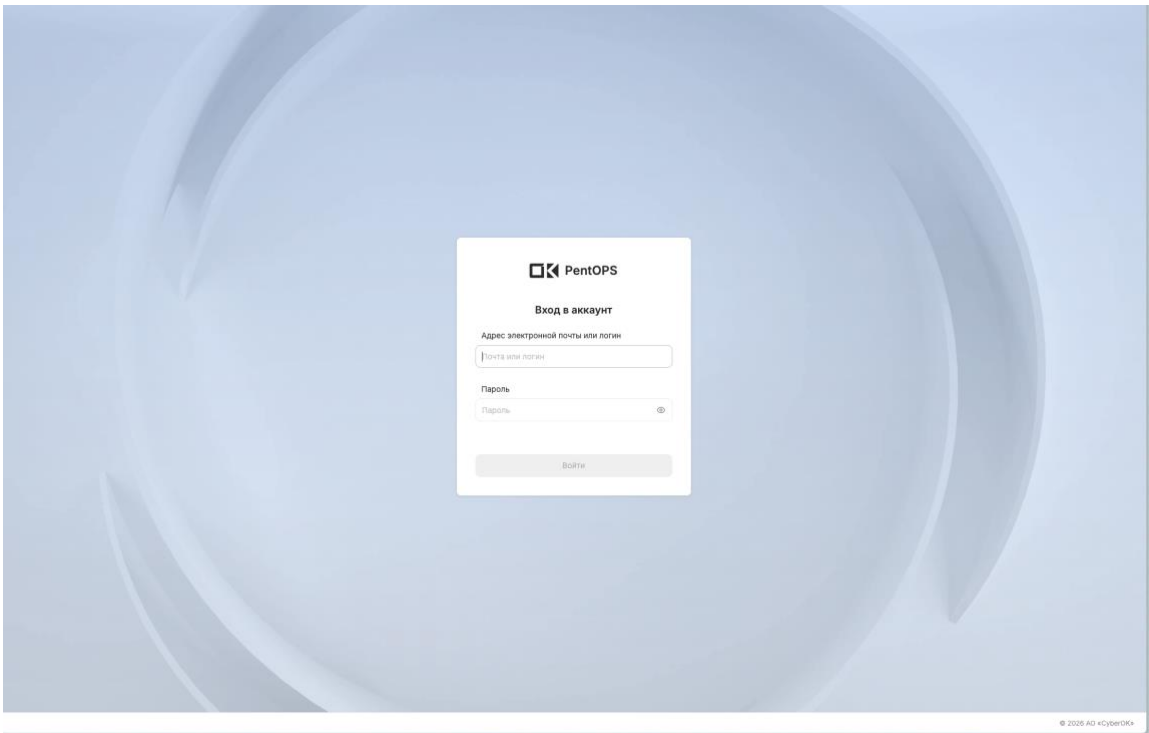


Рисунок 2. Экран авторизации в web-приложении Системы

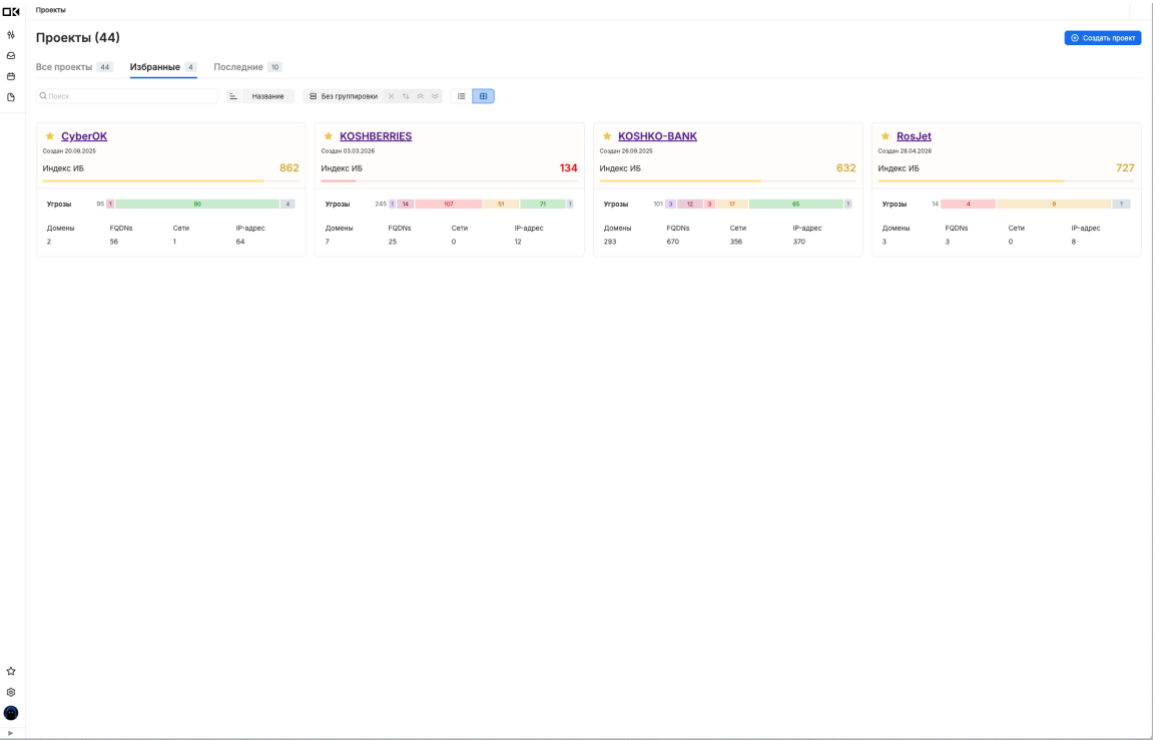


Рисунок 3. Главный экран проектов

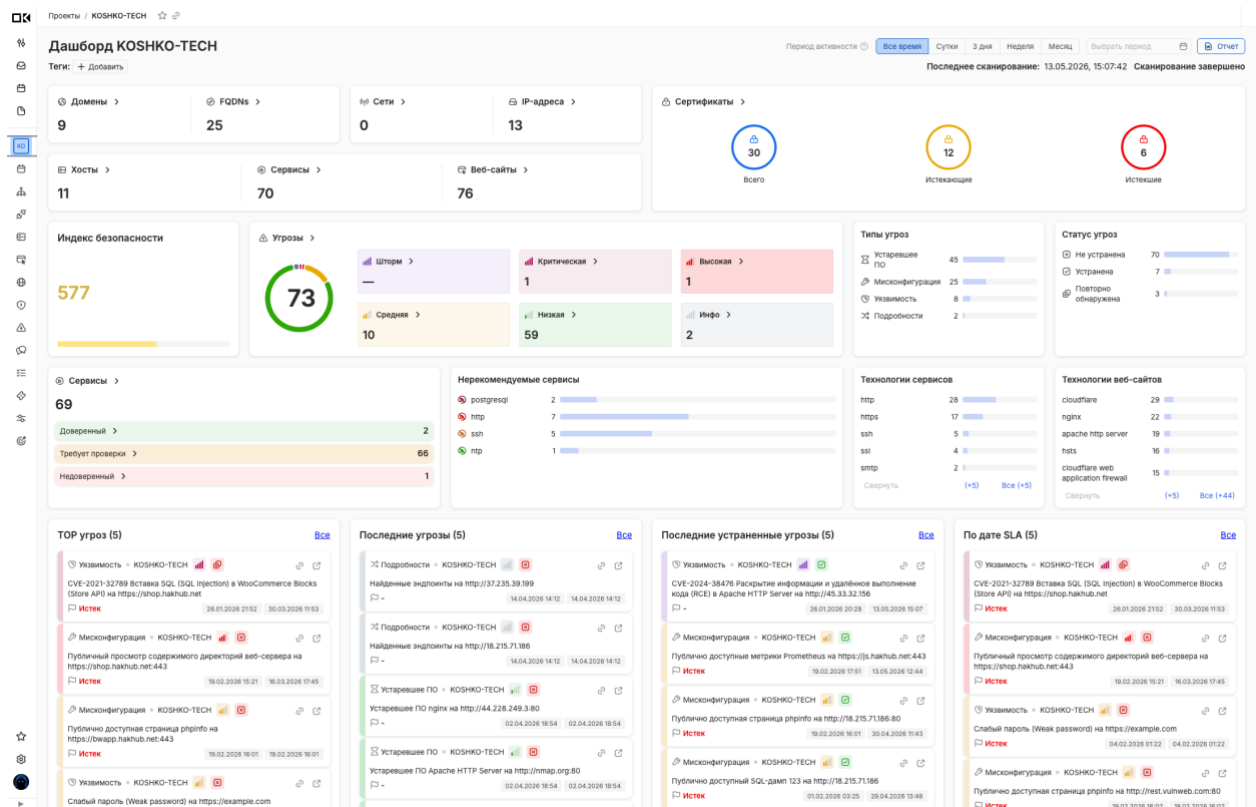


Рисунок 4. Дашборд проекта

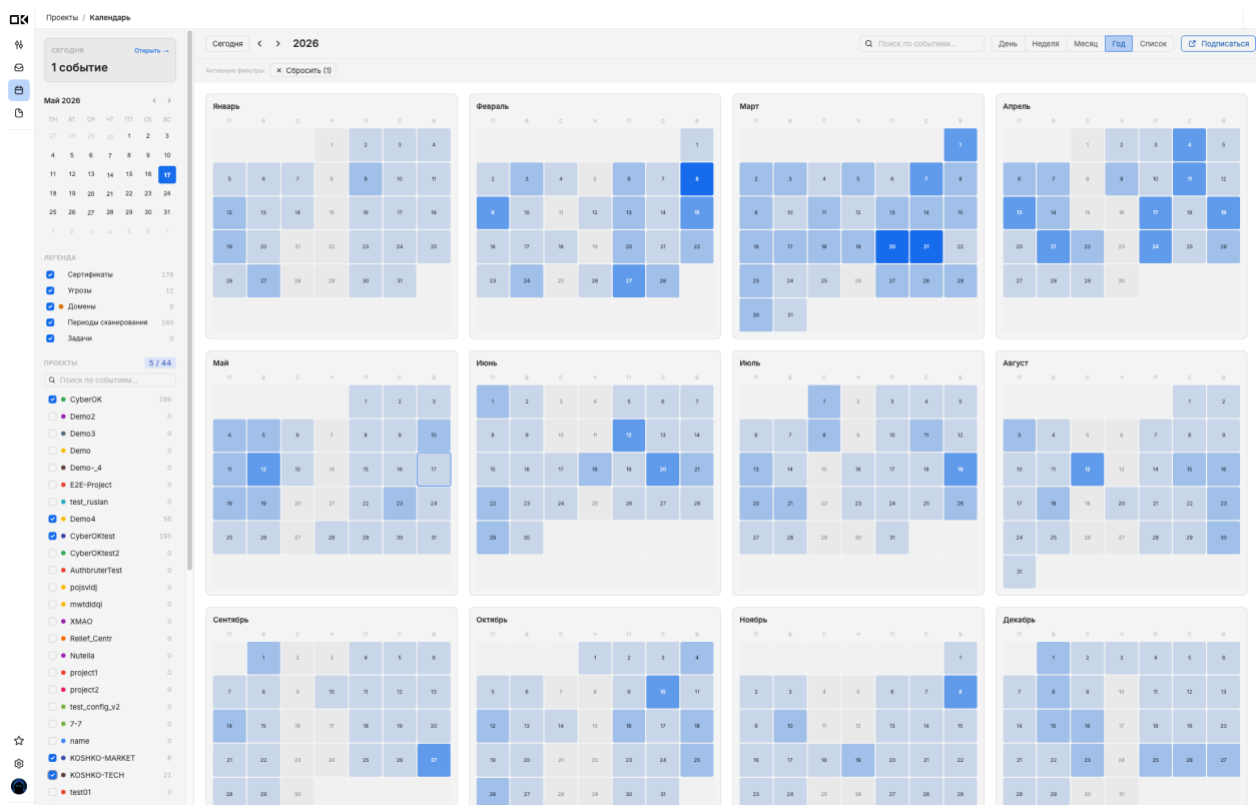


Рисунок 5. Календарь событий

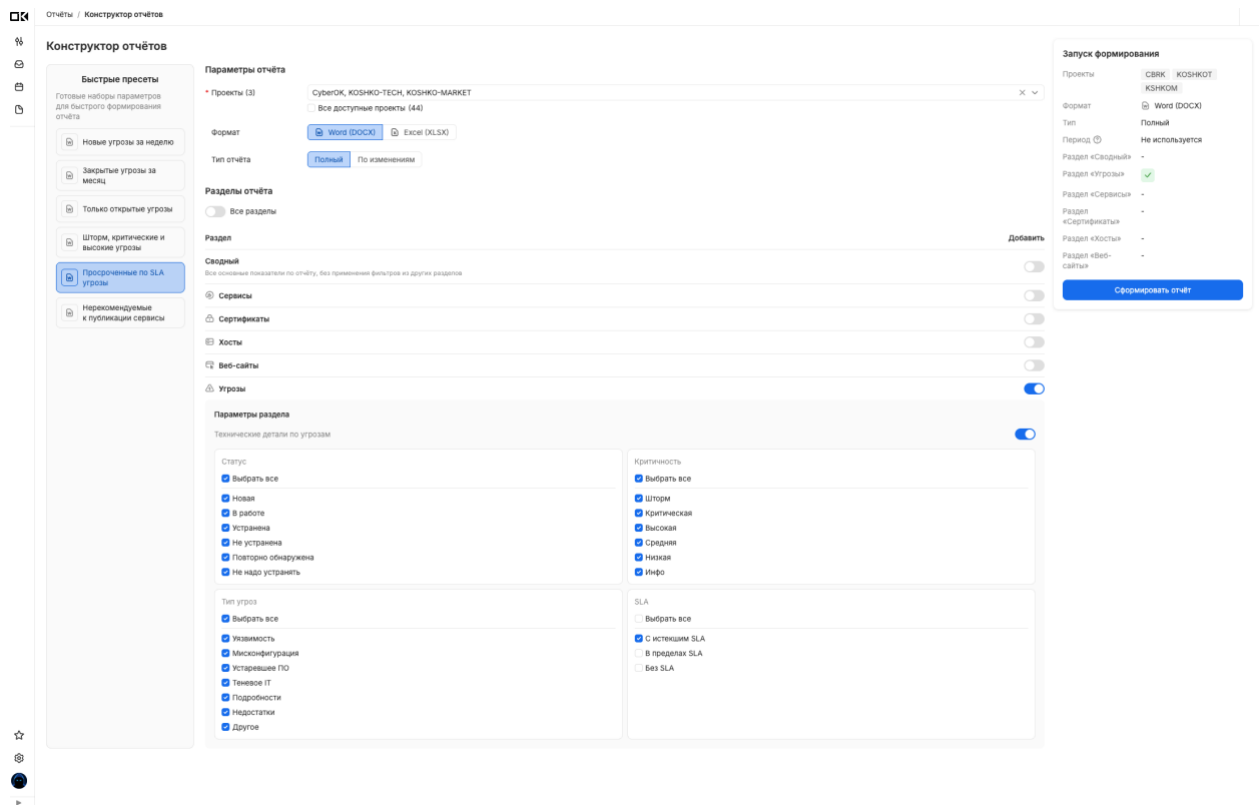


Рисунок 6. Конфигуратор отчетов

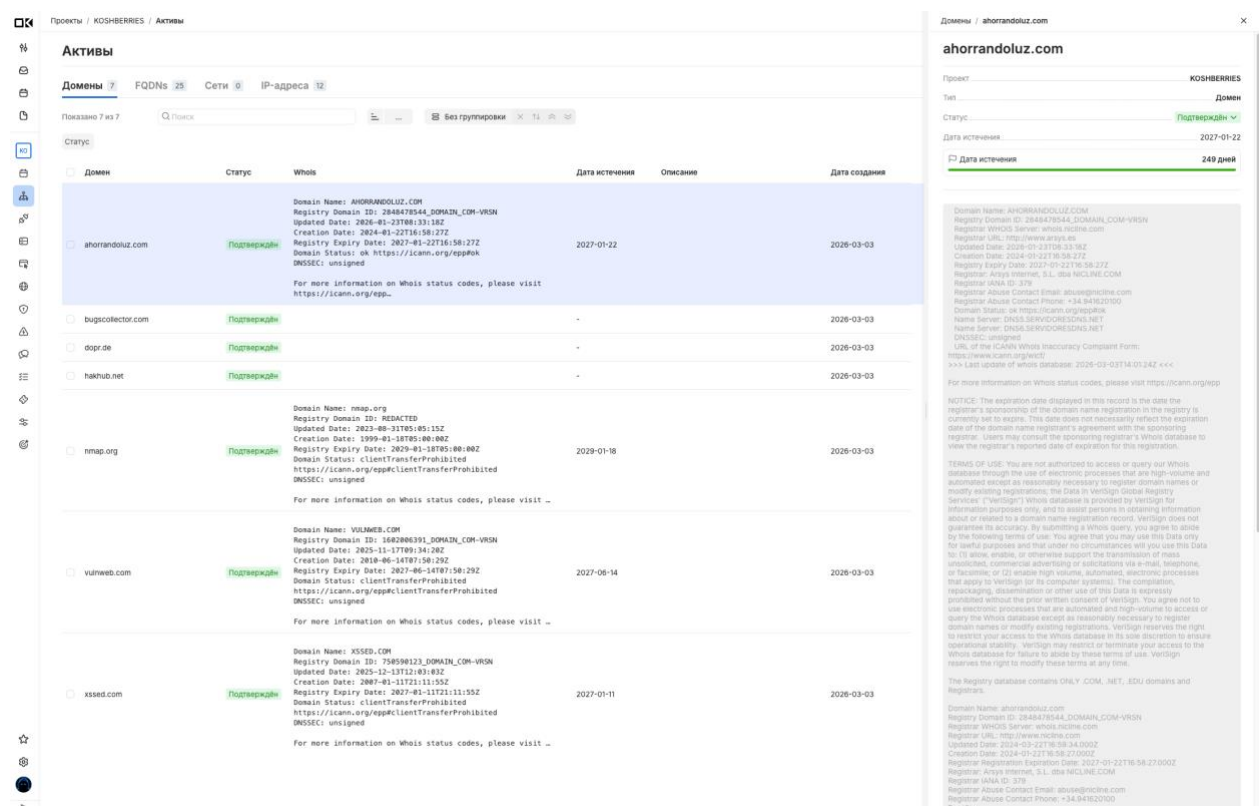


Рисунок 7. Экран с перечнем активов

Проекты / KOSHBERRIES / Сервисы

Сервисы

Период активности: Все время | Сутки | 3 дня | Неделя | Месяц | Выбрать период

Всего 44 | Новые 44

Фасеты: ASN (7) | IP-адрес (10) | Порты (29) | Сервисы (11)

График: Показано 10 из 44 | Экспозиция | По ASN | Сбросить

IP-адрес	ASN	Подсеть	Порты	Протокол	Сервис	Статус	Продукт	Версия	Теги	Экспозиция	Доверие	Первое наблюдение
AKAMAI-LINODE-AP Akamai Connected Cloud 2												
45.33.32.156	AKAMAI-LINODE-AP Akamai C...	80	tcp	http	Открыт	Apache HTTP Server	2.4.7	—	—	Требуется проверки	2026-02-18	
50.176.1184	AKAMAI-LINODE-AP Akamai C...	80	tcp	http	Открыт	Apache HTTP Server	2.4.6	—	—	Требуется проверки	2026-02-18	
AMAZON-02 2												
44.228.249.3	AMAZON-02	80	tcp	http	Открыт	—	—	—	—	Требуется проверки	2026-02-18	
44.238.29.244	AMAZON-02	80	tcp	http	Открыт	Microsoft IIS	8.5	—	—	Требуется проверки	2026-02-18	
AMAZON-AES 2												
18.215.71.186	AMAZON-AES	8081	tcp	http	Открыт	Apache HTTP Server	2.4.25	—	—	Требуется проверки	2026-02-18	
18.215.71.186	AMAZON-AES	80	tcp	http	Открыт	Apache HTTP Server	2.4.25	—	—	Требуется проверки	2026-02-18	
ES-MDC-DATACENTER Malaga Data Center 1												
37.235.59.199	ES-MDC-DATACENTER Malaga ...	80	tcp	http	Открыт	Apache HTTP Server	—	—	—	Требуется проверки	2026-02-18	
HETZNER-AS 1												
null 5												
135.181.246.162	HETZNER-AS	54321	tcp	postgresql	Открыт	PostgreSQL	9.6.0	—	—	Критическая	Требуется проверки	2026-02-18
221.150.96.204	—	1012	tcp	postgresql	Новый	PostgreSQL	—	—	—	Критическая	Требуется проверки	2026-02-18
221.150.96.204	—	50001	tcp	http	Открыт	—	—	—	—	Требуется проверки	2026-02-18	
221.150.96.204	—	80	tcp	http	Открыт	nginx	—	—	—	Требуется проверки	2026-02-18	
221.150.96.204	—	50002	tcp	http	Открыт	nginx	1.4.70	—	—	Требуется проверки	2026-02-18	

Проекты / KOSHBERRIES / Хосты

Хосты

Период активности: О хостах | Веб-сайты 3 | Комментарий 0

Всего 10 | Новые 0 | Избранные 0

Фасеты: Угрозы (6) | IP-адрес (10) | ASN (7) | Сервисы (12)

График: Показано 10 из 10 | Без группировки | Сбросить

Угрозы	IP-адрес	Подсеть	ASN	Сервисы	Теги
72	18.215.71.186	AMAZON-AES	—	http	0 2 3
5	44.228.249.3	AMAZON-02	—	http	0 1 2
3	44.238.29.244	AMAZON-02	—	http	0 1 2
42	45.33.32.156	AKAMAI-LINODE-AP Akamai C...	—	http nginx-echo http ssh unknown	0 5 2
0	188.114.96.1	CLOUDFLARENET	—	https	0 1 2
64	50.176.1184	AKAMAI-LINODE-AP Akamai C...	—	http https smtp ssh	0 4 6
1	135.181.246.162	HETZNER-AS	—	grpc https postgresql ssh ssl unknown	0 10 1
10	51.195.201.11	OVH	—	dns http mail smtp ssh unknown	0 7 3
5	37.235.59.199	ES-MDC-DATACENTER Malaga ...	—	http https	0 2 3
26	221.150.96.204	—	—	http https postgresql ssh unknown	0 11 13

Хосты / 18.215.71.186

О хостах | Веб-сайты 3 | Комментарий 0

Хосты 18.215.71.186

Название хоста: Введите название хоста

Теги: + Добавить

Добавьте пожалуйста информацию об этом хосте...

Например: Основной сайт компании, отвечает за продажи, ответственный - IT-отдел.

Семейство ОС: —

Название ОС: debian

Порты (2): 80/tcp 8081/tcp

Сервисы (1): http

Технологии (1): Apache HTTP Server

FQDNs (1): rest.vulnweb.com

Номер ASN: 14618

Название ASN: AMAZON-AES

Организация: Amazon.com, Inc.

PTR: ec2-18-215-71-186.compute-1.amazonaws.com

Расположение: us

Первое наблюдение: 18.02.2026

Последнее наблюдение: 18.02.2026

Угрозы: 72 42 14 10

Мисконфигурация - KOSHBERRIES

Публично доступный файл резервной копии базы данных WordPress на http://rest.vulnweb.com

Уязвимость - KOSHBERRIES

CVE-2024-38476 Information Disclosure and Remote Code Execution (RCE) in Apache HTTP Server on https://svn.nginx.org via http://18.215.71.186

Уязвимость - KOSHBERRIES

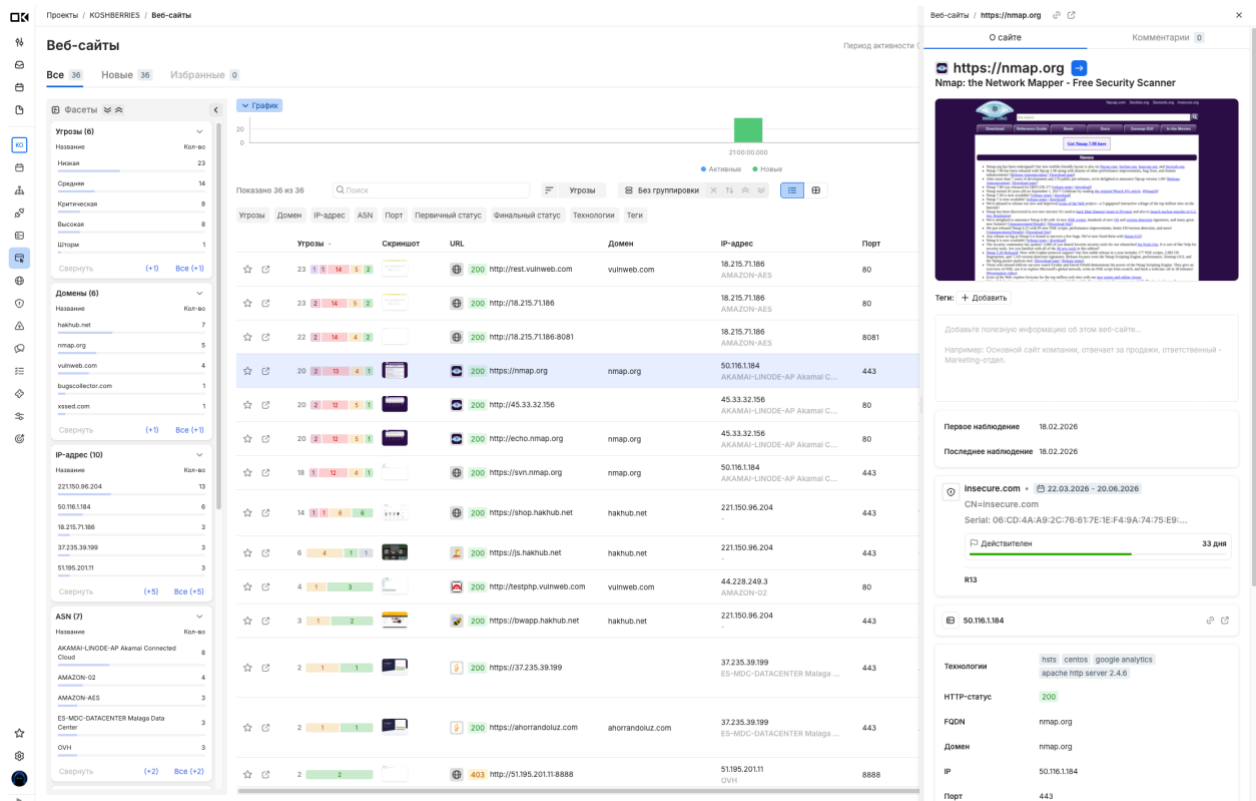


Рисунок 8. Экран с объектами сетевого периметра

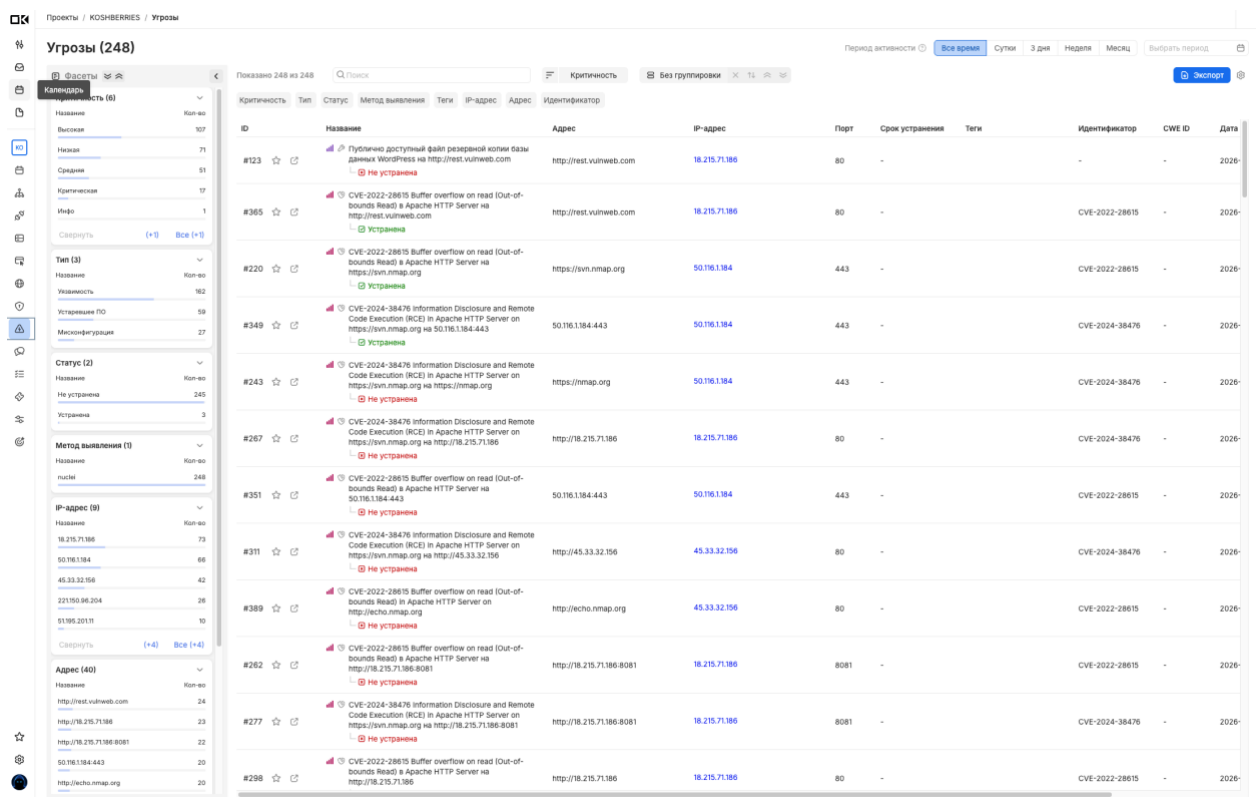


Рисунок 9. Экран угроз сетевого периметра

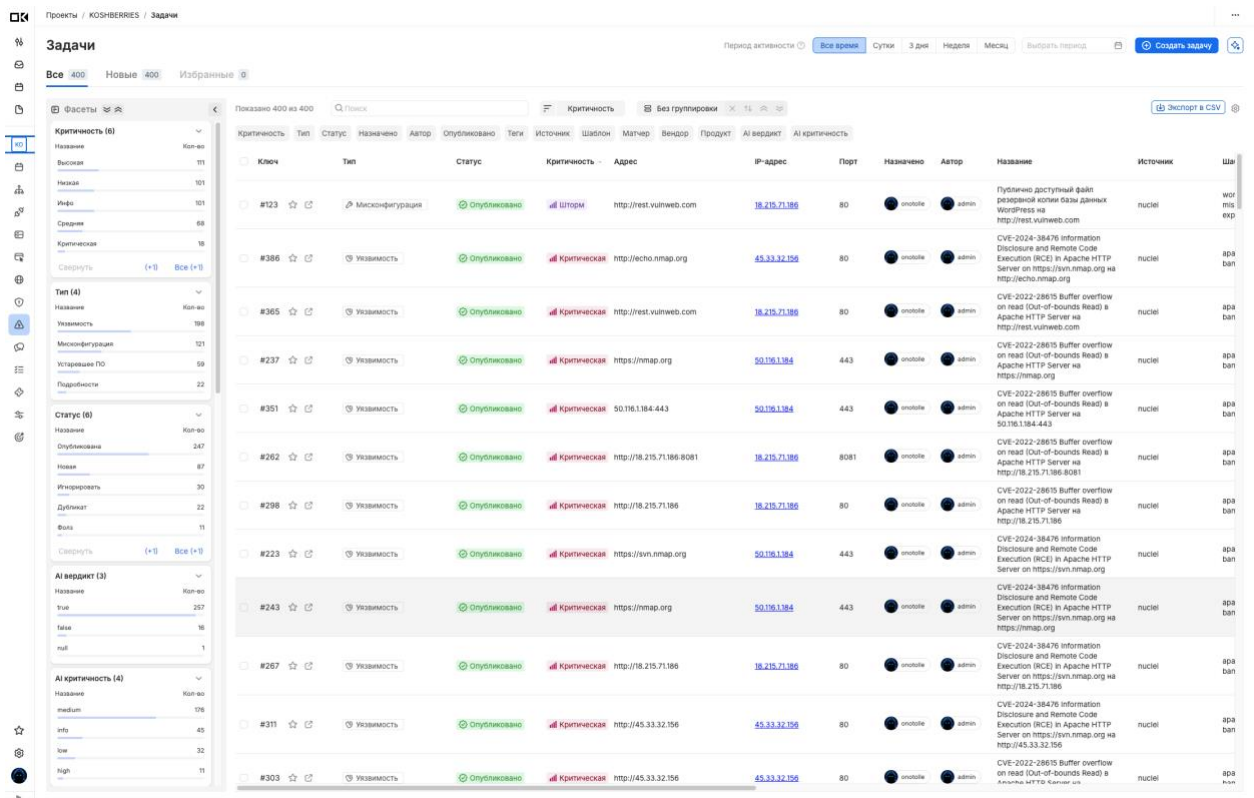


Рисунок 10. Экран задач для экспертов

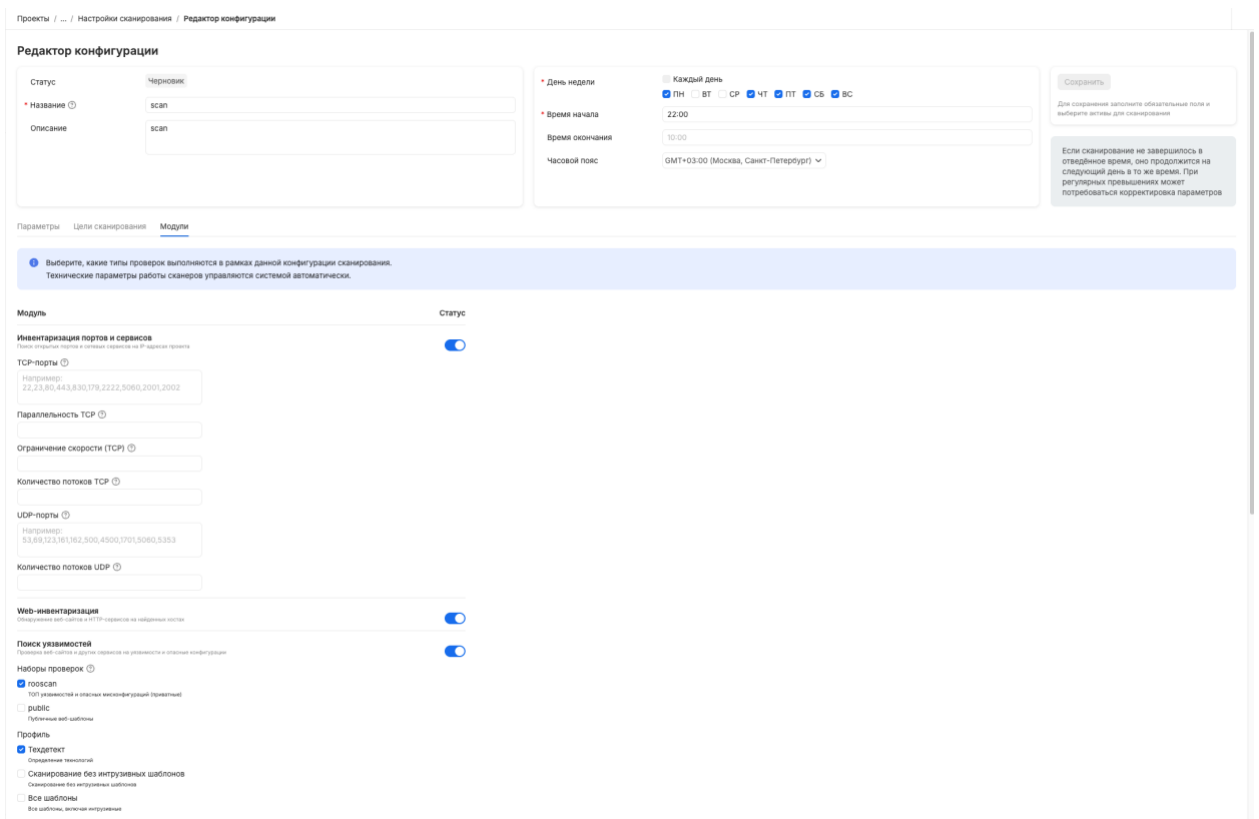


Рисунок 11. Конфигуратор сканирования

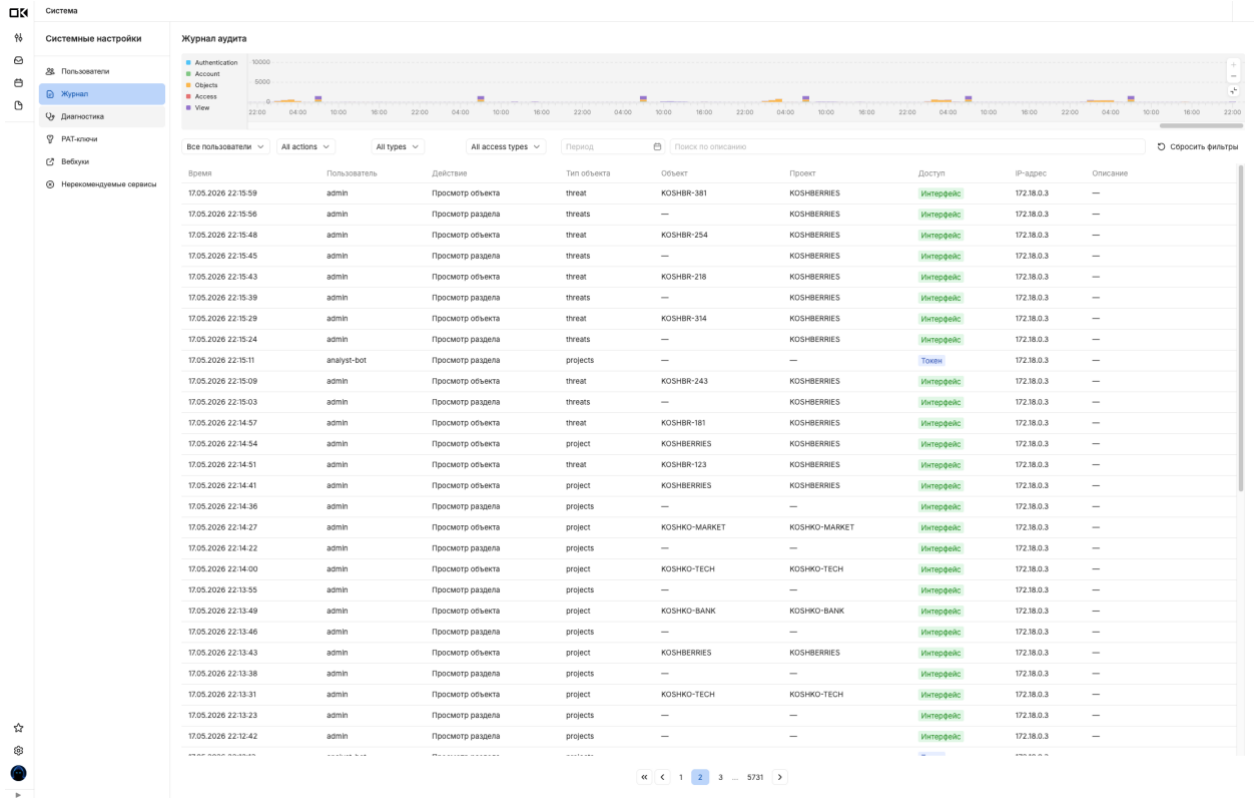


Рисунок 12. Журнал аудита

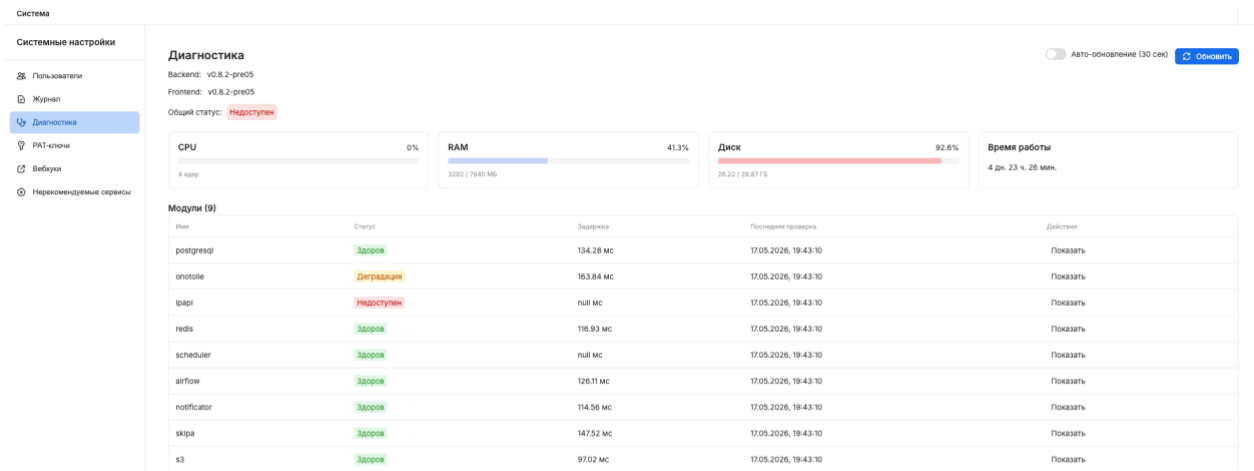


Рисунок 13. Диагностика системы

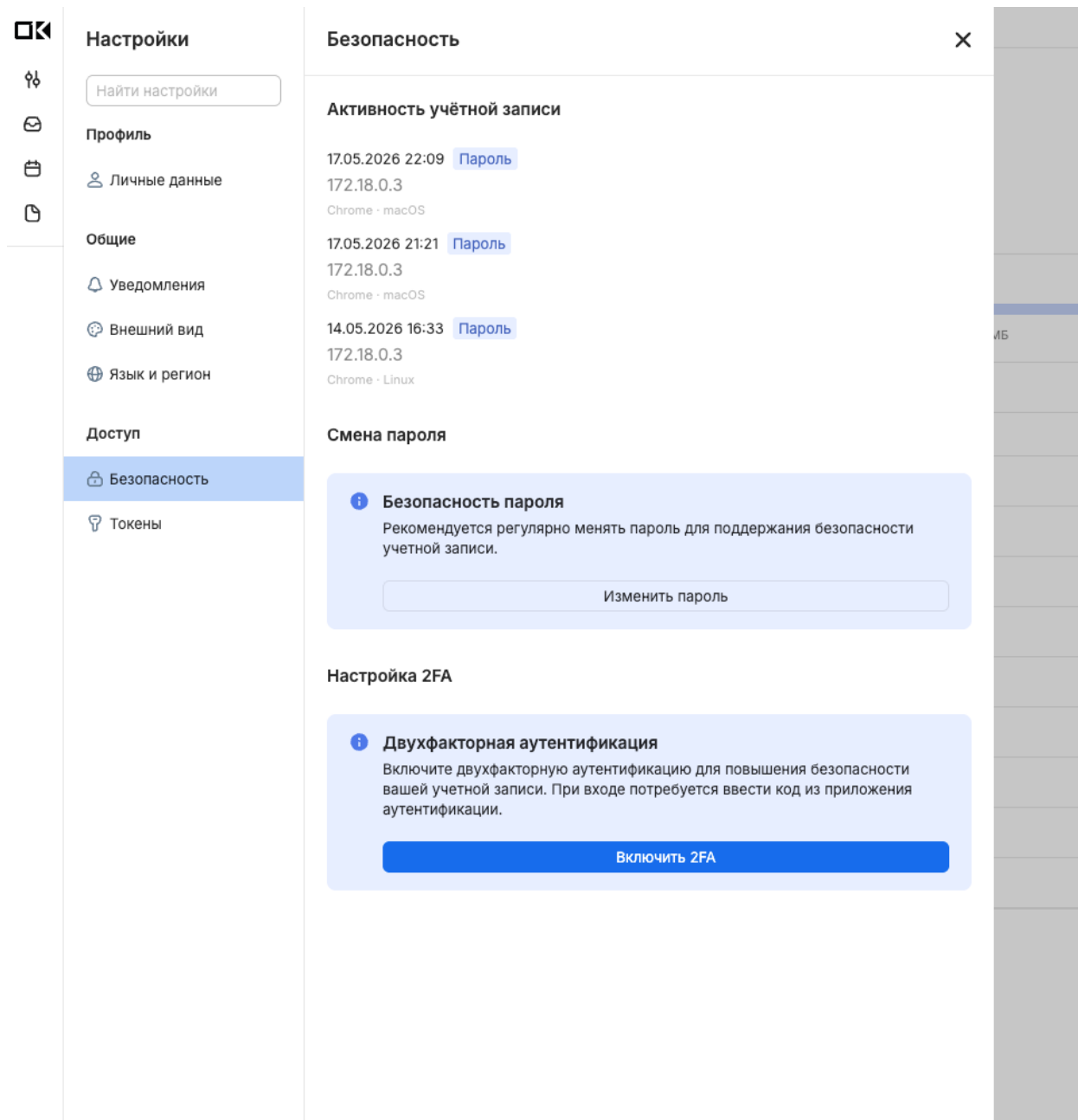


Рисунок 14. Настройки пользователя

АО «Сайбер ОК»
г. Москва, 2026 год

Инструкции в случае развёртывания экземпляра ПО или удалённого доступа к инфраструктуре с развёрнутым экземпляром ПО

«PentOps»

АННОТАЦИЯ

Настоящий документ содержит инструкции для развёртывания программного обеспечения «PentOps» (далее — Система) для случаев:

- удалённого доступа к инфраструктуре с развёрнутым экземпляром ПО;
- развёртывания экземпляра ПО.

ОГЛАВЛЕНИЕ

Аннотация.....	2
Оглавление	3
1 Цели, назначение и области использования системы.....	4
2 Удалённый доступ к инфраструктуре с развёрнутым экземпляром ПО	5
2.1 Импорт образа virtualbox.....	5
2.2 Вход в интерфейс проекта.....	6
2.3 Главная страница веб-интерфейса	7
2.4 Управление активами на сетевом периметре	7
2.4.1 Результаты инвентаризации	8
2.4.2 Угрозы сетевого периметра	10
2.4.3 Инструменты работы с данными	13
3 Развёртывание экземпляра ПО	15
3.1 Локальный запуск	15
3.1.1 Предпосылки.....	15
3.1.2 Запуск проекта посредством Docker Compose.....	16
3.1.3 Первый вход в веб-интерфейс Системы и базовые проверки его функционирования	16
4 Контакты технических специалистов для консультаций	16

1 ЦЕЛИ, НАЗНАЧЕНИЕ И ОБЛАСТИ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ

Цели создания и области применения Системы:

- централизованное планирование и проведение работ по тестированию на проникновение во внешнем периметре заказчика;
- автоматизированная оркестрация и параллельный запуск инструментов определения внешнего сетевого периметра, инвентаризации сетевых сервисов и выявления угроз информационной безопасности на периметре заказчика;
- централизованный сбор, нормализации и хранения результатов работ (артефактов, доказательной базы, отчётов сканеров) с привязкой к активам и проектам;
- управление проектами пентеста, ролями исполнителей, score-документами и взаимодействиями с заказчиками;
- формирование итоговых отчётов (DOCX) по результатам тестирования с привязкой находок к стандартам OWASP, MITRE ATT&CK, PTES и методическим документам ФСТЭК России;
- ведение базы знаний об активах (организации, домены, IP-адреса, FQDN, сети, хосты, сервисы, веб-сайты, идентичности, секреты) с историей состояния.

Внедрение и использование Системы позволит обеспечить выполнение следующих задач:

- поиск, фильтрация, просмотр актуальных данных о состоянии сетевых объектов организации-заказчика с точки зрения наличия угроз информационной безопасности в приложениях и системах;
- оценка уровня защищённости сетевого периметра организации-заказчика.

Система предназначена для следующих ключевых пользователей:

- **Администратор Системы** — сотрудник оператора Системы, обладающий неограниченными полномочиями по действиям в Системе (добавление/блокировка/настройка пользователей Системы, настройка и запуск задач по сбору данных, добавление/редактирование организаций и хостов, настройка справочников);
- **Пользователь-заказчик** — пользователь, имеющий полномочия для просмотра данных связанных с организацией, которую он представляет;
- **Пользователь-эксперт** — пользователь участвующий в сопровождении и подготовке данных о результатах инвентаризации и выявленных угрозах для специалистов организации заказчика.

2 УДАЛЁННЫЙ ДОСТУП К ИНФРАСТРУКТУРЕ С РАЗВЁРНУТЫМ ЭКЗЕМПЛЯРОМ ПО

2.1 Импорт образа virtualbox

2.1.1. Для запуска проекта необходимо скачать следующий образ по ссылке: <https://cloud.mail.ru/public/Yuhf/r4kKLawAT>

После скачивания, указанный образ необходимо импортировать в virtualbox.

После импорта необходимо запустить импортированную виртуальную машину.

2.1.2. Для полного доступа к проекту, необходимо пройти авторизацию.

По умолчанию будет открыт и доступен ssh порт 2222 и ключ private.

Порт 9090 — по 127.0.0.1:9090 откроется на host машинке как раз проект из virtualbox.

Ключ private (приватный ключ ssh для подключения пользователя cybars к виртуальной машине):

-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAA
dzc2gten

NhAAAAAwEAAQAAAYEAscPymiLhZNTr67Mr3Xr6FnM8bzsSdBfm6vZAZfA5szQ1SB0F
nqOz

LZuUG+brJwmkPmbDgyhH7gLy19s1vhVY6IfNdpKN8kcR3y54P1h2vUAFaO6wljkPS3VvNb
P5E/EFeh94UBL9mdXhvR0PVAd4fCvm5cF3fZHwnplanozptUo5IMBXEFfv51rgyk6+v1y9
IDl0A2MMcaKBt543vj+svx8yozAwElrOKns6TT6qqW51NBd0mIRcM4mI4U4GvbVZRD5jN
G

suLlS4rqSsEf07C2MEVUR87UQFiLSKfzWrZivTWRZhL3ob+APJ8p6E88L+NEk0UySZsE9S
KjUUM9LBfZanmXojQjeB9nwDUKYpPgta3AybfPMaTpdj+6BahDZh+HN7Q5OoPH50BXaQ
NG

dBdChkheA3eANEIHZD4dpMHWkapWitmjRs4kjysjpMN7EIoe/SCRCwO9xkAOrj/EBJDCWJ
Xk9lo6sjux6a72/7t70ObXTByrEXAfHI3H5MKEgrAAAFmFOT7b5Tk+2+AAAAB3NzaC1yc2
EAAAGBALHD8poi4WTU6+uzK916+hZzPG87EnQX5ur2QGXwObM0NUgdBZ6jsy2blBvm
6ycJ

pD5mw4MoR+4C8tfbNb4VWOiHzXaSjfJHEd8ueD9Ydr1ABQDusJY5D0t1bzWz+RPxBXofe
F

AS/ZnV4b0dD1QHeHwr5uXBd32R8J6SGp6M6bVKOSDAVxBX7+da4MpOvr9cvZQ5dANjD
HGi

gbeeN74/rL8fMqMwMBJazip7Ok0+qqIudTQXdJiEXDOJiOFoBr21WUQ+YzRrLi5UuK6krB
H9OwtjBFVEfO1EBYi7Cn81q2Yr01kWYS96G/gDyKehPPC/jRJNFMkmbBPUio1FDPSwX2
W

p5l6I0I3gfZ8A1CmKT4LWtwMm3zzGk6XY/ugWoQ2Yfhze0OTqDx+dAV2kDRnQXQoZIXg
N3

gDRCB8w+HaTB1pGqVorZo0bOJI8rI6TDexCKHv0gkXFjvcZADq4/xASQwliV5PZaOrl7se
mu9v+7e9Dm10wcqxFwHxyNx+TChIKwAAAAMBAEAEEAAGAbAPCbmjYpZ0hiXUvt+HSf
6hBfQ

U9I3deiEqre3QH0nx/5GNqBODIavfLCM6K+L/cmlQ9gBaHDSioyPO+GOgHtxuTYO+RNv4Y
isOZjNBEl+lpbKLLLUwyH8NlfQTsuhzs2N6yEQk1ev1Mxpw2yQf2ivd06P5DWAJ6ewL4Ah
Q9TQBjbczTphPmtpX5kS2yPkrP7qzk3fXoReoKAZtHHEMfo511WosuqxNwlwj784qULf4f
sapJ0ovIZk0MrJG4XKeNSDB1+u1Cn1UHw2bgWB7YELbChC5vIr3kA2JiFDgHgn2n2D72W
Q

aQCajzpm9DrqtoYyZ1QPIbLnjs1MtCbWFExhN6MVk7e2O0aEnIJGCH8UGRWshA9QWZfB
Ap

RTWD2bcvalpVyVkIRrapSY5wNBsoG62XBt4OJQpb25u1KZlibRBUpy6iou7qFqDzwo5J15

```
PQzsvOdYVRwvEEPkwjtSwWem5EnUCMqobTT3TGHU0xdCWPvrreN72tjOnMNIQO/ke5A
AAA
wQDLR+Kj9B6BATfsH46pF2LkNN3TskNuc1selFt0i/uk7SFpQD1jIXzZDKHK7KjmHnEFe9
y4Fn9CZHKBPWSRTBsgMvTOQ05igYK6StzeYXFomEAfWQMSr2JQQRKRitSY4A1vVgX
3pHpM
X+N4hLEGP06is5G+GYTYjDW7qecRWSf6qb4cJQ2P1YDTwauN+JEH4uCm0mFBLRdWM
nA5L
1zyrhrLOkR7AFF9d1ApgWWnn92UNenPev3gA3IcLVWk7eIHQ8AAADBAObJQJQmOpGT
nzKi
6CvYbY9PSGB1JwWgjEmLJN3jpqo9kjhYTE7bcm9wKZbk5uJMhxJSqQ/m2mhjMPnEQgWL
dL
oYfqApcJBom3Gd4sVj4ae+hlXvVyo1fGMTgNQ7kp0vR8FLauzVgWwBt5HPMsFvNU5sosdE
VMwxTolltg5xIjnAYAYPcWEQhCAvyImOo6nS8yV3QDA9sCJ4QdMOX+j2b3YLqG3/Db61
RW
hq/f+Falr1pfKRkKrUAiUtKDwVjHymVQAAAMEAxS/IumfQLGwJLF4OaSkQV5xeRhx/veU
1
fBLF+of5VK750klKfT5u3CoHVGQ/5e7hfcQNUITOW2JSDx7UA23WVzQo2srLEvEE+4CtCr
TxWOukJCpT8IHNNPPYlMjVqdDWZQYsWM1hHUrFvC242TMPZ14lQ4hXNdVFNEDcyp
2oKdk
+tG3LnIzq/6hkDUSBi8l9JKUQgwjx/b7yNEcCroizyQJfOGEOCVQAtZvvFKrpmQqVEANOs
SvAX4v7ilx5rR/AAAAH21ha3NpbUBNYWNCb29rLVByby1NYWtzaW0ubG9jYWwBAgM=
-----END OPENSSH PRIVATE KEY-----
```

2.1.3. Для входа по ssh используем либо cybars — пользователь и ssh-ключ который прилагается выше или по логин:паролю cybars:cybars

2.2 Вход в интерфейс проекта

Для каждого компании-пользователя выделяется отдельный URL в домене <https://pentops.cyberok.ru>, например <https://demo.pentops.cyberok.ru>.

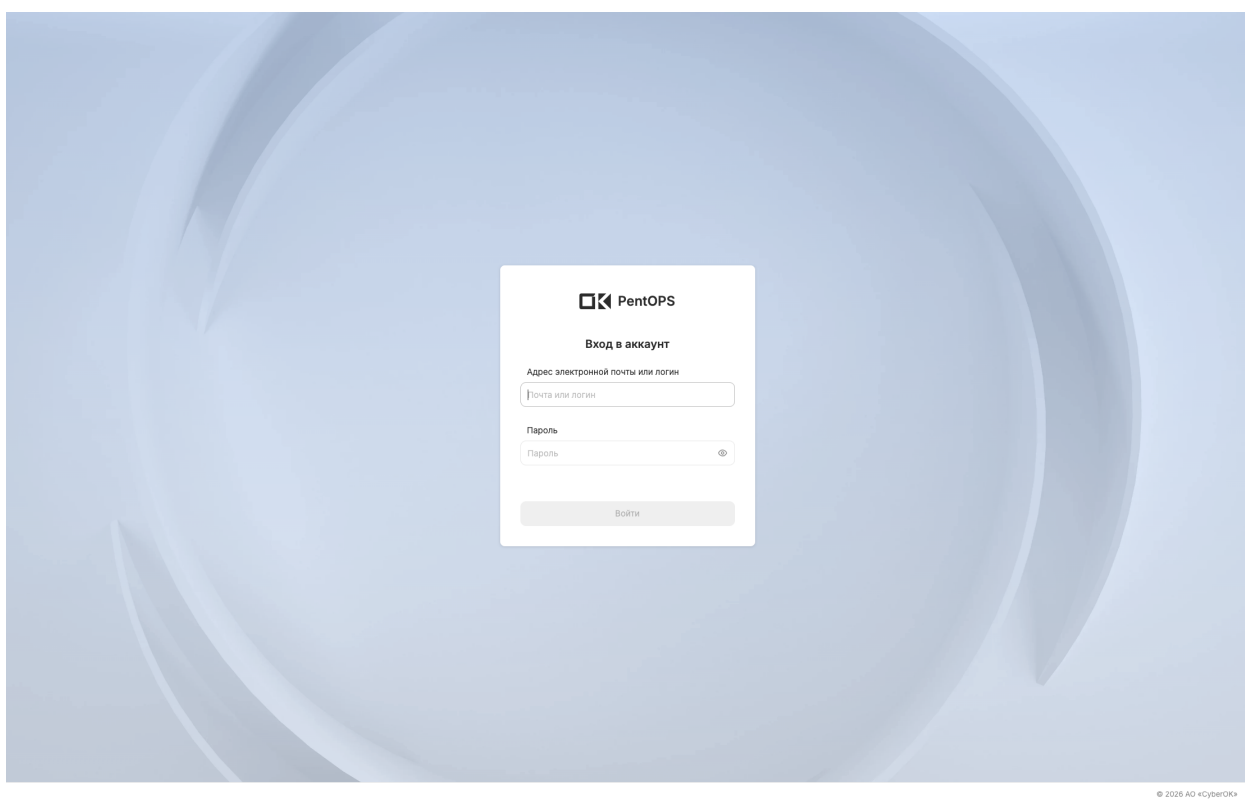


Рисунок 1. Окно ввода логина и пароля

В поле «Имя пользователя» необходимо ввести «admin» (обратите внимание, что ввод чувствителен к регистру, вводите логин маленькими буквами). В поле «Пароль» необходимо ввести «admin». Нажать кнопку «Войти». Пользователю отображается главная страница интерфейса.

2.3 Главная страница веб-интерфейса

Стартовая страница веб-интерфейса позволяет просмотреть список всех проектов, к которым у пользователя есть доступ. Отображаются избранные проекты, последние просмотренные. По каждому проекту демонстрируется краткая сводка в виде индекса безопасности проекта и распределения угроз по уровню критичности.

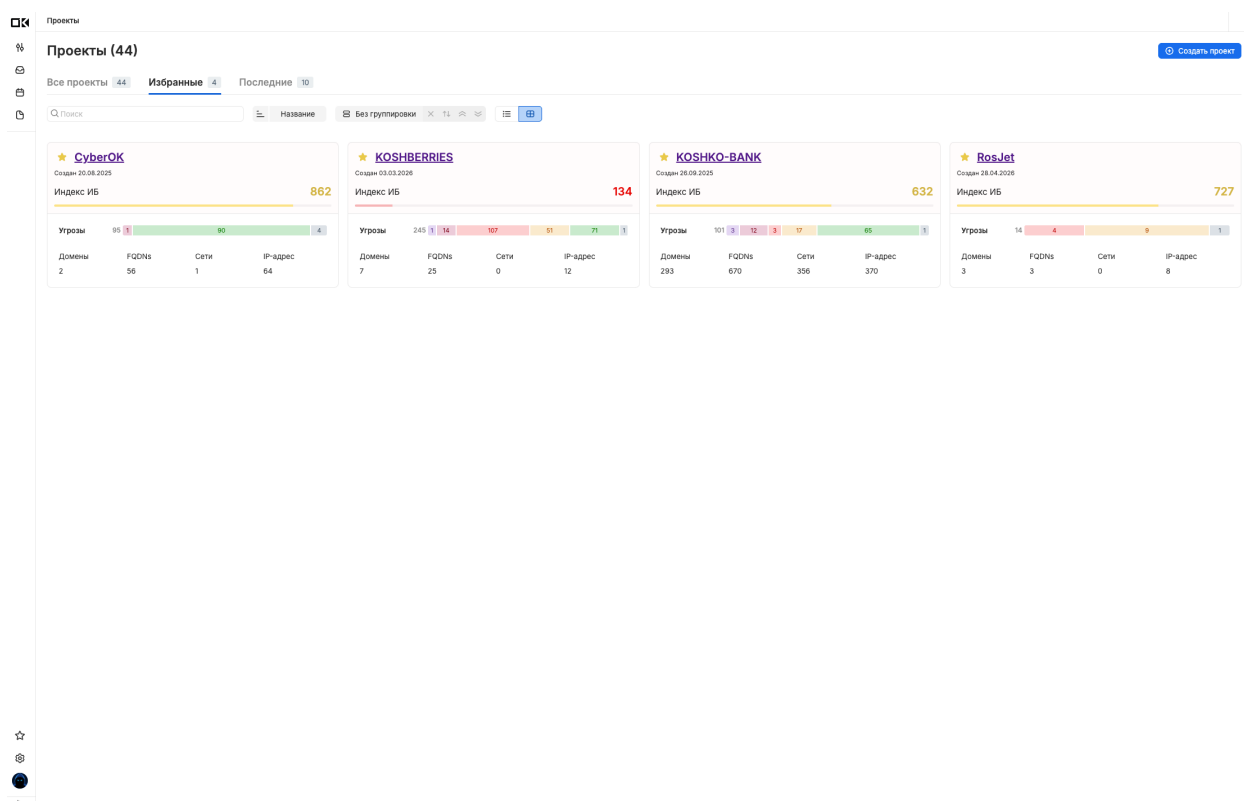


Рисунок 2. Главный экран веб-интерфейса

2.4 Управление активами на сетевом периметре

Для определения границ сетевого периметра организации используется раздел “Активы”

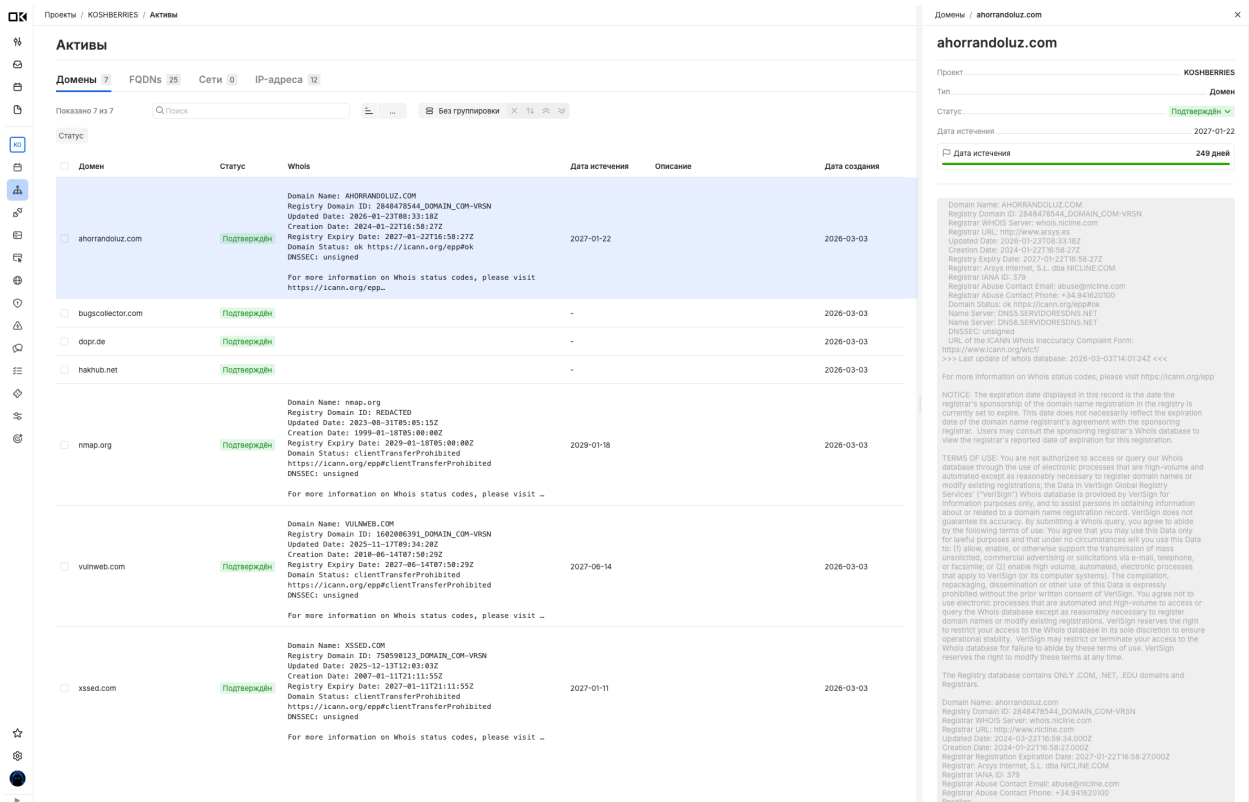


Рисунок 3. Экран со списком активов

Пользователь может управлять такими активами как Domain, FQDN, Network, IP (v4 и v6).

2.4.1 Результаты инвентаризации

Результаты инвентаризации можно изучать в трех разделах – сервисы, хосты, веб-сайты и сертификаты.

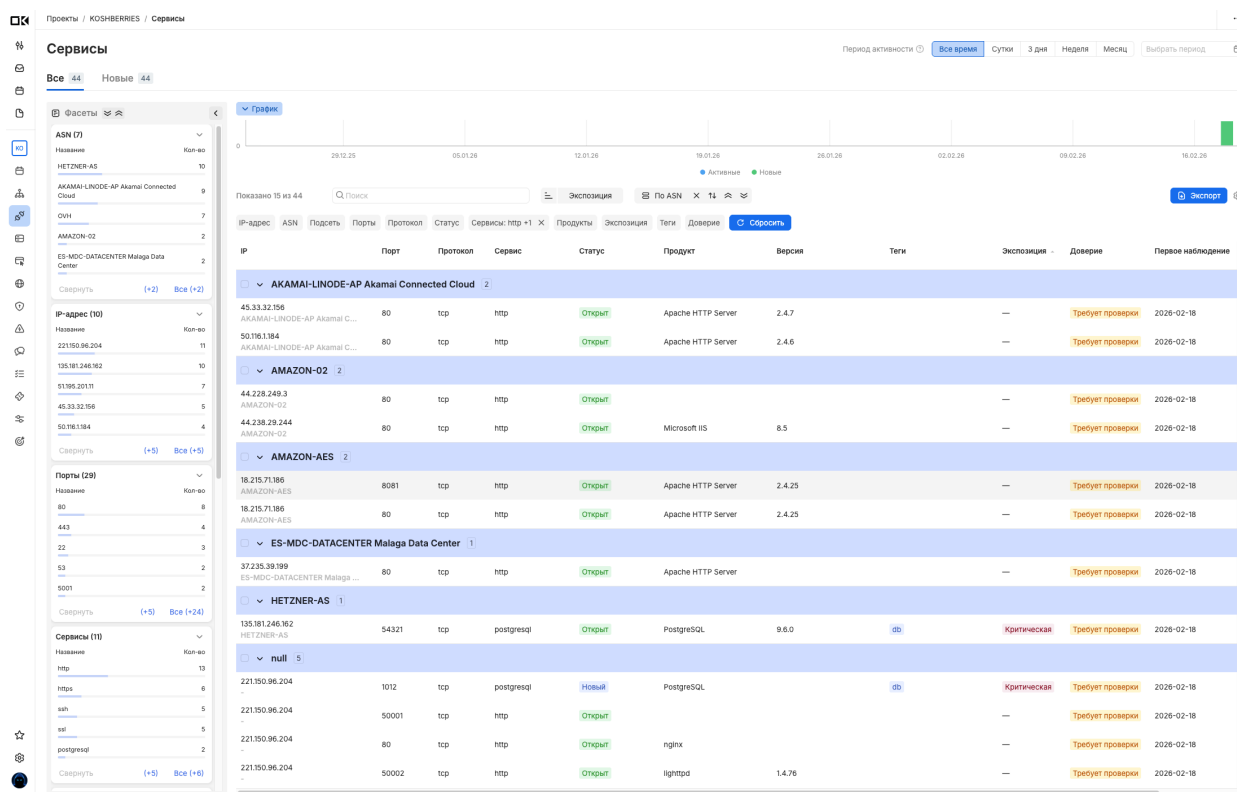


Рисунок 5. Экран с идентифицированными сервисами

Система предоставляет инструменты для инспектирования результатов инвентаризации сетевого периметра в виде списков сервисов, хостов и веб-ресурсов. Типовой раздел предоставляет инструменты группировки, фильтрации, получения детальной информации и карточки инвентаризационного объекта. Состояние фильтров и группировок запоминается для пользователя. Пользователь имеет возможность выгрузки объектов системы в `xlsx` или `csv` формате согласно примененным фильтрам. Для повышения ориентированности во времени – пользователю предоставляется инструмент для работы с временными срезами, где он может выбрать только объекты актуальные на указанный диапазон времени.

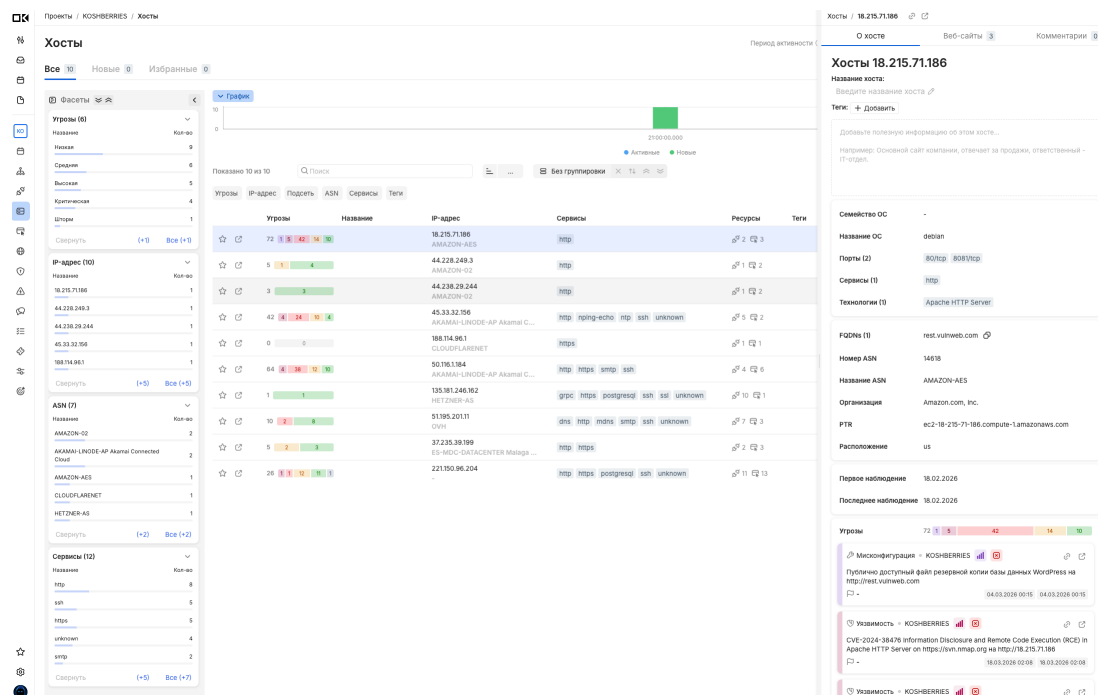


Рисунок 6. Экран с идентифицированными хостами

Веб-сайты также имеют режим просмотра списка в виде галереи:

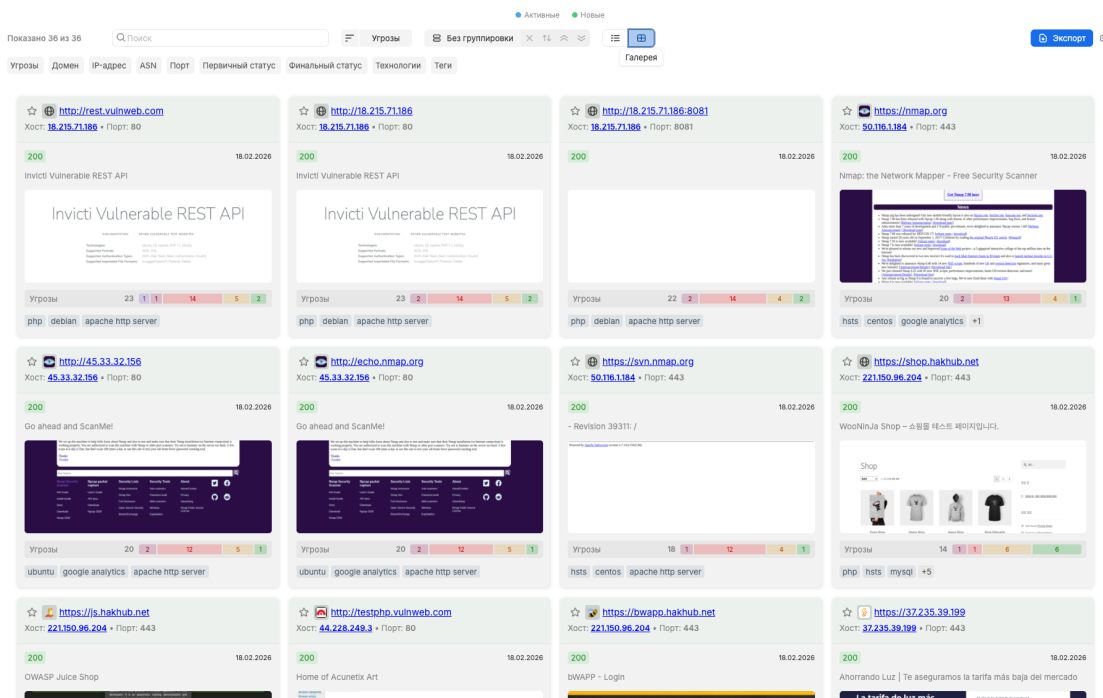


Рисунок 7. Экран с идентифицированными веб-сайтами в режиме галереи

2.4.2 Угрозы сетевого периметра

Пользователю предоставляется штатный механизм фильтрации и группировки угроз. У угроз есть жизненный цикл, который может управляться пользователем:

- Новая
- Исправленная
- Актуальная
- Повторно-обнаруженная
- Ложное срабатывание
- Риск принят

Для удобства угрозы имеют разные типы:

- Уязвимость
- Устаревшее ПО
- Мiskonфигурация
- Раскрытие информации

В качестве оценки критичности угрозы используется шкала со следующими значениями:

- Шторм (максимальная критичность, угроза несет максимальные риски для организации, подлежит немедленному устранению)
- Критическая
- Высока
- Средняя
- Низкая
- Инфо

Угрозы могут быть определены крайние сроки для устранения. Правила расчета крайних сроков устранения указываются в разделе политик. Правила могут полагаться на уровень критичности, тип угрозы и сетевые атрибуты объекта, где угроза была выявлена.

Проекты / KOSHBERRIES / Угрозы											
Угрозы (248)											
Показано 248 из 248											
Критичность Тип Статус Метод выявления Теги IP-адрес Адрес Идентификатор											
ID	Название	Адрес	IP-адрес	Порт	Срок устранения	Теги	Идентификатор	CWE ID	Дата		
#123	Публично доступный файл резервной копии баз данных WordPress на http://rest.vulnweb.com	http://rest.vulnweb.com	18.215.71.186	80	-	Не устранена	-	-	2026-		
#365	CVE-2022-28615 Buffer overflow on read (Out-of-bounds Read) в Apache HTTP Server на https://svn.nmap.org	https://svn.nmap.org	50.196.1.184	443	-	Устранена	CVE-2022-28615	-	2026-		
#220	CVE-2022-28615 Buffer overflow on read (Out-of-bounds Read) в Apache HTTP Server на https://svn.nmap.org	https://svn.nmap.org	50.196.1.184	443	-	Устранена	CVE-2022-28615	-	2026-		
#349	CVE-2024-38476 Information Disclosure and Remote Code Execution (RCE) в Apache HTTP Server на https://svn.nmap.org на 50.196.1.184:443	https://svn.nmap.org на 50.196.1.184:443	50.196.1.184	443	-	Устранена	CVE-2024-38476	-	2026-		
#243	CVE-2024-38476 Information Disclosure and Remote Code Execution (RCE) в Apache HTTP Server на https://svn.nmap.org на https://nmap.org	https://nmap.org	50.196.1.184	443	-	Не устранена	CVE-2024-38476	-	2026-		
#267	CVE-2024-38476 Information Disclosure and Remote Code Execution (RCE) в Apache HTTP Server на https://svn.nmap.org на http://18.215.71.186	http://18.215.71.186	18.215.71.186	80	-	Не устранена	CVE-2024-38476	-	2026-		
#351	CVE-2022-28615 Buffer overflow on read (Out-of-bounds Read) в Apache HTTP Server на 50.196.1.184:443	50.196.1.184:443	50.196.1.184	443	-	Не устранена	CVE-2022-28615	-	2026-		
#311	CVE-2024-38476 Information Disclosure and Remote Code Execution (RCE) в Apache HTTP Server на https://svn.nmap.org на http://45.33.32.156	http://45.33.32.156	45.33.32.156	80	-	Не устранена	CVE-2024-38476	-	2026-		
#389	CVE-2022-28615 Buffer overflow on read (Out-of-bounds Read) в Apache HTTP Server на http://echo.nmap.org	http://echo.nmap.org	45.33.32.156	80	-	Не устранена	CVE-2022-28615	-	2026-		
#262	CVE-2022-28615 Buffer overflow on read (Out-of-bounds Read) в Apache HTTP Server на http://18.215.71.186:8081	http://18.215.71.186:8081	18.215.71.186	8081	-	Не устранена	CVE-2022-28615	-	2026-		
#277	CVE-2024-38476 Information Disclosure and Remote Code Execution (RCE) в Apache HTTP Server на https://svn.nmap.org на http://18.215.71.186:8081	http://18.215.71.186:8081	18.215.71.186	8081	-	Не устранена	CVE-2024-38476	-	2026-		
#298	CVE-2022-28615 Buffer overflow on read (Out-of-bounds Read) в Apache HTTP Server на http://18.215.71.186	http://18.215.71.186	18.215.71.186	80	-	Не устранена	CVE-2022-28615	-	2026-		

Рисунок 8. Таблица угроз

Для более детальной информации пользователю предоставляется отдельная карточка с угрозой:

← Назад

Перепроверить

Скачать отчет

CVE-2024-38476 Information Disclosure and Remote Code Execution (RCE) in Apache HTTP Server on https://svn.nmap.org на http://45.33.32.156

Опубликовано: 18.03.2026 (2 месяца назад) Метод выявления: Авто

Тип: Уязвимость Критичность: Критическая Статус: Не устранена

Теги: + Добавить

The vulnerability in the core of Apache HTTP Server versions prior to 2.4.59 allows an attacker to execute remote code, disclose confidential information, or perform a **Server-Side Request Forgery (SSRF)** attack by manipulating response headers from application servers. The issue arises from improper handling of response headers from backend applications, which can be used to trigger local handlers via internal redirects. An attacker can craft specially formatted response headers that, when processed by the vulnerable server, lead to execution of arbitrary code at the web server level or leakage of confidential data.

Подробности Комментарии

Эксплуатация

Проверка выполняется путем отправки HTTP-запроса к корневому пути и анализа заголовка `Server` в ответе.

В заголовке `Server` обнаружена строка `Apache/2.4.7 (Ubuntu)`, указывающая на версию сервера.

cURL-команда для верификации:

```
curl -s -I -H 'User-Agent: Mozilla/5.0 (compatible; CyberKInspect/1.0; <https://www.cyberok.ru/policy.html>' 'http://45.33.32.156'
```

На скриншоте ниже показан заголовок `Server` с версией 2.4.7.

```
$ curl -sS --connect-timeout 8 --max-time 15 -k -L -H 'User-Agent: Mozilla/5.0 (compatible; CyberKInspect/1.0; <https://www.cyberok.ru/policy.html>' 'http://45.33.32.156' | grep -i -C 2 'Server:'
--- stdout ---
--- stderr ---

$ curl -sS --connect-timeout 8 --max-time 15 -k -L -H 'User-Agent: Mozilla/5.0 (compatible; CyberKInspect/1.0; <https://www.cyberok.ru/policy.html>' 'http://45.33.32.156' | grep -i -C 2 'Server:'
--- stdout ---
--- stderr ---
```

Рекомендации по устранению

- Update Apache HTTP Server to version 2.4.68 or later.
- Apply official security patches provided by the Apache project.
- Restrict access to application servers that could be used as sources of malicious headers.
- Implement validation and sanitization of response headers from backend applications at the Apache configuration level.

Ссылки на источники 4

<https://blog.orange.tw/posts/2024-08-confusion-attacks-en/>

<https://nvd.nist.gov/vuln/detail/CVE-2024-38476>

https://hwd.apache.org/security/vulnerabilities_24.html

<https://access.redhat.com/security/cve/cve-2024-38476>

CVSSv3 9.8

EPSS -

45.33.32.156

http://45.33.32.156

Идентификатор CVE-2024-38476

Вендор apache

Продукт http_server

IP-адрес 45.33.32.156

Порт 80

Протокол tcp

Адрес http://45.33.32.156

Задача KOSHBR-311

Первое наблюдение 18.03.2026

Последнее наблюдение 18.03.2026

Хронология 60 дней

Новая 18.03.2026 02:08 (80 дней)

Рисунок 8. Карточка угрозы

2.4.3 Инструменты работы с данными

Для удобства взаимодействия с информацией сервиса пользователю предоставляются такие инструменты как дашборд, календарь, конфигуратор отчетов и конфигуратор сканирования.

Раздел дашборда проекта содержит сводную информацию о состоянии сетевого периметра организации. Основными элементами этого раздела является индекс безопасности, распределение актуальных угроз по уровню критичности, по типам и состоянию. Отображаются последние угрозы, последние закрытые угрозы, угрозы у которых подходит к концу время устранения. Отображаются топ 5 уязвимых хостов и веб-ресурсов.

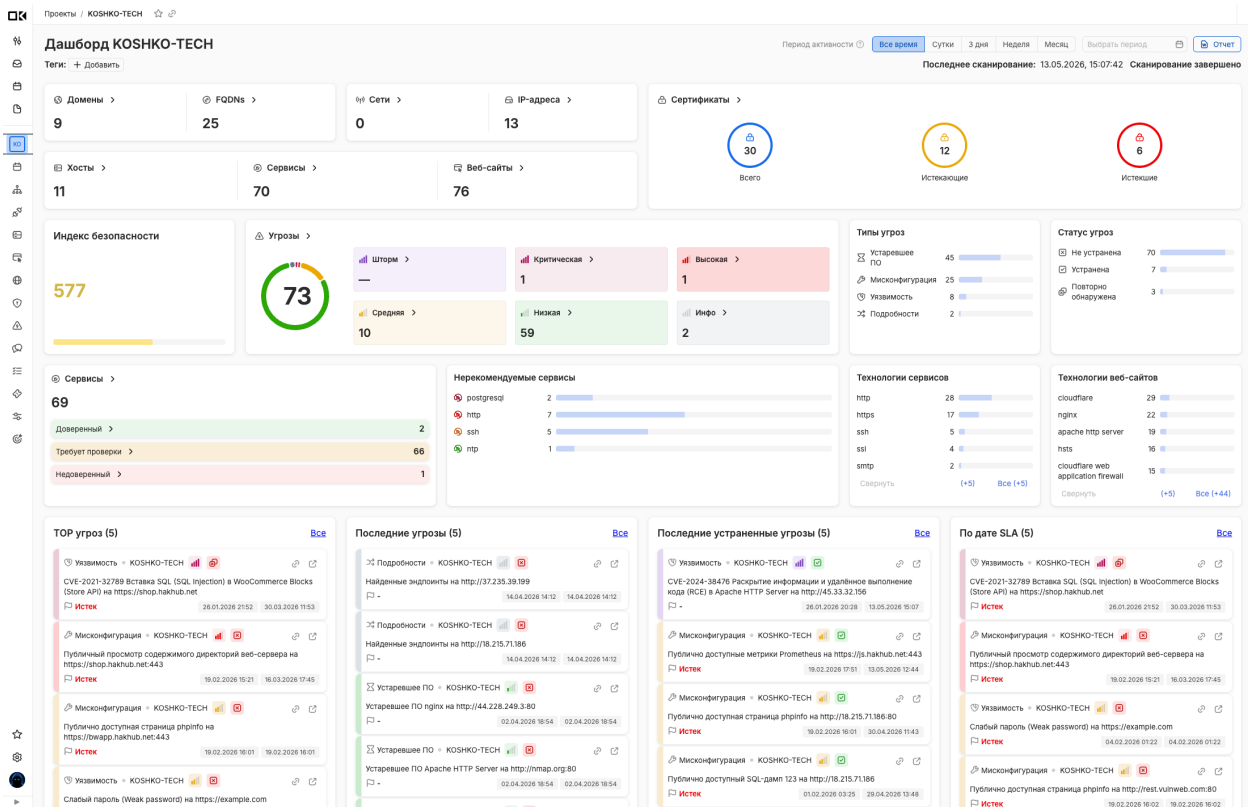


Рисунок 9. Экран со сводной информацией о проекте

Раздел календаря проекта(ов) позволяет отобразить все события организации в сервисе PentOps в календарном представлении. Пользователь может изучить периоды сканирования, время фиксации угроз, окончания доменных имен и сертификатов в срезах дневного, недельного, месячного и годового представления.

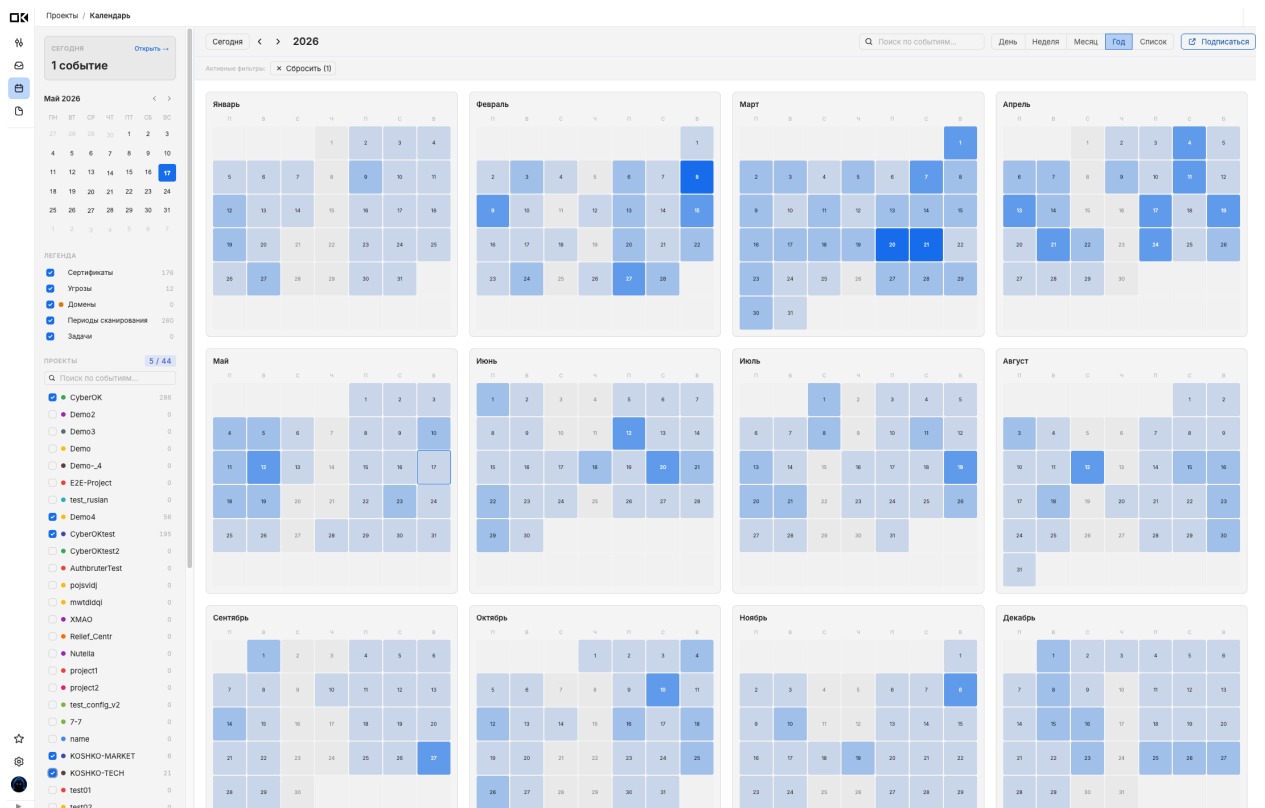


Рисунок 10. Календарь событий

Раздел конфигурации отчетных материалов позволяет сконструировать необходимый отчет в офисном формате, указывая какие блоки информации должен этот отчет включать. Для удобства пользователя предоставляются предопределенные форматы отчетов.

The screenshot shows the 'Конструктор отчетов' (Report Builder) interface. On the left, there is a sidebar with 'Быстрые пресеты' (Quick Presets) and a list of report types. The main area is divided into several sections: 'Параметры отчета' (Report Parameters) with fields for 'Проекты' (Projects) and 'Формат' (Format); 'Разделы отчета' (Report Sections) with a list of sections and their visibility; and 'Параметры раздела' (Section Parameters) with detailed filters for 'Статус' (Status), 'Критичность' (Criticality), 'Тип угрозы' (Threat Type), and 'SLA'. On the right, there is a 'Запуск формирования' (Start Forming) button and a 'Добавить' (Add) button.

Рисунок 12. Карточка организации

Раздел конфигурации сканирований предоставляет пользователю возможность указать периоды и глубину, с которой будет производиться сканирование сетевого периметра. Пользователь может определить те модули, которые будут задействованы в процессах инвентаризации сетевых сервисов и инструменты, которые будут использоваться для активного анализа защищенности сетевого периметра.

The screenshot shows the 'Redactor configuration' (Редактор конфигурации) interface. At the top, there's a breadcrumb: 'Проекты / ... / Настройки сканирования / Редактор конфигурации'. The main area is divided into two columns. The left column contains a 'Статус' (Status) dropdown set to 'Черновик' (Draft), a 'Название' (Name) field with 'scan', and an 'Описание' (Description) field with 'scan'. The right column contains a 'День недели' (Day of the week) section with a 'Каждый день' (Every day) radio button and a list of days (ПН, ВТ, СР, ЧТ, ПТ, СБ, ВС) where ПН, ЧТ, ПТ, and СБ are selected. Below this are fields for 'Время начала' (Start time) set to 22:00, 'Время окончания' (End time) set to 10:00, and a 'Часовой пояс' (Time zone) dropdown set to GMT+03:00 (Москва, Санкт-Петербург). A 'Сохранить' (Save) button is in the top right. A note below it says: 'Для сохранения заполните обязательные поля и выберите активы для сканирования.' Another note at the bottom right says: 'Если сканирование не завершилось в отведенное время, оно продолжится на следующий день в то же время. При регулярных превышениях может потребоваться корректировка параметров.' Below the configuration fields, there's a tabbed interface with 'Параметры' (Parameters), 'Цели сканирования' (Scanning targets), and 'Модули' (Modules) selected. A blue banner says: 'Выберите, какие типы проверок выполняются в рамках данной конфигурации сканирования. Технические параметры работы сканеров управляются системой автоматически.' The 'Модули' section has a table with 'Модуль' (Module) and 'Статус' (Status) columns. The first module is 'Инвентаризация портов и сервисов' (Port and service inventory), which is enabled. It has sub-sections for 'TCP-порты' (TCP ports) and 'UDP-порты' (UDP ports), each with a 'Например:' (For example:) field containing a list of ports. Below these are fields for 'Параллельность TCP' (TCP parallelism), 'Ограничение скорости (TCP)' (TCP speed limit), and 'Количество потоков TCP' (Number of TCP flows). The second module is 'Web-инвентаризация' (Web inventory), which is also enabled. It has a sub-section 'Поиск уязвимостей' (Vulnerability search), which is enabled. Below it are 'Наборы проверок' (Check sets) with 'goosecan' selected, and 'Профиль' (Profile) with 'Техдетект' (Techdetect) selected. There are also checkboxes for 'рублик' (ruble), 'Публичный веб-шаблон' (Public web template), 'Сканирование без интрузивных шаблонов' (Scanning without intrusive templates), 'Все шаблоны' (All templates), and 'Все шаблоны, включая интрузивные' (All templates, including intrusive).

Рисунок 13. Конструктор конфигурации сканирования

3 РАЗВЁРТЫВАНИЕ ЭКЗЕМПЛЯРА ПО

3.1 Локальный запуск

3.1.1 Предпосылки

- [docker-ce](#) — установка Docker Engine, поддерживаемые платформы Linux, macOS, Windows 10
- [docker-compose](#)

Пример: Ubuntu 22.4

```
sudo apt update
```

```
sudo apt install curl git
```

```
#git clone https://cyberok.gitlab.yandexcloud.net/blueteam/pentops-deploy
```

```
# docker
curl -fsSL https://get.docker.com -o get-docker.sh
sudo sh get-docker.sh
```

3.1.2 Запуск проекта посредством Docker Compose

Иметь доступ к внутреннему репозиторию `cyberok.gitlab.yandexcloud.net` и быть аутентифицированным в нем.

Развернуть пакет `pentops-deploy` в папке `/opt` выбранного сервера

```
# cd /opt
# git clone https://cyberok.gitlab.yandexcloud.net/blueteam/pentops-deploy
# cd pentops-deploy
# scripts/cybars-start.sh prod
# docker exec -ti cybars-api sh
Docker> python manage.py set-user-password -u admin -p
Docker>exit
```

3.1.2.1 Остановка сервисов

```
# scripts/cybars-stop.sh prod
```

3.1.3 Первый вход в веб-интерфейс Системы и базовые проверки его функционирования

Для входа в веб-приложение откройте <http://localhost:8080> в браузере. Для входа используется пара логин `admin` и пароль, который был установлен при первом запуске проекта.

4 КОНТАКТЫ ТЕХНИЧЕСКИХ СПЕЦИАЛИСТОВ ДЛЯ КОНСУЛЬТАЦИЙ

Контакты технических специалистов, которые смогут проконсультировать по процессу развёртывания и настройки экземпляра ПО и его функционирования:

Александр Рудаков:

- Контактный телефон: +7 (977) 444-23-78
- Контактный e-mail: aleksandr.rudakov@cyberok.ru