Нейроинформ

Документация, содержащая описание функциональных характеристик ПО

Содержание

1. Введение
2. Основные задачи
3. Функциональные характеристики ПО
4. Затрачиваемые ресурсы и требования
5. Используемые технологические инструменты
6. Выходные данные
7. Взаимодействие с экспертами

1. Введение

Нейроинформ — это программное обеспечение, разработанное для комплексного анализа инфраструктуры компании с целью выявления и предотвращения потенциальных угроз безопасности. ПО позволяет автоматически выявлять уязвимости, оценивать общий уровень безопасности и предоставлять рекомендации для минимизации рисков.

2. Основные задачи

Нейроинформ решает следующие задачи:

- Выявление уязвимостей и слабых мест в инфраструктуре компании;
- Мониторинг изменений в сетевой среде для своевременного обнаружения потенциальных угроз;
- Оценка уровня безопасности с точки зрения возможного несанкционированного доступа;
- Предоставление экспертных рекомендаций для улучшения защиты инфраструктуры.

3. Функциональные характеристики ПО

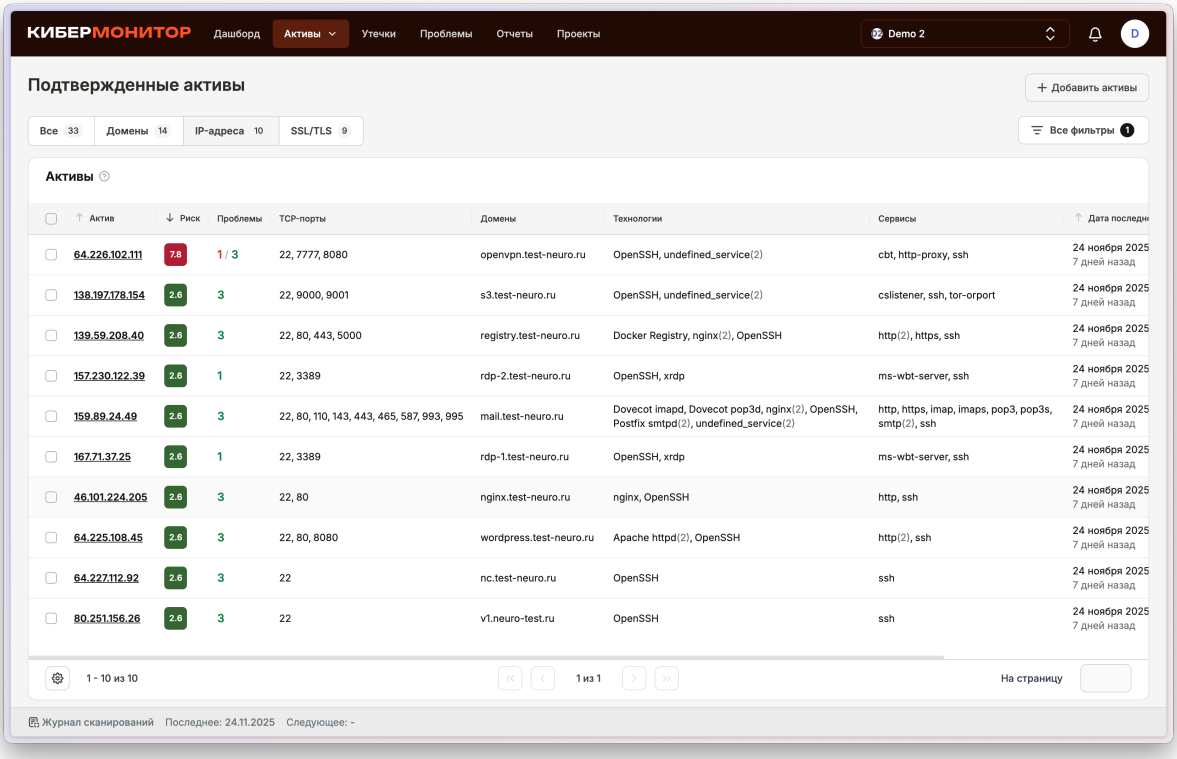
Сканирование периметра

Нейроинформ проводит анализ внешнего периметра компании. Внешнее сканирование помогает выявить потенциальные точки входа для злоумышленников, включая открытые порты, ненадежные службы и устаревшие системы.

Ресурсы: сканирование требует наличия выделенного сервера с доступом к сетевым сегментам, которые необходимо анализировать.

Выходные данные: список обнаруженных уязвимостей, открытых портов и активных служб с указанием их критичности.

Перечисление портов и служб



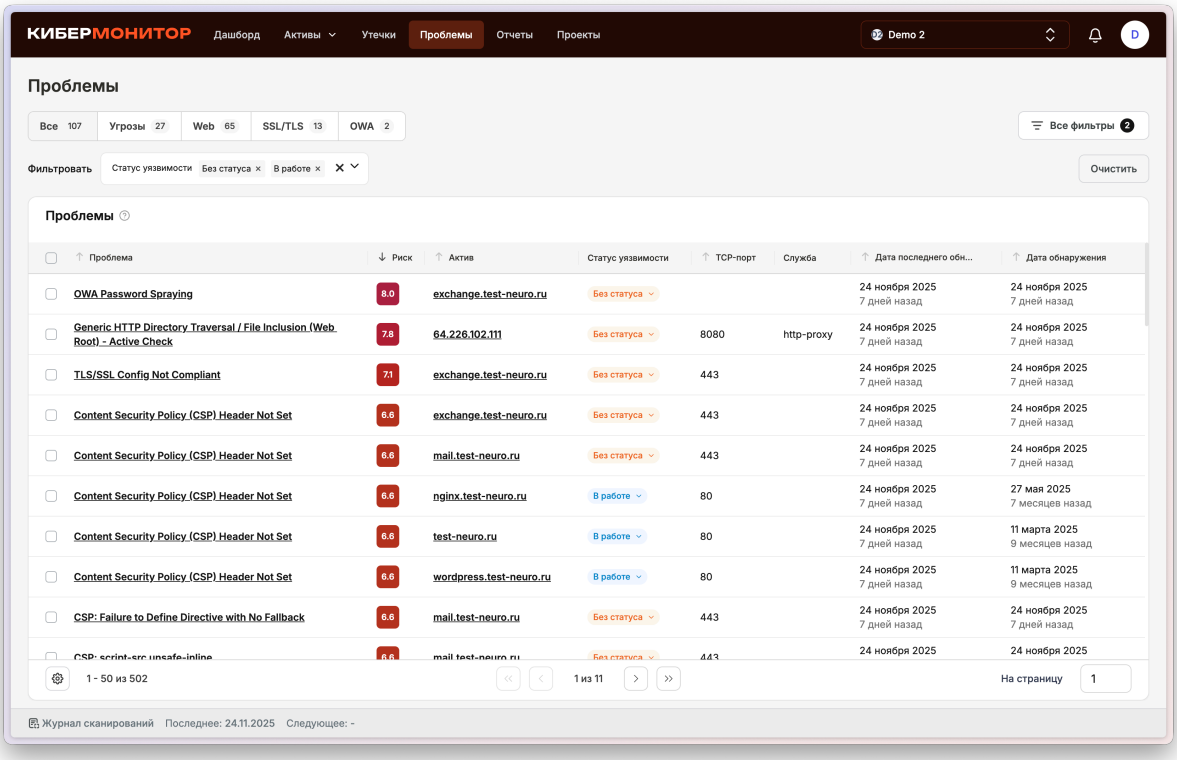
ПО выполняет анализ активных портов и служб на устройствах сети компании. Это позволяет выявить ненужные или потенциально опасные службы, которые могут быть использованы злоумышленниками.

Ресурсы: для выполнения этой задачи требуется доступ к сканируемым устройствам через соответствующие протоколы.

Выходные данные: перечень активных портов и служб, а также их текущего состояния (например, открытые).

Выявление проблем и поиск уязвимостей

Нейроинформ использует базы данных уязвимостей и анализирует состояние инфраструктуры для выявления проблемных мест, таких как устаревшее ПО, слабые пароли, уязвимости в конфигурации систем.



Ресурсы: ПО требует регулярного обновления базы данных уязвимостей для обеспечения актуальности обнаруживаемых угроз.

Выходные данные: список уязвимостей с оценкой риска и рекомендациями по их устранению.

Мониторинг изменений

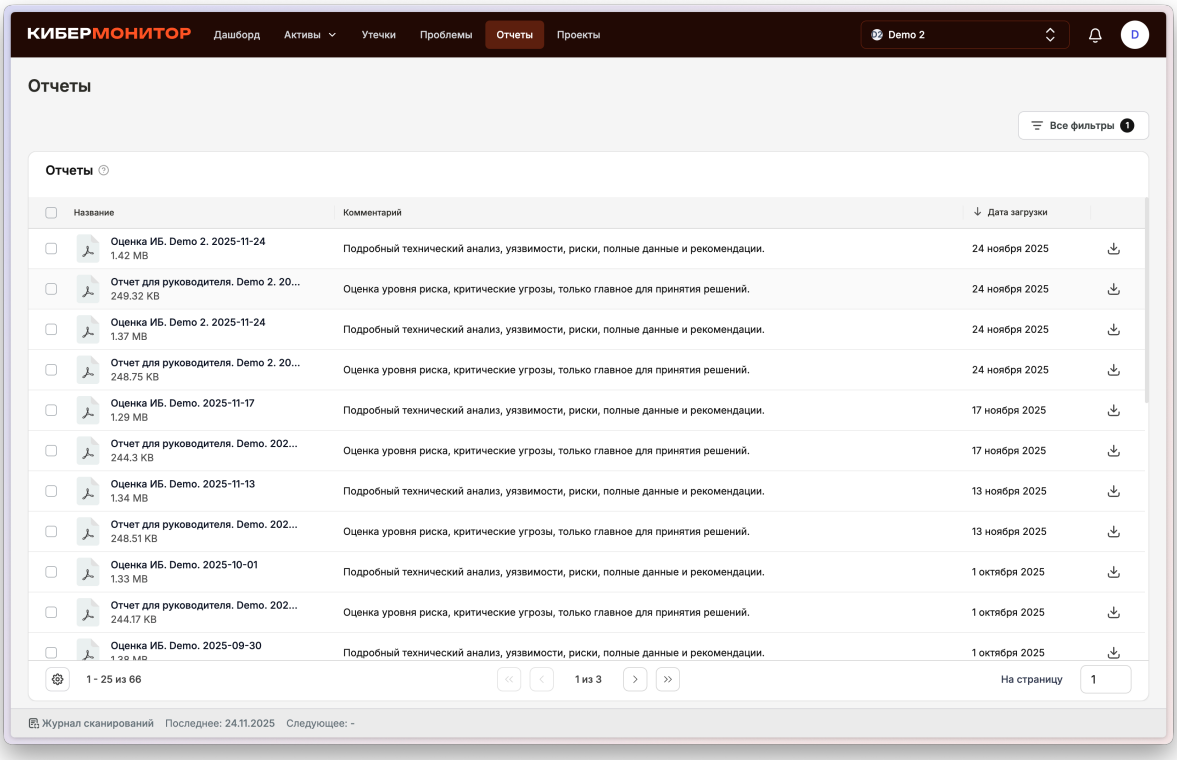
ПО отслеживает изменения в сетевой инфраструктуре, такие как добавление новых устройств, изменение конфигураций и т. д., что позволяет своевременно выявлять новые потенциальные угрозы.

Ресурсы: для мониторинга требуется постоянный доступ к сети и возможность отправки уведомлений о выявленных изменениях.

Выходные данные: Уведомления о значимых изменениях в инфраструктуре.

Предоставление отчетов и рекомендаций

После завершения сканирования и анализа, Нейроинформ генерирует подробные отчеты с оценкой текущего состояния безопасности и рекомендациями по устранению выявленных проблем.



Ресурсы: для создания отчетов используется выделенный сервер с установленным ПО.

Выходные данные: отчеты с рекомендациями, разделенные на разделы по типам, приоритетам и областям улучшения.

4. Затрачиваемые ресурсы и требования

Для полноценной работы Нейроинформ требуется серверное оборудование. Необходим доступ к сети, которую планируется анализировать, а также актуальная база данных уязвимостей.

5. Используемые технологические инструменты

Для функционирования программного обеспечения «Нейроинформ» используются современные технологические решения, обеспечивающие масштабируемость, надежность и соответствие требованиям информационной безопасности.

Языки программирования

- PHP — серверная логика и микросервисы

- Go — высокопроизводительные сервисные компоненты
- TypeScript — клиентский интерфейс и фронтенд-приложение

Программное обеспечение и платформы

- Kubernetes — оркестрация контейнеров
- Docker — контейнеризация приложений
- PostgreSQL — основное реляционное хранилище данных
- Apache Kafka — брокер сообщений и событийное взаимодействие сервисов
- S3-совместимое объектное хранилище — хранение файлов и артефактов
- GitLab — система управления исходным кодом и CI/CD
- Temporal — платформа оркестрации бизнес-процессов и рабочих процессов
- RoadRunner — высокопроизводительный сервер приложений
- Node.js — среда исполнения для фронтенда и вспомогательных сервисов
- Composer и npm — системы управления зависимостями
- — Prometheus, Grafana - системы мониторинга и визуализации метрик
- Российские облачные платформы для размещения компонентов и масштабирования ресурсов

Фреймворки и библиотеки

- Spiral Framework, Laravel — серверные компоненты и микросервисы
- Nuxt.js — одностраничное веб-приложение (SPA) для клиентского интерфейса

Протоколы и SDK

- gRPC — высокопроизводительное взаимодействие микросервисов
- HTTP/HTTPS (REST) — внешние и внутренние API
- WebSocket — онлайн-обновление данных в пользовательском интерфейсе

6. Выходные данные

Основные выходные данные включают:

- Отчет по выявленным уязвимостям;
- Перечень обнаруженных активов, активных портов и служб; - Оценка уровня безопасности;
- Рекомендации по улучшению защиты.

7. Взаимодействие с экспертами

Нейроинформ предлагает возможность взаимодействия с экспертами по кибербезопасности для детального анализа отчетов и получения дополнительных рекомендаций.

Ресурсы: для этой функции требуется возможность передачи данных и отчетов.

Выходные данные: Дополнительные рекомендации и предложения по улучшению безопасности от экспертов.