# Руководство пользователя «Программа для сканирования уязвимостей HScan»

Крайон

# Оглавление

## Общая информация

**ПО «Программа для сканирования уязвимостей Hscan» (далее – ПО) предназначено для сканирования внешнего периметра и внутренней ИТ-инфраструктуры организаций в целях выявления наличия на хостах актуальных уязвимостей в программном обеспечении и системных компонентах, а также для выстраивания процесса управления уязвимостями**

ПО «Программа для сканирования уязвимостей HScan» обладает следующими функциональными характеристиками:

инвентаризация активов, обнаружение связанных хостов, сопоставление программного обеспечения и системных компонентов (и их версий) на хостах с актуальными базами уязвимостей, приоритезация уязвимостей по критичности, предоставление рекомендаций по устранению уязвимостей, настройка регулярности сканирования, отслеживание прогресса по устранению уязвимостей, топологическое управление активами.

**Преимущества и особенности ПО:**

- **Интеграция с SIEM и системами ИБ:** ПО поддерживает полную интеграцию с внешними системами информационной безопасности через API. Результаты сканирования могут передаваться в SIEM-платформы и другие инструменты мониторинга для корреляции событий и центрального управления инцидентами.
- **Автоматизированные отчёты:** По завершении каждого сканирования ПО автоматически формирует подробный отчет о выявленных уязвимостях. Отчёт включает описания обнаруженных уязвимостей, уровни критичности, списки затронутых узлов и **практические рекомендации** по устранению проблем.
- **Соответствие требованиям ИБ:** Продукт разработан в соответствии с отечественными стандартами информационной безопасности.
- **Актуальная база угроз:** ПО обладает собственным сканирующим ядром и регулярно обновляемой базой данных уязвимостей. Благодаря своевременным обновлениям в продукте появляются проверки на новейшие обнаруженные угрозы, что обеспечивает высокий уровень выявления актуальных уязвимостей в инфраструктуре.
- **Наглядный интерфейс на русском языке:** Веб-интерфейс ПО предоставлен на русском языке и содержит удобные визуализации. Пользователи могут просматривать карту сети, список активов и детали уязвимостей через понятный и функциональный интерфейс, облегчающий анализ результатов сканирования.

**ПО «Программа для сканирования уязвимостей Hscan»** (далее также – ПО, система) помогает организациям оптимизировать процесс управления уязвимостями: автоматизирует поиск слабых мест в ИТ-инфраструктуре, снижает трудозатраты специалистов по информационной безопасности и повышает общий уровень защиты корпоративных систем

# Работа с аккаунтом

## Работа с результатами

### Выгрузка отчётов

Выгрузка отчётов позволяет создавать файлы-отчёты с информацией об обнаруженных хостах, запущенных на них сервисах и найденных уязвимостях. Этот функционал объединяет ключевые результаты сканирования в удобном формате, который можно сохранить и просматривать вне системы.

Создание отчёта о хостах, сервисах и уязвимостях

С помощью функции экспорта пользователь может сгенерировать отчёт, содержащий сводные сведения о проверяемых объектах. В одном файле собирается информация обо всех выявленных хостах, их активных сервисах (открытых портах) и обнаруженных на них уязвимостях. Отчёт предоставляет целостную картину результатов сканирования, что упрощает анализ данных и последующую работу с ними.

Доступные форматы файлов

Отчёт можно сохранить в одном из следующих форматов:

HTML – веб-страница, которая открывается в браузере и отображает отчёт в удобно читаемом виде с форматированием.

CSV – текстовый табличный формат (значения, разделённые запятыми), который удобен для импорта в электронные таблицы или другие программы для анализа (например, Microsoft Excel).

Настройка содержимого отчёта:

Окно экспорта отчёта с выбором содержимого и формата перед сохранением. Перед выгрузкой отчёта система позволяет настроить его содержимое и включить только нужные данные. Пользователь может выбрать, какие разделы информации добавить в отчёт, или исключить ненужные. Например, доступно включение следующих данных:

- списка обнаруженных хостов;
- перечня открытых портов и сервисов на каждом хосте;
- списка URL-адресов, связанных с найденными хостами (если применимо);
- информации об обнаруженных уязвимостях на хостах.

- Если какая-то часть информации не нужна, соответствующий раздел можно не добавлять, чтобы отчёт содержал только актуальные сведения.

Экспорт и сохранение отчёта

Для выгрузки отчёта в интерфейсе предусмотрена специальная кнопка экспорта. После нажатия кнопки «Выгрузка отчётов» открывается диалоговое окно настройки, в котором пользователь выбирает содержимое отчёта и формат файла (как описано выше). При подтверждении (нажатии кнопки сохранения) система сформирует файл отчёта и предложит сохранить его на компьютер. Файл будет загружен в выбранном формате, после чего отчёт можно открыть локально – например, HTML-файл откроется через браузер, а CSV-файл через программу для работы с таблицами.

## Топологическое управление

Что такое «Топологическое управление»?

Это специальный раздел системы, позволяющий в наглядном режиме создавать и редактировать схему вашей сети или инфраструктуры. С его помощью вы сможете:

- Добавлять активы (устройства, сервера и т. д.) на топологическую карту, передвигать их, а также менять их иконки и визуальное оформление под нужды вашего проекта.
- Объединять активы в группы, что особенно полезно при работе с большим числом устройств: так вы избежите «загромождения» схемы и сможете быстро находить нужные объекты.
- Запускать задачи (сканирование, проверку конфигураций, обновления и т. п.) для конкретных активов прямо с карты, не открывая дополнительные окна или разделы.
- Просматривать сводку уязвимостей как для всей группы, так и для каждого отдельного актива, чтобы моментально видеть, где находятся потенциальные риски.

Вся эта функциональность значительно упрощает работу с безопасностью и обслуживанием множества систем, позволяя действовать точно и оперативно.

1. Построение топологической схемы и настройка активов

### Шаг 1: Открытие раздела

Перейдите в «Топологическое управление» в интерфейсе системы.

При необходимости создайте новую схему или загрузите существующую.

### Шаг 2: Добавление активов

Используйте инструменты в верхней (или боковой) панели, чтобы добавить новые элементы (серверы, рабочие станции и т. д.).

Присвойте активам уникальные названия или идентификаторы.

### Шаг 3: Перемещение и визуальное расположение

Расставьте активы на карте так, чтобы она была удобна для восприятия.

Перетаскивайте объекты мышью, располагая их в логических зонах или сегментах.

### Шаг 4: Изменение изображений

Кликните по нужному активу и выберите «Изменить изображение».

Подберите иконку или схематическое изображение, соответствующее назначению устройства (например, сервер, сетевой коммутатор и т. д.).

2. Запуск задач прямо с топологической схемы

### Шаг 1: Выбор актива

Выберите интересующий актив, на котором нужно провести работу (например, сканирование на уязвимости).

### Шаг 2: Запуск задачи

В контекстном меню или боковой панели найдите список доступных действий (сканирование, проверка конфигураций и т. п.).

Выберите нужную задачу и подтвердите запуск. Результаты будут доступны в отчётах или окне статуса задач.

3. Работа с группами активов

Шаг 1: Создание или выбор группы

Сгруппируйте объекты по определённому признаку (отдел, тип устройств и т. д.).

Выделите несколько активов и используйте функцию «Создать группу», либо воспользуйтесь уже имеющимися группами.

Шаг 2: Просмотр сводки по группе

Нажмите на значок группы, чтобы увидеть список входящих в неё активов и суммарное число уязвимостей.

Это позволяет быстро узнать, есть ли критические проблемы среди объектов группы.

Шаг 3: Переход к конкретному активу

Кликните на нужный элемент в списке, чтобы открыть быструю сводку, где будут детализированы уязвимости и их уровень критичности.

4. Быстрый просмотр информации об активе

Шаг 1: Выбор объекта

Нажмите на актив в топологической схеме, чтобы отобразить краткую информацию о нём.

Шаг 2: Ознакомление со сводкой

В открывшемся окне вы увидите:

- Название и тип актива
- Общее число уязвимостей
- Краткое описание каждой уязвимости (при наличии)

Если необходимо больше подробностей, вы можете перейти в детальное описание уязвимостей или запустить отдельное сканирование.

Раздел «Топологическое управление» позволяет смотреть на всю инфраструктуру «с высоты птичьего полёта», объединяя в одном интерфейсе визуальное расположение устройств, работу с группами, быстрый доступ к задачам и сводку уязвимостей. Такой подход обеспечивает:

- Упрощённое администрирование: Вся сетка устройств и сервисов отображается на одной карте, что делает работу более наглядной и ускоряет поиск нужных ресурсов.
- Сокращение времени реакции: Благодаря возможности запускать проверки и сканирования непосредственно на схеме вы оперативно устраняете риски, не переключаясь между модулями.
- Гибкую организацию сети: Группируя активы по логическим признакам, вы лучше структурируете схему и мгновенно видите сводную информацию для каждой группы.
- Повышение прозрачности управления: Быстрая сводка уязвимостей даёт полное представление об актуальном состоянии безопасности, помогая своевременно выявлять узкие места.

Используя «Топологическое управление» в повседневной работе, вы с лёгкостью настраиваете структуру своей сети, контролируете критичные устройства и организуете совместную работу различных систем в едином пространстве.

## Управление уязвимостями

Раздел «Управление уязвимостями» предоставляет сводную информацию о потенциальных проблемах безопасности, обнаруженных на хостах вашей инфраструктуры. Здесь вы можете увидеть, на каких системах выявлены уязвимости, узнать их критичность и текущее состояние устранения, а также перейти к детальным отчётам и инструментам управления. Этот раздел служит центральной точкой контроля безопасности и даёт возможность оперативно реагировать на угрозы.

Ниже представлено техническое описание структуры страницы и её основных элементов:

### Шапка страницы

Отображает название модуля или раздела (например, «Управление уязвимостями»).

Может содержать дополнительные кнопки или ссылки для переключения на другие разделы (например, «Главная», «Мониторинг», «Отчёты»).

### Список хостов и их статус

В центральной части экрана перечисляются хосты (сервера, рабочие станции) или их IP-адреса.

Напротив каждого хоста может отображаться краткий статус безопасности (например, «Найдено X уязвимостей»), чтобы пользователь сразу видел, где есть проблемы.

Общее количество уязвимостей и уровни критичности

Приводится сводка по всем обнаруженным уязвимостям в инфраструктуре, а также их распределение по уровням критичности (низкий, средний, высокий, критический).

Это помогает быстро оценить общий риск для системы и понять, где нужна приоритетная защита.

Фильтры и настройки

В верхней или боковой части страницы могут располагаться поля поиска и фильтрации.

Благодаря фильтрам можно выбирать конкретные хосты, группы хостов, интересующие типы уязвимостей или временные интервалы, чтобы быстрее находить нужные данные.

Сводные карточки/блоки

В верхней части (или сбоку) могут быть сводные карточки, показывающие ключевые метрики: общее число хостов, общее число уязвимостей, число критических уязвимостей и т. д.

Это даёт наглядную картину состояния безопасности и помогает мгновенно определить первоочередные задачи.

Табличная часть с деталями уязвимостей

Ниже (либо при открытии конкретного хоста) отображается детальный список найденных уязвимостей.

Для каждой проблемы указываются такие сведения, как название, уровень критичности, статус (например, «Не решено», «Исправлено»), дата обнаружения и краткое описание. Это помогает понять, насколько серьёзна уязвимость и какие меры предприняты или ещё требуются.

Кнопки действий

В таблице или рядом с каждой записью могут быть кнопки для быстрого перехода к исправлению, к дополнительному описанию уязвимости или к повторному сканированию.

Например, «Просмотреть детали», «Исправить», «Пересканировать».

Информационные и статусные метки

Рядом с элементами страницы зачастую размещаются цветовые индикаторы или иконки (например, красный для критических уязвимостей, зелёный для устранённых).

Такие метки помогают визуально определять, какие проблемы самые срочные.

## Результаты сканирования

Результаты сканирования представляют собой отчёт, который содержит список проверенных хостов, найденные уязвимости, их уровень критичности и другую информацию о состоянии безопасности. Понимание этого отчёта позволяет быстро определить, какие проблемы требуют немедленного решения, а какие носят менее критичный характер.

### Структура отчёта:

### Перечень проверенных хостов

Здесь перечислены все системы (сервера, рабочие станции и т. д.), которые были просканированы. Указывается название или IP-адрес, чтобы вы могли понять, какой именно хост имел те или иные проблемы.

### Найденные уязвимости

В этом разделе выводится список обнаруженных проблем. Каждая уязвимость имеет краткое или расширенное описание. Например, может быть указано, что обнаружена старая версия сервера баз данных или небезопасная конфигурация.

### Уровни критичности

Уязвимости разделяются по степени их опасности (низкий, средний, высокий или критический). Эта градация показывает, насколько быстро нужно реагировать на данную проблему. Критические уязвимости обычно требуют немедленных мер, поскольку их эксплуатация злоумышленником может привести к серьёзным последствиям.

### Подробности по сервисам и программному обеспечения

Здесь указывается, какие именно сервисы, приложения или версии программного обеспечения оказались уязвимыми. Это помогает определить, какие компоненты системы нуждаются в обновлении или корректировке настроек.

### Как читать результаты

Оцените уровень угроз: Сосредоточьтесь в первую очередь на высоких и критических уязвимостях. Они представляют наибольший риск для системы.

Посмотрите общее количество уязвимостей: Это число даёт общее представление о том, сколько проблем найдено на конкретном хосте или во всей инфраструктуре.

Изучите описание проблем: Более детальные пояснения помогут понять, почему уязвимость опасна, как её могут эксплуатировать и какие могут быть последствия.

Проверьте версии программного обеспечения: Сравните указанные версии с текущими доступными обновлениями. Если обнаружена устаревшая версия, её стоит обновить в первую очередь.

### Статусы уязвимостей

Не решено: Уязвимость зарегистрирована, но ещё не исправлена (выявлена сканером впервые).

Подтверждено: Уязвимость проверена вручную и признана актуальной. Её ещё нужно устранить.

Исправлено: Проблема устранена (обычно после установки патча или изменения настроек). Сканер или администратор повторно убедились, что уязвимость более не обнаруживается.

Ложное срабатывание: Запись не представляет реальной угрозы и признана ошибкой сканирования. Это обычно выясняется при ручной проверке.

Информация о уязвимости

Информация о уязвимости предоставляет детальный обзор проблемы безопасности, которая была обнаружена на вашем хосте или в программном обеспечении.

Ниже описаны ключевые элементы, которые могут присутствовать в карточке уязвимости, и как их правильно интерпретировать:

- CVE/CWE-идентификатор и уровень критичности
- CVE/CWE-идентификатор – это уникальный код (например, CVE-2016-6662), присвоенный конкретной уязвимости. Он помогает идентифицировать проблему во всех базах данных уязвимостей и в отчётах по безопасности.
- CVE/CWE-SCORE или другая оценка уровня угрозы показывает, насколько опасна эта уязвимость (чем выше значение, тем она критичнее). Это помогает определить приоритет устранения.

### Описание уязвимости

Здесь указывается, в чём суть уязвимости и какие механизмы защиты она способна обойти. В описании часто упоминают, какие версии программного обеспечения подвержены проблеме. Если, например, указано несколько версий MySQL, MariaDB или другой системы, это означает, что все они могут быть уязвимы.

### Воздействие (или последствия) уязвимости

Раздел объясняет, что произойдёт, если злоумышленник воспользуется брешью. Например, возможность выполнения произвольного кода с правами администратора или

обход существующих настроек. Это даёт понимание, насколько серьезны возможные последствия и помогает расставить приоритеты в устранении.

### Решение

В этом блоке описаны основные шаги по устранению уязвимости. Обычно говорится о необходимости установить актуальные патчи безопасности, обновить используемую версию программного обеспечения или внести изменения в конфигурацию. Если вариант с обновлением недоступен, могут указываться временные меры защиты, снижающие риск эксплуатации.

### Эксплоит

Раздел показывает, что уже существует или публично доступна реализация атаки (так называемый «эксплоит»). Если такая информация есть, это повышает угрозу, потому что злоумышленники могут легко применить готовое решение. Появление эксплоита говорит о том, что уязвимость известна и эксплуатируется на практике.

### Ресурсы

Блок с дополнительными материалами или ссылками, которые помогают разобраться в деталях уязвимости, её исправлениях и сопутствующих рекомендациях. Они могут содержать более обширную информацию для тех, кто хочет глубже понять техническую сторону проблемы.

## Краткая сводка

Краткая сводка — это блок информации о выбранном хосте, который открывается при нажатии на его FQDN или IP-адрес. Здесь представленны основные показатели состояния безопасности и быстрого анализа уязвимостей. Ниже приведены ключевые элементы этой сводки:

### IP-адрес хоста

Отображается сетевой адрес устройства, чтобы вы могли сразу понять, о каком именно хосте идёт речь.

Общее количество уязвимостей

Показывает общее число проблем, обнаруженных во время сканирования. Чем выше это значение, тем больше потенциальных рисков на хосте.

Уровни угроз

Найденные уязвимости распределяются по степени серьёзности (критические, высокие, средние, низкие). Это помогает понять, какие проблемы требуют немедленного внимания, а какие можно исправить позже.

Список обнаруженного программного обеспечения

Здесь перечисляются приложения и службы, работающие на хосте, вместе с их версиями. Такие сведения важны для понимания, какое именно программное обеспечение может содержать уязвимости.

Детали уязвимостей

Каждая обнаруженная уязвимость имеет краткое описание (указывающее, в чём именно проблема), её уровень критичности и дату выявления. Это позволяет быстро определить, что за уязвимость, насколько она опасна и когда была найдена.

Доступность и состояние хоста

Этот раздел показывает, был ли хост в сети во время сканирования и насколько он уязвим в целом. Если хост недоступен, некоторые данные могут быть неактуальны, и сканер не сможет корректно отобразить информацию об уязвимостях.

## Управление системой

### Создание и управление пользователями

1. Назначение функционала

Раздел «Пользователи» предназначен для добавления новых учетных записей и управления существующими пользователями системы Hscan. Он позволяет назначать пользователям предустановленные роли или задавать индивидуальные права доступа. Таким образом администратор контролирует, к каким модулям и функциям системы имеет доступ каждый пользователь, обеспечивая необходимый уровень безопасности и разграничения прав.

2. Создание нового пользователя

Для добавления нового пользователя в систему выполните следующие шаги:

Открытие формы добавления: Перейдите в раздел «Пользователи» через меню навигации. На странице списка пользователей нажмите кнопку «Добавить» – откроется форма для создания нового пользователя.

Заполнение данных: В появившейся форме введите данные нового пользователя и настройте его доступ:

Имя – укажите имя или идентификатор пользователя (например, ФИО сотрудника).

Электронная почта – введите адрес e-mail, который будет использоваться в качестве логина для входа в систему.

Пароль – задайте пароль для нового пользователя. При вводе пароля можно воспользоваться кнопкой показа/скрытия, чтобы проверить правильность ввода.

Роль – выберите подходящую роль из предустановленного списка ролей (перечень ролей и их права описаны в разделе «Создание пользовательских ролей» документации). Роль определяет набор типовых прав доступа пользователя.

Разрешения – при необходимости настройте права доступа индивидуально. Отметьте галочками одно или несколько дополнительных прав из списка доступных разрешений:

- Все разрешения без исключения
- Управление данными пользователя
- Просмотр списка пользователей
- Общая сводка
- Просмотр списка уязвимостей
- Отмечать уязвимости как (не)исправленные
- Управление пользовательскими списками портов
- Просмотр списка учетных данных

- Управление учетными данными
- report
- Управление задачами
- Просмотр списка задач
- Изменение статуса задачи
- Просмотр результатов задачи
- Управление активами
- Просмотр списка активов
- Доступ к краткой информации об активах

Сохранение: После заполнения всех обязательных полей и настройки прав нажмите кнопку «Сохранить». Новый пользователь будет создан и появится в общем списке пользователей. Теперь он сможет войти в систему, используя указанную электронную почту и пароль, с теми правами доступа, которые вы ему назначили.

3. Редактирование и удаление пользователей

В разделе «Пользователи» вы также можете редактировать данные учетной записи или удалить пользователя при необходимости.

Редактирование пользователя: чтобы изменить информацию о существующем пользователе, выберите его из списка и нажмите значок «карандаш» (иконка редактирования) напротив имени. Откроется форма редактирования, аналогичная форме создания пользователя. Внесите необходимые изменения — например, отредактируйте имя, сбросьте или измените пароль, измените роль или права доступа. После корректировки данных сохраните изменения, нажав «Сохранить». Изменения вступят в силу сразу, и пользователь будет иметь обновленные права при следующем входе в систему.

Удаление пользователя: чтобы удалить учетную запись, установите флажок (чекбокс) рядом с именем нужного пользователя в списке. Затем нажмите кнопку «Удалить» (обычно расположена над или под списком) и подтвердите удаление во всплывающем окне. После подтверждения пользователь будет удален из системы (его учетная запись исчезнет из списка). Рекомендуется удалять только тех пользователей, которые больше не должны иметь доступ к системе, поскольку это действие может быть необратимо.

Создание пользовательских ролей

1. Назначение функционала

Раздел «Роли» предназначен для создания и управления ролевыми моделями доступа, которые затем назначаются пользователям.

Каждая созданная роль определяет, какие права имеет пользователь в системе.

Данный функционал позволяет гибко разграничивать доступ к различным модулям системы в соответствии с должностными обязанностями или уровнем ответственности пользователей.

2. Создание новой роли

Чтобы создать новую роль, выполните следующие действия:

Открытие формы добавления

Перейдите в раздел «Роли» в системе.

Нажмите кнопку «Добавить» для создания новой роли.

Заполнение данных

Введите Название роли – например, «Аналитик», «Администратор» или «Оператор».

Выберите Права доступа, установив флажки напротив необходимых пунктов. Можно отметить одно или несколько прав из списка:

- Все разрешения без исключения
- Управление данными пользователя
- Просмотр списка пользователей
- Общая сводка
- Просмотр списка уязвимостей
- Отмечать уязвимости как (не)исправленные
- Управление пользовательскими списками портов
- Просмотр списка учетных данных
- Управление учетными данными
- report
- Управление задачами
- Просмотр списка задач
- Изменение статуса задачи
- Просмотр результатов задачи
- Управление активами
- Просмотр списка активов

- Доступ к краткой информации об активах

Сохранение

После заполнения всех необходимых полей нажмите кнопку «Сохранить».

Новая роль сохранится в системе и появится в общем списке ролей. Теперь эту роль можно назначить пользователям при необходимости.

3. Редактирование и удаление ролей

Редактирование роли: Чтобы изменить существующую роль:

Выберите нужную роль из списка.

Нажмите значок «карандаш» (редактирование) рядом с названием роли, чтобы открыть форму редактирования.

Внесите необходимые изменения (например, скорректируйте название роли или добавьте/уберите права доступа).

Нажмите «Сохранить» для сохранения изменений. Изменения вступят в силу сразу после сохранения.

Удаление роли: Чтобы удалить одну или несколько ролей

Отметьте флажками роль или роли, которые нужно удалить (можно выбрать несколько одновременно).

Нажмите кнопку «Удалить» и подтвердите действие в появившемся диалоговом окне. Выбранные роли будут удалены из системы.

Добавление рабочих областей

1. Назначение функционала

- **Изолированное пространство.** Рабочая область – это отдельное, изолированное пространство внутри системы, где назначенные пользователи могут работать независимо от основного тенанта. Данные и настройки каждой рабочей области отделены от остальных, что повышает безопасность и удобство работы.

- **Разграничение доступа.** Рабочие области позволяют гибко разграничивать права доступа. Администратор может управлять пользователями внутри каждой области отдельно, предоставляя доступ только к нужным данным и функциям. Пользователи, добавленные в одну рабочую область, не имеют доступа к содержимому другой области (если им туда не предоставлены права).
- **Главный тенант (по умолчанию).** При установке системы по умолчанию используется главный тенант **"default"** – это основная рабочая область, которая существует всегда. Вы можете создавать дополнительные рабочие области для разделения проектов, команд или клиентов, сохраняя "default" как общую или административную зону.

### 2. Создание новой рабочей области

Чтобы создать новую рабочую область в системе Hscan, выполните следующие шаги:

1. **Открытие формы добавления.** Перейдите в раздел **«Рабочие области»** через главное меню системы. На странице списка рабочих областей нажмите кнопку **«Добавить»** на панели инструментов. Эта кнопка обычно расположена вверху списка и отмечена соответствующим значком. После нажатия откроется форма для создания новой рабочей области.
    - **Название рабочей области:** укажите понятное имя, отражающее назначение области (например, название команды или проекта).
    - **Пользователи:** выберите из списка тех пользователей, которым хотите предоставить доступ к этой рабочей области. Вы можете отметить нескольких пользователей; они получат права работать внутри данной области. Если пользователей пока добавлять не нужно, этот шаг можно пропустить или выполнить позже через редактирование области.
      **Заполнение данных.** В появившейся форме введите основные сведения о новой рабочей области:
2. **Сохранение.** После заполнения всех необходимых полей нажмите кнопку **«Сохранить»**. Система сохранит новую рабочую область. Теперь она появится в общем списке рабочих областей. Назначенные пользователи получат доступ к этой области и смогут в ней работать. Убедитесь, что новая область отображается в списке и что указанные пользователи корректно перечислены в ее настройках.

### 3. Редактирование и удаление рабочих областей

В процессе использования системы может потребоваться изменить параметры существующей рабочей области или удалить ненужную. Ниже описано, как редактировать и удалять рабочие области.

- **Редактирование рабочей области.** Чтобы отредактировать существующую рабочую область, перейдите в раздел **«Рабочие области»** и выберите область, которую нужно изменить, из списка. Нажмите на значок «карандаш» (редактирование) рядом с названием области или откройте область для просмотра и выберите функцию редактирования. В открывшейся форме внесите необходимые изменения – например, скорректируйте название или добавьте/удалите пользователей, имеющих доступ. После внесения правок нажмите **«Сохранить»**, чтобы обновить параметры области. Убедитесь, что изменения применились (новые пользователи добавлены, лишние удалены и т.д.).

- **Удаление рабочей области.** Для удаления рабочей области (или нескольких сразу) также откройте раздел **«Рабочие области»**. В списке установите флажки напротив одной или нескольких областей, которые хотите удалить. Затем нажмите кнопку **«Удалить»** (обычно помечена значком корзины или крестика) на панели инструментов. Система попросит подтвердить удаление – согласитесь, если уверены в удалении. После подтверждения выбранные рабочие области будут удалены из системы. **Внимание:** удаление необратимо, и данные внутри удалённой области станут недоступны, поэтому убедитесь, что область действительно не нужна, и в ней нет ценной информации, прежде чем удалять.

### Пользовательские списки tcp udp портов

**1. Назначение функционала**

Раздел **«Пользовательские списки TCP/UDP портов»** предназначен для управления списками TCP- и UDP-портов, используемыми при выполнении задач сканирования. Он позволяет создавать и редактировать пользовательские (кастомные) списки портов для более гибкой настройки сканирования.

**2. Предустановленные списки портов**

По умолчанию пользователю доступны следующие предустановленные списки портов:

- **Все TCP & UDP** – включает все 65 535 TCP-портов и 65 535 UDP-портов
- **Все TCP** – включает все 65 535 TCP-портов
- **Все UDP** – включает все 65 535 UDP-портов
- **Все системные TCP & UDP** – включает все системные порты от 0 до 1023 для TCP и UDP
- **Все системные TCP** – включает системные TCP-порты от 0 до 1023
- **Все системные UDP** – включает системные UDP-порты от 0 до 1023
- **Без портов (PING)** – используется только для ICMP-запросов (сканирование портов не выполняется)

**3. Добавление нового пользовательского списка**

Чтобы добавить новый пользовательский список портов, выполните следующую последовательность действий:

1. **Открытие формы добавления**
   - Перейдите в раздел **«Пользовательские списки TCP/UDP портов»** в системе
   - Нажмите кнопку **«Добавить»** (для добавления нового списка)
2. **Заполнение данных**
   - Введите **Название списка** (уникальное имя для нового списка)
   - Добавьте **Комментарий** (необязательно, пояснение или описание назначения списка)
   - Укажите TCP-порты в поле ввода в формате 32,64,100-200 и нажмите символ «+», чтобы добавить их в список
   - Укажите UDP-порты в том же формате и также нажмите «+»
3. **Сохранение списка**
   - После ввода необходимых данных нажмите кнопку **«Добавить пользовательский список»**

- Новый список появится в общем списке доступных списков портов и станет доступен для использования при сканировании

4. Редактирование и удаление списков

В данном разделе можно изменять ранее созданные пользовательские списки или удалять ненужные. Для этого предназначены функции **редактирования** и **удаления** списков:

- **Редактирование**
  - Выберите существующий пользовательский список из перечня
  - Откройте его для редактирования (например, двойным щелчком или через кнопку «Редактировать»)
  - Внесите необходимые изменения (добавьте или удалите порты, скорректируйте название или комментарий)
  - Сохраните изменения списка
- **Удаление**
  - Отметьте флажком один или несколько списков, которые необходимо удалить
  - Нажмите кнопку **«Удалить»**
  - Подтвердите удаление в диалоговом окне (после подтверждения выбранные списки будут удалены из системы)

### Добавление учетных данных

В этом руководстве описаны шаги по добавлению, редактированию и удалению учётных данных в системе **Hscan**. Также приведены ограничения и рекомендации по безопасному использованию этих учётных записей.

1. Добавление учетных данных

1. **Доступ к функционалу**:
   - Перейдите в меню **"Управление системой"** и выберите раздел **"Учётные данные"**.
   - Нажмите кнопку **"Добавить"** для создания новой записи учётных данных.
2. **Выбор типа подключения**:
   - **SSH** – выберите этот тип для Linux/Unix-систем. Доступные методы аутентификации: **без пароля**, **с паролем**, **с публичным ключом**.
   - **WinRM** – выберите этот тип для Windows-систем. Доступные методы аутентификации: **с паролем**, **NTLM-хэш**.
3. **Настройка параметров**:
   - **Для SSH** – в зависимости от выбранного метода аутентификации заполните следующие поля:
     - Без пароля: укажите **Логин** (имя пользователя), **Порт** (по умолчанию 22) и при необходимости отметьте опцию **Привилегированный доступ** (если требуется выполнение команд с повышенными привилегиями, например через sudo).

- С паролем: укажите **Логин**, **Пароль**, **Порт** (обычно 22) и опцию **Привилегированный доступ** (если нужен административный доступ).
- С публичным ключом: укажите **Логин**, вставьте **Приватный ключ** (SSH private key) в соответствующее поле, при необходимости введите **Кодовую фразу** (парольную фразу к ключу). Укажите **Порт** (22 по умолчанию) и отметьте **Привилегированный доступ**, если требуется.

- **Для WinRM** – заполните поля согласно выбранному методу:
  - С паролем: укажите **Логин** (учётная запись Windows), **Домен** (если используется доменная учётная запись; для локальной учетной записи можно оставить пустым или указать имя компьютера) и **Пароль**.
  - NTLM-хэш: укажите **Логин**, **Домен** и вместо пароля введите **NTLM-хэш** пароля данной учётной записи (32-символьный хэш NTLM).

4. **Сохранение данных**:
   - После заполнения всех необходимых параметров проверьте корректность введённых данных. Убедитесь, что логин, пароль/ключ и другие параметры указаны верно.
   - Нажмите **"Сохранить"** для добавления новых учётных данных в систему.
   - Убедитесь, что новая запись появилась в списке в разделе **"Учётные данные"**. При необходимости протестируйте подключение под этой учётной записью.

## 2. Редактирование и удаление учетных данных

1. **Редактирование**:
   - Откройте раздел **"Учётные данные"** через меню **"Управление системой"**.
   - В списке существующих учётных записей найдите нужную запись (при большом списке можно воспользоваться поиском или фильтрацией).
   - Выделите эту запись и нажмите **"Редактировать"** (значок карандаша).
   - В открывшейся форме внесите необходимые изменения – например, обновите пароль, ключ или другие параметры учётной записи.
   - После внесения правок нажмите **"Сохранить"**. Убедитесь, что изменения применились (в списке обновятся соответствующие поля записи).
2. **Удаление**:
   - В разделе **"Учётные данные"** отметьте (выберите) одну или несколько учётных записей, которые требуется удалить.
   - Нажмите кнопку **"Удалить"** .
   - Подтвердите действие в появившемся диалоговом окне (система запросит подтверждение, чтобы предотвратить случайное удаление).
   - После подтверждения удаления проверьте, что выбранные учётные записи исчезли из списка. Удалённые данные больше не будут доступны для операций (для авторизации при сканировании удалённых хостов).

Добавление и удаление активов

## 1.1. Ручное добавление

**Шаги для ручного добавления нового актива:**

1. **Открытие формы добавления.** Перейдите в раздел **«Активы»** в системе Hscan. Нажмите кнопку **«Добавить актив»** (или аналогичную кнопку для добавления нового актива). Откроется форма ввода данных нового актива.
2. **Ввод адресной информации.** В появившейся форме укажите идентификатор актива:
   - В поле ввода можно ввести **FQDN** (Fully Qualified Domain Name, полное доменное имя), **IP-адрес** или **подсеть**.
     Например: server.example.com, 192.168.10.5 или 192.168.10.0/24.
   - Для ввода **нескольких адресов** сразу (например, список IP-адресов или доменов) перечислите их через запятую, пробел или с новой строки. Система автоматически распознает разделители. **Пример:** вы можете вставить список из нескольких IP (192.168.10.5, 192.168.10.6, 192.168.10.7) или нескольких доменных имен, и система создаст отдельный актив для каждого адреса.
   - Если указана **подсеть (CIDR)**, система воспримет это как команду добавить **все IP-адреса из данного диапазона**. Например, маска 192.168.10.0/30 приведет к созданию активов для адресов 192.168.10.1–192.168.10.3 (все адреса в диапазоне /30).
3. **Выбор группы (опционально).** При добавлении актива можно привязать его к определенной группе:
   - В форме добавления имеется выпадающий список **«Группа»** (или аналогичное поле). Выберите из списка группу, к которой должен принадлежать новый актив. Группы помогают организовать активы по категориям (например, по отделам, типам устройств или локации).
   - Если подходящей группы нет, сначала создайте новую группу в разделе **«Группы активов»** (если функционал системы это предусматривает), и затем повторите добавление актива, выбрав новую группу.
4. **Подтверждение добавления.** После ввода всех необходимых данных нажмите кнопку **«Сохранить»** или **«Добавить»** для подтверждения:
   - Проверьте еще раз правильность введённых адресов и выбранной группы. Убедитесь, что адрес не содержит опечаток, а маска подсети указана корректно.
   - При подтверждении система создаст актив(ы) на основе введённых данных. Если было указано несколько адресов или подсеть, будет автоматически создано несколько записей — по одной на каждый распознанный адрес.
   - После успешного добавления вы увидите новые активы в списке раздела **«Активы»**. Как правило, появляется уведомление об успешном создании актива(ов).

### 1.2. Автоматическое разбиение пула активов

При вводе нескольких адресов одновременно система **Hscan** автоматически разделяет их на отдельные активы. Ниже описано, **как интерпретируется введённый пул данных** и **какие форматы поддерживаются**:

- **Список отдельных адресов:** Если вы вводите несколько IP-адресов или FQDN, разделённых запятыми, пробелами или переносами строк, **каждый из них будет создан как отдельный актив**. Вам не нужно добавлять их по одному — достаточно вставить весь список в поле ввода, и система сама разобьёт его. Например, ввод строк:
- server1.example.com
- server2.example.com
- 10.0.0.5
- 10.0.0.6

  создаст четыре актива: два для указанных доменов и два для IP-адресов.
- **Диапазоны адресов по маске (CIDR):** Вы можете указать подсеть в формате CIDR (например, 10.0.0.0/24). Система распознает маску и **создаст активы для каждого IP-адреса из этого диапазона**. Например, если ввести сеть 10.0.0.0/30, будут созданы активы для 10.0.0.1, 10.0.0.2 и 10.0.0.3 (адрес 10.0.0.0 рассматривается как адрес сети, а 10.0.0.255 как широковещательный, они не добавляются как хосты). **Важно:** будьте осторожны с крупными сетями (например, /16 или /8) — добавление слишком большого числа активов может занять время и создать длинный список.
- **Диапазоны адресов по шаблону:** В некоторых случаях система может поддерживать ввод диапазона через дефис (например, 192.168.10.5-192.168.10.20). Если такой формат поддерживается, все адреса в указанном диапазоне также будут добавлены. Однако, если официальный способ – только CIDR, предпочитайте использовать именно маски подсети для добавления диапазонов.
- **Обработка и исключения:** Система игнорирует пустые строки и автоматически удаляет лишние пробелы или недопустимые символы. Если какой-либо введённый адрес имеет **неверный формат** (например, опечатка в доменном имени или недопустимый IP-адрес), Hscan может выдать сообщение об ошибке и не добавит этот элемент. Already existing addresses (дубликаты) обычно **не добавляются повторно** – система может предупредить, что такой актив уже существует, и пропустит его в процессе создания.

Подводя итог, функциональность автоматического разбиения позволяет быстро добавлять большие списки активов. Все распознанные адреса из поля ввода будут зарегистрированы отдельно, **упрощая массовое добавление** без необходимости повторять операцию для каждого актива.

### 2. Массовое удаление активов

Массовое удаление активов позволяет одновременно удалить сразу несколько записей из раздела **«Активы»**. Этот функционал полезен, когда нужно очистить систему от устаревших или ошибочно добавленных активов. Ниже рассмотрены шаги выполнения массового удаления:

### 2.1. Вызов формы массового удаления

Чтобы перейти к функции массового удаления, найдите соответствующий элемент управления в разделе **«Активы»**:

- В верхней панели управления или меню раздела **«Активы»** должна присутствовать команда **«Массовое удаление активов»**. Как правило, это кнопка или пункт выпадающего меню (например, иконка с несколькими чекбоксами или надпись "Удалить несколько").
- Нажмите на **«Массовое удаление активов»**. Система откроет специальную форму или диалоговое окно для ввода данных об активах, которые требуется удалить. Эта форма похожа на форму добавления, но предназначена именно для удаления множества объектов.

### 2.2. Выбор активов для удаления

В появившейся форме укажите, **какие активы нужно удалить**:

- В текстовое поле формы массового удаления введите **идентификаторы активов** – это могут быть IP-адреса, FQDN (имена хостов) или обозначения подсетей. Формат ввода аналогичен добавлению: перечисляйте несколько адресов через запятую, пробел или с новой строки.
- **Удаление по маске (CIDR):** Вы можете указать сеть в CIDR-нотации, чтобы разом удалить все активы из этого диапазона. Например, ввод 192.168.10.0/24 обозначит удаление всех активов с IP из подсети 192.168.10.0/24. Система найдёт **все активы, попадающие в эту подсеть**, и подготовит их к удалению.
- **Выбор по списку:** Если нужно удалить конкретный набор разрозненных адресов, просто перечислите их. Например, вы можете вставить список:
- 192.168.10.5
- 192.168.10.7
- old-server.example.com
- 10.0.0.1

  Система проанализирует каждую строку и отметит соответствующие активы на удаление (если такие существуют в системе).

- **Проверка ввода:** Убедитесь, что все адреса введены правильно. Ошибка в записи адреса (например, лишний символ или неправильная маска) может привести к тому, что нужный актив не будет найден и, соответственно, не будет удалён. Также, если вы укажете адрес, которого нет в базе активов, система, скорее всего, просто пропустит его (или сообщит, что некоторые из указанных активов не найдены).

### 2.3. Подтверждение удаления

После ввода адресов для удаления инициируйте процесс и **подтвердите удаление**:

- Нажмите кнопку **«Удалить»** (или **«Применить»**) в форме массового удаления. Система сформирует список активов, которые подпадают под заданные критерии.
- **Просмотр списка перед удалением:** Перед окончательным удалением система обычно отображает перечень найденных активов, которые будут удалены. Внимательно проверьте этот список:
    - Убедитесь, что в него входят именно те активы, которые вы хотели удалить. Обратите внимание, не затесался ли лишний адрес из-за неточного ввода (например, слишком широкая маска могла захватить лишние узлы).

- Если список содержит нежелательные позиции, откажитесь от выполнения операции (нажмите **«Отмена»** или закройте диалог) и скорректируйте введённые данные.

- **Необратимость операции:** При подтверждении удаления (например, повторным нажатием **«Удалить»** в окне подтверждения) выбранные активы будут **безвозвратно удалены** из системы. Система может запросить дополнительное подтверждение (диалог «Вы уверены, что хотите удалить X активов?») – подтвердите своё решение, чтобы завершить операцию.
- После подтверждения в журнале или уведомлениях появится информация об успешном удалении. Удалённые активы исчезнут из списка активов. Учтите, что вместе с активами могут удаляться и связанные с ними данные (например, результаты сканирования или метаданные), поэтому важно было убедиться в правильности выбора перед удалением.

### Топологическое управление активами

Раздел **«Топологическое управление активами»** системы Hscan предназначен для визуализации инфраструктуры и эффективного управления активами и их группами. Ниже перечислены основные возможности этого раздела и краткие инструкции по их использованию.

#### Общий вид топологии

**Общий вид топологии** предоставляет наглядное представление всех активов в виде топологической схемы. Активы отображаются как узлы (иконки), а связи между ними отражают их принадлежность к группам или другие взаимосвязи. Эта схема помогает понять структуру инфраструктуры:

- **Отображение активов и групп:** Все группы представлены как кластерные узлы, внутри которых находятся их активы. Индивидуальные активы показаны отдельно и соединены линиями с группами, к которым относятся.
- **Визуальная иерархия:** Иерархия «группа – подгруппа – актив» отображается графически. Например, центральный узел может представлять главную группу, от которого отходят линии к подгруппам и отдельным активам.
- **Навигация по топологии:** Вы можете перемещать обзор схемы (прокруткой или перетаскиванием фона), чтобы рассмотреть разные части инфраструктуры. Для увеличения или уменьшения масштаба используйте функции масштабирования (значки «+/-» или прокрутку колесиком мыши).

#### Управление активами

**Управление активами** позволяет изменять состав и характеристики узлов прямо на топологической схеме. Вы можете перемещать активы между группами, удалять устаревшие объекты или редактировать их параметры. Основные операции:

- **Перемещение активов:** Чтобы переместить актив в другую группу, перетащите его значок мышью из текущей группы в целевую. После отпускания кнопки мыши актив окажется в новой группе, а топологическая схема автоматически обновит связи.

- **Редактирование актива:** Для редактирования свойств актива (например, имени, типа или описания) щелкните по нему дважды либо выберите актив и нажмите кнопку «Редактировать». В появившемся окне внесите необходимые изменения и сохраните их.
- **Удаление актива:** Чтобы удалить актив, выберите его на схеме и нажмите кнопку **Удалить** (или используйте пункт контекстного меню "Удалить"). Система запросит подтверждение; подтвердите действие, после чего актив будет удалён из топологии. Важно: при удалении актива все связанные с ним данные (например, результаты сканирования) могут быть недоступны.
- **Перемещение групп:** Аналогично активам, целую группу (включая подгруппы и активы) можно переместить внутрь другой группы для реорганизации структуры. Перетащите группу на новый узел-группу; после подтверждения вся выбранная группа станет подгруппой нового родителя.
- **Редактирование групп:** Вы можете переименовать группу или изменить её свойства. Для этого выделите группу и нажмите **Редактировать**. В диалоговом окне укажите новое имя группы или другие параметры, затем сохраните изменения. Топология обновится с учётом нового наименования.
- **Удаление групп:** Для удаления группы целиком выберите группу и воспользуйтесь командой **Удалить группу**. Система, как правило, запросит подтверждение, особенно если внутри группы есть активы или подгруппы. После подтверждения группа и все её подчинённые элементы будут удалены из топологической схемы. Рекомендуется предварительно переместить или удалить активы вручную, если не требуется удалять их вместе с группой.

### Работа с группами

**Работа с группами** включает создание новых групп, организацию групп во вложенные структуры и общее структурирование активов. Группы помогают логически разделять активы (по отделам, локациям, типам и т.д.) в иерархию для удобства управления:

- **Создание новой группы:** Чтобы создать группу, нажмите кнопку **Добавить группу** (или аналогичный пункт меню). Укажите название новой группы в появившемся окне и подтвердите создание. Новая группа появится на топологической схеме, обычно рядом с уже существующими группами или в составе текущей выбранной группы.
- **Вложенные группы:** Система поддерживает иерархию групп (группы внутри групп). Для создания вложенной группы выберите группу, которая станет родительской, и затем создайте новую группу – она автоматически станет её подгруппой. Альтернативный способ: перетащите одну группу на другую, как описано выше, чтобы сделать первую подгруппой второй. В топологии вложенные группы отображаются связанными узлами: подгруппа соединена линией со своей родительской группой.
- **Структурирование активов:** Распределяйте активы по группам так, чтобы они отражали реальную структуру вашей инфраструктуры. Например, вы можете создать группы по географическому признаку (офис Нью-Йорк, офис Москва) или по типу (Серверы, Рабочие станции) и переместить соответствующие активы в эти группы. Грамотная иерархия облегчает последующий контроль уязвимостей и управление сканированием.

- Удаление и реорганизация групп: Если группа больше не нужна, вы можете её удалить (как описано выше). Также группы можно переупорядочивать: например, переименовать для ясности или переместить под другую родительскую группу. Все эти изменения сразу отражаются на топологической схеме, обеспечивая актуальность представленной структуры.

### Запуск задач сканирования

Запуск задач сканирования непосредственно из топологического представления позволяет проверять безопасность активов на уязвимости. Вы можете инициировать сканирование как для отдельного узла-актива, так и для целой группы (т.е. всех активов в ней):

- Сканирование отдельного актива: Щёлкните по нужному активу правой кнопкой мыши и выберите команду Запустить сканирование (или нажмите соответствующую кнопку на панели инструментов, если актив выбран). Система начнёт сканировать выбранный актив на наличие уязвимостей. Статус задачи сканирования обычно отображается рядом с активом (например, индикатор выполнения или изменение цвета значка).
- Сканирование группы активов: Выберите узел группы и инициируйте сканирование для неё (через правый клик — Сканировать группу, либо через меню интерфейса). Это запустит задачи сканирования для всех активов, входящих в данную группу (включая вложенные подгруппы, если предусмотрено). Такой массовый запуск удобен для регулярной проверки большого числа систем. Прогресс сканирования может отображаться агрегировано для группы или индивидуально на каждом узле.
- Отслеживание выполнения: После запуска сканирования вы можете наблюдать за ходом выполнения. Обычно система показывает уведомления или статус прямо на схеме (например, значок сканера на активе во время проверки). По завершении сканирования обновятся показатели уязвимостей для соответствующих активов/групп.
- Планирование сканирования: В некоторых случаях может быть доступна функция планирования – например, добавить задание в очередь или расписание. Если это предусмотрено, вы можете указать при запуске, немедленно выполнить сканирование или отложить его на заданное время.

### Пиктографическое отображение активов

Пиктографическое отображение активов означает, что каждый тип актива представлен своей иконкой, упрощающей визуальное различение различных видов устройств и систем. В топологической схеме Hscan это реализовано следующим образом:

- Уникальные значки для типов: Серверы, рабочие станции, сетевое оборудование, базы данных и другие категории активов помечены разными пиктограммами. Например, значок сервера может выглядеть как стоечный компьютер, рабочая станция – как монитор или ПК, а сеть – как сетевой коммутатор. Благодаря этому вы сразу видите, какой тип системы представляет каждый узел.
- Легенда или подсказки: Обычно интерфейс содержит легенду, объясняющую значения пиктограмм. Наведите курсор на незнакомую иконку, чтобы увидеть подсказку с типом актива. Это помогает быстро ориентироваться даже в сложной схеме с множеством разнообразных устройств.

- **Визуальная консистентность:** Все активы отображаются однородно в пределах своего типа. Если, к примеру, у вас 10 серверов, все они будут помечены одинаковым значком сервера. Это облегчает подсчёт и поиск активов определённого типа в группе или во всей топологии.

### Боковая оперативная сводка группы

Для каждой группы активов доступна **боковая оперативная сводка**, предоставляющая ключевую информацию по безопасности этой группы. Когда вы выбираете (кликаете) группу на топологической схеме, в боковой панели интерфейса отображаются сводные данные:

- **Число активов в группе:** Общее количество активов, принадлежащих выбранной группе (включая активы во всех её подгруппах). Это число позволяет оценить размер данной категории или сегмента инфраструктуры.
- **Количество уязвимостей:** Суммарное число обнаруженных уязвимостей во всех активах данной группы. Обычно указывается общее количество, а возможно, и разбивка по уровням серьезности (например, критические, высокие, средние, низкие).
- **Состояние безопасности группы:** Общая оценка состояния безопасности группы на основе количества и критичности уязвимостей. Это может быть текстовый статус (например, "Высокий риск" или "Безопасность удовлетворительная") или цветовой индикатор. **Пример:** зелёный цвет – нет критичных уязвимостей, жёлтый – присутствуют уязвимости средней тяжести, красный – критических уязвимостей много, требуются срочные меры.
- **Оперативное обновление:** Эти показатели обновляются автоматически после каждого сканирования или изменения состава группы. Таким образом, боковая сводка всегда отражает актуальное состояние безопасности выбранной группы.

(Примечание: Боковая панель обычно располагается слева в окне приложения. Убедитесь, что панель не скрыта – при необходимости откройте её через меню отображения интерфейса.)

### Просмотр состояния безопасности актива

При выборе конкретного узла-актива на топологической схеме вы получаете доступ к подробной информации о его состоянии безопасности и связанным действиям. **Просмотр состояния безопасности актива** включает несколько возможностей:

- **Добавление задачи на устранение уязвимостей:** Если для выбранного актива обнаружены уязвимости, вы можете сразу назначить задачу на их устранение. Для этого нажмите кнопку **Устранить уязвимости** (она может также называться «Добавить задачу» или «Remediation») в панели актива. Далее выберите конкретные уязвимости или общее действие (например, установить патчи) и задайте параметры задачи. Эта функция помогает планировать и отслеживать выполнение работ по повышению безопасности прямо из интерфейса.
- **Просмотр установленного программного обеспечения:** В деталях актива имеется список всего установленного программного обеспечения на данном узле. Переключитесь на вкладку **Установленное программное обеспечение** (если интерфейс разделён на вкладки) или раздел, где перечислены приложения,

версии и даты установки. Этот список полезен для выявления устаревших программ или ненужных сервисов, которые могут представлять угрозу безопасности.

- **Список уязвимостей:** Отдельный раздел посвящён перечню всех уязвимостей, обнаруженных на активе. Здесь приводятся сведения по каждой уязвимости: идентификатор или название, уровень опасности, описание проблемы и рекомендации по устранению. Пользователь может изучить этот список, чтобы понять, какие конкретно угрозы актуальны для выбранного узла. Часто предусмотрена возможность сортировки или фильтрации списка (например, показать сначала критические уязвимости).
- **Детальное состояние актива:** Этот подраздел содержит общие сведения и индикаторы состояния актива. В него обычно входят: имя и тип устройства, IP-адрес или другие сетевые реквизиты, операционная система и её версия, дата последнего сканирования, общее количество уязвимостей (по категориям) и интегральная оценка риска (если рассчитана системой). Здесь же могут отображаться статусы агента безопасности (если используется) или примечания администратора. Детальный обзор позволяет получить целостное представление о безопасности данного актива без необходимости просматривать разрозненные данные.
- **Навигация по информации актива:** Интерфейс может предоставлять удобную навигацию между этими разделами (например, вкладки или выпадающее меню). Просто выбирайте нужную вкладку/раздел, чтобы переключиться между списком программного обеспечения, уязвимостей и другими сведениями. Все данные связаны с выбранным активом и обновляются после каждого сканирования или изменения состояния (например, после применения патчей).

### Состояние безопасности

Этот раздел – главная панель (дашборд), где собрана ключевая информация о выявленных уязвимостях и общем уровне риска в инфраструктуре. Он предназначен для быстрой оценки текущего состояния безопасности и приоритизации действий.

#### Сводные показатели

В верхней части панели отображаются основные числовые индикаторы:

- **Всего уязвимостей**
  Показывает суммарное количество уязвимостей, обнаруженных в процессе сканирований за всё время. Этот показатель даёт общее представление о масштабах проблем в инфраструктуре.
- **Новые уязвимости**
  Отражает, сколько уязвимостей было найдено впервые за выбранный временной промежуток. Рост этого числа указывает на появление новых рисков или расширение объёма проверок.
- **Количество хостов**
  Отображает число активов (серверы, рабочие станции, сетевые устройства и т.д.), находящихся в зоне мониторинга. Позволяет понять, насколько широко охвачена система безопасности.

Слева или сверху (в зависимости от настроек интерфейса) могут располагаться **фильтры** для выбора группы активов и временного диапазона (например, за последний месяц). При изменении этих фильтров сводные показатели пересчитываются.

### Распределение уязвимостей по критичности

Под сводными числами обычно идёт блок, показывающий, сколько уязвимостей относится к различным уровням критичности:

- **Критические** – наиболее опасные уязвимости, требующие незамедлительных действий.
- **Высокие** (или «Значительные») – серьёзные проблемы, которые также рекомендуется устранять в короткие сроки.
- **Средние** – уязвимости со средним уровнем риска.
- **Низкие** – относительно незначительные, но всё же заслуживающие внимания.

Для каждой категории указано общее количество проблем и доля от их совокупного числа (процент). Нередко рядом может отображаться небольшая стрелка или цветной маркер (например, зелёный, если количество снизилось, и красный, если выросло за выбранный период). Это упрощает мониторинг динамики.

### График динамики

Центральная часть панели часто содержит **график**, визуализирующий изменение числа уязвимостей во времени. По оси X отложены даты, по оси Y – количество обнаруженных проблем. Чаще всего кривые или «столбики» окрашены в разные цвета в зависимости от критичности (например, красным – критические, оранжевым – высокие, жёлтым – средние, зелёным – низкие).

- По графику можно отследить, возрастает или снижается суммарное количество уязвимостей.
- Резкие всплески могут означать крупные обновления системы или запуск новых задач сканирования, тогда как постепенное снижение указывает на успешную работу по исправлению уязвимостей.
- Наведение курсора на определённую точку может дать дополнительную информацию (количество уязвимостей в конкретный день и их категории).

### Таблицы «Топ-10»

В нижней части часто располагаются две сравнительные таблицы:

1. **Топ-10 уязвимых хостов**
    - Показывает устройства (IP-адрес или имя) с наибольшим количеством обнаруженных уязвимостей.
    - Позволяет быстро определить, какие хосты наиболее подвержены рискам и требуют первоочередного внимания.
    - Для каждого хоста может выводиться суммарная критичность или отдельно критические, высокие и пр. проблемы.
2. **Топ-10 уязвимостей**

- Список наиболее распространённых уязвимостей, встречающихся в сети.
- Позволяет увидеть, какие типы проблем чаще всего обнаруживаются (например, устаревшие версии программного обеспечения).
- Указывается, на скольких хостах была найдена та или иная уязвимость, и её уровень критичности.

Обе таблицы упрощают процесс приоритизации: вы видите, какие конкретные проблемы встречаются особенно часто (и на каких машинах), а также какие хосты нуждаются в повышенном внимании.

### Табличное управление активами

Раздел предназначен для работы со списком хостов (активов), обнаруженных или добавленных в систему для мониторинга уязвимостей. Представлен в виде таблицы, где каждая строка соответствует отдельному активу.

#### Основные столбцы таблицы

1. **Имя (хоста или сервера)** – сетевое или логическое название актива.
2. **IP-адрес** – один или несколько адресов, связанных с активом.
3. **Количество уязвимостей** – общее число найденных проблем (суммарно или в разбивке по критичности).
4. **Дата последнего сканирования** – когда система в последний раз обновляла данные об уязвимостях на данном хосте.
5. **Статус** – текущее состояние актива (например, «Активен», «Выключен»), если предусмотрено в системе.

#### Фильтры и поиск

- **Строка поиска** в верхней части таблицы – для быстрого нахождения нужного хоста по имени или IP.
- **Выбор группы активов** – при необходимости можно переключаться между заранее определёнными группами (если они созданы), чтобы ограничивать список отображаемых хостов.
- **Быстрые фильтры** – в некоторых столбцах (например, «Статус») доступно выпадающее меню для показа только активов с определённым значением.

#### Работа с активами

- **Просмотр подробностей**: при клике на имя актива или специальную кнопку в строке открывается отдельное окно/панель с детальной информацией по уязвимостям и свойствам хоста.
- **Добавление актива**: кнопка «Добавить» (или аналогичная) позволяет вручную ввести название, IP-адрес и при необходимости дополнительные данные.
- **Редактирование**: если нужно изменить информацию об активе (например, уточнить имя), в строке таблицы доступна кнопка «Редактировать».
- **Удаление**: при наличии прав можно удалить неактуальные или ошибочно добавленные хосты, используя соответствующую кнопку или пункт меню.

### Управление уязвимостями хоста

- **Список уязвимостей**: внутри карточки актива (открывается из таблицы) отображаются уязвимости, обнаруженные системой.
- **Статусы уязвимостей**: если предусмотрено, можно отметить уязвимость как «Исправлена» или «Ложное срабатывание».
- **Дата обнаружения**: показывает, когда конкретная уязвимость была впервые найдена.
- **Рекомендации по устранению**: при наличии – ссылка или краткое описание, что нужно сделать для исправления.

## Контактная информация

Контактная информация ООО “Крайон”, 119285, г. Москва, МЖД Киевское, 5-й км, д. 1, строен. 1, этаж 4, помещение 6/4, + 7 (495) 269 0584 Info@krayon.ru

### Контакты службы поддержки

Связаться со службой технической поддержки можно по электронной почте support@hscan.io.