RedCheck

СРЕДСТВО АНАЛИЗА ЗАЩИЩЕННОСТИ

Руководство пользователя

АЛМЮ.501410.RC02-01.РП

Версия документа 2.8.0.ru

Содержание

Перед началом работы

RedCheck – современное средство анализа защищенности, позволяющее выявлять уязвимости операционных систем и приложений, потенциально опасные настройки, осуществлять оценку соответствия требованиям политик и стандартов, проводить инвентаризацию оборудования и программ, а также формировать детальные отчеты.

Данное руководство пользователя для RedCheck (далее – RedCheck, Система) содержит описание возможностей и функций программы, рекомендации по использованию, условия и порядок работы в RedCheck.

Руководство предназначено для администраторов ИБ. Разработчик может вносить в Руководство изменения, связанные с улучшением Системы. Актуальная версия документации публикуется в новой редакции Руководства, а также на сайте компании.

Что нового в RedCheck 2.8.0

- Обновлен инструмент создания хостов (значительное повышение скорости работы и новые возможности)
- Добавлен функционал подбора учетных записей для сканирования
- Добавлен мониторинг служб сканирования
- Добавлен функционал повторного перезапуска недоступных хостов во время сканирования
- Новый модуль Аналитики

Содержание

- 3 Учетные записи для сканирования
- 4 Задания для сканирования
- 5 Расширенные возможности для заданий сканирования
- 6 Результаты сканирований
- 7 Отчеты
- 8 Аналитика
- Дополнительные возможности

Дополнительный материал перед началом работы

- Рабочий процесс в RedCheck
- Ролевая модель RedCheck
- Сведения об интегральной оценке по базовым метрикам CVSS

Рабочий процесс в RedCheck

Рабочий процесс подразумевает под собой взаимодействие с хостами, которые добавляются в RedCheck через Менеджер учетных записей. Ниже предлагается рекомендуемая последовательность работы в Системе.

Алгоритм работы с активами

Этап 1. Интерпретация сканируемой инфраструктуры в объекты RedCheck

На данном этапе производится создание групп (1 Группы) и добавление в них хостов (2 Хосты) для дальнейшего сканирования.

Этап 2. Подготовка учетных записей для доступа к сканируемым хостам

Для доступа к хостам во время выполнения задач сканирования используются учетные записи RedCheck, которые добавляются в Систему в Менеджере учетных записей (3 Учетные записи). На данном этапе создаются учетные записи для каждой сканируемой в дальнейшем платформы.

Этап 3. Создание заданий для сканирования

На данном этапе создаются задания для проведения сканирований инфраструктуры, ранее интерпретированной в объекты RedCheck (4 Задания / 5 Расширенные возможности для создания заданий)

Этап 4. Просмотр результатов сканирования

На данном этапе пользователь может ознакомиться с результатами выполнения ранее созданных заданий (6 Результаты сканирований), создает отчеты (7 Отчеты). Результаты сканирований находятся во вкладке **История**. Сформированные отчеты находятся во вкладке **Отчеты**.

Ролевая модель RedCheck

RedCheck для разграничения прав доступа использует ролевую модель. Роль пользователя в Системе определяется его принадлежностью к одной (или нескольким) из четырех групп RedCheck:

- **REDCHECK_ADMINS** – суперпользователь;
- **REDCHECK_ADMINIS** – администратор ИБ;
- **REDCHECK_SYSTEMS** – системный администратор;
- **REDCHECK_USERS** – пользователь ИБ.

Подробную информацию о возможностях каждой из ролей смотрите в Руководстве администратора (1.5 Ролевая модель RedCheck).

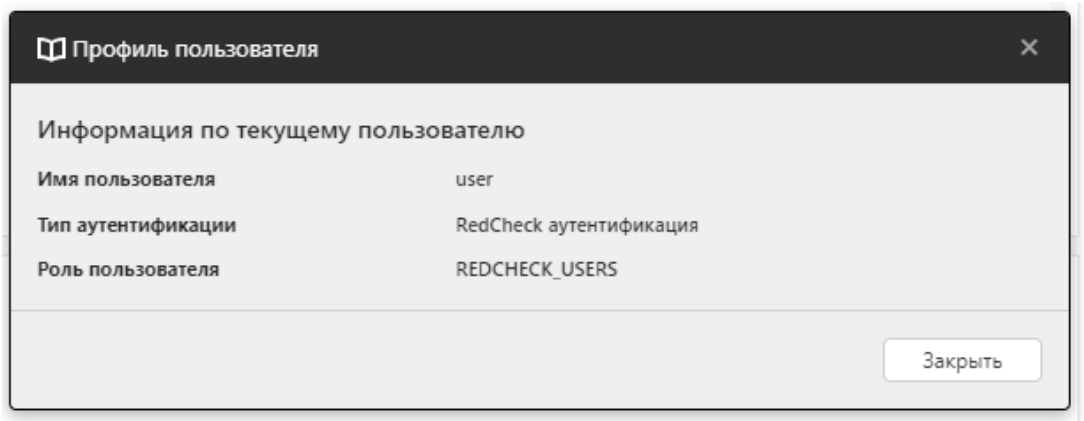
Просмотр активных сессий

Для просмотра активных сессий (информация о пользователях, работающих с консолью управления на текущий момент) нажмите 

. В открывшемся окне будет информация: имя и роль пользователя; IP-адрес, с которого выполнен вход; клиент (браузер); время начала сессии; тип авторизации (Локальный пользователь).

Просмотр информации о пользователе

Для просмотра информации о пользователе, под которым вы вошли в консоль управления, нажмите на имя пользователя.


Профиль пользователя
Информация по текущему пользователю
Имя пользователя
user
Тип аутентификации
RedCheck аутентификация
Роль пользователя
REDCHECK_USERS
Закрыть

Сведения об интегральной оценке по базовым метрикам CVSS

Обращаем внимание, что уровень критичности для уязвимости рассчитывается согласно CVSS из самого приоритетного источника. Порядок приоритетов:

- ALTEX-SOFT (экспертная оценка);
- Вендор продукта;
- BDU;
- NKCKI;
- NVD.

Возможно расхождение в уровне критичности, если уязвимость имеет CVSS из источника, более приоритетного, чем NVD. То-есть CVSS из NVD отличается от CVSS из более приоритетного источника настолько сильно, что числовые значения попадают в диапазоны разных уровней критичности.

Если уязвимость имеет статус риска **Недоступно**, но в какой-либо из вышеперечисленных баз уязвимостей есть значение CVSS, это означает, что вендор продукта не предоставил своей оценки уровня критичности для данного продукта.

1 Группы

Группа - это список хостов, которые являются ключевыми объектами для работы в RedCheck. При добавлении хостов в RedCheck обязательно указывается группа, поэтому при начале работы необходимо создать как минимум одну группу.

Группировка позволяет управлять сложной сетью, упрощая процесс работы в RedCheck.

Примеры использования группирования хостов

Ниже представлены самые распространенные варианты объединения хостов.

По платформе (ОС): Если в инфраструктуре сети находятся хосты с разными ОС, целесообразно будет сгруппировать их по этому признаку.

По установленным продуктам: В случае, когда для работы используется несколько серверов, например Nginx и IIS. Объединение хостов в соответствии с установленным на хосте сервером будет правильным решением.

По сетевому расположению: Хосты на предприятии могут находиться в разных подсетях. Полезно разделить их по данному критерию.

По подразделению управления: У каждого сотрудника отдела ИБ может быть своя зона ответственности, поэтому группировка хостов каждого сотрудника в отдельную группу является хорошей практикой.

> Реализованный метод группировки позволяет одному хосту входить в несколько групп, но не подразумевает вложенность групп одна в другую.

Содержание

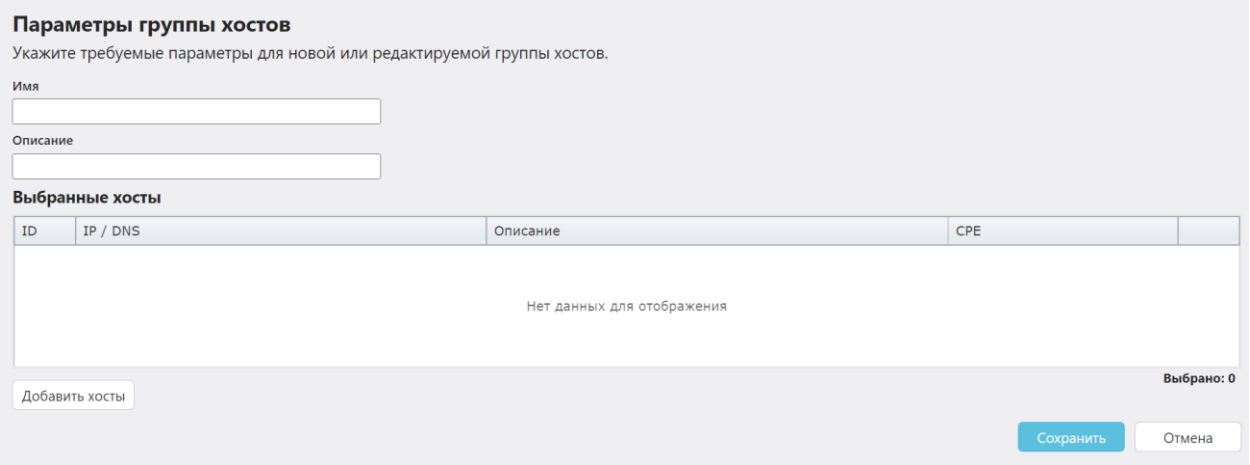
1.1 Создание группы

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Systems

Чтобы создать пустую группу, выполните следующие шаги.

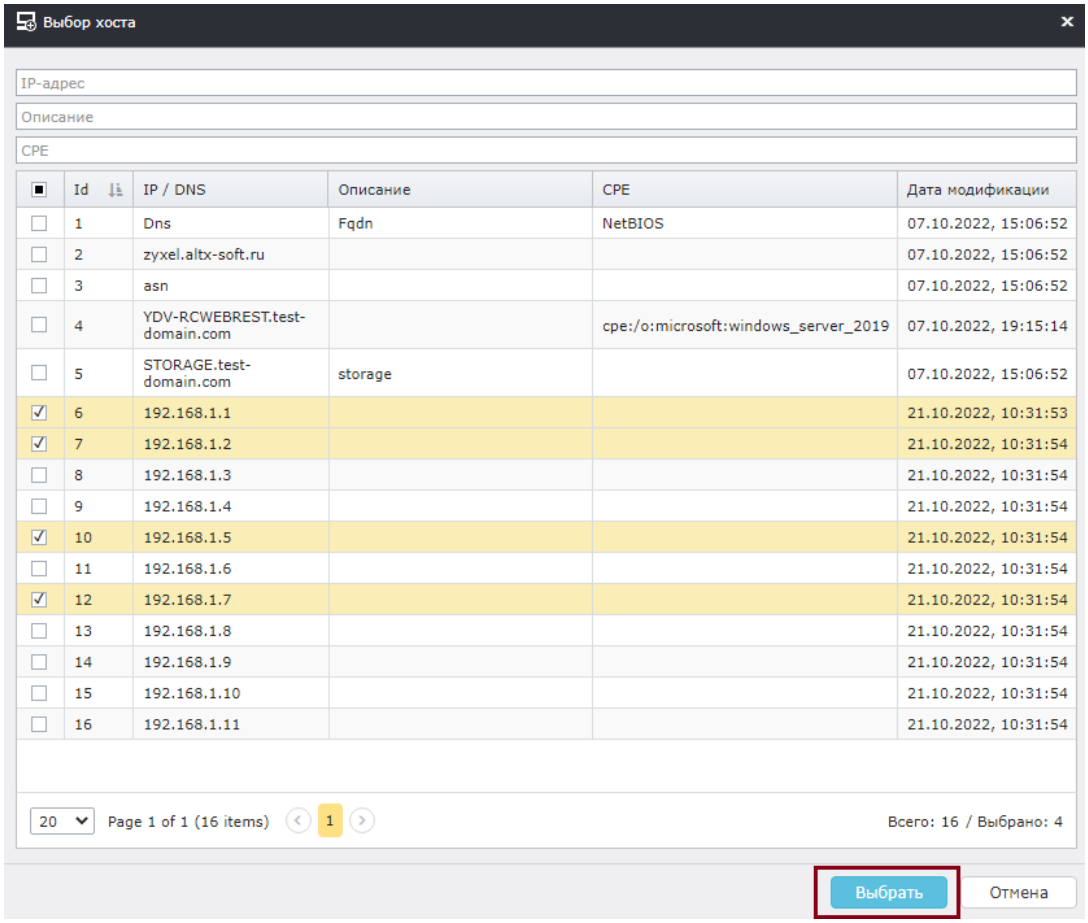
Шаг 1. Откройте **Инструменты** → **Создать группу**;

Шаг 2. Укажите имя группы и описание при необходимости → **Сохранить**;



> Так как в RedCheck хосты могут входить в несколько групп, то при создании новой группы есть возможность добавить в нее уже имеющиеся в других группах хосты.

Нажмите **Добавить хосты** → отметьте необходимые хосты → **Выбрать**;

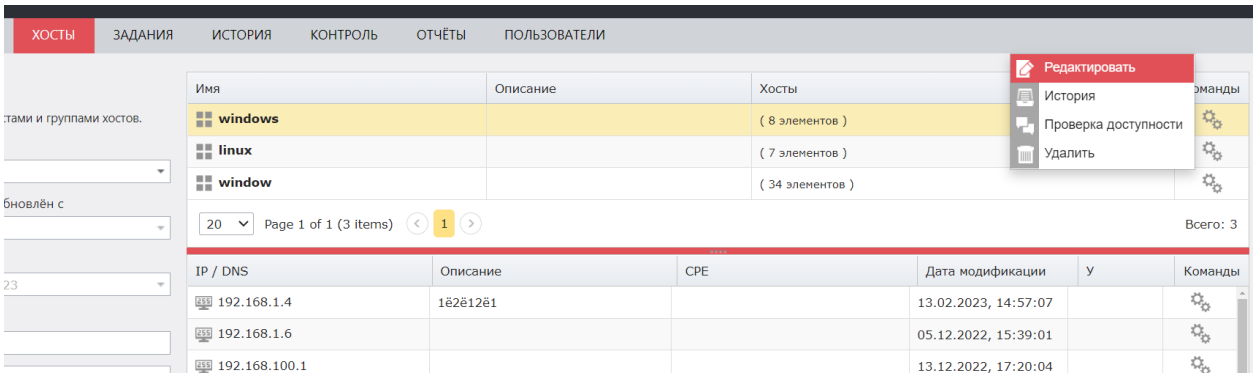

Выбор хоста
IP-адрес
Описание
CPE
Id
IP / DNS
Описание
CPE
Дата модификации
1 Dns Fqdn NetBIOS 07.10.2022, 15:06:52
2 zyxel.altx-soft.ru 07.10.2022, 15:06:52
3 asn 07.10.2022, 15:06:52
4 YDV-RCWEBREST.test-domain.com cpe:/o:microsoft:windows_server_2019 07.10.2022, 19:15:14
5 STORAGE.test-domain.com storage 07.10.2022, 15:06:52
6 192.168.1.1 21.10.2022, 10:31:53
7 192.168.1.2 21.10.2022, 10:31:54
8 192.168.1.3 21.10.2022, 10:31:54
9 192.168.1.4 21.10.2022, 10:31:54
10 192.168.1.5 21.10.2022, 10:31:54
11 192.168.1.6 21.10.2022, 10:31:54
12 192.168.1.7 21.10.2022, 10:31:54
13 192.168.1.8 21.10.2022, 10:31:54
14 192.168.1.9 21.10.2022, 10:31:54
15 192.168.1.10 21.10.2022, 10:31:54
16 192.168.1.11 21.10.2022, 10:31:54
20
Page 1 of 1 (16 items)
1
Всего: 16 / Выбрано: 4
Выбрать
Отмена

1.2 Возможности группы

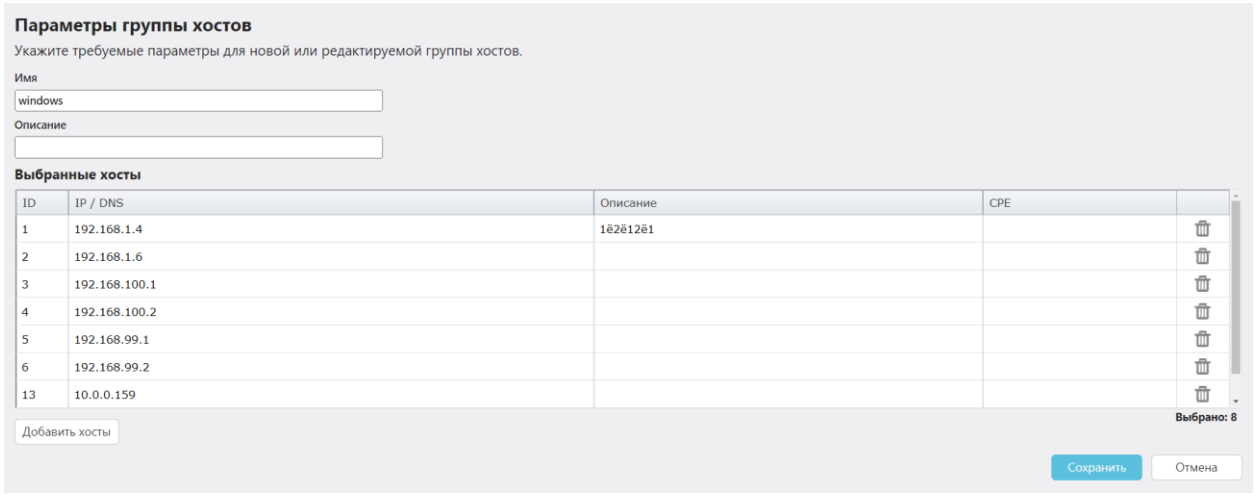
Для того, чтобы отредактировать ранее созданную группу, выполните следующие шаги.

Шаг 1. Перейдите в **Хосты**. Верхняя таблица будет содержать список групп. При нажатии на строку какой-либо группы в нижней таблице появятся хосты, входящие в группу;

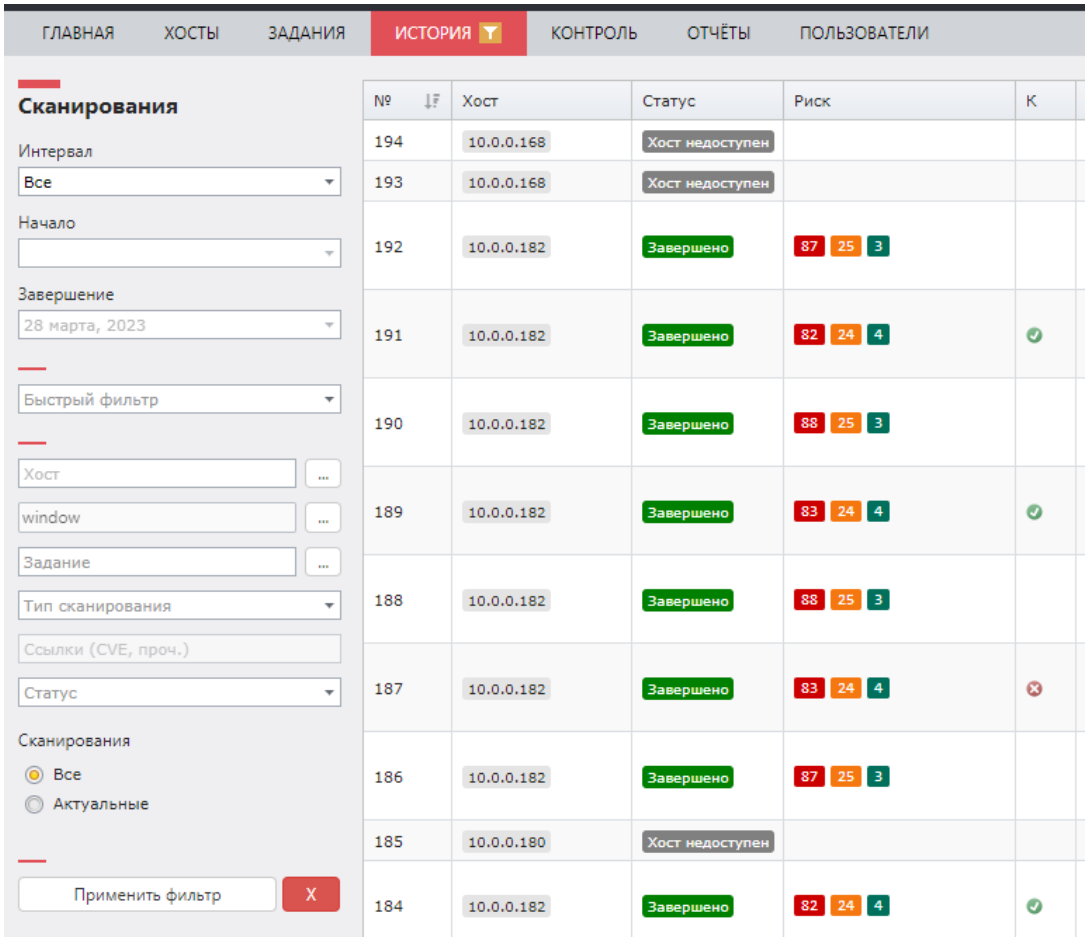
Шаг 2. Для редактирования группы нажмите → **Редактировать**.



RedCheck позволяет изменить имя, описание и состав группы после ее создания.



Для просмотра результатов сканирования хостов, находящихся в выбранной группе, нажмите **История** (6 Результаты сканирований)



Для проверки доступности к хостам, входящим в выбранную группу, нажмите **Проверка доступности**. Данная функция создаст задание типа **Проверка доступности** (4.11 Проверка доступности) и автоматически укажет выбранную группу (все входящие в нее хосты) как цель сканирования.

2 Хосты

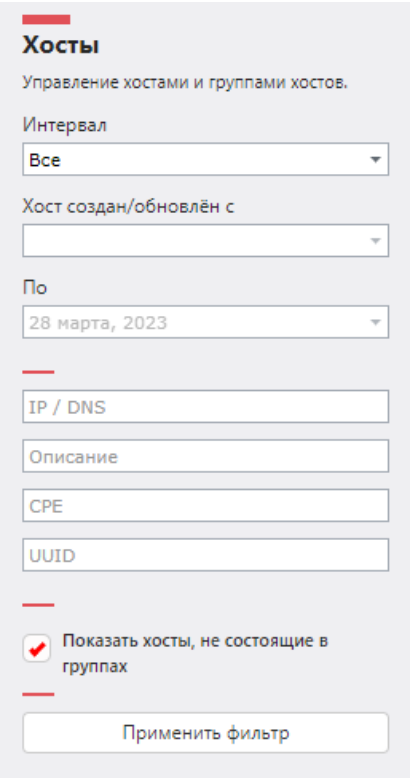
Хост – объект сканирования RedCheck. Каждый хост в Системе входит в одну или несколько групп.

> Перед добавлением хостов в Систему необходимо, чтобы была создана как минимум одна группа, в которой будут состоять новые хосты (1.1 Создание группы).

> При удалении группы возможна ситуация, когда хосты, входящие в нее, перестают относиться к какой-либо группе.

Для того, чтобы посмотреть хосты, не состоящие в группах, выполните следующее действие.

Перейдите в **Хосты** → отметьте соответствующий параметр в свойствах фильтра. В нижней таблице отобразятся хосты.



Способы добавления хостов

Добавить хосты в БД RedCheck можно несколькими способами:

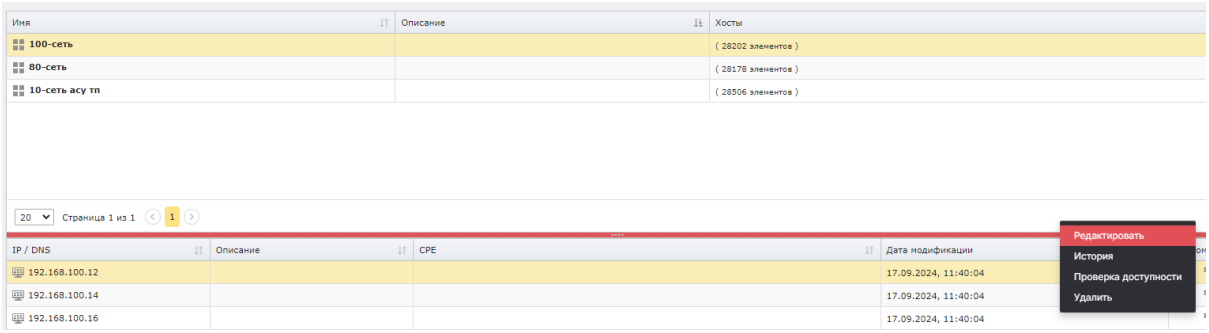
- 2.1 Создание хостов вручную
- 2.2 Импорт из CSV-файла
- 2.3 Импорт из AD
- 2.4 Импорт из Host Discovery
- 2.5 Экспорт хостов в CSV

Редактирование хоста

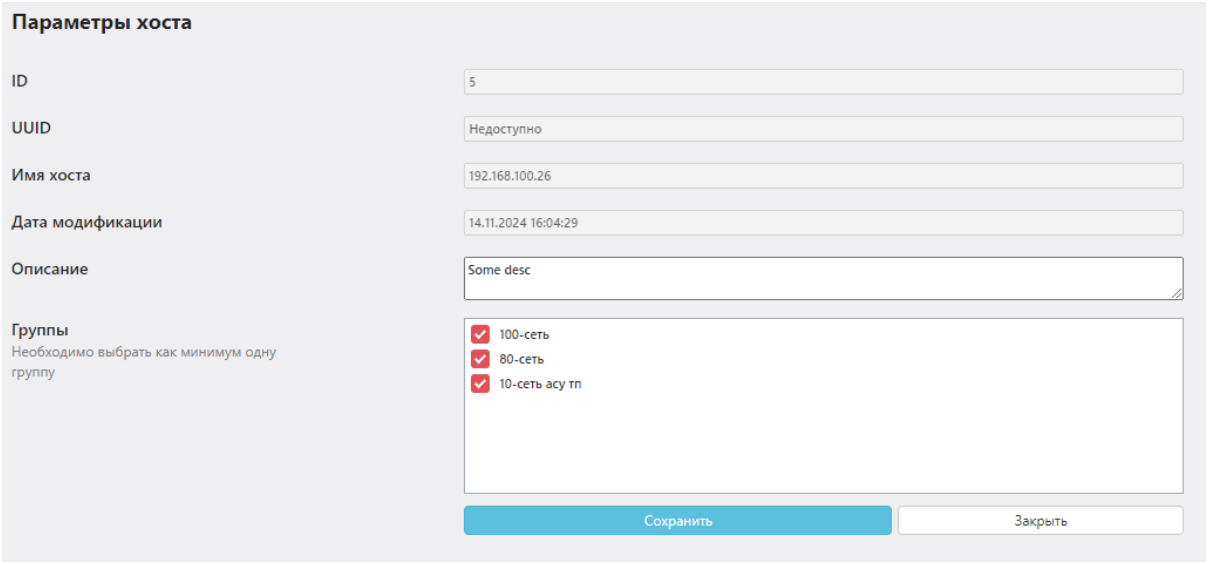
Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Systems

Для того, чтобы изменить данные хоста, выполните следующие действия.

Шаг 1. Перейдите в **Хосты** → выберите группу, в которой находятся нужные хосты → нажмите → **Редактировать**;



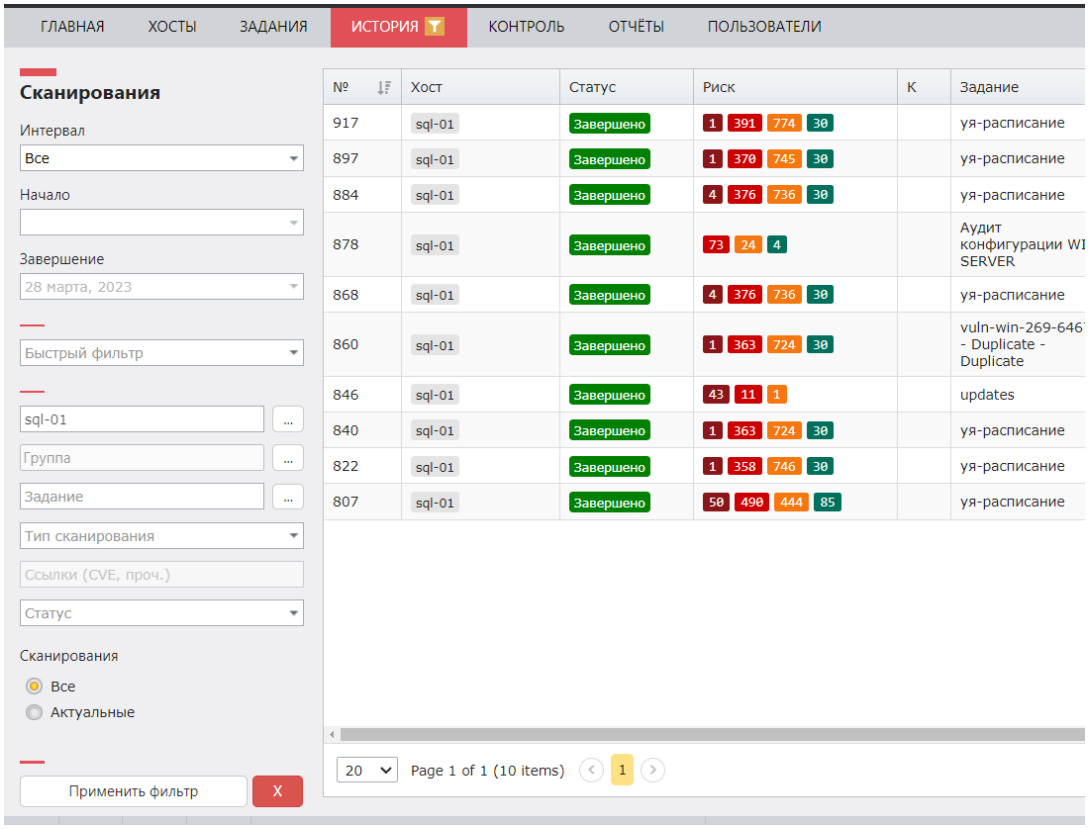
При редактировании хоста можно изменить описание и группы, в которые входит хост.



Шаг 2. Внесите изменения → **Сохранить**.

Просмотр результатов сканирования

Для просмотра результатов сканирования хоста нажмите **История** (6 Результаты сканирований)



Для проверки доступности хоста нажмите **Проверка доступности**. Данная функция создаст задание типа **Проверка доступности** (4.11 Проверка доступности) и автоматически укажет выбранный хост как цель сканирования.

2.1 Создание хостов вручную

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Systems

Для создания хостов выполните следующие шаги.

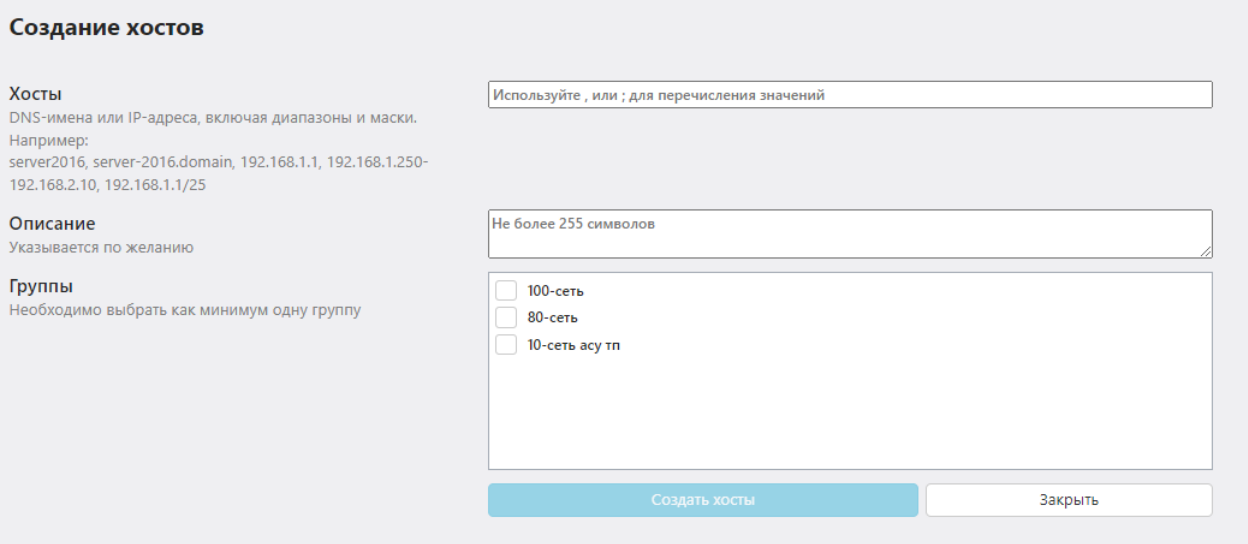
Шаг 1. Раскройте **Инструменты** → **Создать хост**;

Шаг 2. Заполните форму → **Сохранить**.

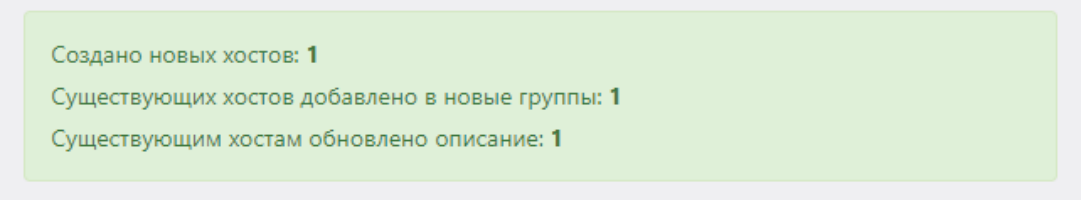
- Хосты – можно указывать IP-адреса, DNS-имена, диапазоны IP-адресов и маски подсети;
- Группы – группы, в которые будут входить добавляемые хосты;

Если среди указанных хостов есть уже существующие в RedCheck, то:

- Описание таких хостов будет обновлено на указанное, если на момент изменения оно было у хоста пустым. Если у существующего хоста уже есть описание, оно обновлено не будет;
- Существующие хосты будут добавлены в указанные группы, если ранее в них не состояли.



При успешном создании хостов будет выведена дополнительная информация:



Перед добавлением хостов в Систему необходимо, чтобы была создана как минимум одна группа, в которой будут состоять новые хосты (1.1 Создание группы).

2.2 Импорт из CSV-файла

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Systems

Формат csv – это текстовый файл с разделителями. В первой строке через разделитель **«;»** указываются названия столбцов. Последующие строки являются записями с информацией о хостах. Значения в строке также указываются через разделитель **«;»**.

Структура csv-файла

Базовая структура csv-файла для импорта хостов в RedCheck должна соответствовать:

Group	GroupDesc	Host	HostDesc	CPE	Action
Название группы	Описание группы	Имя/адрес хоста	Описание хоста	Конфигурация устройства	Определяет действие, выполняемое над хостом Принимает значение Delete

> В случае отсутствия первой строки-заголовка информация о хостах будет обрабатываться в соответствии с вышеуказанной структурой столбцов.

Базовая структура может быть переопределена. Например, при заголовке **Group;Host** в строке с информацией о хосте достаточно указать только название группы и имя/адрес хоста.

Файл должен иметь кодировку UTF-8, чтобы избежать проблем с импортом русскоязычных символов.

Сценарии использования

Структура (Group;Host). Создается группа G1 без описания, в которую добавляются хосты H1, H2, H3 без описания, CPE опускается, параметр Action пустой, так как ничего не удаляется.

Код

```
Group;Host
G1;H1
G1;H2
G1;H3
```

Структура (Group;Host;Action). Хосты удаляются из группы G1 и становятся непривязанными к какой-либо группе. После удаления трех хостов из группы в нее добавляется новый хост H11 (столбец Action остается пустым).

Код

```
Group;Host;Action
G1;H1;Delete
G1;H2;Delete
G1;H3;Delete
G1;H11;
```

Структура (Group;Action). Будут удалены все группы, а привязанные хосты станут непривязанными к какой-либо группе.

Код

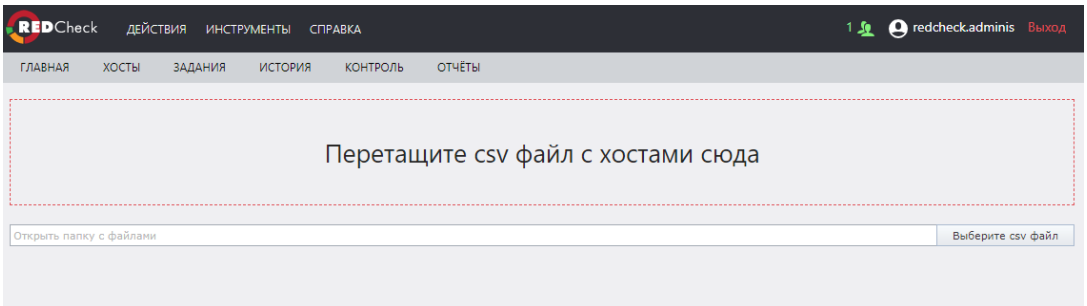
```
Group;Action
*;Delete
```

Импортирование csv-файла

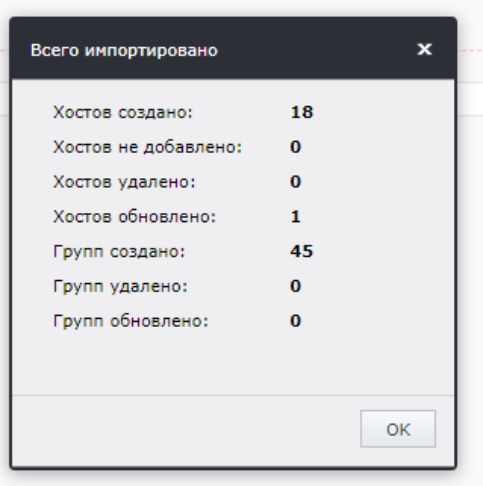
Для добавления хостов с помощью csv-файла выполните следующие шаги.

Шаг 1. Раскройте **Инструменты** → **Импорт хостов** → **Csv file**;

Шаг 2. Перетащите csv-файл в поле или нажмите **Выберите csv файл**;



После завершения импорта появится уведомление с результатом операции.



2.3 Импорт из AD

> Для автоматического импорта хостов из Active Directory по расписанию рекомендуется использовать утилиту RedCheck Import AD (Руководство по эксплуатации утилиты RedCheck Import Active Directory).

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Systems

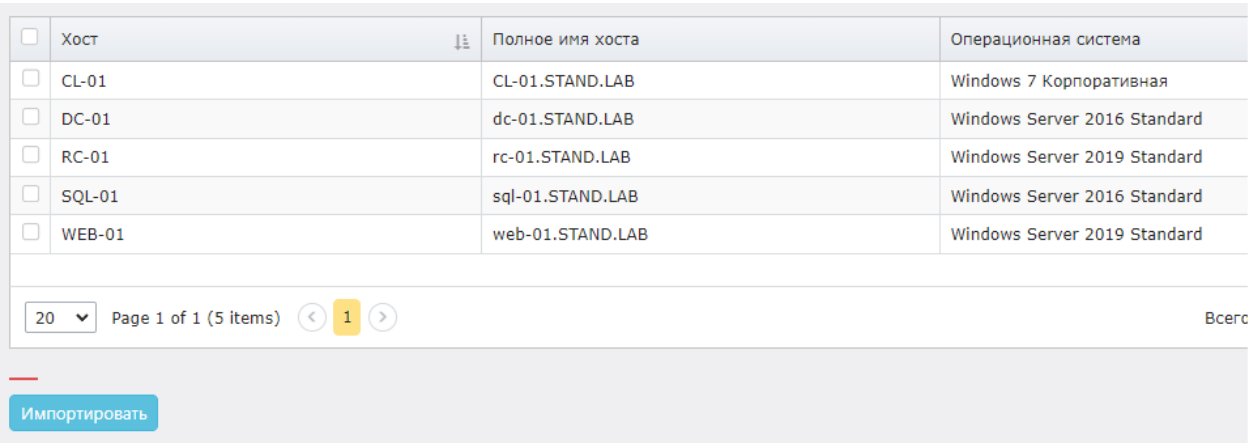
RedCheck предоставляет возможность вручную импортировать хосты, находящиеся в домене. Для этого выполните следующие шаги.

Шаг 1. Раскройте **Инструменты** → **Импорт хостов** → **Active Directory**;

Шаг 2. Заполните форму для поиска → **Искать хосты**;

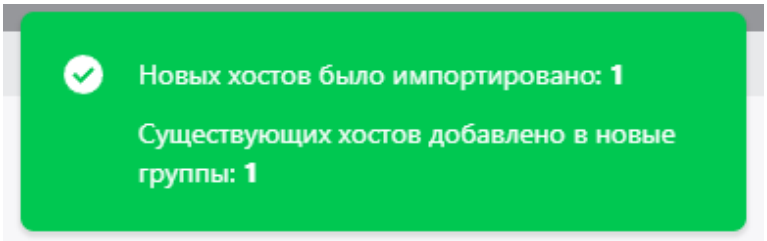
- Тип протокола – ActiveDirectory, ALD, FreeIPA;
- Адрес контроллера домена – хост контроллера домена, имеющийся в RedCheck, или указанный самостоятельно адрес хоста;
- Профиль – учетная запись RedCheck любого пользователя домена (создание учетных записей для сканирования);
- Группа – группа, в которую будут добавлены импортированные хосты;
- AD путь – путь к хостам в Active Directory (опционально);
- Фильтр – критерий, по которому происходит поиск. Рекомендуется оставить значение по умолчанию;
- Импортировать:
  - Хост – будет импортировано FQDN или IP-адрес хоста;
  - Полное имя хоста – будет импортировано DNS-имя хоста.

Шаг 3. Отметьте необходимые хосты → **Импортировать**;



Если хост уже существует в RedCheck, он будет добавлен в указанную группу, если ранее в ней не состоял

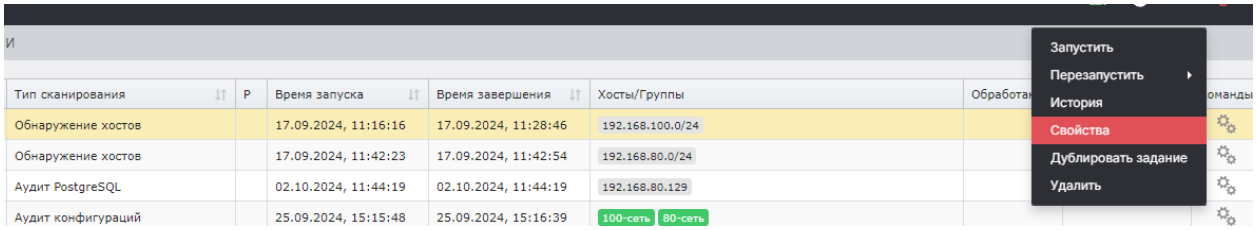
Если импорт прошел успешно, появится уведомление с информацией:


Новых хостов было импортировано: 1
Существующих хостов добавлено в новые группы: 1

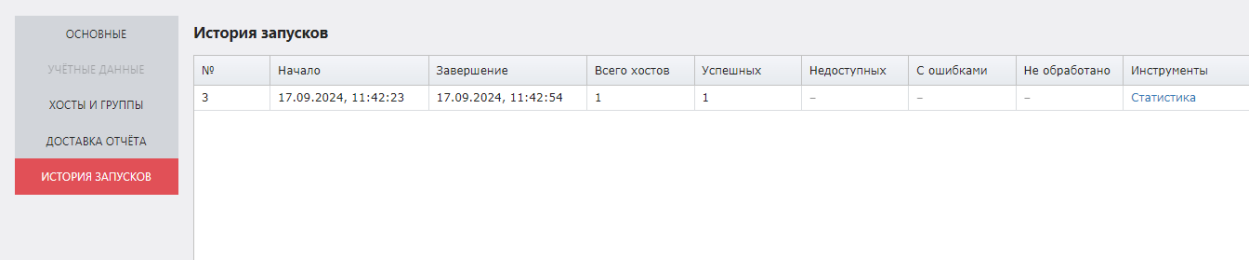
2.4 Импорт из Host Discovery

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

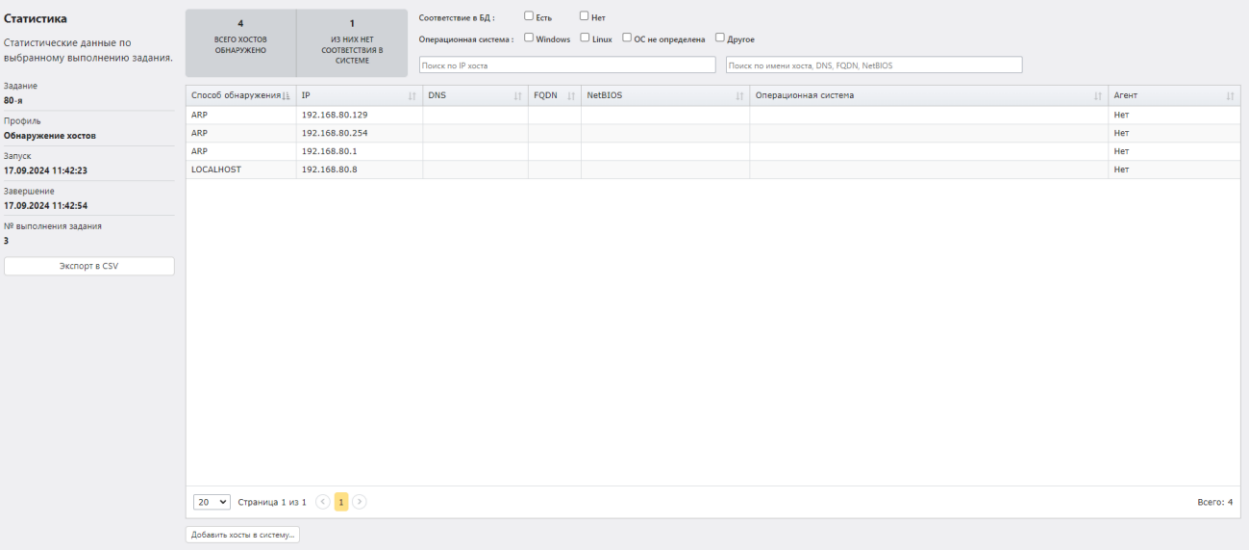
Шаг 1. Перейдите в свойства задания типа Обнаружение хостов, нажав ⚙ → **Свойства**;



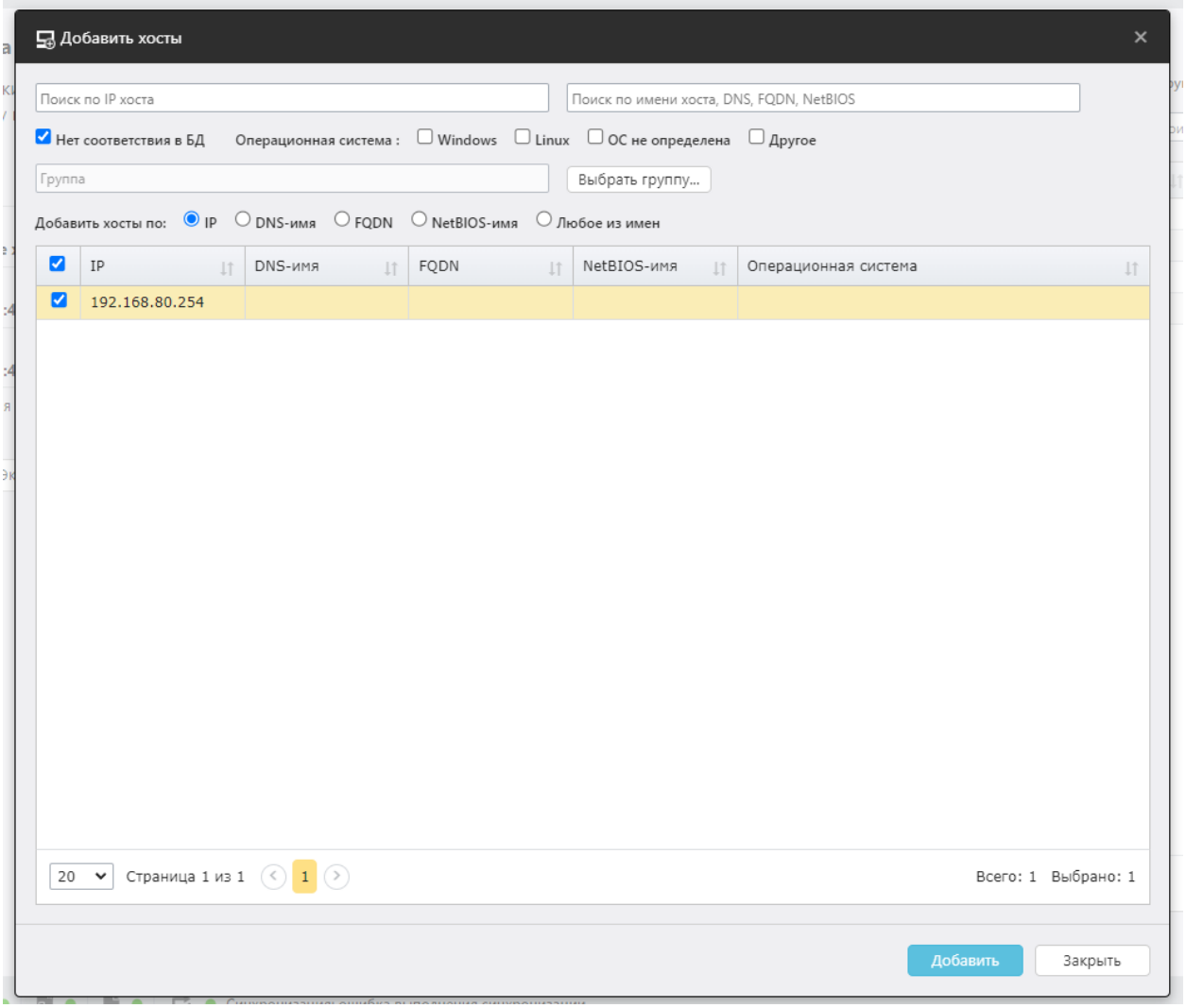
Шаг 2. Перейдите во вкладку **История запусков** → нажмите **Статистика** напротив нужного завершенного сканирования;



В появившемся окне можно просмотреть все найденные хосты и доступную для них информацию.

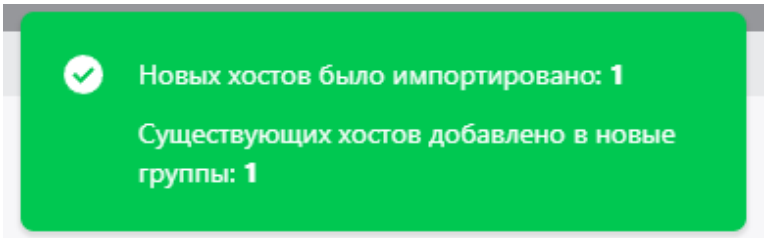


Шаг 3. Нажмите **Добавить хосты в систему** → в появившемся окне отметьте хосты, которые хотите добавить в БД → выберите группу, в которую будут добавлены хосты, нажав **Выбрать группу** → выберите что именно будет добавлено (IP, DNS, FQDN или NetBIOS), нажав на соответствующий radio-button → нажмите **Добавить**;



Если хост уже существует в RedCheck, он будет добавлен в указанную группу, если ранее в ней не состоял

Если импорт прошел успешно, появится уведомление с информацией:



2.5 Экспорт хостов в CSV

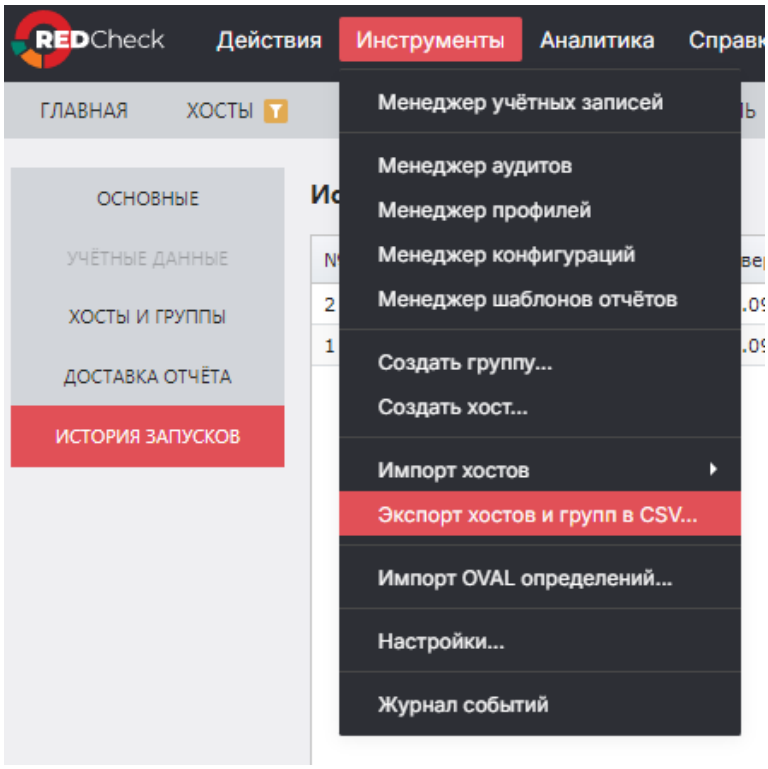
RedCheck позволяет экспортировать имеющуюся в базе данных инфраструктуру в CSV-файл. Получающийся файл можно импортировать в RedCheck.

Структура csv-файла

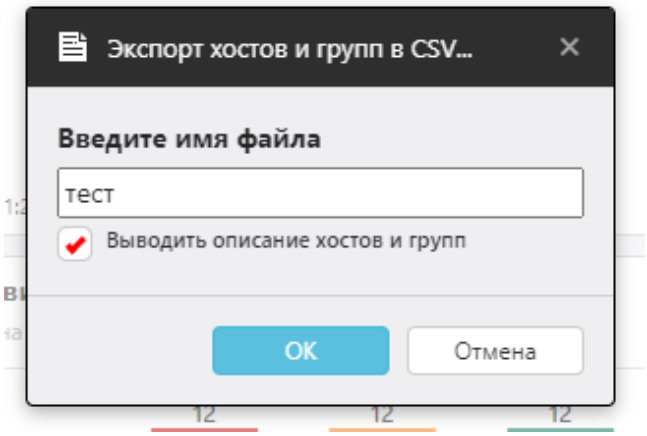
Group	GroupDesc	Host	HostDesc	CPE
Название группы	Описание группы	Имя/адрес хоста	Описание хоста	Конфигурация устройства

> Базовая структура может быть переопределена. (2.2 Импорт из CSV-файла).

Шаг 1. Раскройте **Инструменты → Экспорт хостов и групп в CSV**;



Шаг 2. Введите имя файла → отметьте по необходимости опцию **Выводить описание хостов и групп** → **ОК**.



После нажатия **OK** начнется скачивание файла.

3 Учетные записи для сканирования

Учетная запись – объект RedCheck, необходимый для доступа к хостам во время выполнения сканирования. Учетная запись состоит из данных для подключения к сканируемому хосту (учетные данные пользователя, порты для протоколов доступа), настроек привилегий и других параметров. Управление учетными записями для сканирования производится через Менеджер учетных записей (3.1 Менеджер учетных записей)

> Задания Аудит в режиме Пентест, Обнаружение хостов и Аудит АСУ ТП не требуют создания учетных записей для сканирования.

RedCheck позволяет сканировать следующие платформы:

- Windows;
- Linux-системы;
- Сетевое оборудование;
- Системы виртуализации и контейнеризации;
- СУБД;
- Контролеры и протоколы АСУ ТП.

В Системе реализовано два режима доступа к сканируемому хосту:

- Режим черного ящика – сетевое сканирование без привилегий;
- Режим белого ящика:
    - сканирование с использованием непривилегированной учетной записи и агента сканирования RedCheck;
    - сканирование с использованием привилегированной учетной записи без использования агента сканирования;

С подробным перечнем платформ и доступных для них режимов сканирования можно ознакомиться в Руководстве администратора (1.9 Перечень поддерживаемых платформ).

Типы учетных записей

RedCheck предлагает следующие типы учетных записей для соответствующих платформ:

- Windows;
- SSH;
- SQL:
  - Microsoft SQL Server;
  - MySQL;
  - Oracle;
  - PostgreSQL;
- Cisco:
  - Cisco IOS;
  - Cisco NX-OS;
- Huawei VRP;
- VMware:
  - VMware ESXi;
  - VMware vCenter;
  - VMware NSX;
- Solaris;
- FreeBSD;
- Check Point (GAiA);
- Fortinet FortiOS;
- UserGate NGFW.

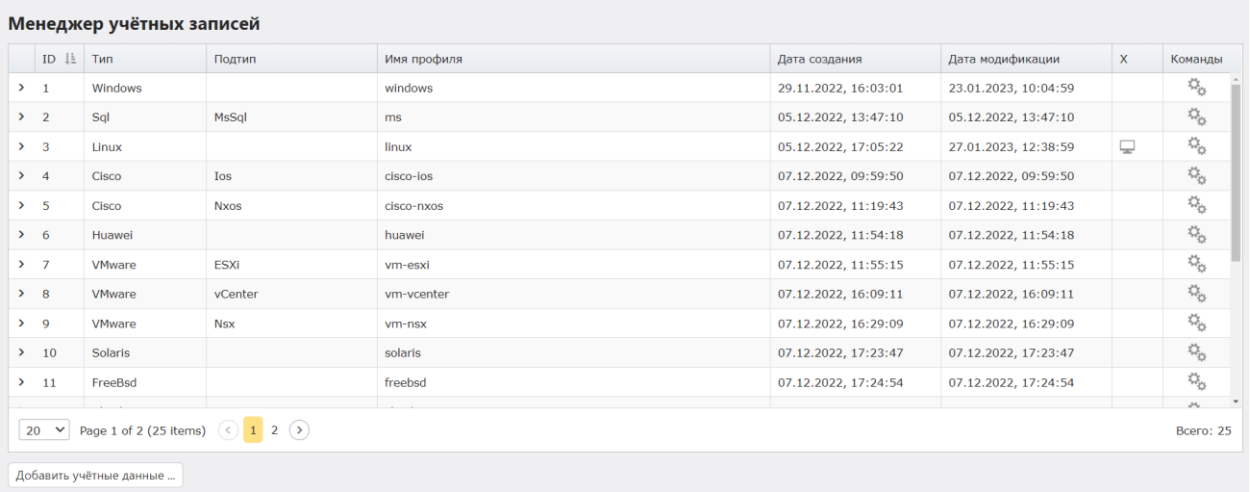
3.1 Менеджер учетных записей

Создание учетной записи для сканирования

Необходимая роль: RedCheck_Admins / RedCheck_Systems

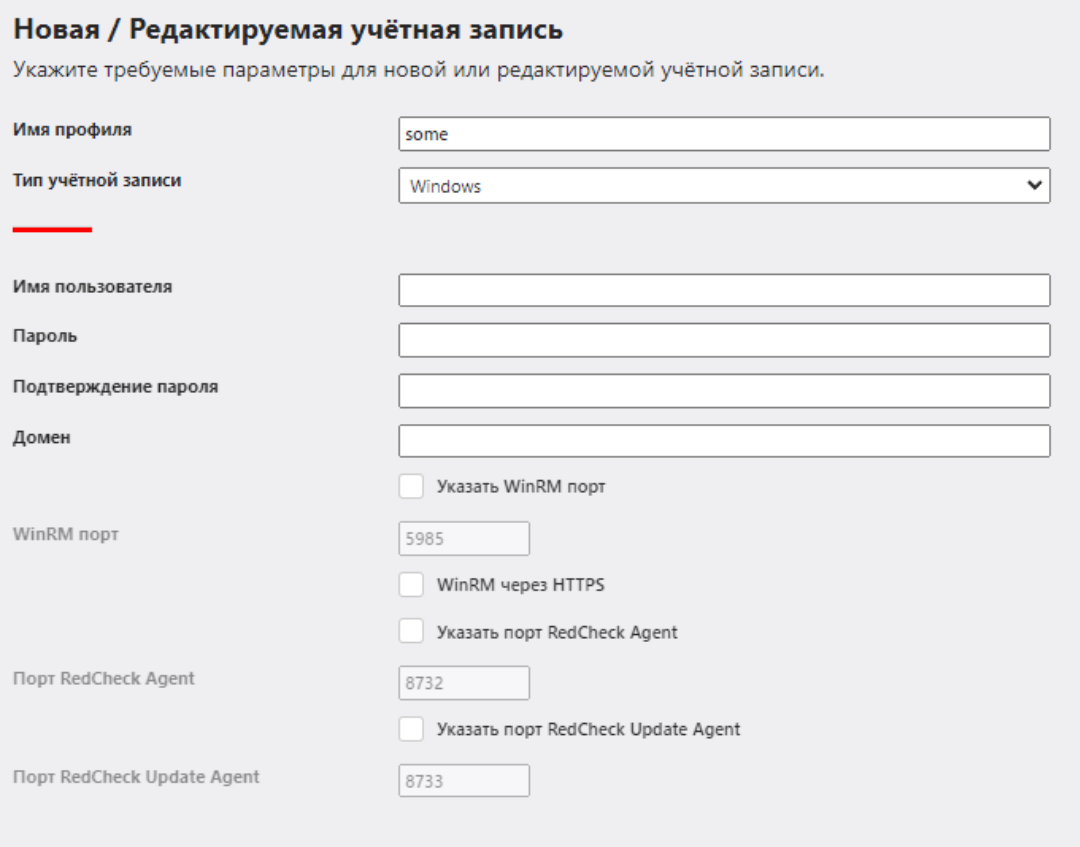
Для создания учетной записи выполните следующие шаги.

Шаг 1. Раскройте **Инструменты** → **Менеджер учетных записей** → **Добавить учетные данные**;



Шаг 2. Укажите имя и выберите тип учетной записи → заполните необходимые параметры для выбранного типа учетной записи → **Сохранить**.

> Значения, находящиеся в неактивных полях, могут быть изменены при выборе соответствующего режима сканирования. Например, активация поля **Указать SSH порт** откроет доступ для изменения порта.



Для того, чтобы быстро создать копию уже существующей учетной записи, в Менеджере учетных записей нажмите ⚙ → **Дублировать;**

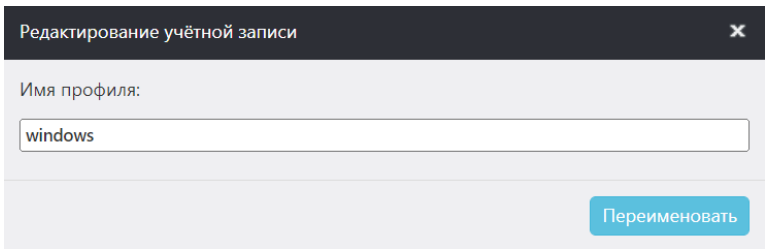
Редактирование учетной записи

Необходимая роль: RedCheck_Admins / RedCheck_Systems

RedCheck предоставляет возможность изменить имя, параметры доступа и привилегий. Нажмите **Инструменты** → **Менеджер учетных записей** → ⚙ → **Редактировать**;

Чтобы быстро сменить имя учетной записи, в Менеджере учетных записей

нажмите ⚙ → **Переименовать** → введите новое имя → **Переименовать**;



3.2 Подбор учетных записей для сканирования

При создании задания можно указать несколько учетных записей, которые будут использоваться для сканирования. В процессе выполнения задания служба сканирования будет последовательно пробовать пройти аутентификацию на хосте с помощью каждой учетной записи. Перебор будет происходить до первой удачной аутентификации. Хост считается недоступным, если ни одна из учетных записей не подошла.

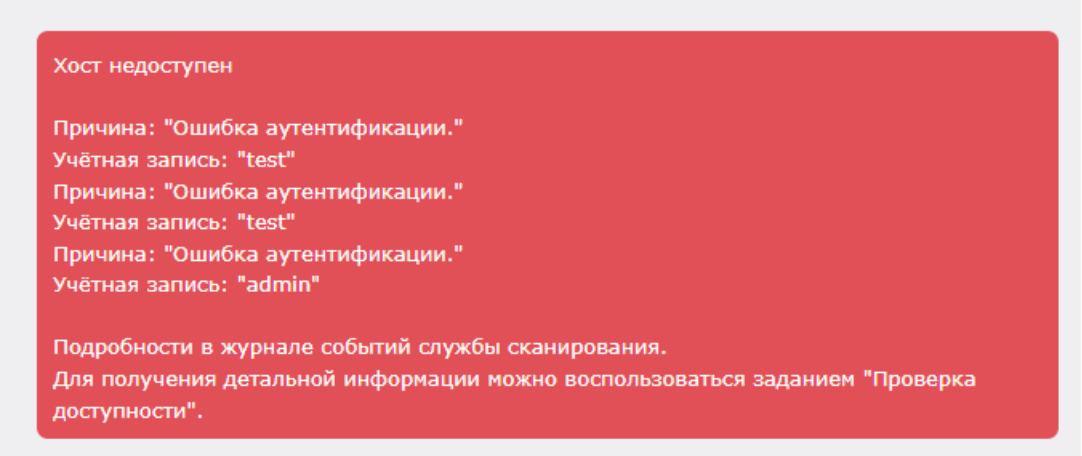
Задания, для которых реализован данный функционал:

- Аудит уязвимостей / обновлений
- Аудит конфигураций
- Инвентаризация
- Аудит СУБД

Порядок проверки учетной записи. При создании и редактировании задания можно задавать порядок учетных записей, согласно которому служба сканирования будет проверять учетные данные во время аутентификации на хосте. Чтобы изменить порядок, перетащите строку на нужное место в таблице, используя ⇅ рядом с именем учетной записи.

Удаление из списка. Для удаления учетной записи из списка нажмите ⚙ → **Удалить**.

Результаты сканирования. В случае, если служба сканирования не смогла пройти аутентификацию ни одной из указанных учетных записей, будет создан результат сканирования со статусом Хост недоступен, где будут перечислены логины учетных записей, не прошедших аутентификацию.



В результате сканирования со статусом Завершено / Ошибка не отображается учетная запись, прошедшая аутентификацию.

Ограничения

> Нельзя указывать две и более учетные записи с одинаковыми логинами и протоколами, используемыми во время сканирования.

Некоторые типы учетных записей используют один и тот же протокол для сканирования. Например, SSH, FreeBSD, Solaris, Cisco и еще несколько типов используют SSH протокол. Такие учетные записи не могут быть добавлены в одно и то же задание в случае, если у них один и тот же логин для аутентификации.

На добавление в задание нескольких учетных записей одного типа и с одинаковыми логинами, но разными паролями, ограничений нет.

Например:

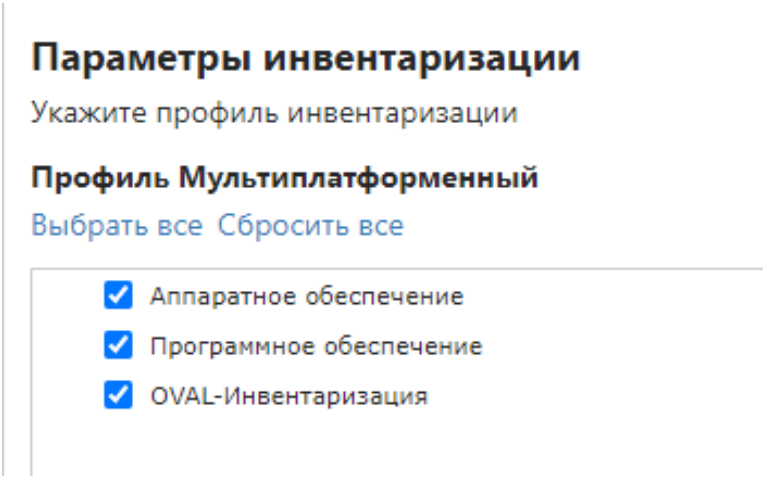
1. Учетные записи с типом Windows, «server 2012» с логином test и «server 2019» с логином test, но с другим паролем, **МОГУТ** быть добавлены в одно задание;

2. SSH учетная запись «astra server» с логином test и FreeBSD учетная запись «freebsd server» с логином test **НЕ МОГУТ** быть добавлены в одно задание.

Особенности

Аудит конфигураций. Список доступных для выбора конфигураций будет составлен согласно выбранным типам учетных записей. Например, если указаны две учетные записи Windows и SSH, то выбрать можно будет как Unix, так и Windows конфигурации.

Инвентаризация. В случае, если для задания указаны учетные записи разных типов, профиль инвентаризации будет установлен как Мультиплатформенный, т.е. для каждого хоста будет применен подходящий профиль с включением всех возможных параметров, но детализировать профиль (добавить или исключить параметры) будет нельзя.



4 Задания для сканирования

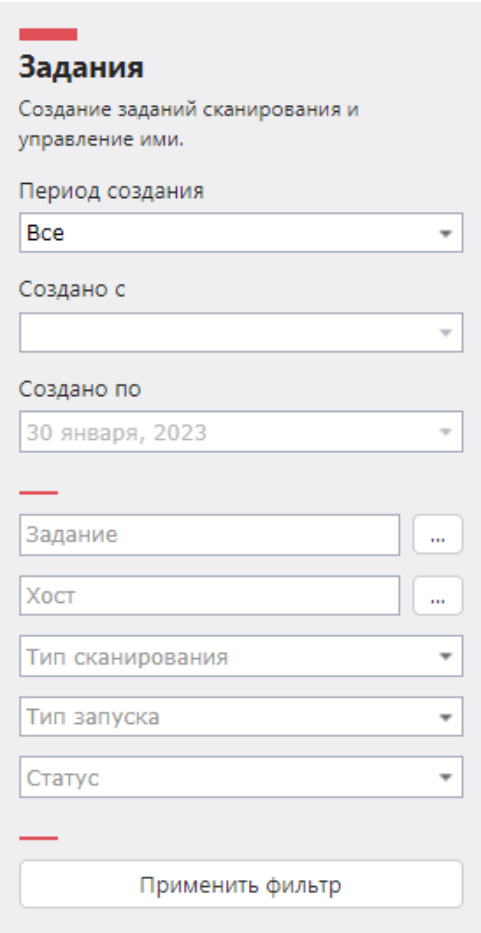
RedCheck предоставляет 10 различных типов задания:

Запуск задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Чтобы просмотреть список заданий, перейдите в **Задания** → нажмите  → **Запустить**;

Для сортировки заданий воспользуйтесь фильтром:



Остановка задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Для остановки задания нажмите → **Остановить**;

Остановка задания подразумевает завершение сканирования без возможности запуска с точки остановки.

Приостановка и возобновление задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Для приостановки выполнения задания нажмите → **Приостановить**;

Приостановка задания позволяет:

- Возобновить выполнение задания с точки приостановки (текущие сканирования хостов будут закончены);
- Посмотреть результаты уже отсканированных хостов;
- Создать отчет по уже отсканированным хостам.

Для возобновления задания нажмите → **Запустить**;

Перезапуск задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Для перезапуска задания нажмите → **Перезапустить** → выберите один из вариантов:

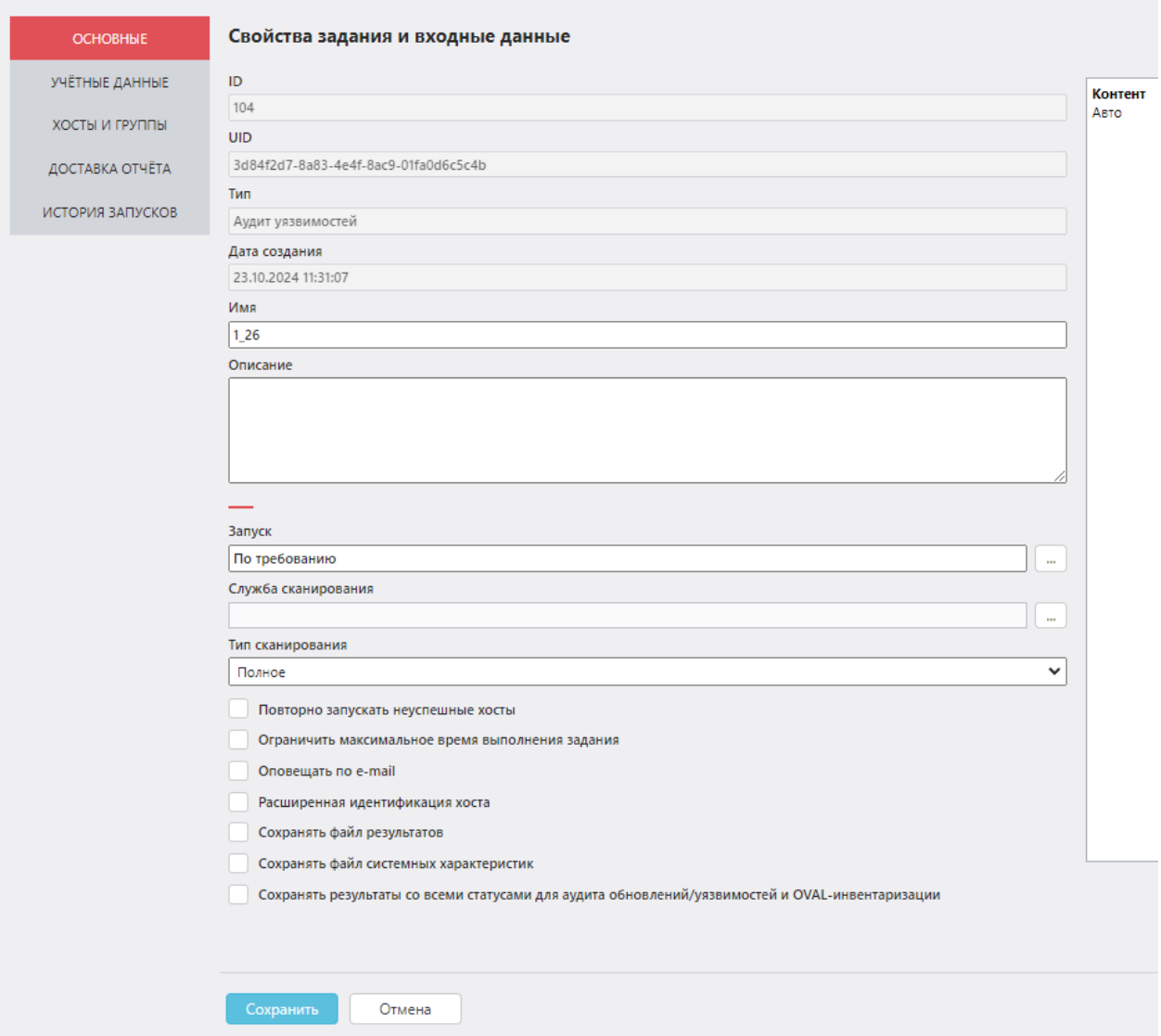
- Все – будет выполнено сканирование всех хостов, указанных в задании на момент перезапуска;
- Кроме успешных (последний запуск) – будет выполнено сканирование хостов, указанных в задании на момент перезапуска, которые при последнем выполнении задания завершились со статусом, отличным от **Завершено**;
- Только ошибочные (последний запуск) – будет выполнено сканирование хостов, указанных в задании на момент перезапуска, которые при последнем выполнении задания завершились со статусом **Ошибка**;
- Только недоступные (последний запуск) – будет выполнено сканирование хостов, указанных в задании на момент перезапуска, которые при последнем выполнении задания завершились со статусом **Хост недоступен**;

Редактирование задания

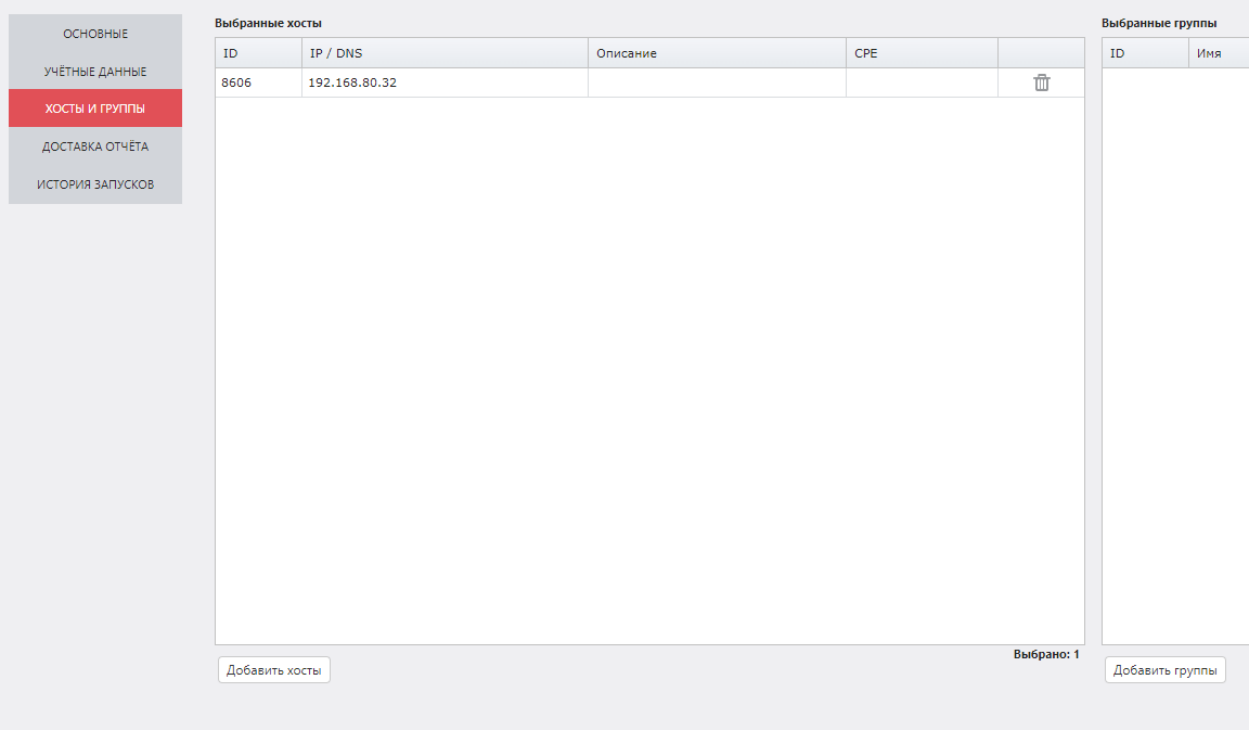
Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Нажмите ⚙ → **Свойства**;

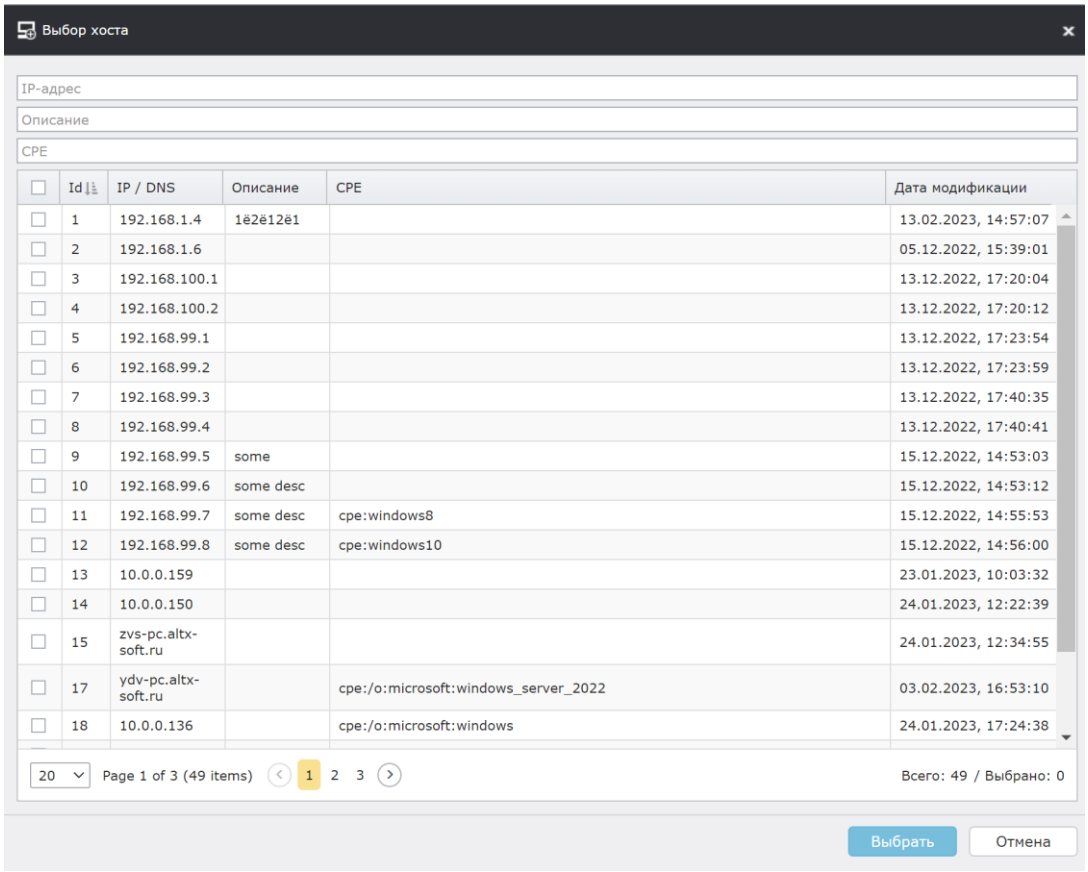
- Основные – возможность изменить имя, тип запуска, транспорт и другую информацию;



- Учетные данные – возможность изменить список учетных записей для сканирования (3.2 Подбор учетных записей для сканирования);
- Хосты и группы – возможность изменить список сканируемых хостов и групп;

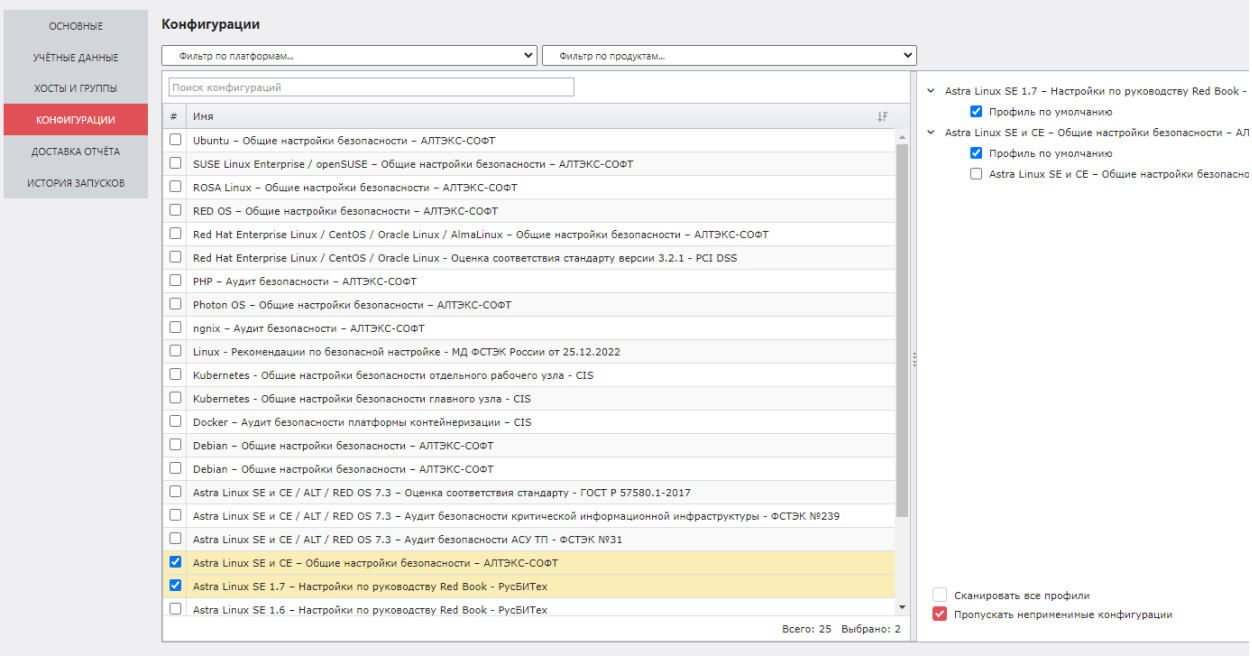


Чтобы удалить хост или группу, нажмите . Чтобы добавить хост или группу, нажмите **Добавить хосты** / **Добавить группы** → отметьте необходимые хосты → **Выбрать**.



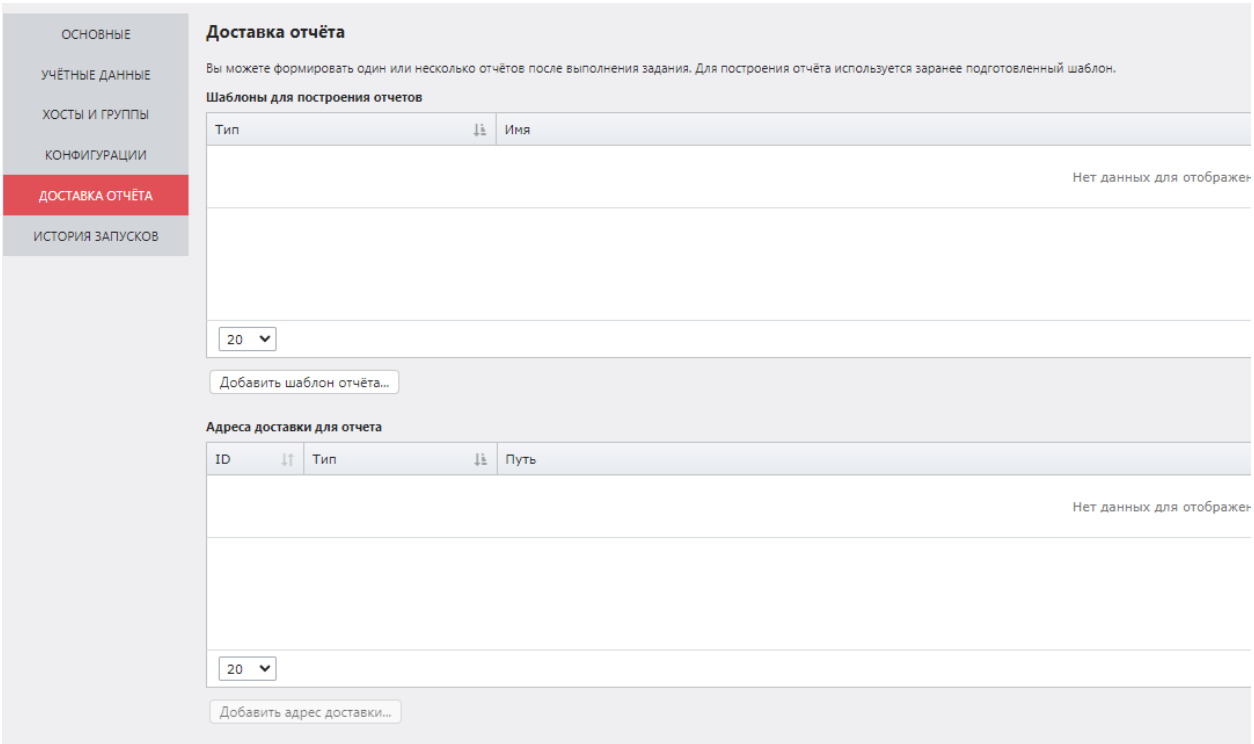
Нажмите **Сохранить** для внесения изменений.

- Конфигурации – возможность изменить список конфигураций и профилей для задания. Доступно для Аудита конфигураций.

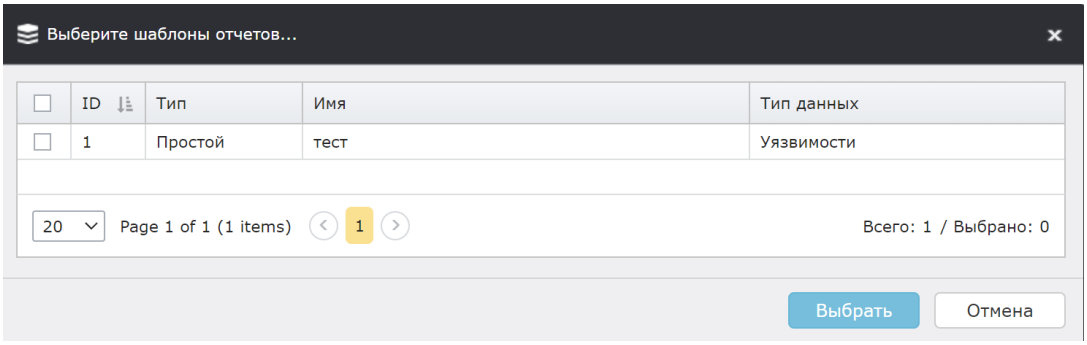


Чтобы добавить или убрать конфигурацию / профиль конфигурации, отметьте или снимите отметку с конфигурации / профиля → **Сохранить**.

- Доставка отчета – возможность назначить шаблоны для отчетов и адреса для их доставки;



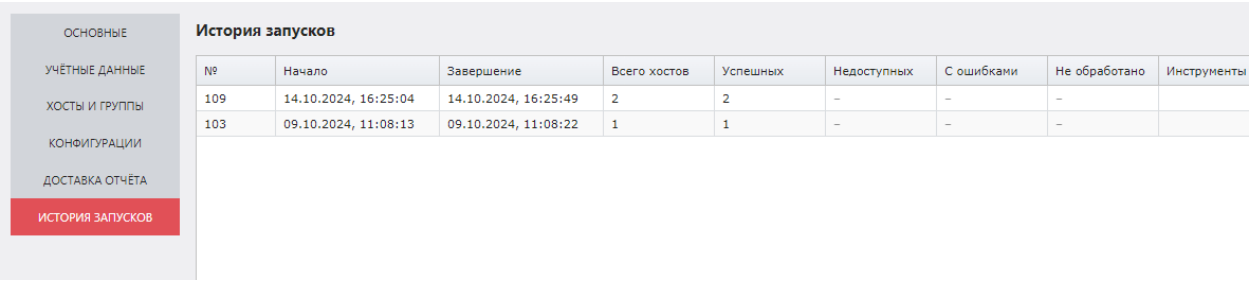
Чтобы указать шаблон отчета (7.3 Шаблоны отчетов), нажмите **Добавить шаблон отчета** → выберите шаблон отчета → **Выбрать**.



Чтобы указать адрес доставки, выберите добавленный шаблон отчета и нажмите **Добавить адрес доставки** → выберите адрес доставки → **Выбрать**.

Для внесения изменений нажмите **Сохранить**.

- История запусков – история сканирований и статистика по каждому из них.



Статистика актуальна для следующих типов заданий:

- Аудит в режиме «Пентест»;
- Обнаружение хостов;
- Проверка доступности

4.1 Аудит уязвимостей

RedCheck выполняет централизованное сетевое или локальное сканирование хостов на наличие уязвимостей ОС, общесистемного и прикладного ПО, а также сетевого оборудования. Во время сканирования сопоставляется состояние параметров системы сигнатурам уязвимостей, содержащихся в открытом Репозитории OVALdb и описанных в формате SCAP.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

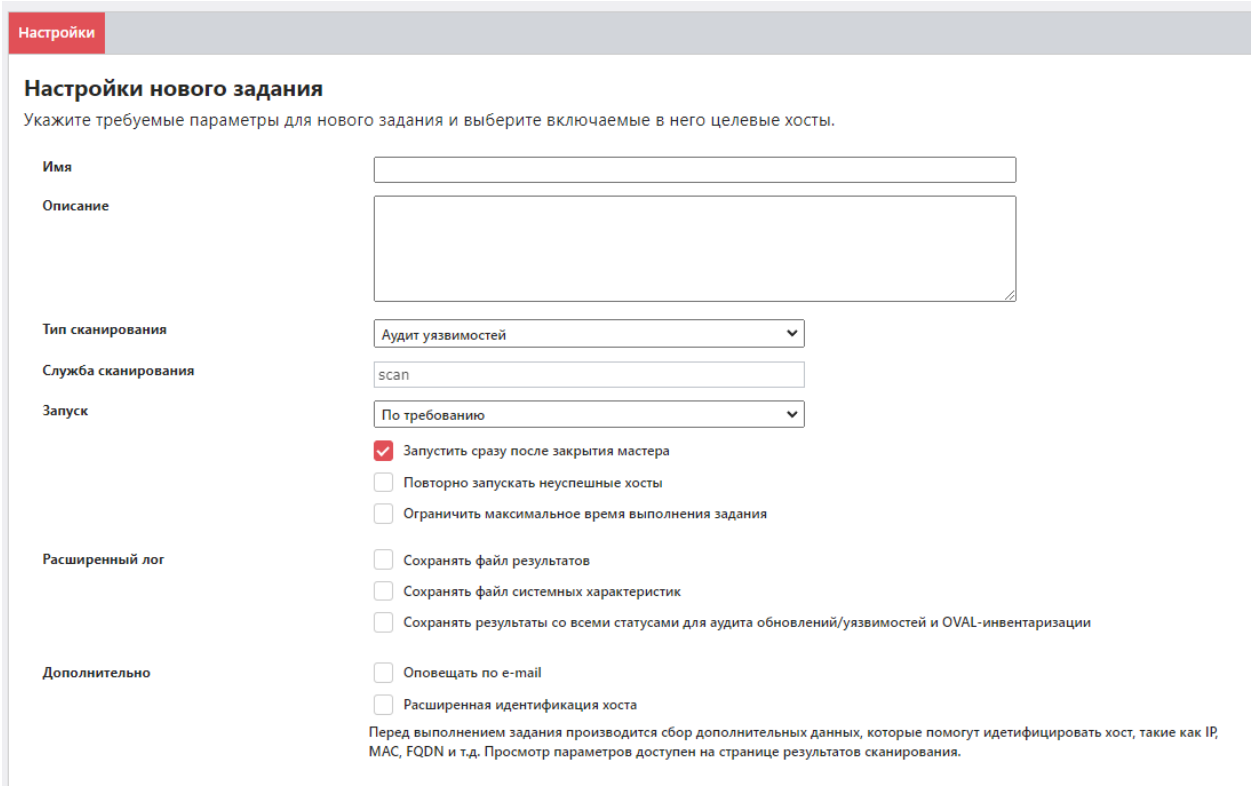
Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Аудит уязвимостей**;

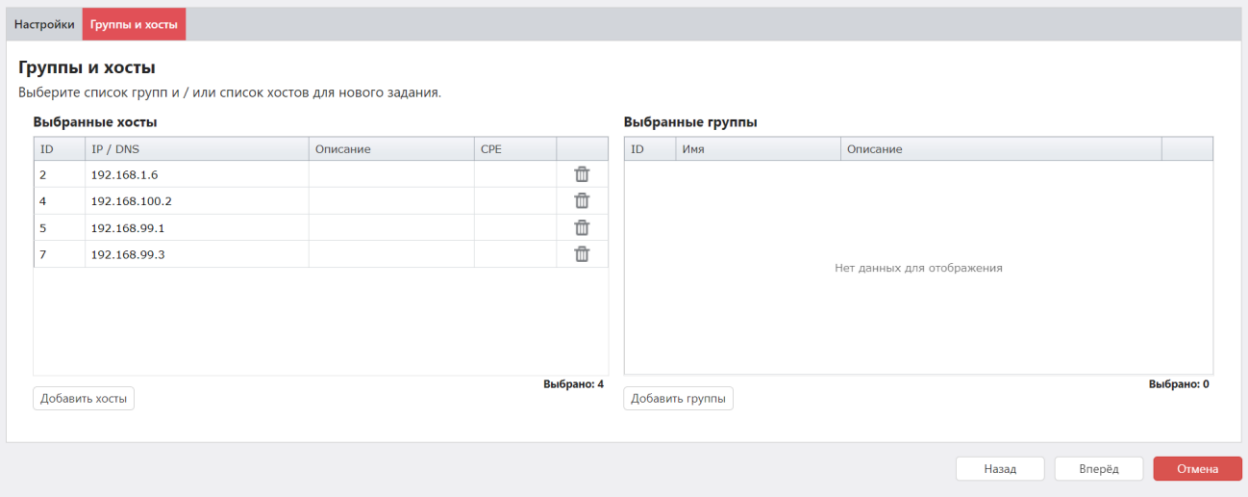
Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ... (Мониторинг служб сканирования);
- Тип запуска:
  - По требованию – запуск задания вручную;
  - По расписанию – задание будет выполняться согласно настроенному расписанию (Настройка расписания);
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;
- Повторно запускать неуспешные хосты – функция Повторного перезапуска недоступных хостов;

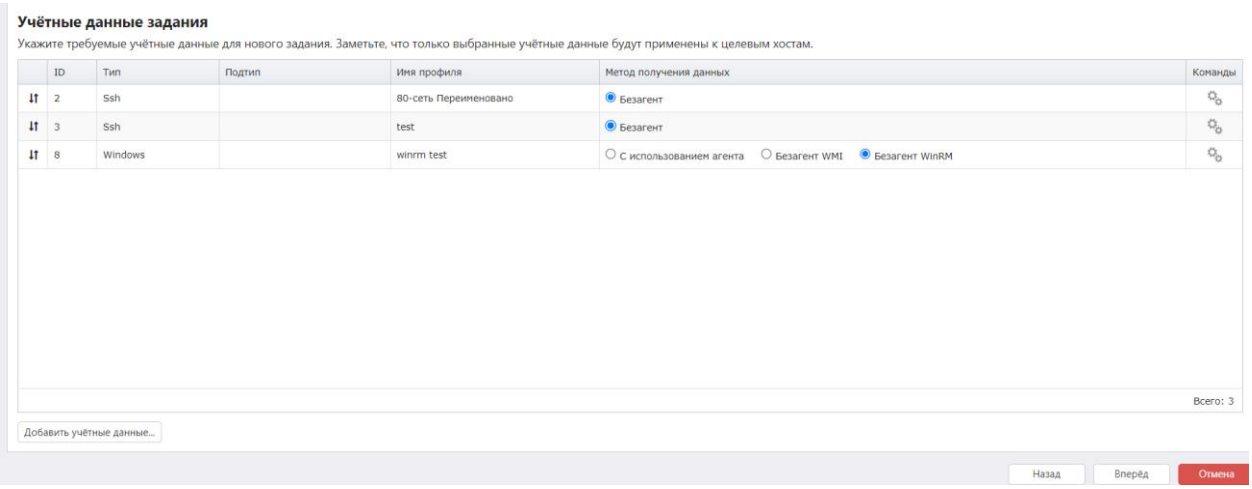
- Ограничить максимальное время выполнения задания – функция Остановки задания по времени выполнения;
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по-умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;
- Сохранять файл системных характеристик – сохранение информации о найденных состояниях на хосте без информации о контенте, который был проверен во время сканирования (по-умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/system-characteristics.xml**);
- Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации – при включенном параметре служба сканирования сохраняет в БД информацию о всех уязвимостях, которые были проверены во время сканирования, даже если они не были обнаружены. При выключенном параметре сохраняются только обнаруженные уязвимости. Выключенный параметр экономит место в БД;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;



Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;



Шаг 4. Выберите учетные записи для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

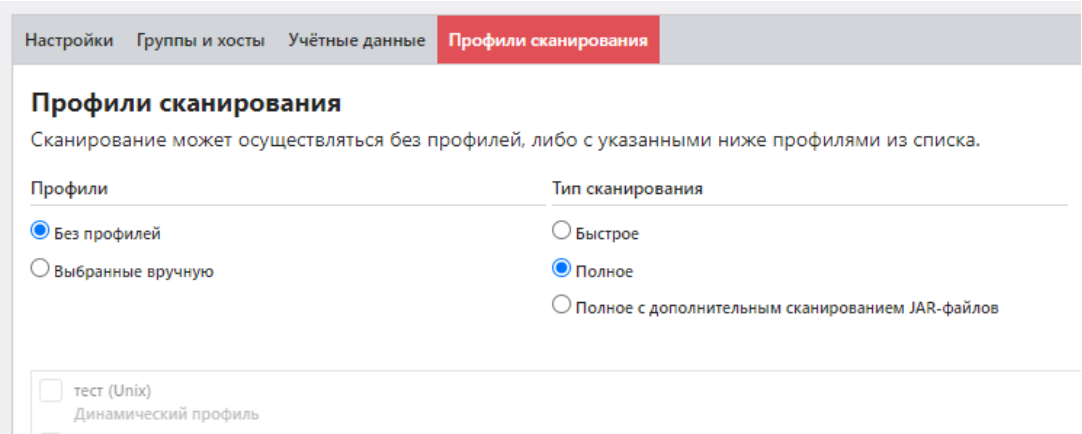


Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед**;

> [Подробнее про подбор учетных записей]

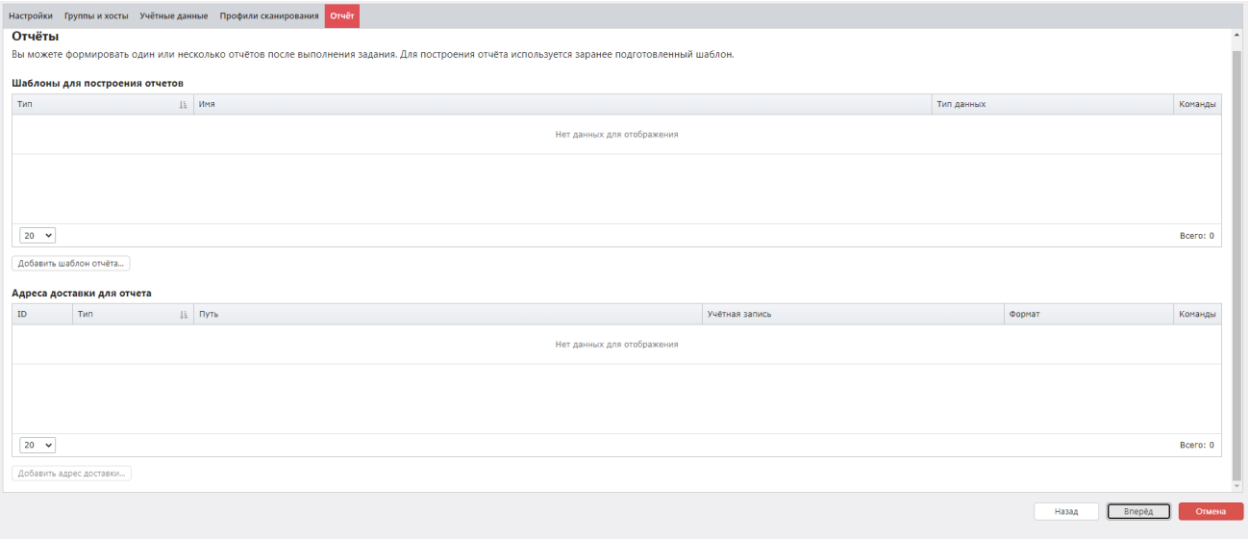
Шаг 5. Выберите профиль и тип сканирования → **Вперед**:

- Быстрое – не будут применяться рекурсивные сигнатуры. Сканирование выполнится быстрее.
- Полное – при сканировании будут использоваться глубокие (рекурсивные) сигнатуры, являющиеся трудоемкими. Аудит займет больше времени;
- Полное с дополнительным сканированием JAR-файлов – при сканировании будут использоваться дополнительные сигнатуры для проверки jar-файлов. Аудит займет больше времени. Только для сканирования Linux-платформ;



> О создании профилей сканирования смотрите в 5.1 Профили сканирования.

Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;



Шаг 7. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

4.2 Аудит обновлений

RedCheck позволяет обнаружить неустановленные обновления безопасности на узлах сети и сформировать необходимые ссылки для загрузки недостающих обновлений. Результат аудита обновлений содержит: наименования обновлений, сведения о рисках, связанных с отсутствием недостающего обновления на узле сети, ссылку на производителя, заявившего о выходе обновления, ссылку на репозиторий (базу), где хранятся доступные для загрузки обновления.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

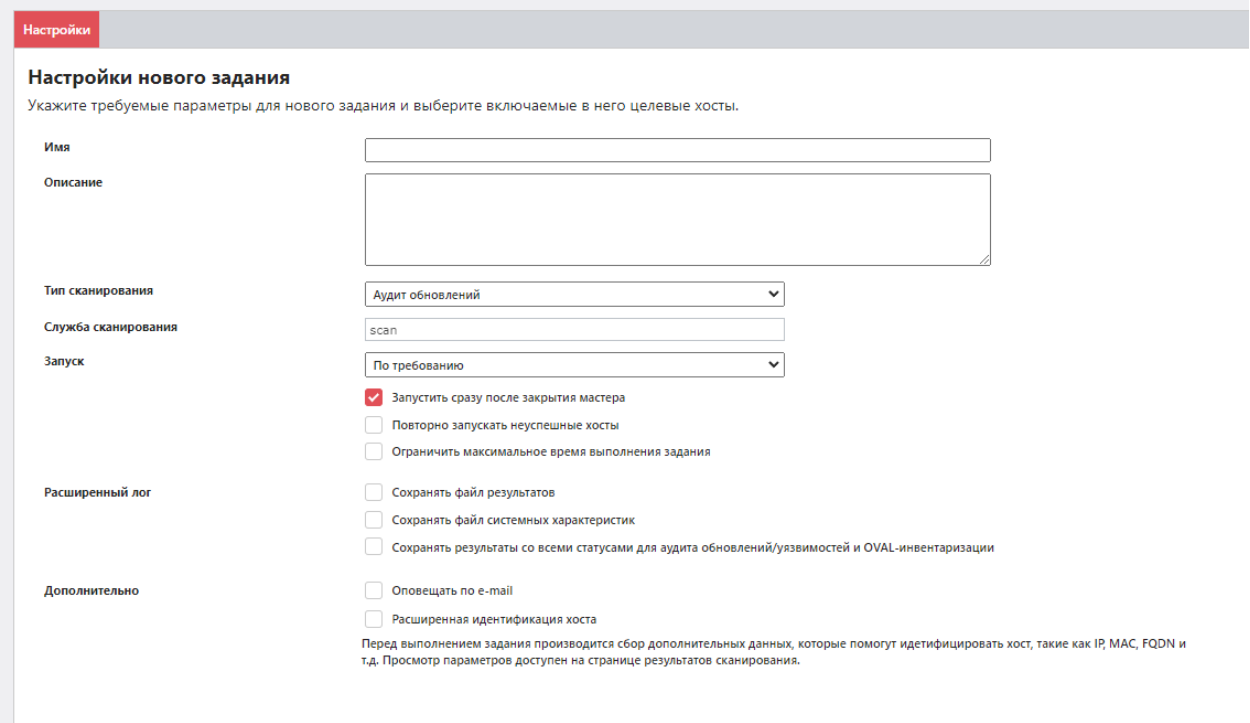
Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Аудит обновлений**;

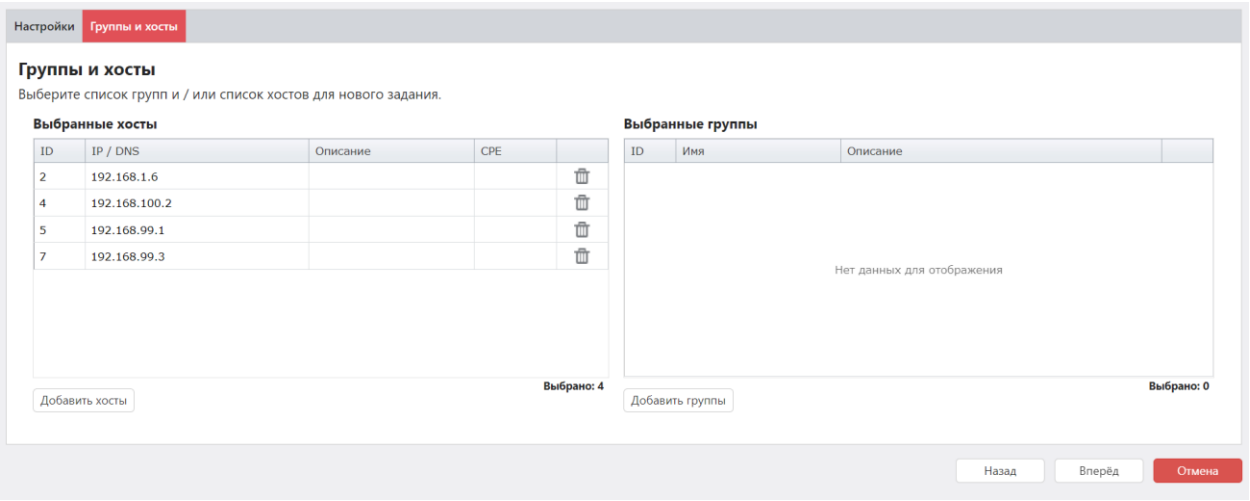
Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ... (Мониторинг служб сканирования);
- Тип запуска:
  - По требованию – запуск задания вручную;
  - По расписанию – задание будет выполняться согласно настроенному расписанию (Настройка расписания);
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;

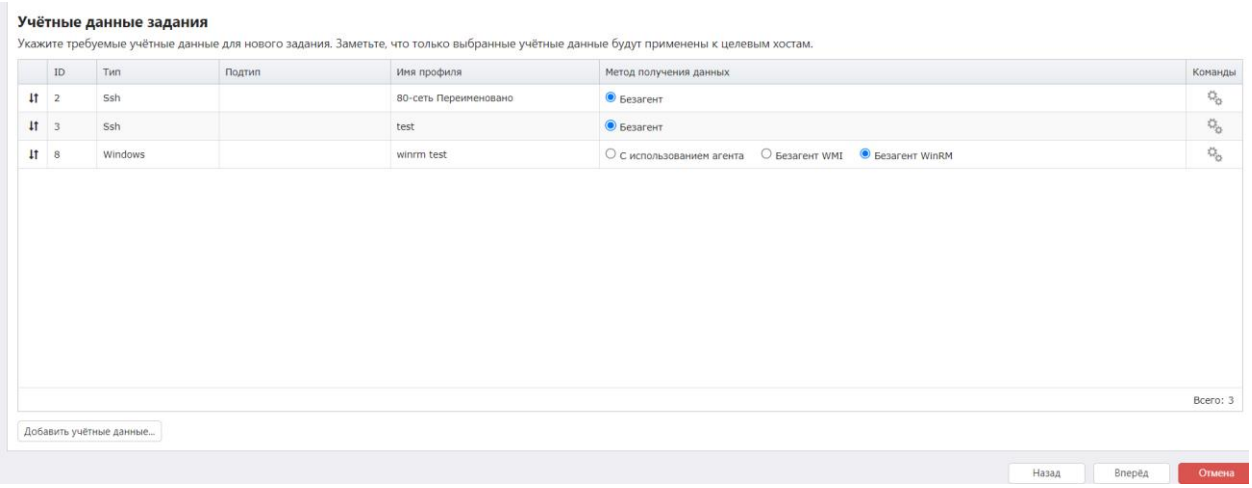
- Повторно запускать неуспешные хосты – функция Повторного перезапуска недоступных хостов;
- Ограничить максимальное время выполнения задания – функция Остановки задания по времени выполнения;
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по-умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;
- Сохранять файл системных характеристик – сохранение информации о найденных состояниях на хосте без информации о контенте, который был проверен во время сканирования (по-умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/system-characteristics.xml**);
- Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации – при включенном параметре служба сканирования сохраняет в БД информацию о всех уязвимостях, которые были проверены во время сканирования, даже если они не были обнаружены. При выключенном параметре сохраняются только обнаруженные уязвимости. Выключенный параметр экономит место в БД;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;



Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;



Шаг 4. Выберите учетные записи для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

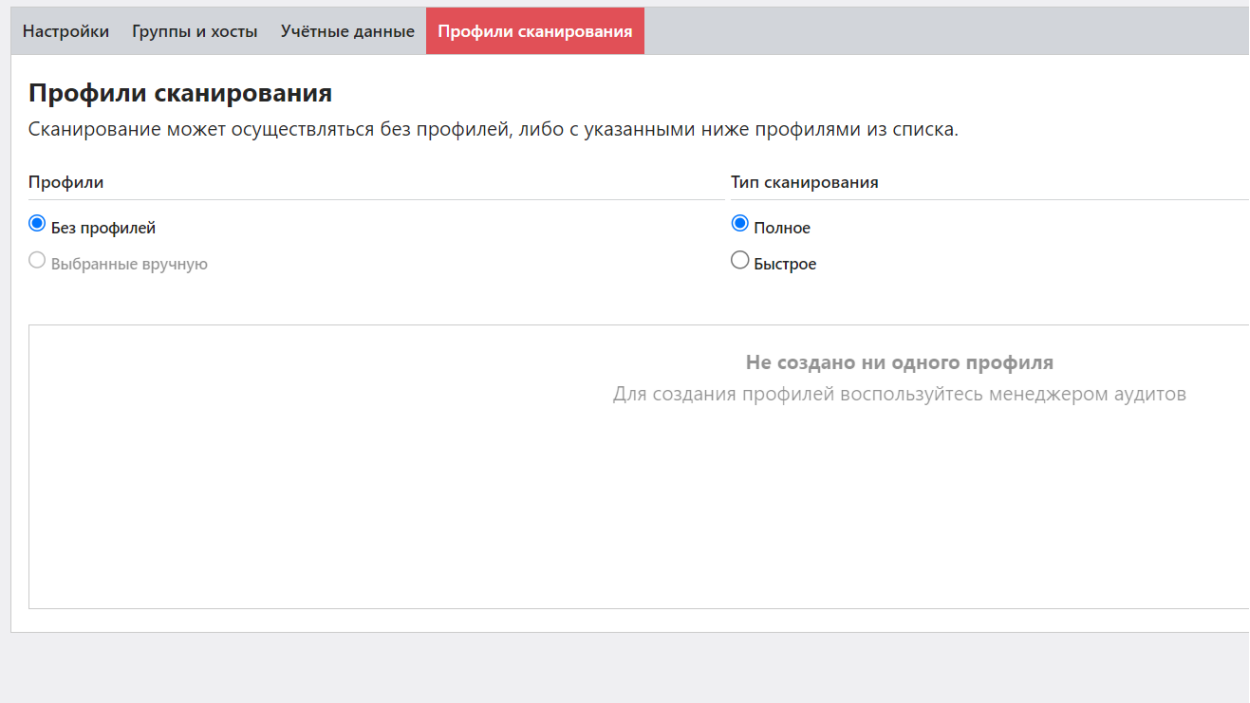


Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед**;

> Подробнее про подбор учетных записей

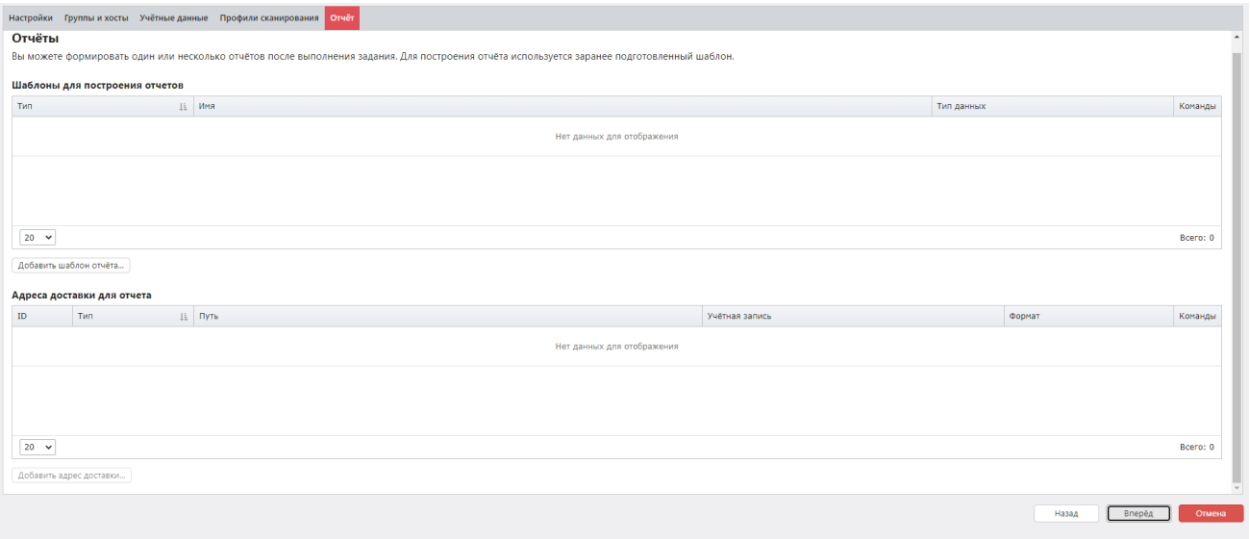
Шаг 5. Выберите профиль и тип сканирования → **Вперед**:

- Полный – при сканировании будут использоваться детальные (рекурсивные) сигнатуры, являющиеся трудоемкими. Аудит займет больше времени;
- Быстрый – не будут применяться детальные сигнатуры. Сканирование будет выполняться быстрее.



> О создании профилей сканирования смотрите в [5.1 Профили сканирования](#).

Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;



Шаг 7. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

4.3 Аудит конфигураций

RedCheck позволяет автоматизировать процесс контроля параметров безопасности и осуществлять оценку соответствия информационных систем, ее отдельных компонентов или хостов, стандартам, политикам безопасности, рекомендациям вендоров или другим «признанным практикам» (best practices). RedCheck содержит большое количество готовых конфигураций, разработанных на основе требований международных стандартов и рекомендаций. Поддержка стандартизованного формата SCAP позволяет пользователям загружать сторонние конфигурации, или использовать собственные.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

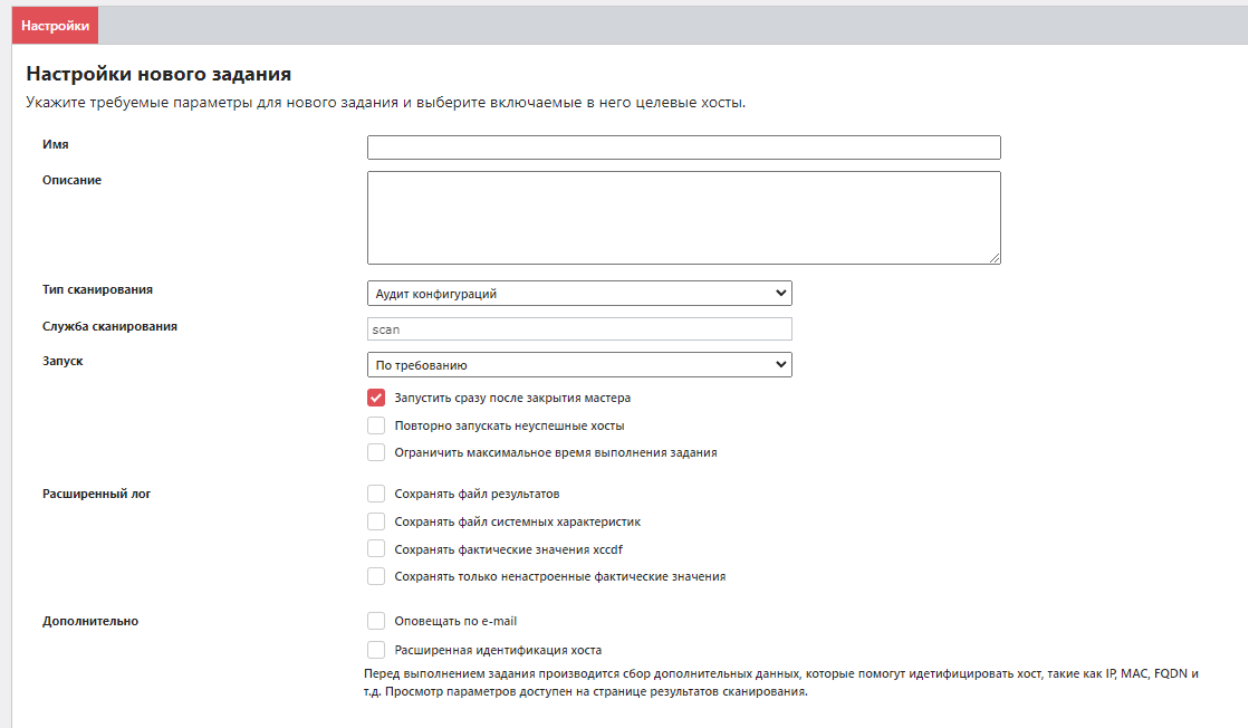
Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Аудит конфигураций**;

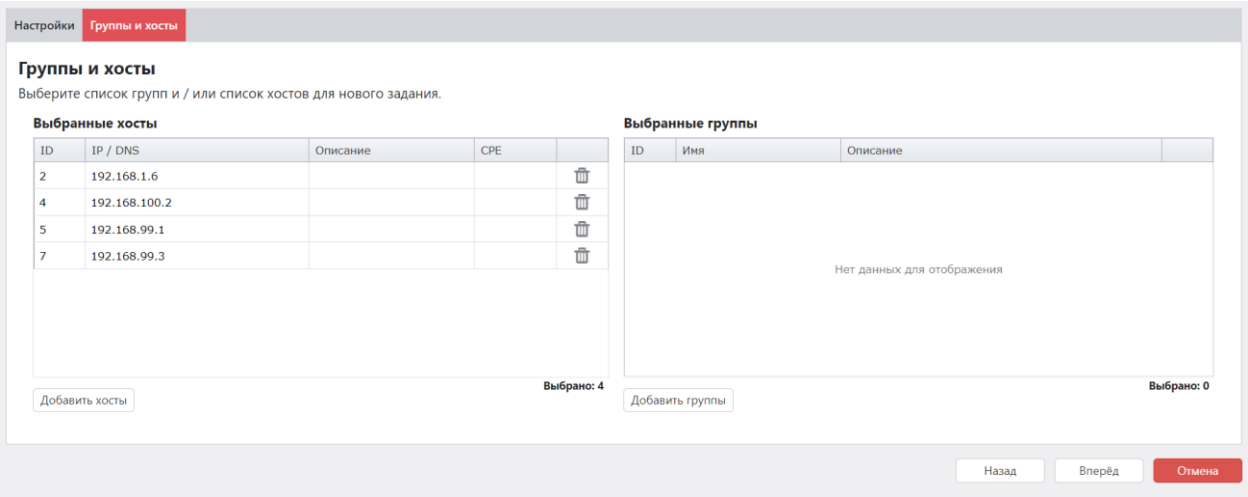
Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав (Мониторинг служб сканирования);
- Тип запуска:
  - По требованию – запуск задания вручную;
  - По расписанию – задание будет выполняться согласно настроенному расписанию (Настройка расписания);

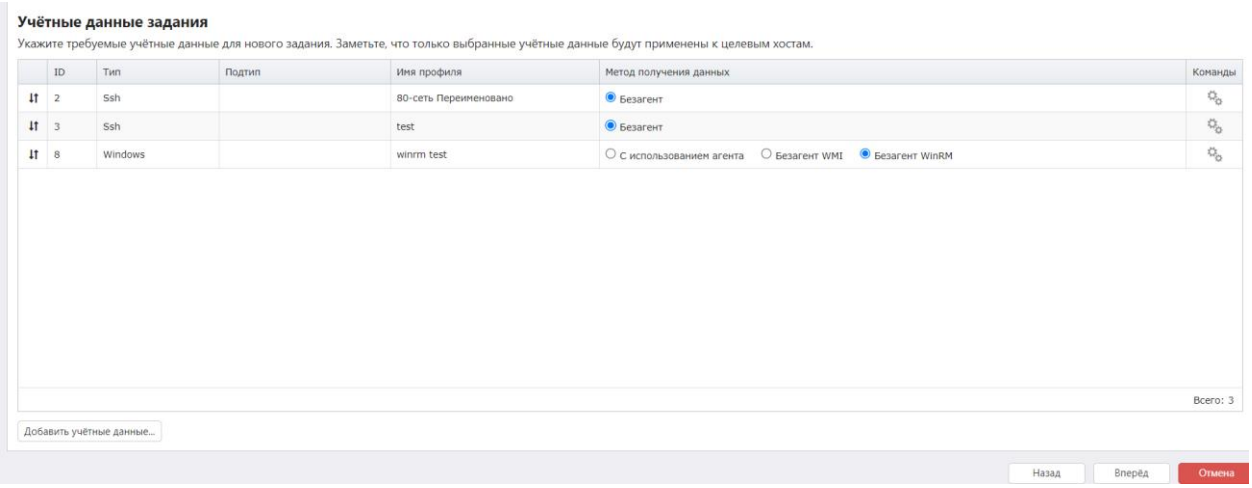
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;
- Повторно запускать неуспешные хосты – функция Повторного перезапуска недоступных хостов;
- Ограничить максимальное время выполнения задания – функция Остановки задания по времени выполнения;
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по-умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;
- Сохранять файл системных характеристик – сохранение информации о найденных состояниях на хосте без информации о контенте, который был проверен во время сканирования (по-умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/system-characteristics.xml**);
- Сохранять фактические значения xccdf – сохранение фактических значений для проверяемых в процессе сканирования правил, имеющих *любой статус проверки*;
- Сохранять только настроенные фактические значения – сохранение фактических значений для проверяемых в процессе сканирования правил, имеющих *статус проверки, отличный от* ***Соответствие***. Можно активировать только при отмеченном параметре **Сохранять фактические значения xccdf**;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;



Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;



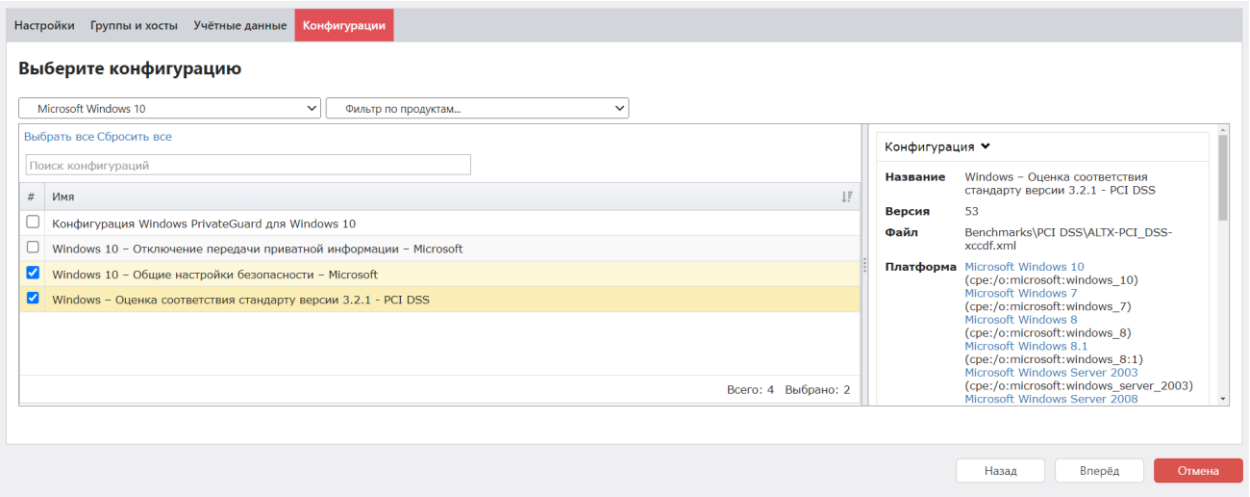
Шаг 4. Выберите учетные записи для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;



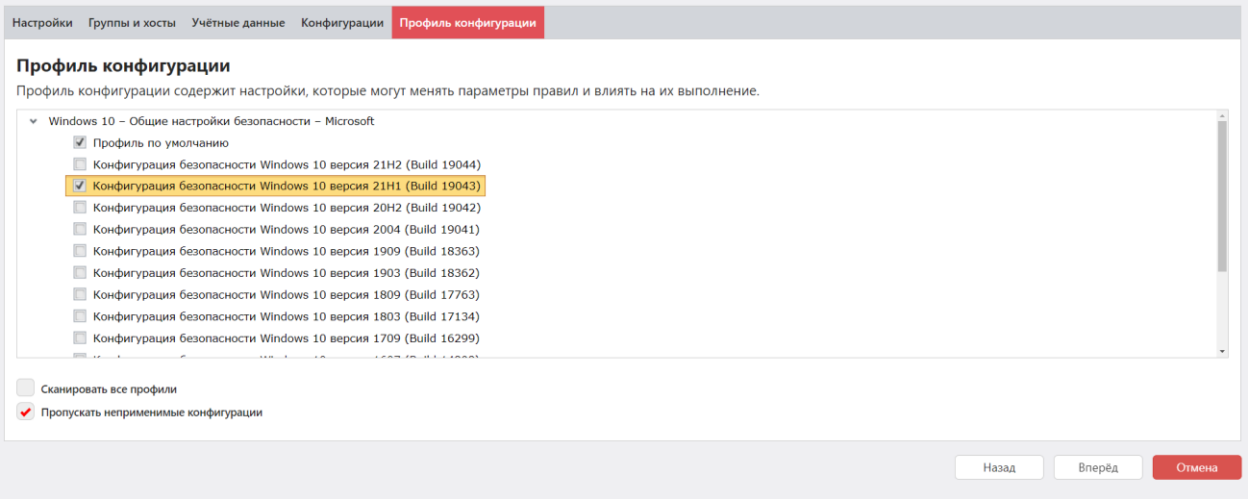
Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед**;

[Подробнее про подбор учетных записей]

Шаг 5. Отметьте в списке необходимые конфигурации → **Вперед**;

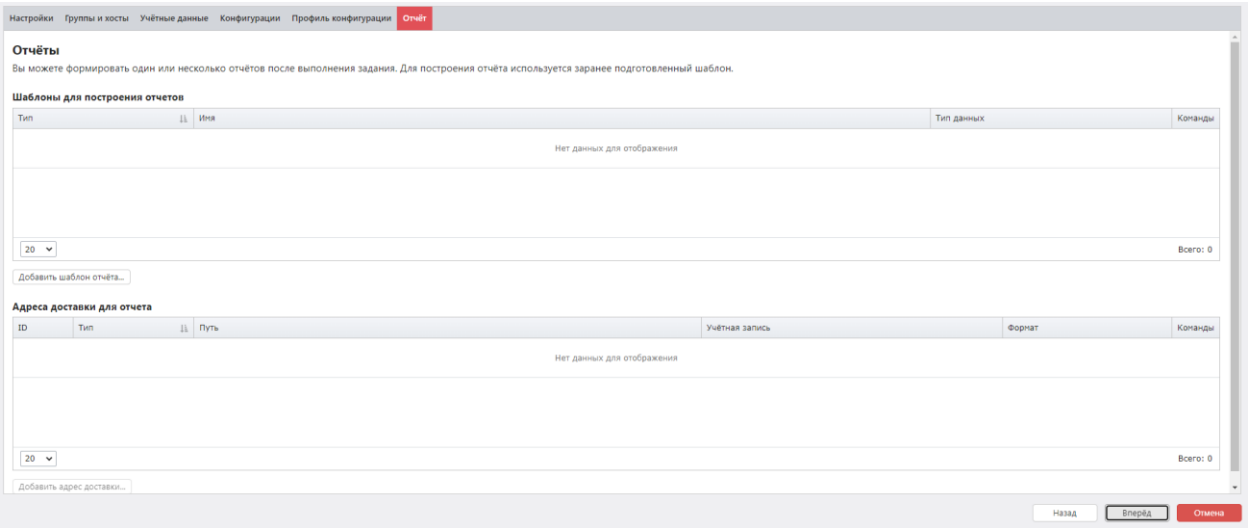


Шаг 6. Выберите необходимый профиль для каждой из конфигураций → **Вперед;**



О добавлении новых конфигураций и редактировании профилей для них смотрите в 5.2 Конфигурации.

Шаг 7. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;



Шаг 8. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

4.4 Инвентаризация

RedCheck позволяет получать детальную информацию об аппаратных и программных средствах сканируемых хостов, включая: типы и описание оборудования, версии и редакции операционных систем, установленные пакеты обновлений и исправлений, установленное ПО, запущенные службы, пользователей и групп, сведения об общих папках. Глубокая детализация отчетов и использование функции Контроль позволяет отслеживать самые незначительные изменения в составе программного и аппаратного обеспечения сети. Реализована возможность инвентаризации образов Docker.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

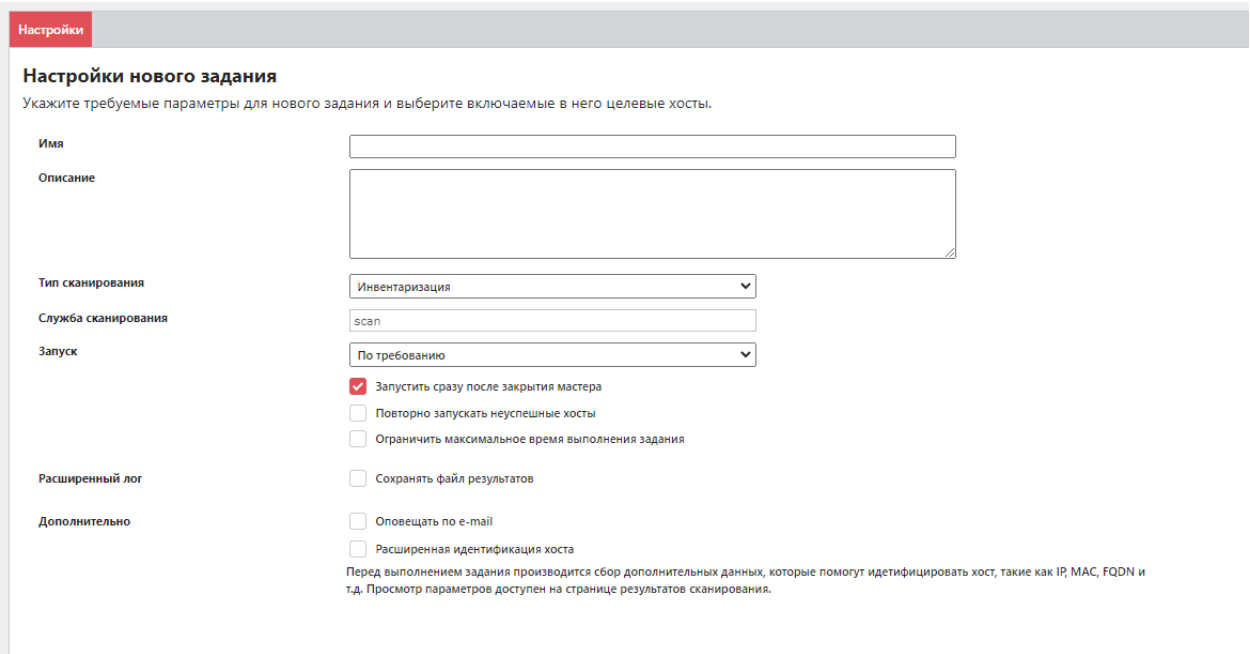
Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Инвентаризация**;

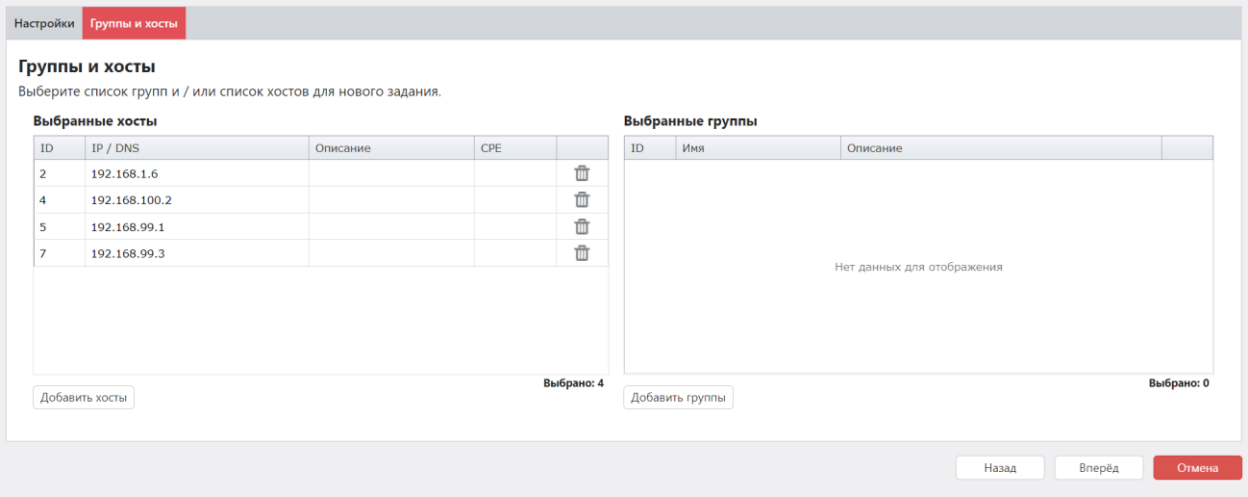
Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ... (Мониторинг служб сканирования);
- Тип запуска:
  - По требованию – запуск задания вручную;
  - По расписанию – задание будет выполнять согласно указанному расписанию;

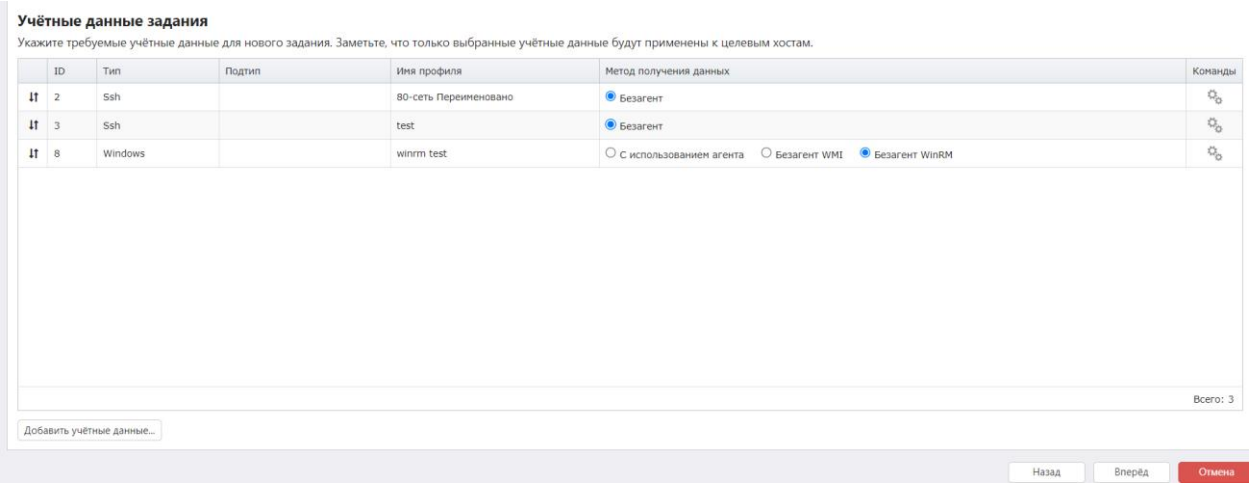
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания (Настройка расписания);
- Повторно запускать неуспешные хосты – функция Повторного перезапуска недоступных хостов;
- Ограничить максимальное время выполнения задания – функция Остановки задания по времени выполнения;
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по-умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;



Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;



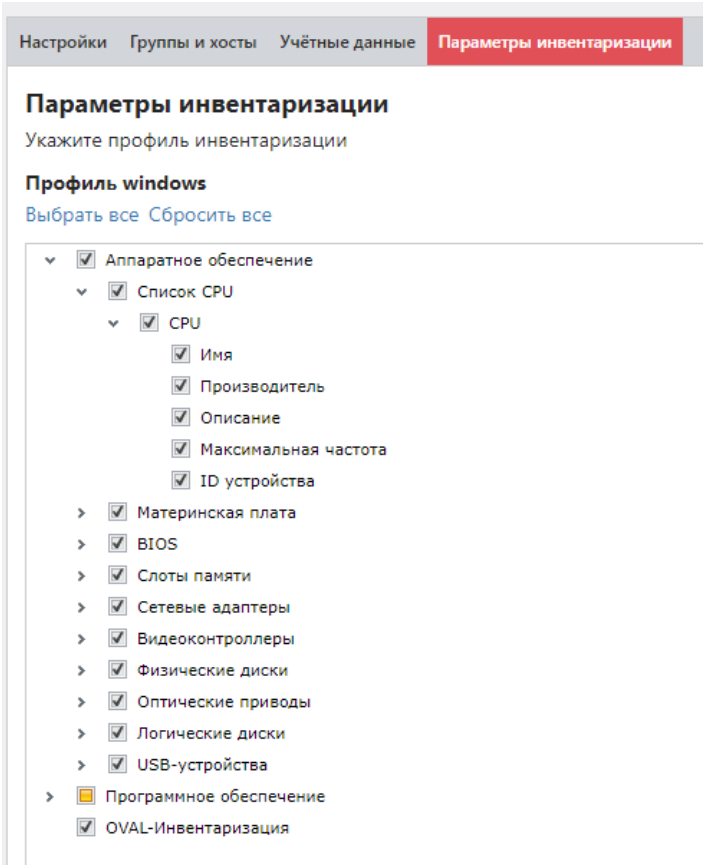
Шаг 4. Выберите учетные записи для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;



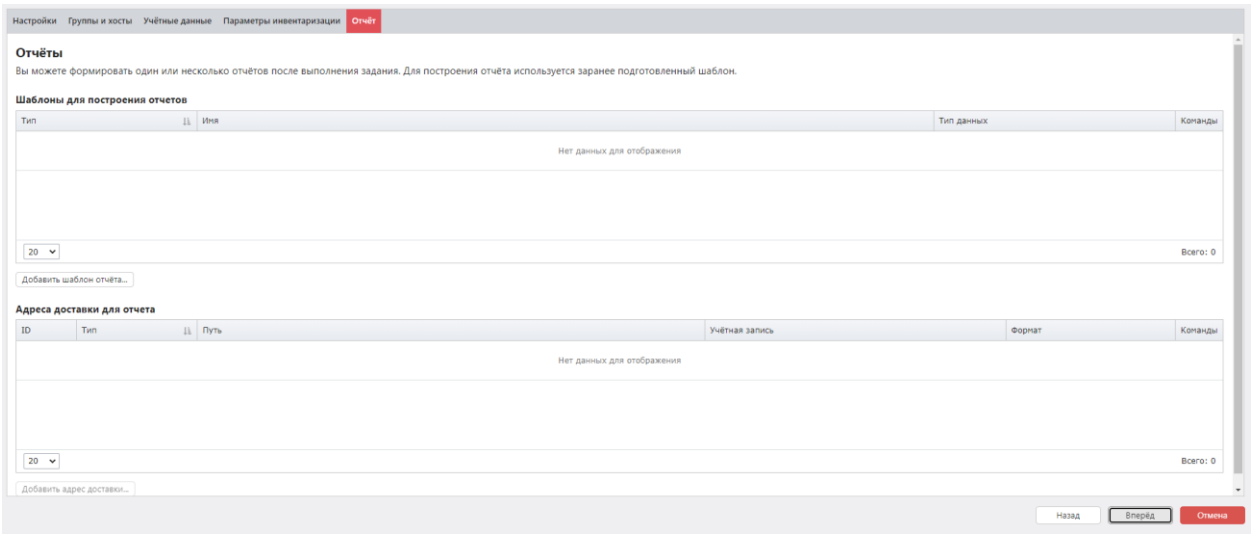
Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед**;

> [Подробнее про подбор учетных записей]

Шаг 5. Выберите параметры инвентаризации → **Вперед**;



Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;



Шаг 7. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

4.5 Фиксация (контроль целостности)

RedCheck может обнаружить и оповестить о несанкционированных изменениях целостности в конфигурационных файлах, папках, ветках реестра (автозагрузка, файл hosts, файл конфигурации межсетевого экрана). Включение режима Контроль позволяет с заданной периодичностью осуществлять проверку целостности эталонных файлов.

Контроль целостности папок и файлов осуществляется по выбранной маске наименования методом контрольного суммирования по алгоритмам MD5, SHA1, SHA256, SHA512, ГОСТ 34.11-2012.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

> Не рекомендуется выполнять фиксацию файлов размером более 500Мб на **Linux-платформах**, т.к. это приводит к максимальной нагрузке ЦП на длительное время, что может привести к сбоям в работе, а также повлечь за собой отказ сканируемого оборудования.

Создание задания

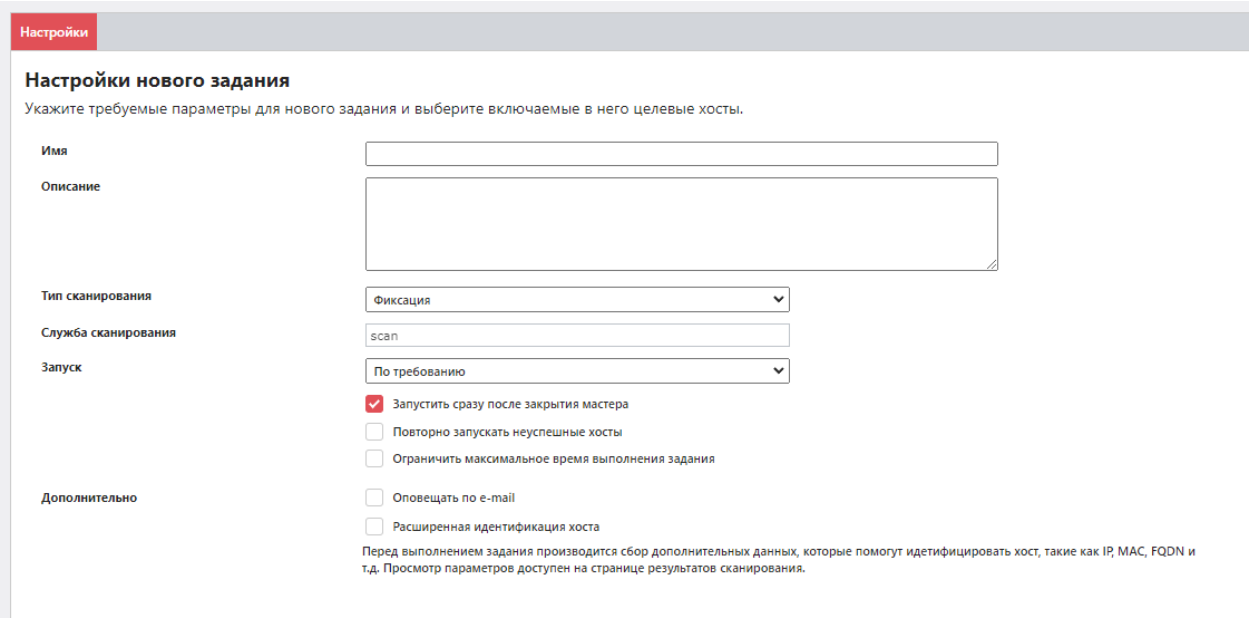
Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

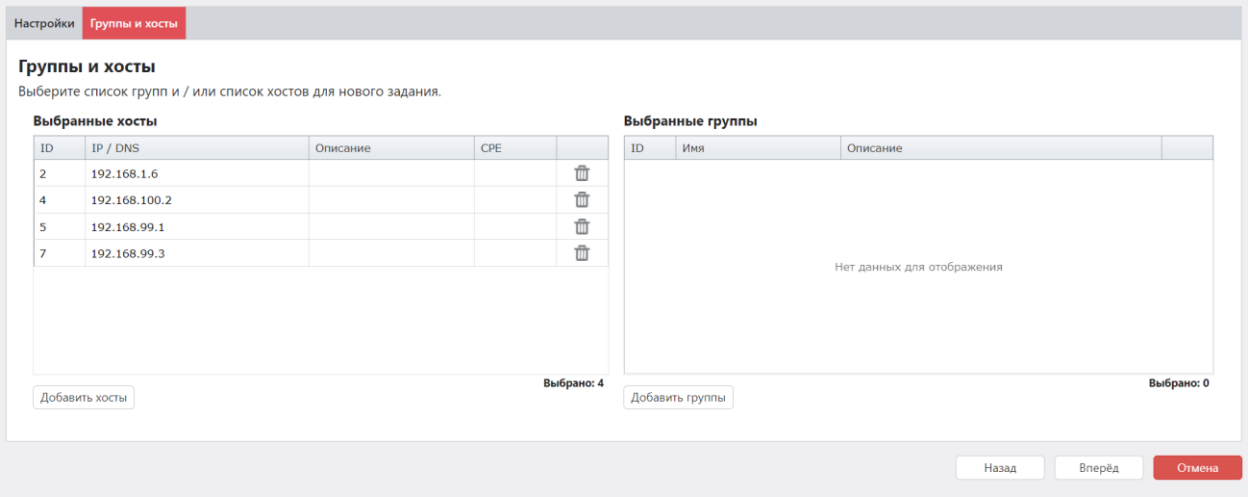
Шаг 1. Откройте **Действия** → **Фиксация**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

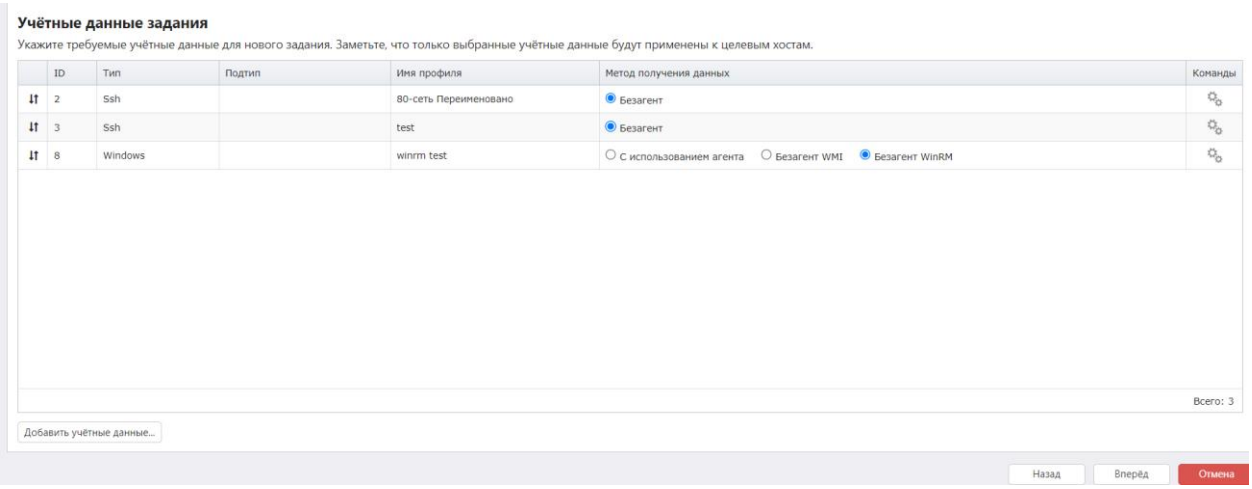
- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ... (Мониторинг служб сканирования);
- Тип запуска:
  - По требованию – запуск задания вручную;
  - По расписанию – задание будет выполнять согласно указанному расписанию;
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания (Настройка расписания);
- Повторно запускать неуспешные хосты – функция Повторного перезапуска недоступных хостов;
- Ограничить максимальное время выполнения задания – функция Остановки задания по времени выполнения;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;



Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;



Шаг 4. Выберите учетные записи для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

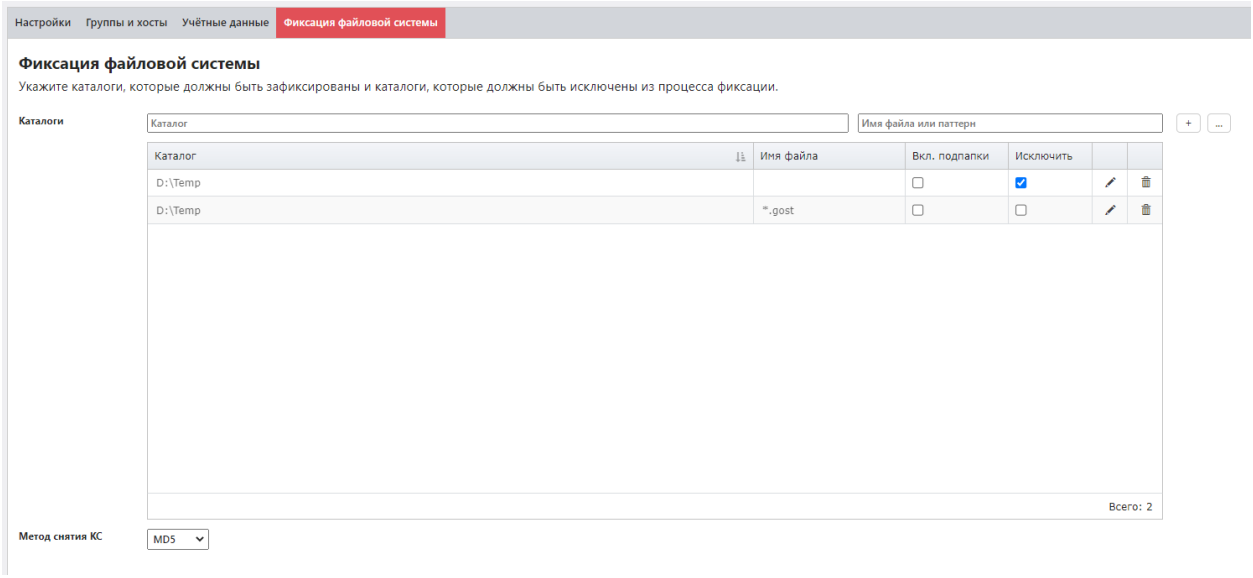


Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед**;

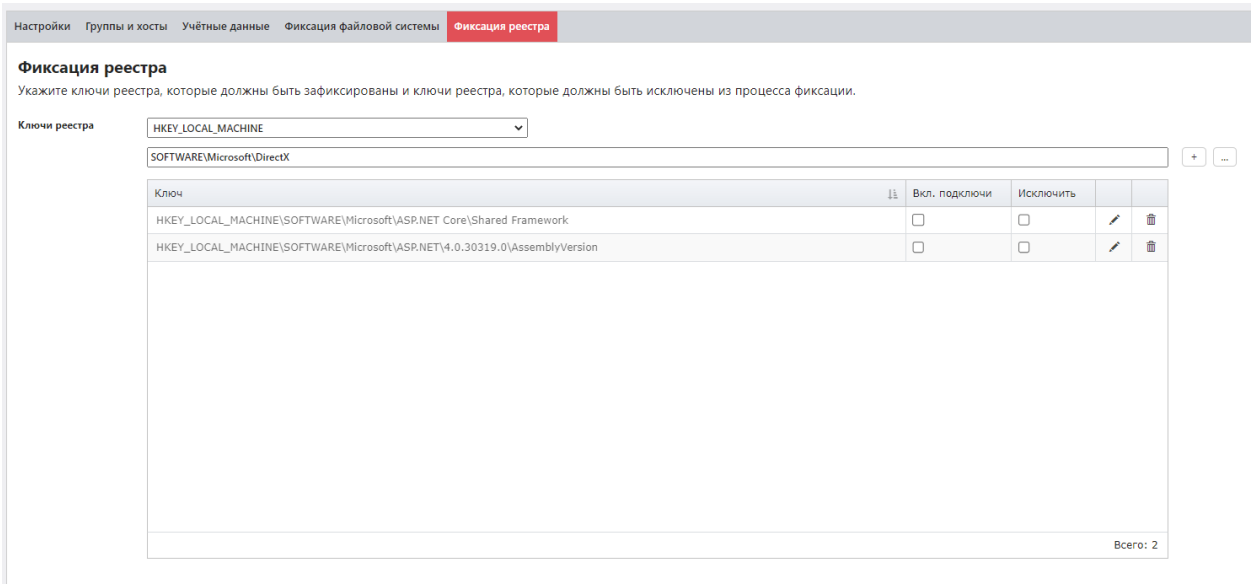
> [Подробнее про подбор учетных записей]

Шаг 5. Укажите в поле **Каталог** полный путь к директории, которую хотите зафиксировать / исключить → при необходимости введите имя файла или паттерн (или воспользуйтесь кнопкой ... [импорта каталогов из csv-файла]) →

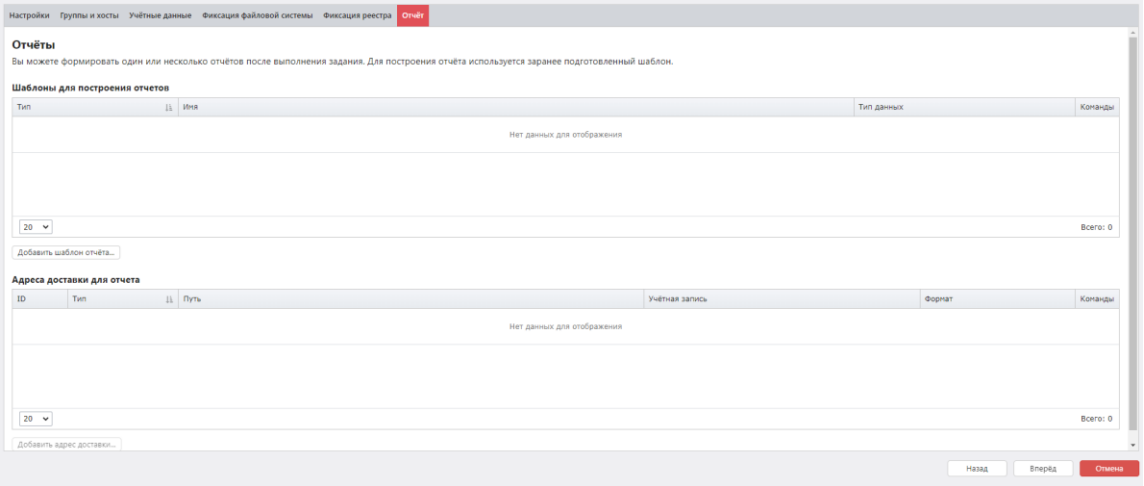
нажмите + → выберите необходимый метод снятия контрольной суммы из списка, расположенного после таблицы → **Вперед**;



Шаг 5.1. Для фиксации на Windows хостах. Укажите при необходимости ветки реестра и параметры, которые нужно зафиксировать → **Вперед**;



Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;



Шаг 7. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

Структура CSV-файла

Формат CSV – это текстовый файл с информацией, представленной в виде таблицы. В первой строке через разделитель **«,»** указываются названия столбцов. Последующие строки таблицы являются записями с информацией.

Path	FileName	IncludeSubdirectories	IsExclusion
Каталог	Имя файла или паттерн	# – включить подпапки	! – исключить

Пример

Код

```
Path,FileName,IncludeSubdirectories,IsExclusion
C:\ALTEX-SOFT\Red*,,,
C:\ProgramData\Test0,*.exe,#,
C:\ProgramData\Test1,*.dll,,!
C:\ProgramData\Test2,*.ocr,#,!
C:\ProgramData\Test3,,,!
```

Не допускается использование спецсимволов в Path

4.6 Аудит уязвимостей АСУ ТП

Аудит уязвимостей АСУ ТП предназначен для проведения проверок на наличие уязвимостей протоколов АСУ ТП. Выявление уязвимостей проводится путем сопоставления сигнатур, хранящихся в БД RedCheck, с идентификационными сведениями о запущенном и опубликованном на сканируемом хосте ПО.

Сканирование выполняется на сетевом уровне, без использования привилегий или учетных записей (Черный ящик).

Создание задания

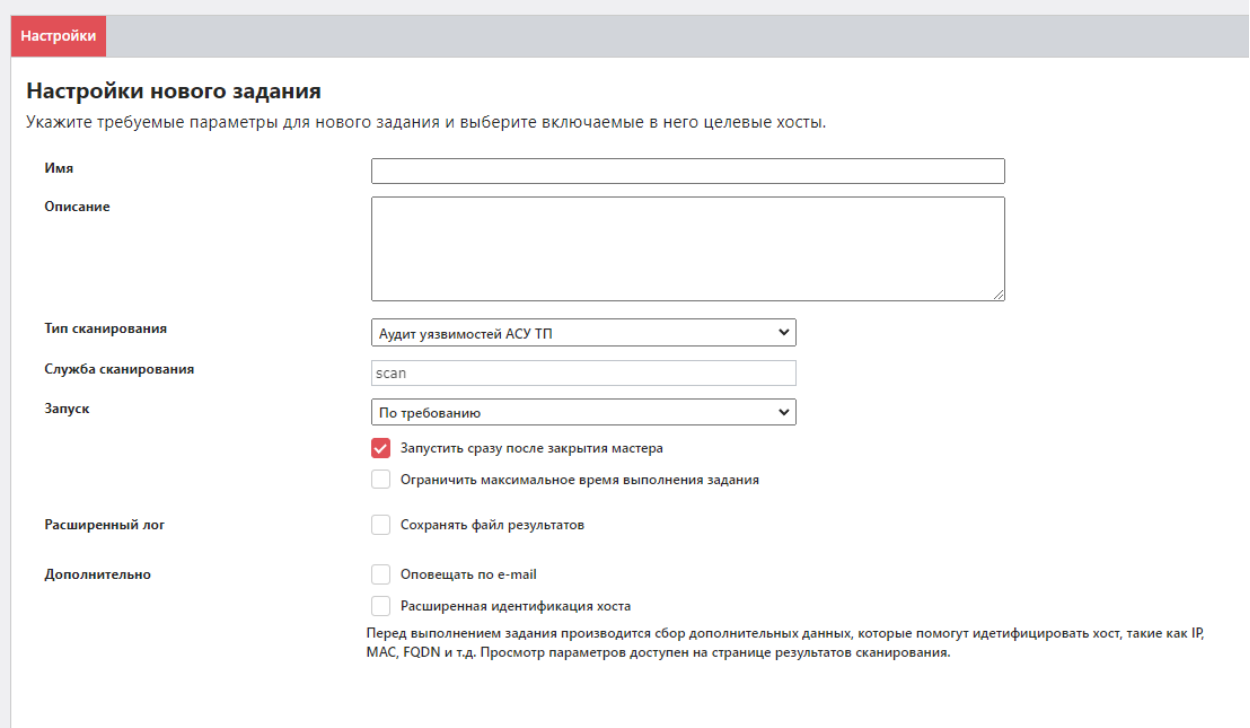
Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

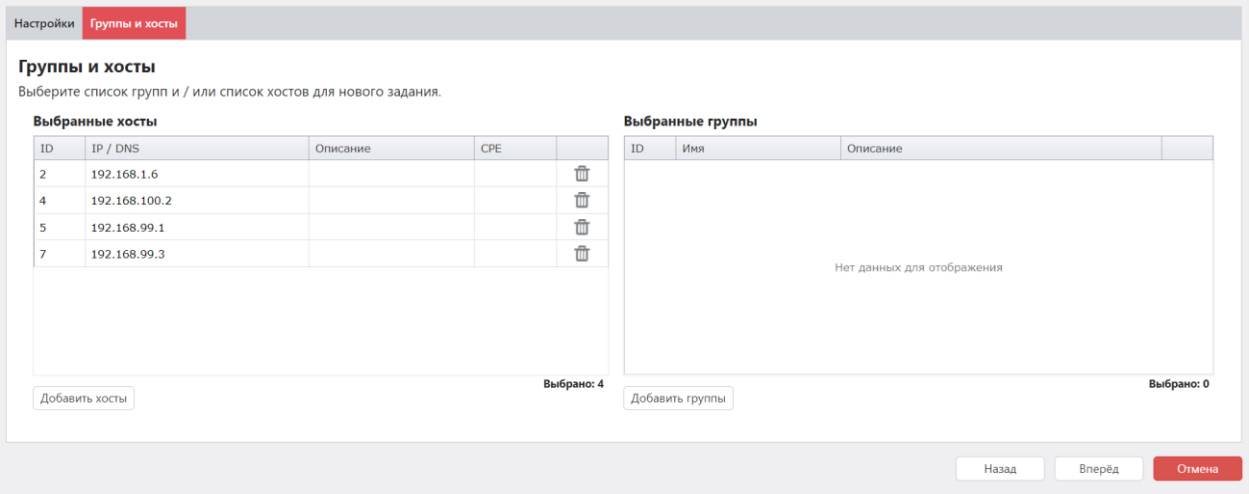
Шаг 1. Откройте **Действия** → **Аудит уязвимостей АСУ ТП**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

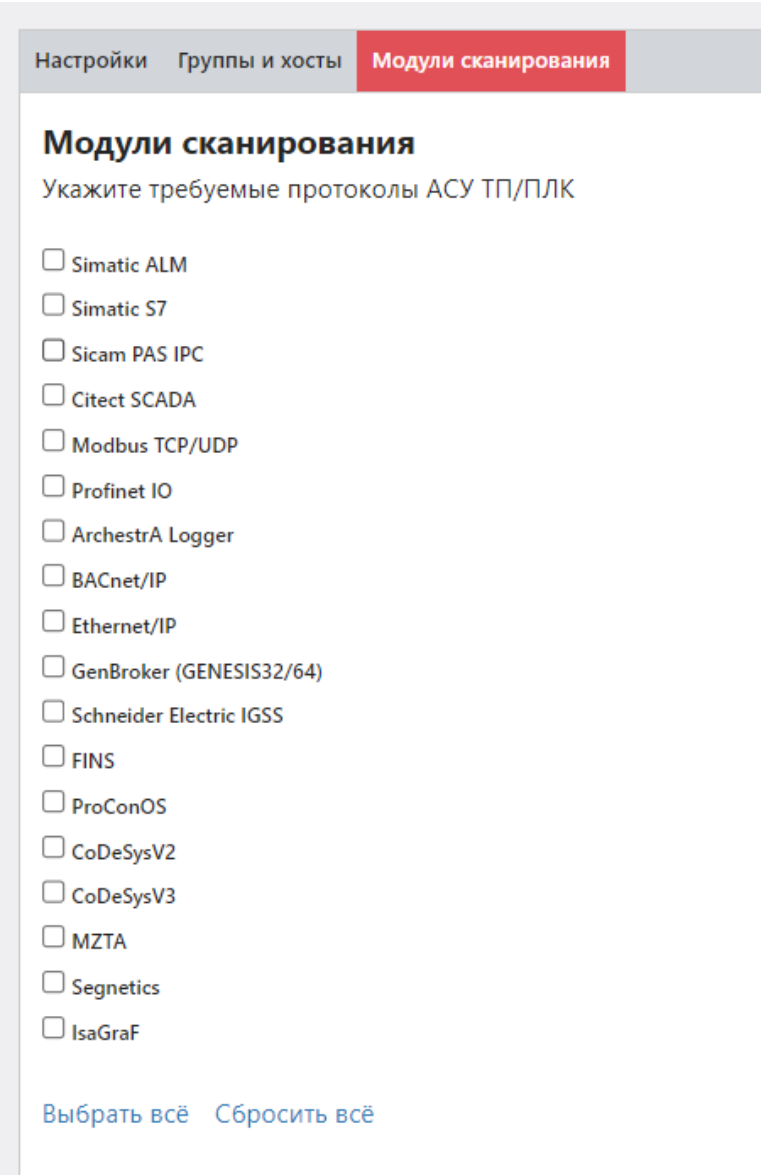
- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав (Мониторинг служб сканирования);
- Тип запуска:
  - По требованию – запуск задания вручную;
  - По расписанию – задание будет выполнять согласно указанному расписанию;
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания (Настройка расписания);
- Ограничить максимальное время выполнения задания – функция Остановки задания по времени выполнения;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;



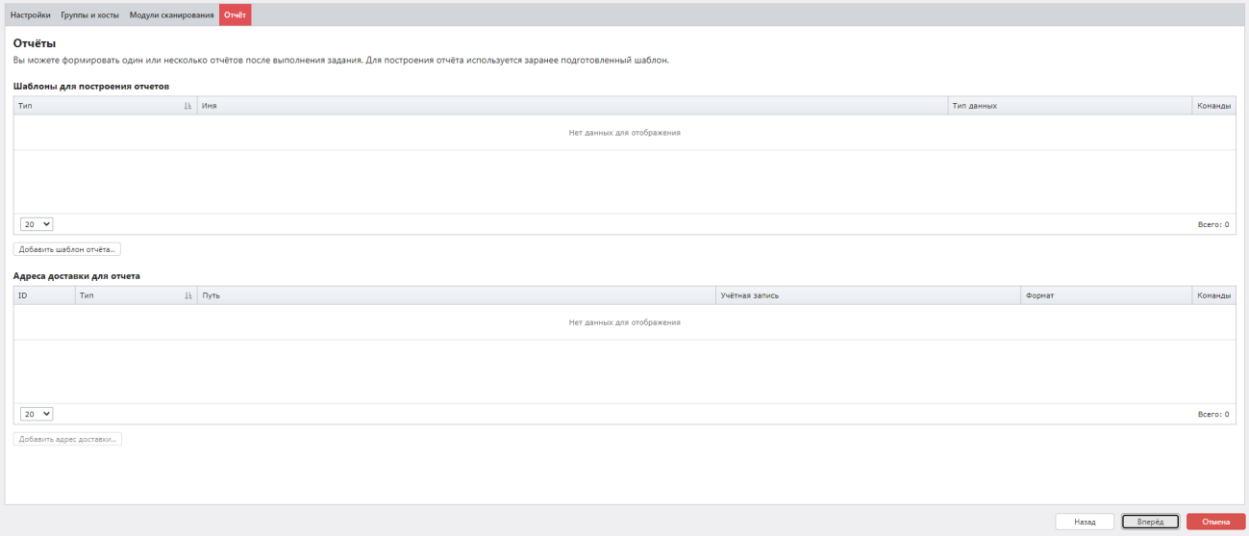
Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;



Шаг 4. Отметьте необходимые протоколы АСУ ТП / ПЛК → **Вперед**;



Шаг 5. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;



Шаг 6. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

4.7 Аудит СУБД

Функция Аудит СУБД в RedCheck предназначена для проверки соответствия параметров конфигурации или политике безопасности, например:

- требованию к парольной политике;
- требованию к методам аутентификации;
- требованию к разграничению доступа БД;
- требованию к резервному копированию и восстановлению БД.

Сканирование выполняется либо с использованием агентов RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

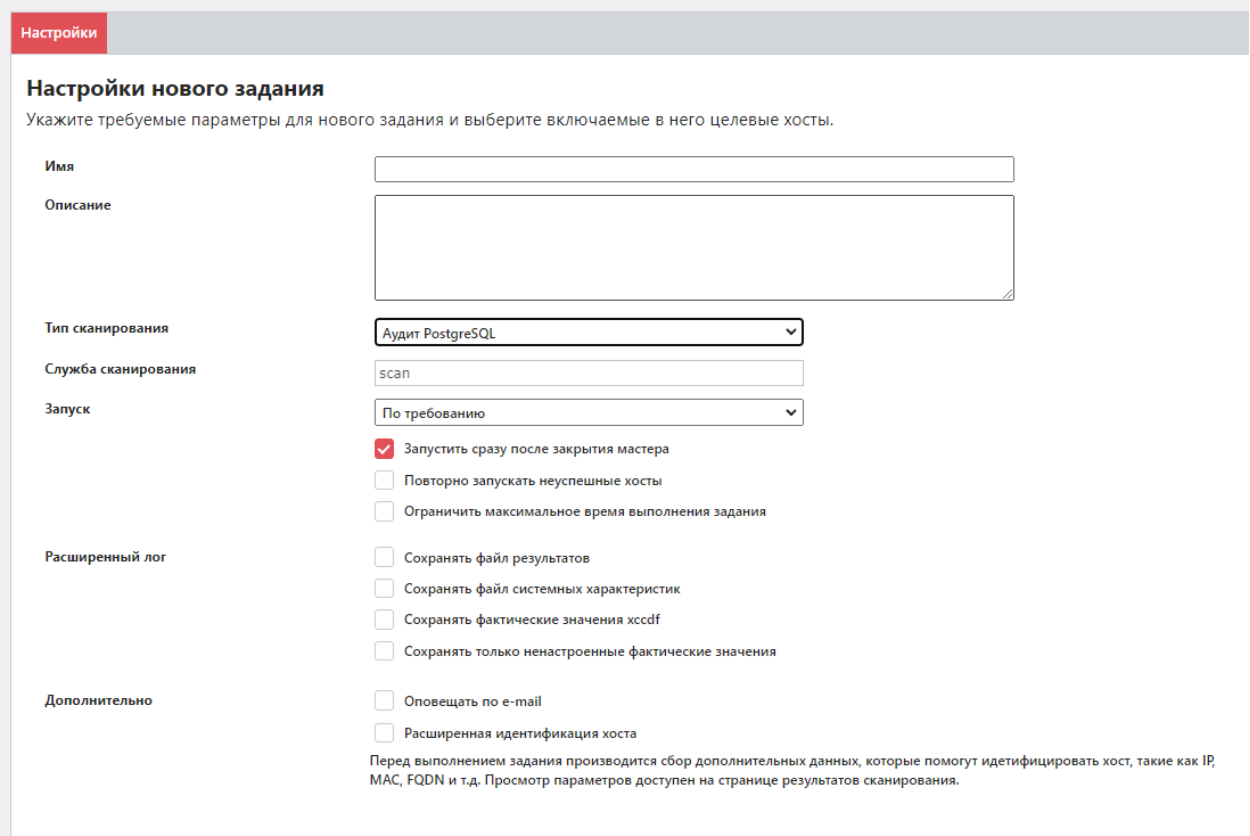
Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Аудит СУБД** → нужная СУБД;

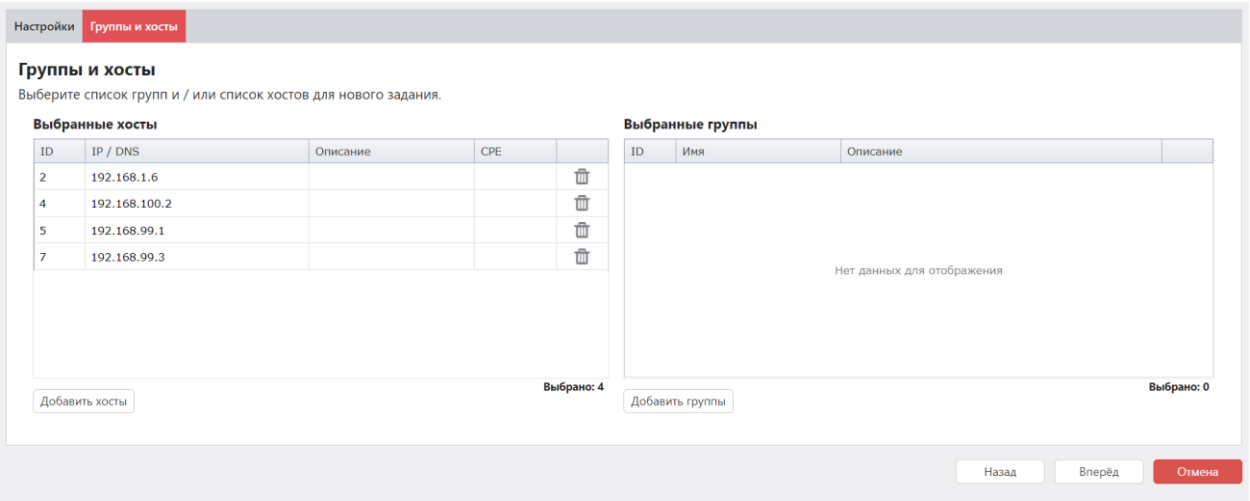
Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ... (Мониторинг служб сканирования);
- Тип запуска:
  - По требованию – запуск задания вручную;
  - По расписанию – задание будет выполняться согласно настроенному расписанию (Настройка расписания);
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;

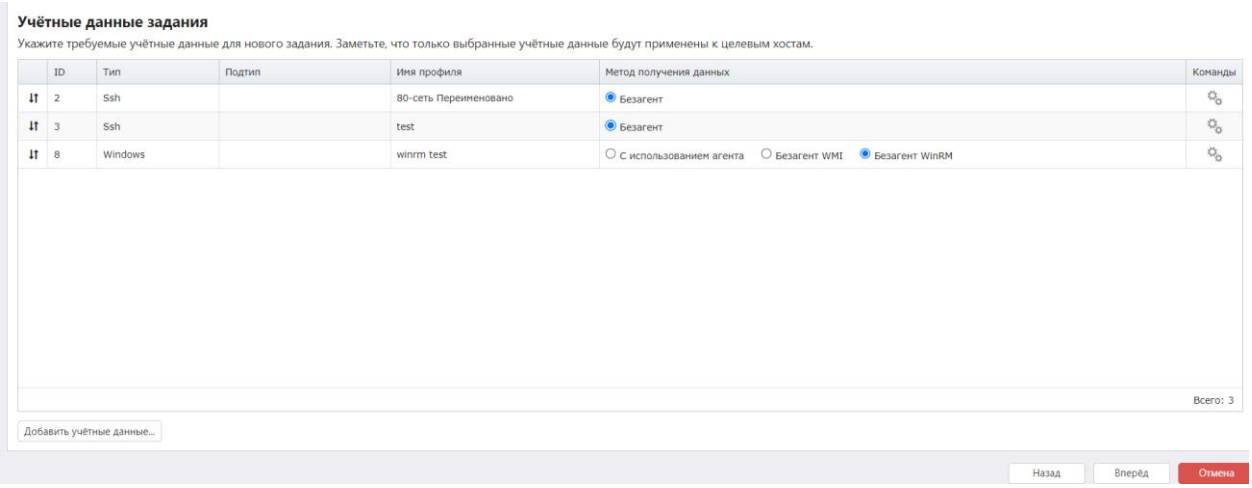
- Повторно запускать неуспешные хосты – функция Повторного перезапуска недоступных хостов;
- Ограничить максимальное время выполнения задания – функция Остановки задания по времени выполнения;
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по-умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;
- Сохранять файл системных характеристик – сохранение информации о найденных состояниях на хосте без информации о контенте, который был проверен во время сканирования (по-умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/system-characteristics.xml**);
- Сохранять фактические значения xccdf – сохранение фактических значений для проверяемых в процессе сканирования правил, имеющих *любой статус проверки*;
- Сохранять только настроенные фактические значения – сохранение фактических значений для проверяемых в процессе сканирования правил, имеющих *статус проверки, отличный от* ***Соответствие***. Можно активировать только при отмеченном параметре **Сохранять фактические значения xccdf**;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;



Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;



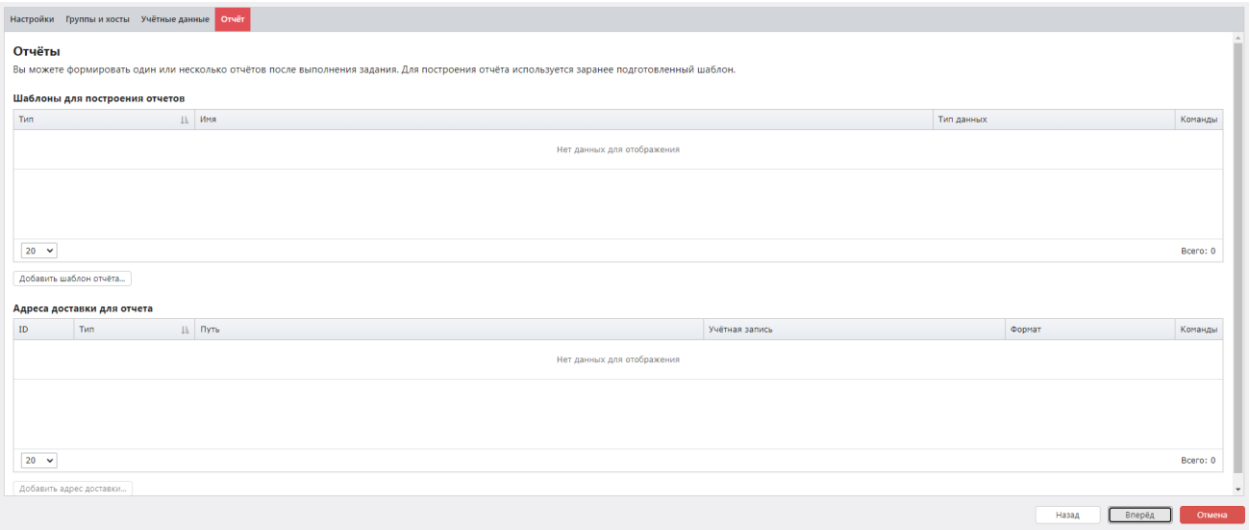
Шаг 4. Выберите учетные записи для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;



Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед**;

[Подробнее про подбор учетных записей]

Шаг 5. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;



Шаг 6. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

4.8 Проверка доступности

RedCheck обладает возможностью проверки доступности добавленных хостов для любых системных режимов сканирования с привилегиями **(**Белый ящик), учитывая настроенные транспорты/протоколы доступа и учетные записи RedCheck для сканирования.

Результатом выполнения задания является информация о доступности хоста для выполнения сканирования с привилегиями (Белый ящик), либо конкретный отсутствующий параметр настройки.

Сканирование выполняется в комбинированном режиме на сетевом уровне, без использования привилегий (Черный ящик) и с использованием привилегий (Белый ящик).

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

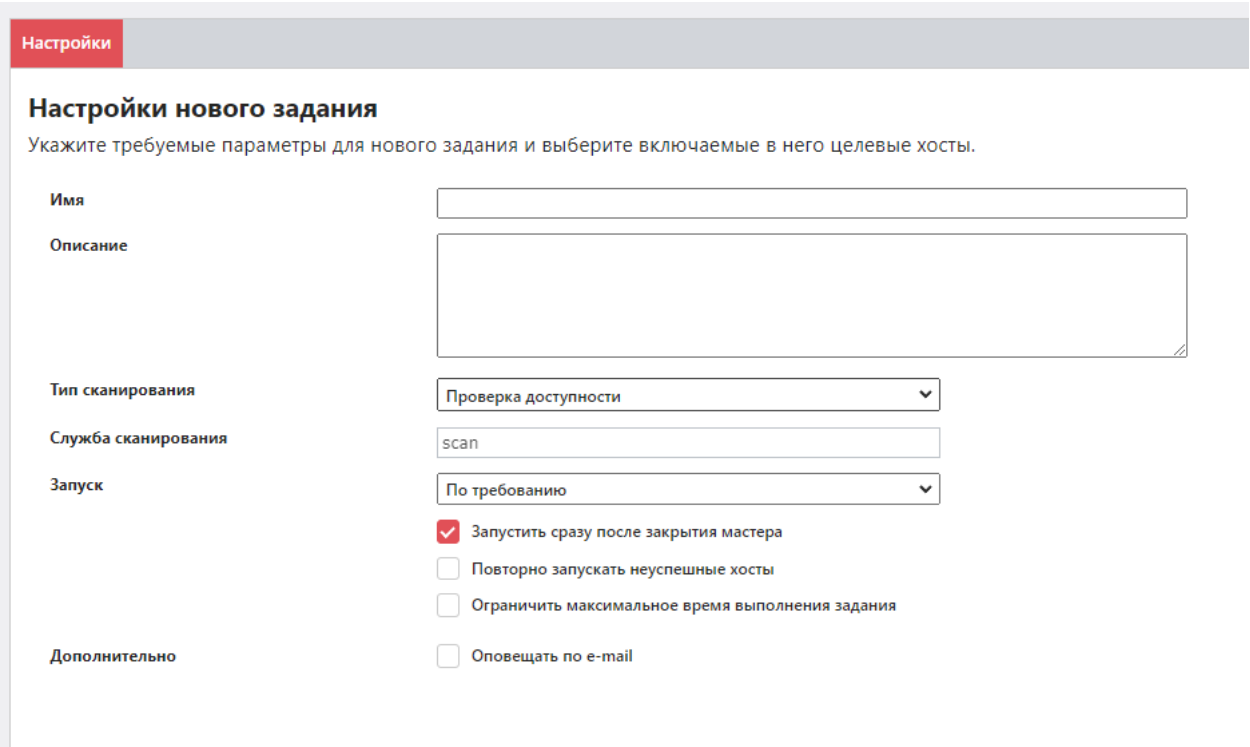
Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Обнаружение хостов**;

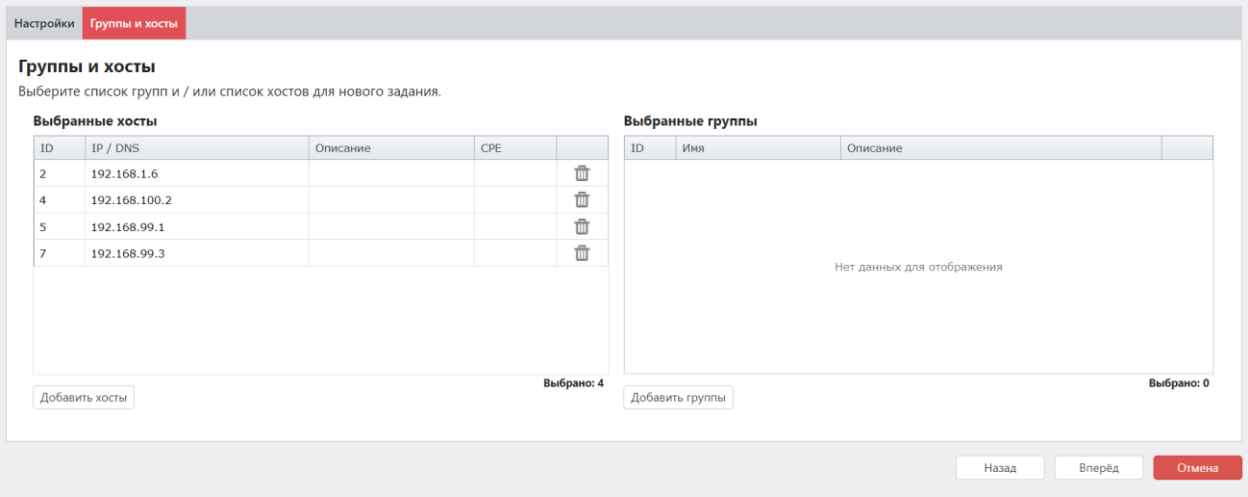
Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ... (Мониторинг служб сканирования);
- Тип запуска:
  - По требованию – запуск задания вручную;
  - По расписанию – задание будет выполняться согласно настроенному расписанию (Настройка расписания);

- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;
- Повторно запускать неуспешные хосты – функция Повторного перезапуска недоступных хостов;
- Ограничить максимальное время выполнения задания – функция Остановки задания по времени выполнения;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;

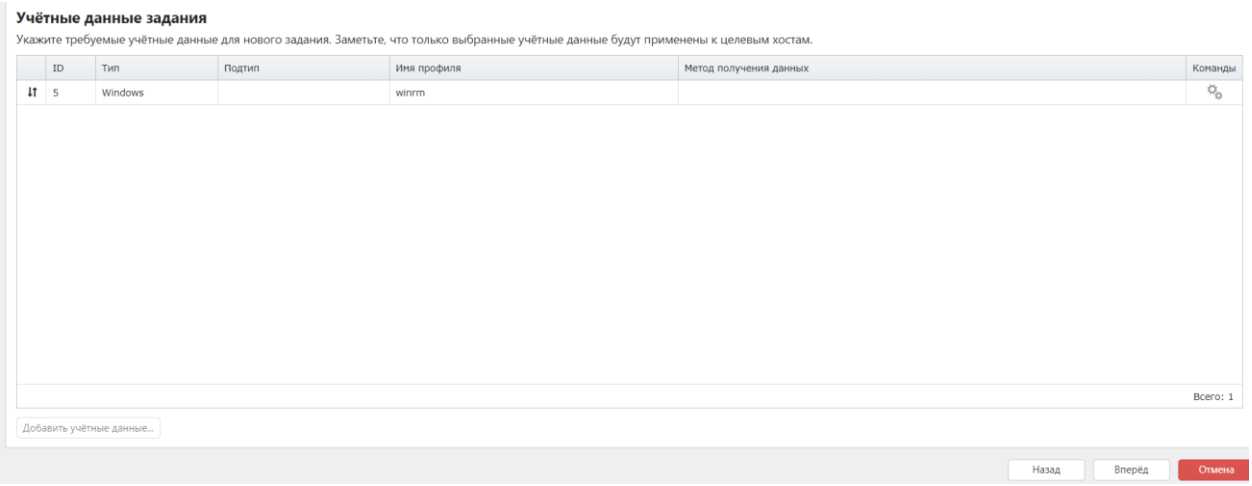


Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;



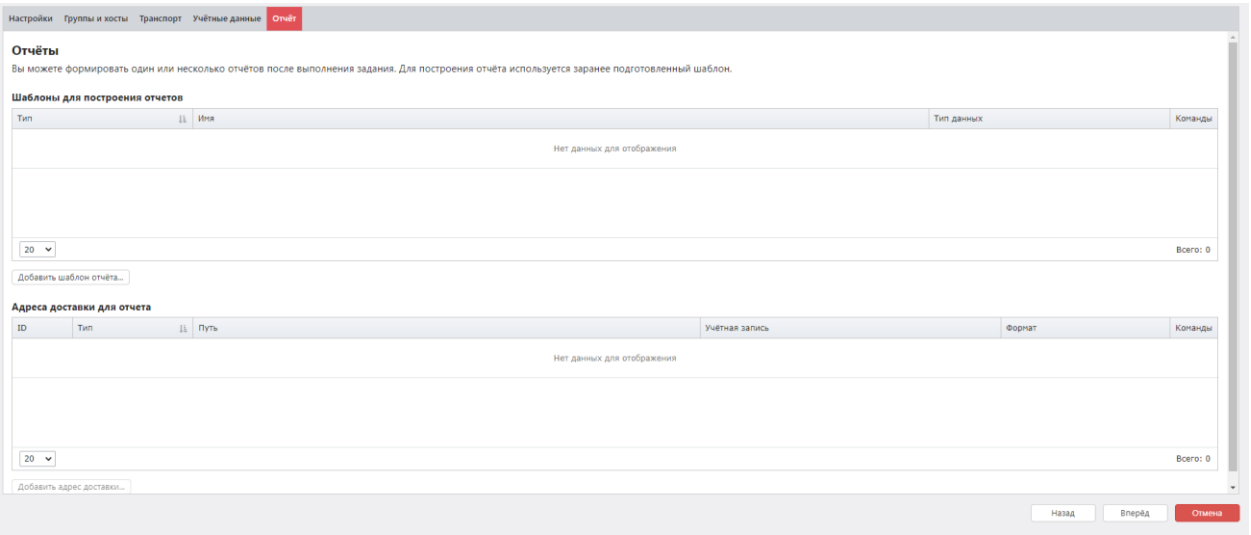
Шаг 4. Укажите тип транспорта, доступность которого необходимо проверить → **Вперед**;

Шаг 5. Выберите учетную запись для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;



[Подробнее про подбор учетных записей]

Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;



Шаг 7. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

4.9 Обнаружение хостов

RedCheck выполняет поиск активных хостов и контроль целостности сети по заданному пулу сетевых адресов. Для обнаруженных в сети хостов определяется их IP-адрес, DNS, FQDN, NetBIOS, тип операционной системы. Также имеется возможность определить наличие агента RedCheck. По результатам выполнения задания впервые выявленные хосты могут быть импортированы в одну из существующих групп Системы, или экспортированы во внешний файл.

Сканирование выполняется без привилегий в режиме Черного ящика.

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

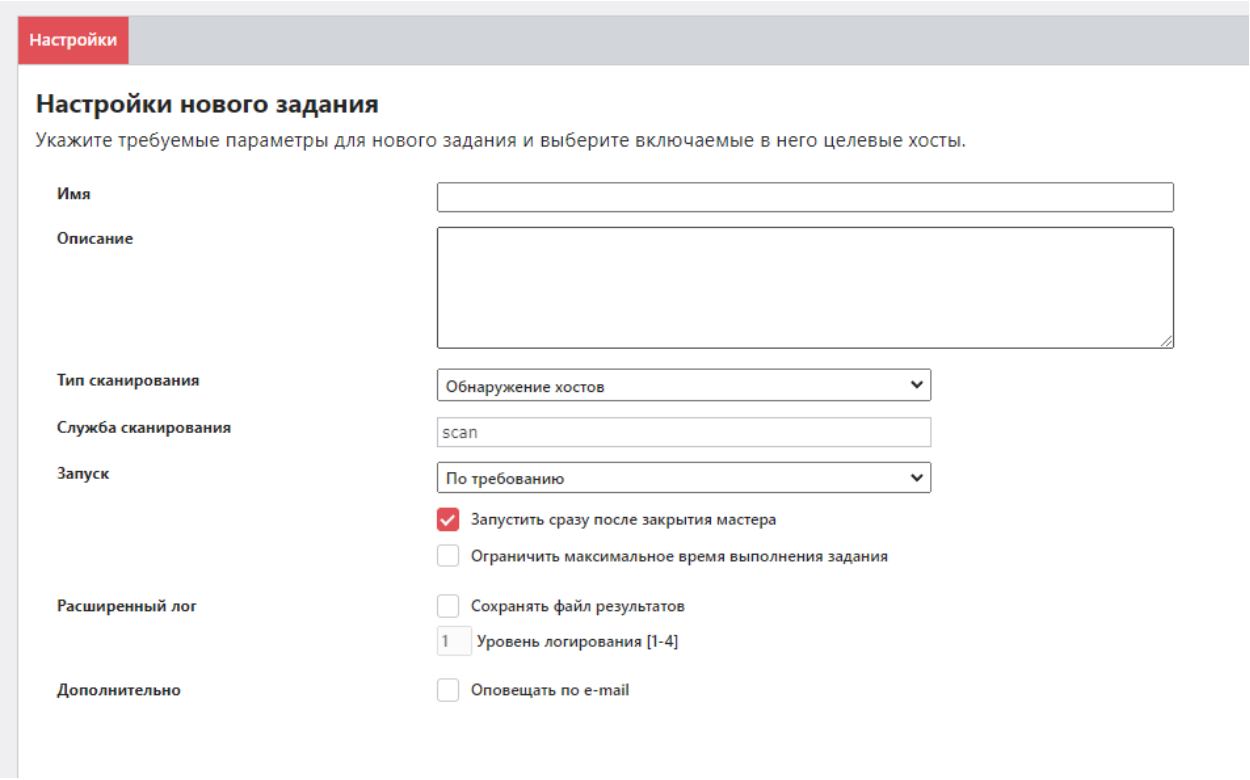
Шаг 1. Откройте **Действия** → **Обнаружение хостов**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав (Мониторинг служб сканирования);
- Тип запуска:
  - По требованию – запуск задания вручную;
  - По расписанию – задание будет выполняться согласно настроенному расписанию (Настройка расписания);
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;
- Ограничить максимальное время выполнения задания – функция Остановки задания по времени выполнения;
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по-умолчанию располагается в **/var/opt/scan-**

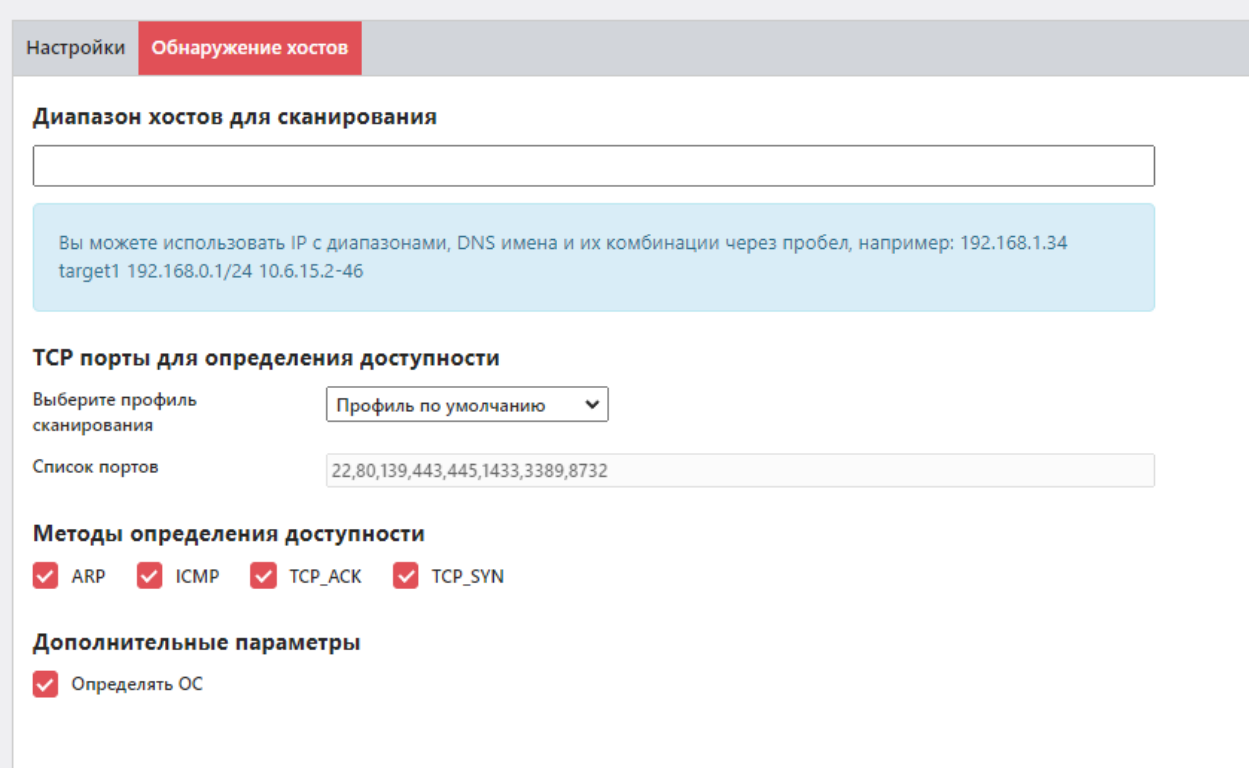
service/jobs/executionId/uuid/results.xml). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;

- Уровень логирования [1-4] – уровень детализации логов Altxmap. Чем больше значение, тем детальнее будет лог;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;



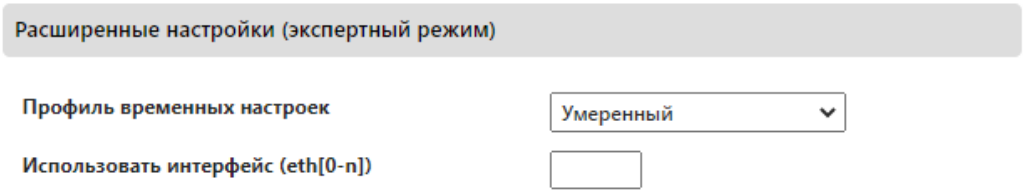
Шаг 3. Укажите настройки для задания → **Вперед**;

- Профиль сканирования – указываются TCP порты, которые будут сканироваться для определения доступности хоста;
- Определять ОС – ОС будет отображаться в формате CPE. Время сканирования увеличится;

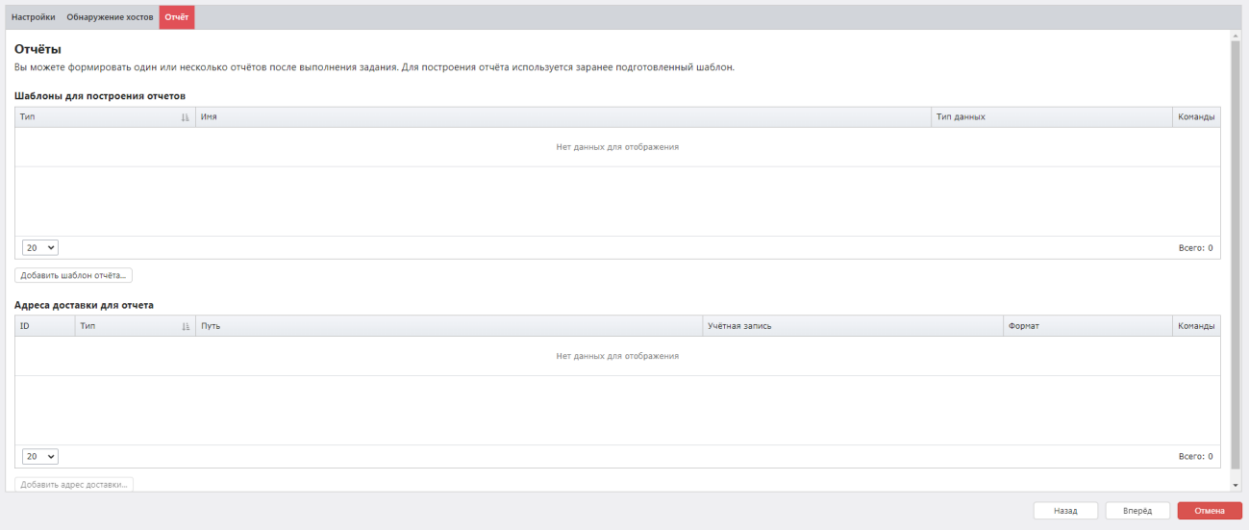


Расширенные настройки:

- Профиль временных настроек – настройка для nmap, которой регулируется количество и частота отправляемых пакетов на хост.



Шаг 4. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;



Шаг 5. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

4.10 Аудит в режиме "Пентест"

В рамках данного аудита RedCheck позволяет выполнить сетевое сканирование без привилегий в режиме Черного ящика. Аудит в режиме «Пентест» может выполнить следующие типы сканирований в рамках одного задания:

- Сканирование портов — проведение сетевой инвентаризации без привилегий для опубликованных служб каждого хоста, выявление ПО и его версии;
- Поиск уязвимостей — проведение аудита уязвимостей без привилегий с выполнением дополнительных скриптов для выявленного по итогам сетевой инвентаризации ПО.
- Подбор паролей — выполнение подбора паролей на основе указанных словарей для требуемых сетевых служб.

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

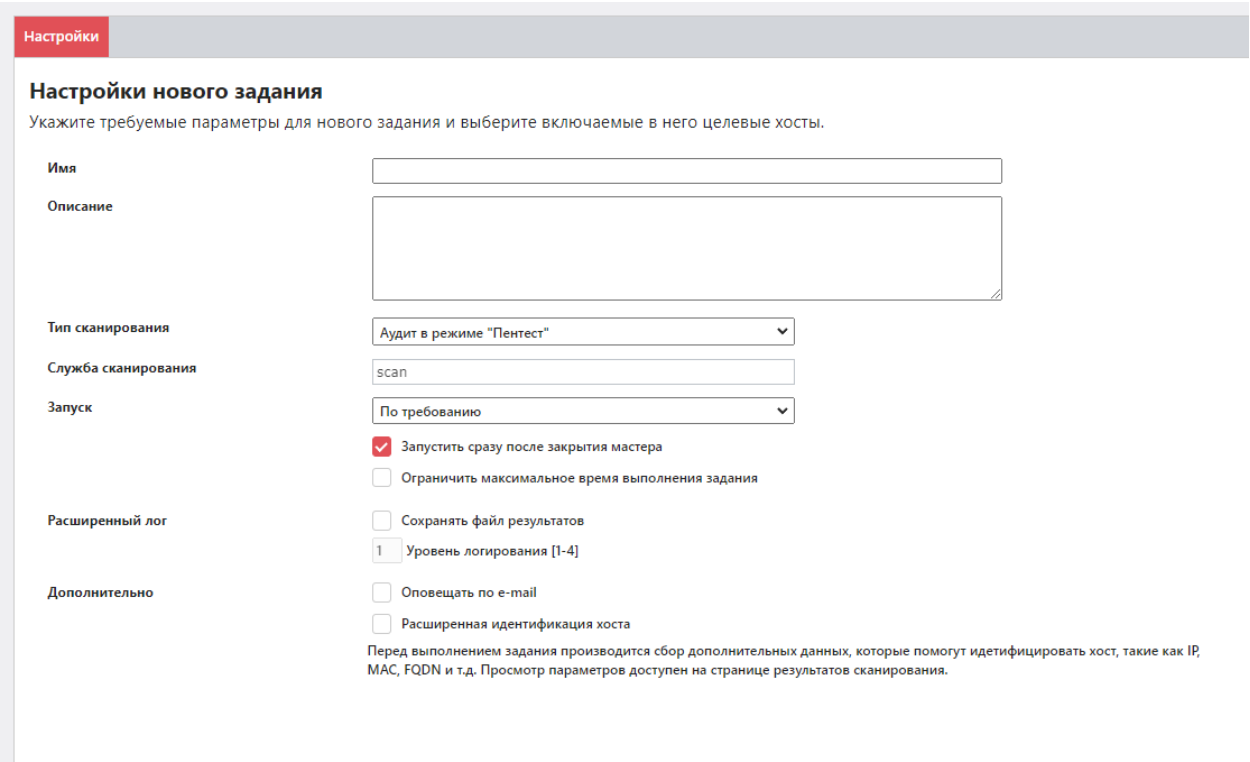
Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Аудит в режиме «Пентест»**;

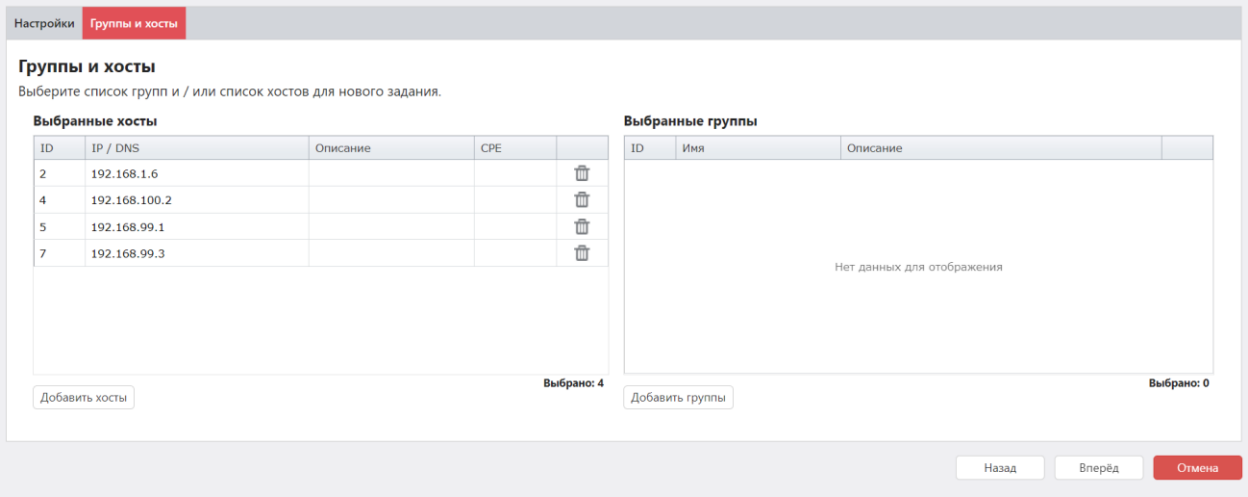
Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ... (Мониторинг служб сканирования);
- Тип запуска:
  - По требованию – запуск задания вручную;
  - По расписанию – задание будет выполняться согласно настроенному расписанию (Настройка расписания);

- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;
- Ограничить максимальное время выполнения задания – функция Остановки задания по времени выполнения;
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по-умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;
- Уровень логирования [1-4] – уровень детализации логов Altxmap. Чем больше значение, тем детальнее будет лог;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;

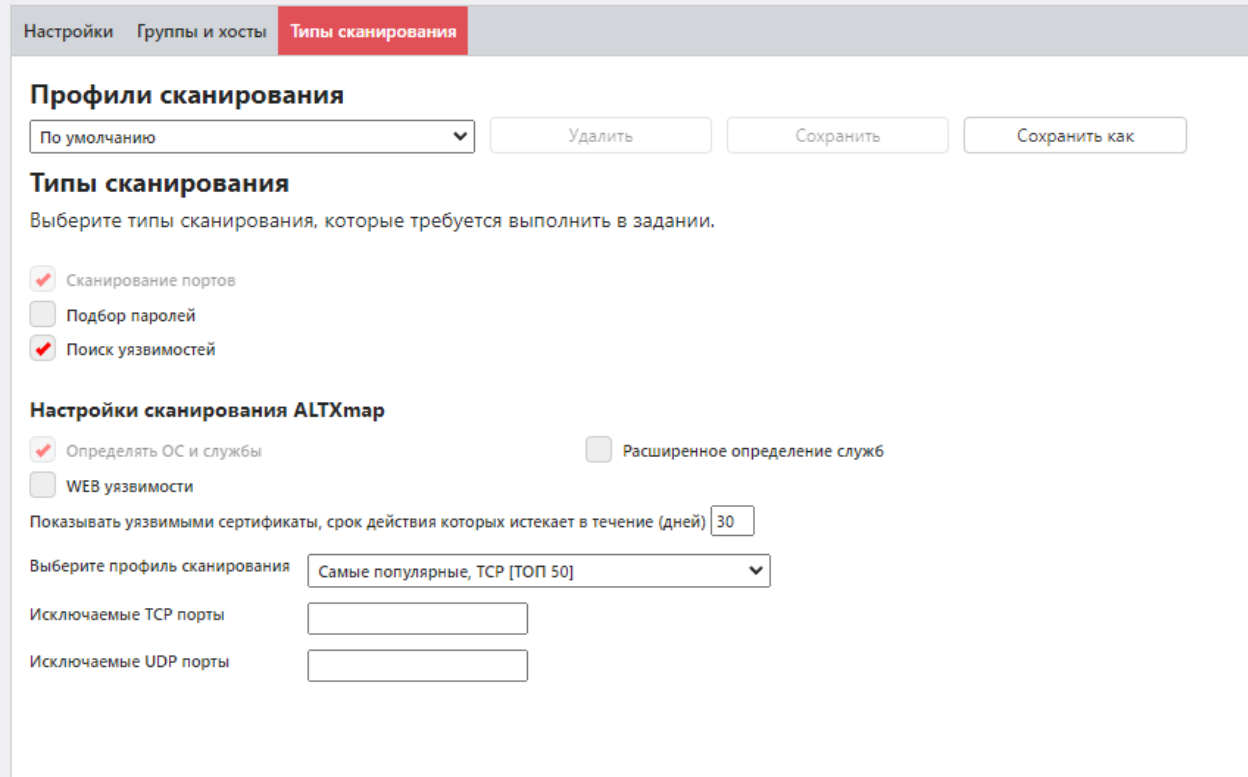


Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;



Шаг 4. Укажите настройки для сканирования → **Вперед**;

- Профили сканирования – можно выбрать ранее созданный профиль сканирования Altxmap;
- Подбор паролей – разрешить службе сканирования подбирать пароли к:
  - СУБД: Microsoft SQL Server, PostgreSQL, Oracle (+парольные хеши), MySQL;
  - SSH, FTP;
  - Почтовый сервер POP3;
- Поиск уязвимостей – разрешить обнаружение уязвимостей методом Черного ящика;
- Расширенное определение служб –
- WEB уязвимости – разрешить применение скриптов для Altxmap с тегом intrusive. Такие скрипты требуют значительное количество вычислительных ресурсов, что увеличивает время сканирования;
- Профили сканирования – порты, с которыми служба сканирования будет создавать соединение во время сканировани;
  - Перечень портов для профиля TCP [ТОП 50]
  - Перечень портов для профиля TCP [ТОП 1000]
  - Перечень портов для профиля TCP-UDP [ТОП 1000]

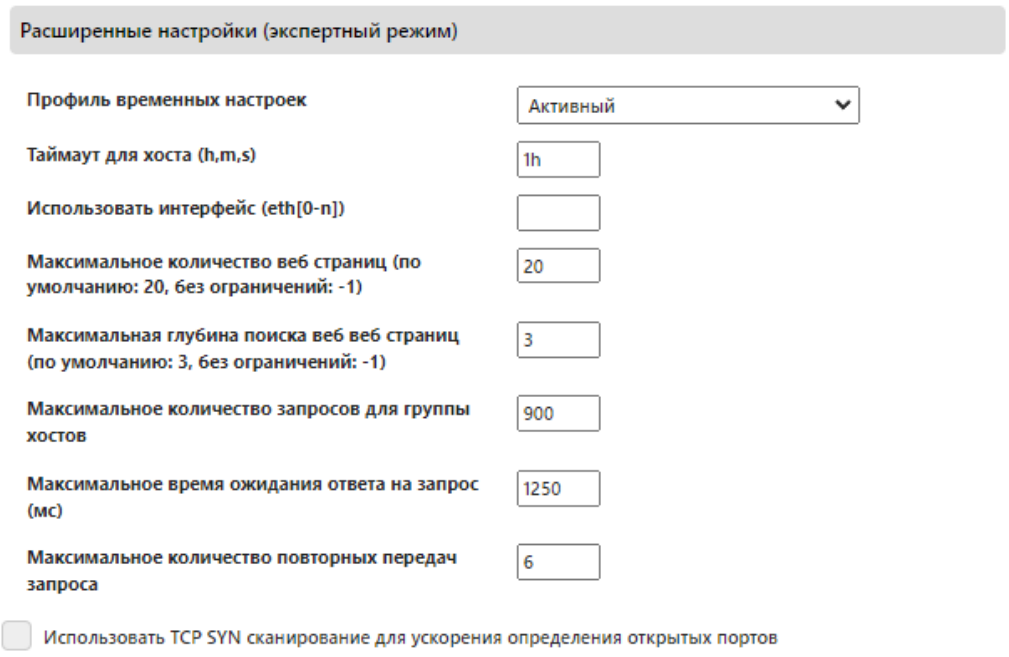


Расширенные настройки:

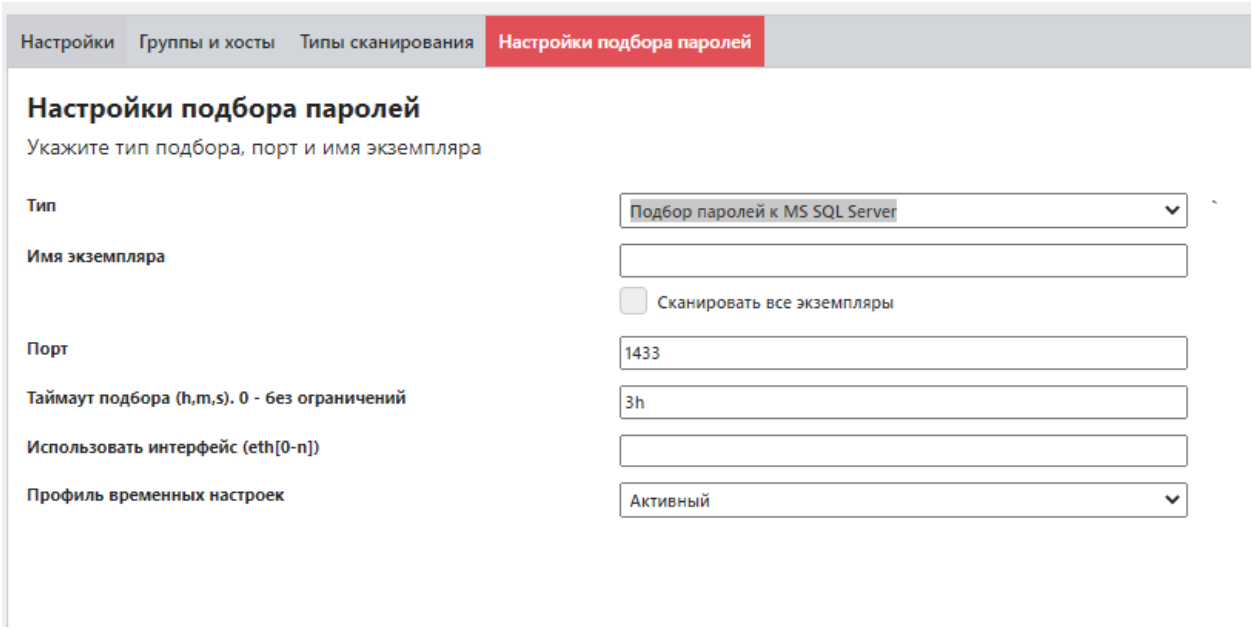
- Профиль временных настроек – настройка для сетевого сканера, которой регулируется количество и частота отправляемых пакетов на хост;
- Таймаут для хоста (h,m,s) – параметр --host-timeout. Задайте максимальное время ожидания, например, 30 мин, чтобы Altxmap не тратил более получаса на один хост. В течение этого времени Altxmap может сканировать другие хосты. Хост, чье время истекло, пропускается, и для него не собирается ни таблица портов, ни информация об ОС;
- Максимальное кол-во веб страниц – сколько всего страниц будет просканировано в результате рекурсивного поиска по web-приложениям;
- Максимальная глубина поиска веб страниц – параметр глубины для рекурсивного поиска по web-приложениям;
- Максимальное количество запросов для группы хостов – параметр --max-parallelism. По умолчанию Altxmap определяет степень параллелизма на основе производительности сети, начиная с 1 при плохих условиях и до нескольких сотен при идеальных. Опция иногда устанавливается для предотвращения отправки хостам более одного запроса за раз;
- Максимальное количество повторных передач запроса – если Altxmap не получил ответ на запрос сканирования порта, это может означать, что

порт фильтруется или запрос потерялся в сети. Также возможно, что хост ограничивает количество ответов, что привело к временной блокировке запроса. В этом случае Altxmap повторяет передачу запроса. Если сеть кажется ненадежной, Altxmap может предпринять множество попыток передачи запроса перед прекращением сканирования. Это увеличивает время сканирования, но повышает достоверность результатов. Для ускорения сканирования можно ограничить количество повторных передач с помощью --max-retries. Установка --max-retries на 0 предотвратит все повторные попытки, хотя это не рекомендуется;

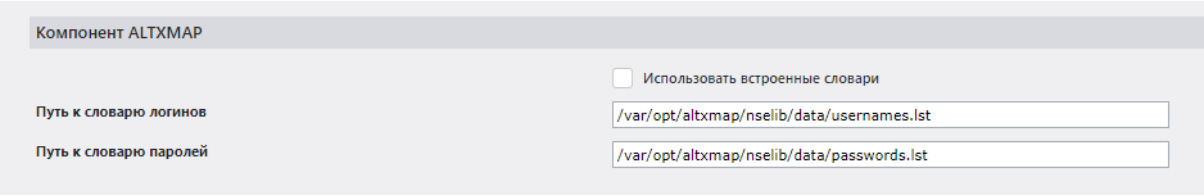
- Использовать TCP SYN сканирование для ускорения определения открытых портов – позволяет сканировать несколько сот портов в секунду, сохраняя при этом сканирующий хост в тени, поскольку никогда не завершает TCP-соединение (большинство утилит мониторинга не регистрируют данные соединения).



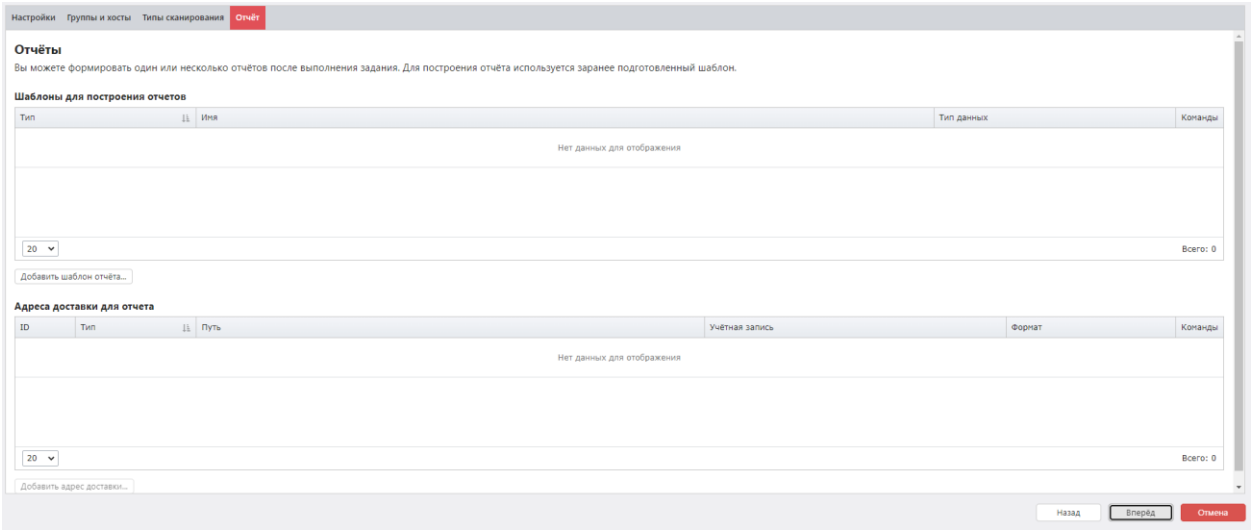
Шаг 5. Если параметр Подбор паролей был отмечен, мастер предложит настроить данную функцию → **Вперед**;



Подбор паролей происходит на основе словарей. Чтобы заменить словарь, откройте **Инструменты** → **Настройки** → **Сканирование** → **Компонент ALTXMAP** → укажите путь к новому словарю, находящемуся на хосте с установленной службой сканирования



Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;



Шаг 7. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

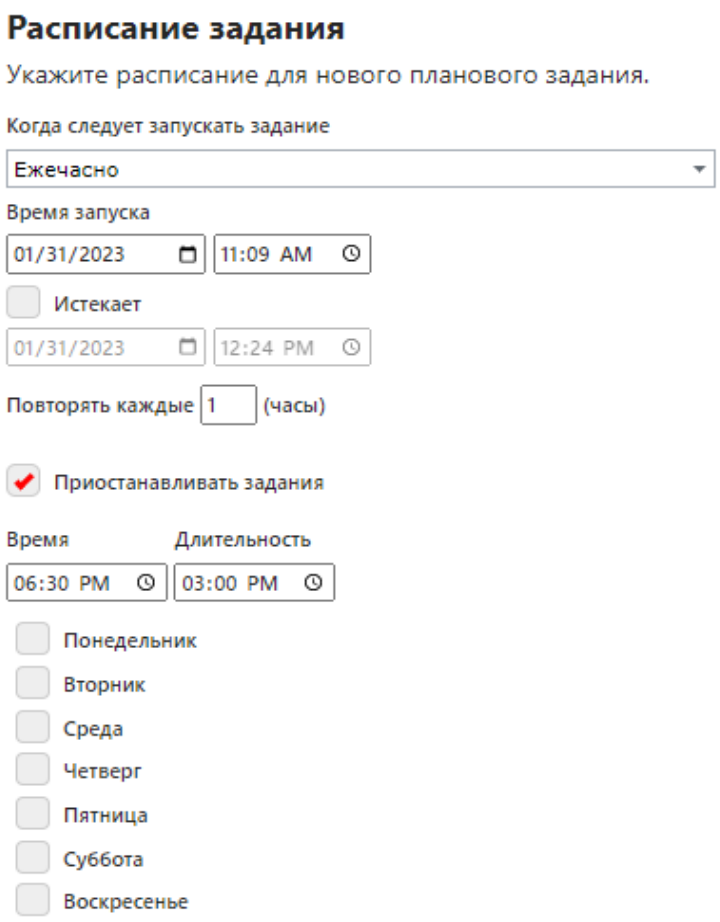
Настройка расписания для задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Расписание можно настроить как в момент создания задания, так и при редактировании ранее созданного.

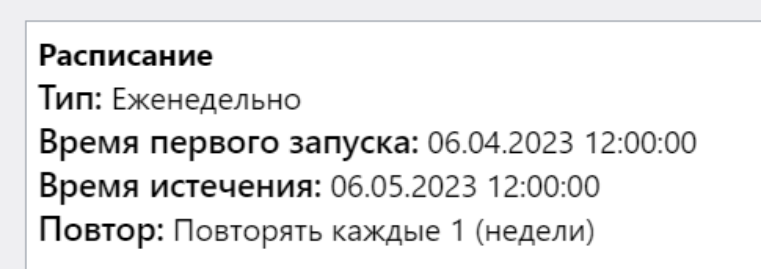
Форма с параметрами выглядит следующим образом:

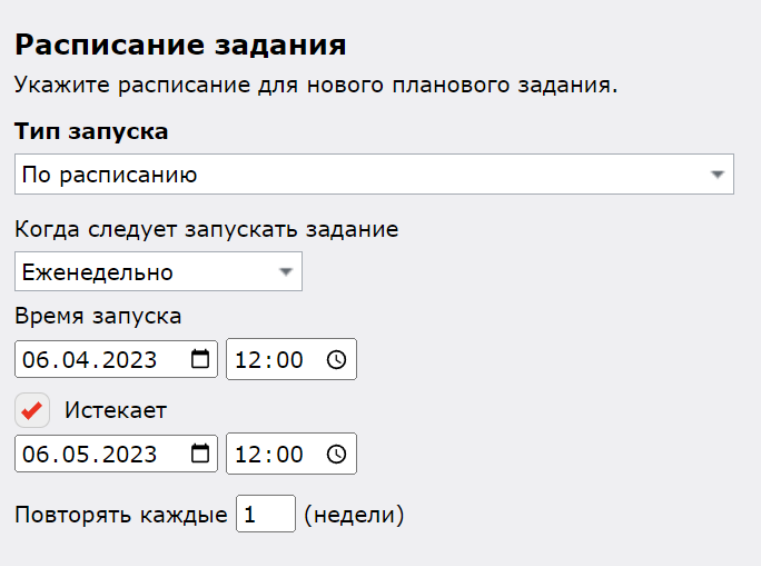
- Когда следует запускать задание – периодичность запуска задания;
- Время запуска – дата и время запуска задания;
- Истекает – дата и время окончания работы расписания;
- Повторят каждые – показатель, через сколько задание будет запускаться повторно;
- Приостанавливать задание – дата, время и дни недели, когда расписание не будет выполняться.



Пример использования

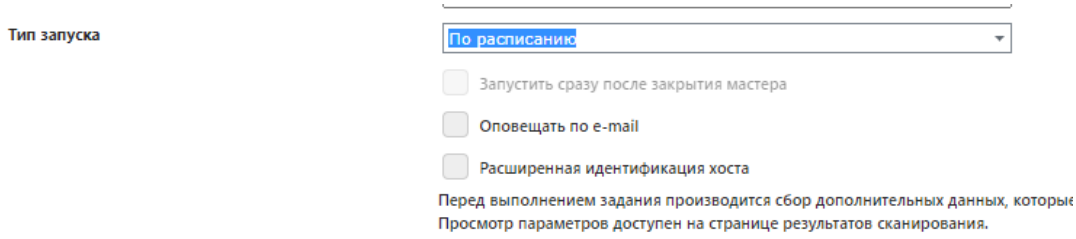
Запуск задания каждую неделю в 12:00 на протяжении месяца.





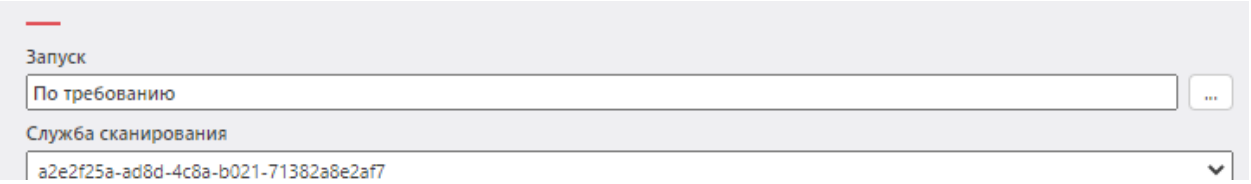
Настройка в момент создания

Выберите на начальной странице мастера тип запуска **По расписанию**. В одном из последующих шагов будет страница с настройками расписания.



Настройка при редактировании задания

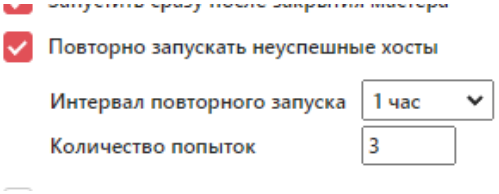
Зайдите в свойства задания → нажмите ... в параметре **Запуск**.



Повторный перезапуск недоступных хостов во время сканирования

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Функции повторного запуска неуспешных хостов и ограничения максимального времени выполнения задания можно настроить как в момент создания задания, так и при редактировании ранее созданного.

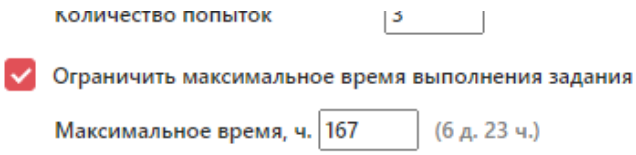


а) Повторный перезапуск касается хостов, которые служба определила как недоступные (например, не смогла подключиться за определенный интервал времени). Под повторный перезапуск не попадают хосты, для которых не подошла ни одна из указанных при создании задания учетных записей (на данный момент для транспорта WinRM не применяется данное условие). Результаты сканирования таких хостов будут сразу записаны в Историю.

б) Хост, который оказался недоступен, будет запущен через указанное в параметре **Интервал повторного запуска** время. Точкой отсчета для интервала является время завершения неудачного сканирования. Если на момент запланированного перезапуска служба не закончила основное сканирование, то приоритетно будут сканироваться основные хосты, а только потом будут перезапущены недоступные. В случае повторной недоступности перезапуск хоста произойдет через указанное в параметре **Интервал повторного запуска** время с момента завершения очередного неудачного сканирования. Количество повторных попыток задается в параметре **Количество попыток**

в) В случае, если время перезапуска недоступного хоста приходится на время приостановки задания по расписанию, то перезапуск будет отложен на момент возобновления сканирования. Если на момент возобновления сканирования служба не завершила сканирование основных хостов, то недоступный хост будет перезапущен после окончания основного сканирования.

Ограничение максимального времени выполнения задания



Данная функция позволяет останавливать задание, которое выполняется больше указанного времени. Точкой отсчета является время начала сканирования. Не учитывается время приостановки задания по расписанию. Например, задание запускается в 14:00, приостановка с 15:00 по 19:00, для параметра **Ограничение максимального времени выполнения задания** установлено значение в 6 часов → остановка задания произойдет в 20:00.

5 Расширенные возможности для заданий сканирования

RedCheck предлагает следующие расширенные возможности для заданий:

- Создавать профили сканирования, в которых можно указывать конкретные OVAL-определения для поиска на хосте;
- Добавлять собственную конфигурацию для необходимого продукта, или изменять уже имеющуюся в БД RedCheck;
- Добавлять свои собственные OVAL-определения в Систему.

Содержание

5.1 Профили аудитов

RedCheck позволяет выбрать OVAL-определения уязвимостей и обновлений для добавления их в профиль аудитов. Такой профиль позволяет искать на хостах только нужные уязвимости и неустановленные обновления, а также наоборот, исключать из отчетов указанные в профиле OVAL-определения. Создание профилей аудитов происходит в Менеджере профилей.

Типы профилей

Существует два типа профилей:

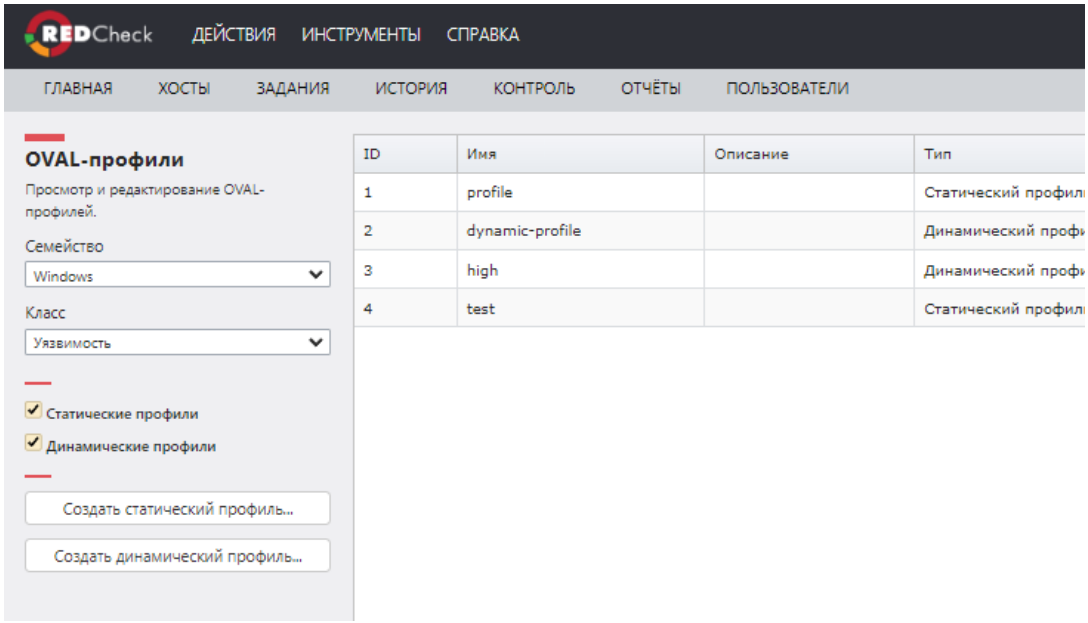
- Статический – сигнатуры указываются вручную;
- Динамический – сигнатуры находятся автоматически, исходя из указываемых параметров поиска.

> Профили сканирования можно применить только для аудитов уязвимостей и обновлений.

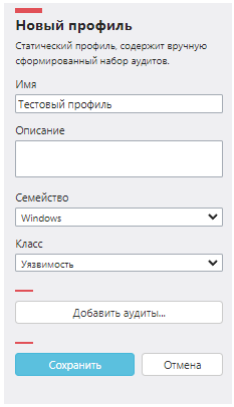
Пример использования

Создадим статический профиль для поиска на хостах нескольких интересующих нас уязвимостей.

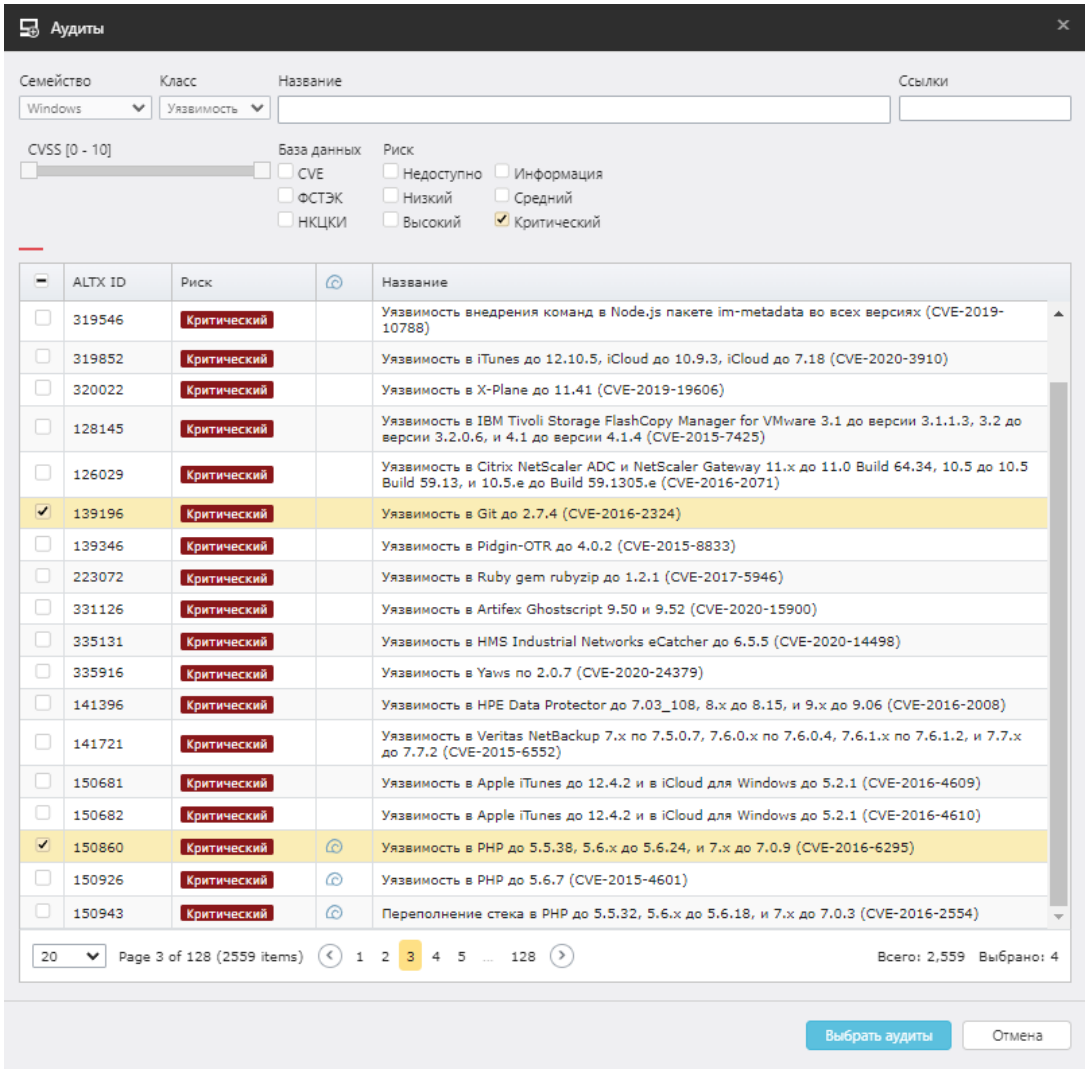
Раскроем **Инструменты** → **Менеджер профилей** → **Создать статический профиль;**



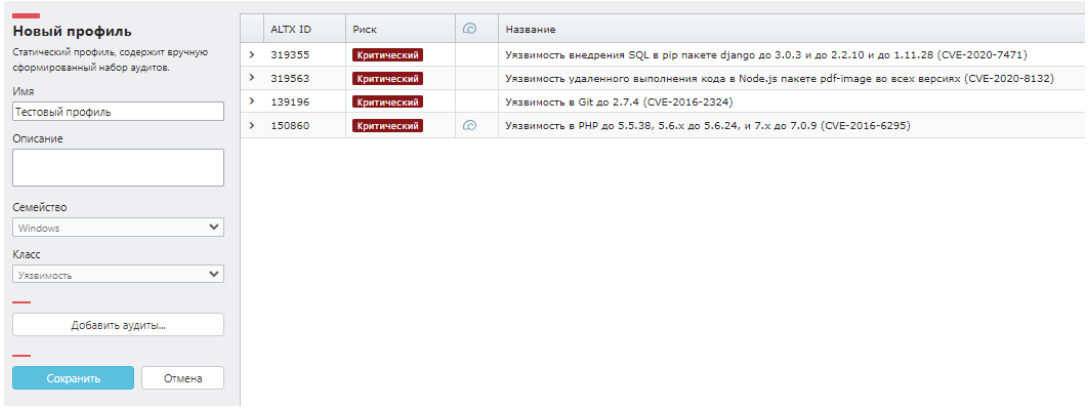
Укажем имя, платформу и класс OVAL-определений для нашего профиля (подробнее в [5.1.1 Менеджер профилей]).



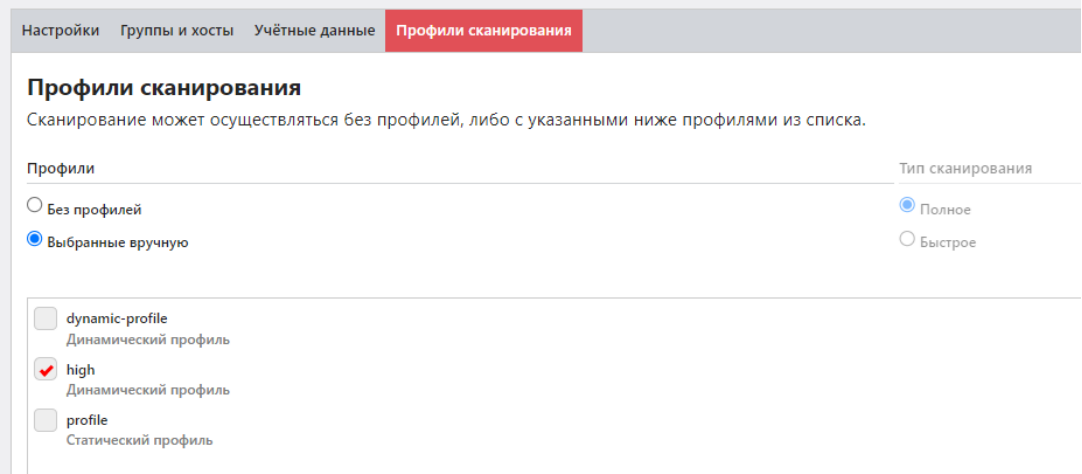
Нажав **Добавить аудиты**, выберем необходимые OVAL-определения → **Выбрать аудиты**.



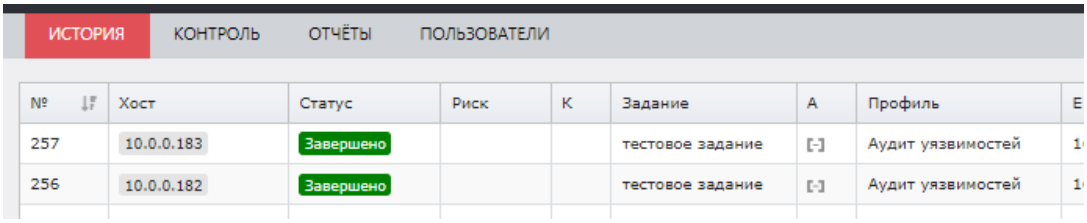
Сохраним созданный профиль, нажав соответствующую кнопку.



Создадим задание Аудит уязвимостей. Дойдем до шага **Профили сканирования** → отметим **Выбранные вручную** и укажем созданный нами профиль.



Перейдем в **История** и посмотрим результаты сканирования;



Видим, что на двух просканированных хостах указанных в профиле уязвимостей не найдено.

5.1.1 Менеджер профилей

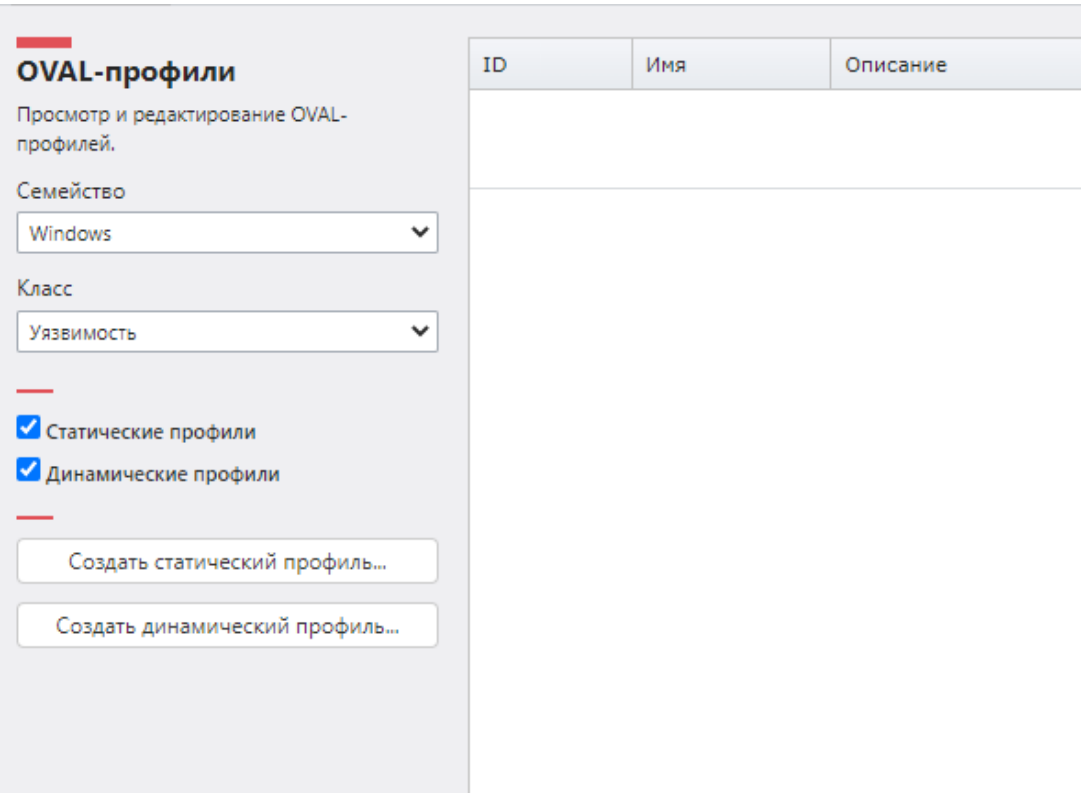
Создание профиля аудитов

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Для того, чтобы создать профиль аудитов, выполните следующие шаги.

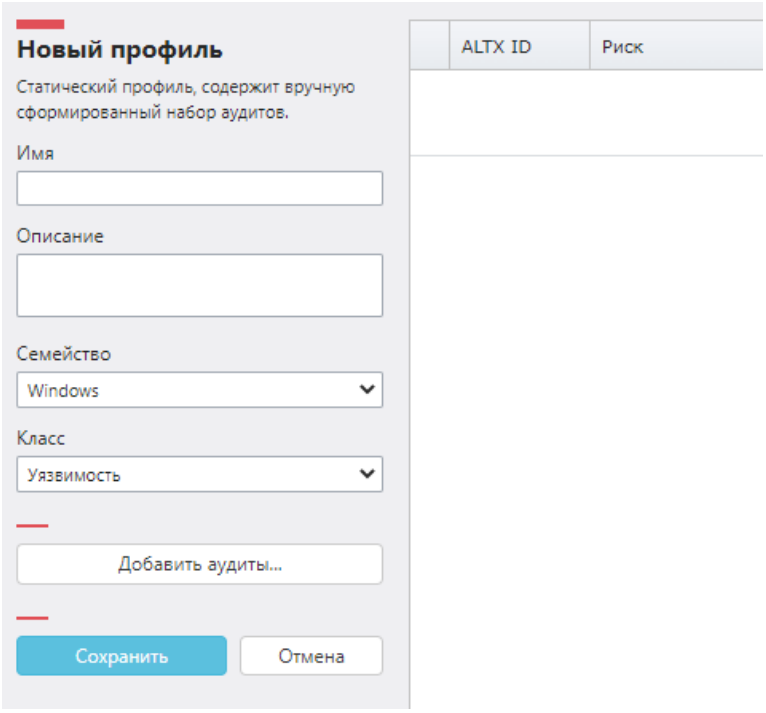
Шаг 1. Откройте **Инструменты** → **Менеджер профилей**;

Шаг 2. Выберите необходимый тип профиля, нажав **Создать статический профиль** / **Создать динамический профиль**;

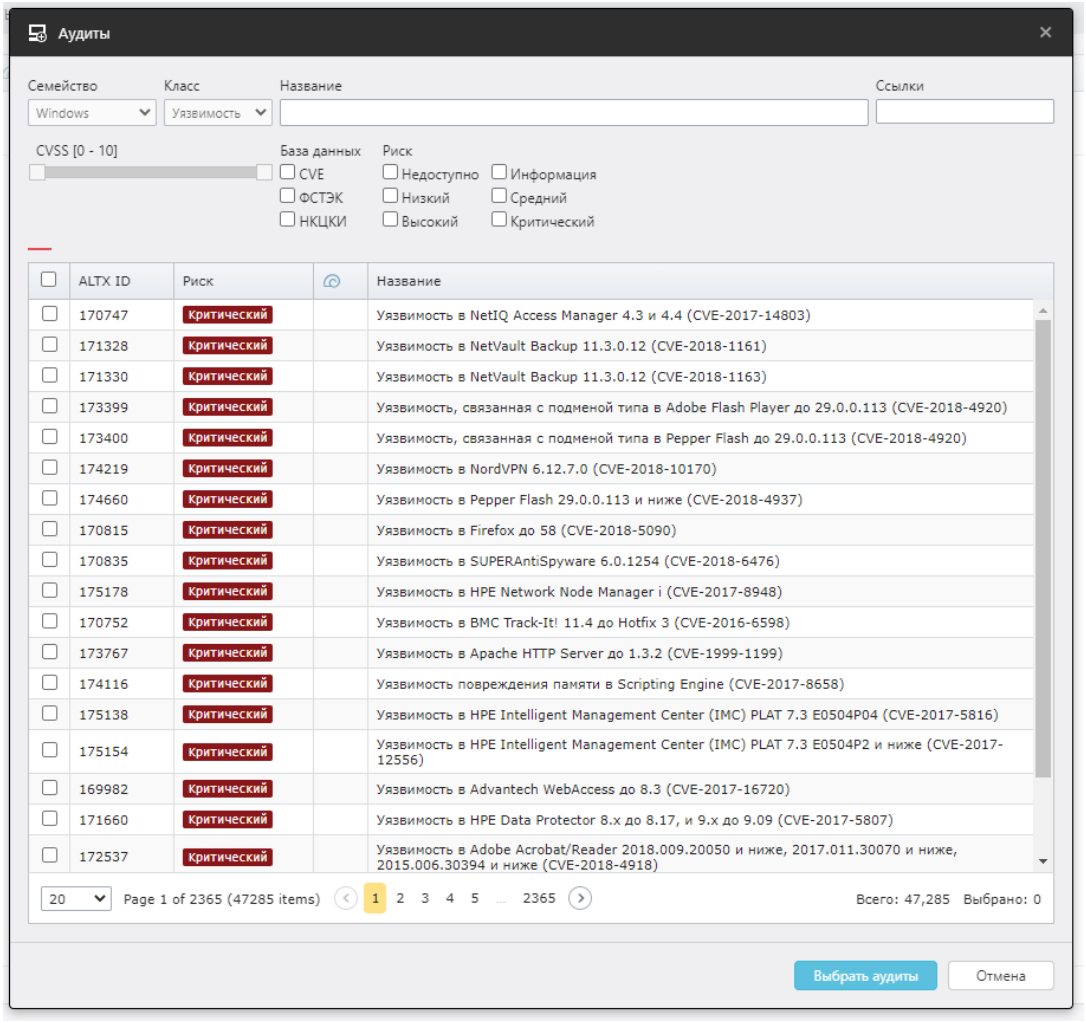


Статический профиль

Шаг 3. Укажите имя, платформу и класс OVAL-определения для создаваемого профиля → **Добавить аудиты;**



Шаг 4. Отметьте в списке нужные OVAL-определения, воспользовавшись фильтром при необходимости → **Выбрать аудиты;**

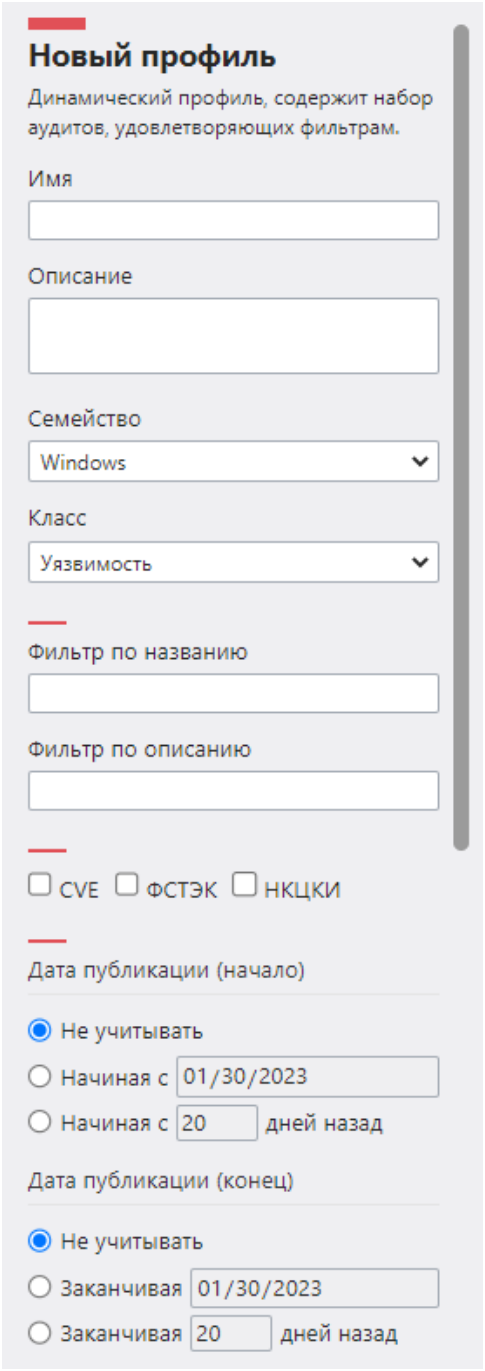


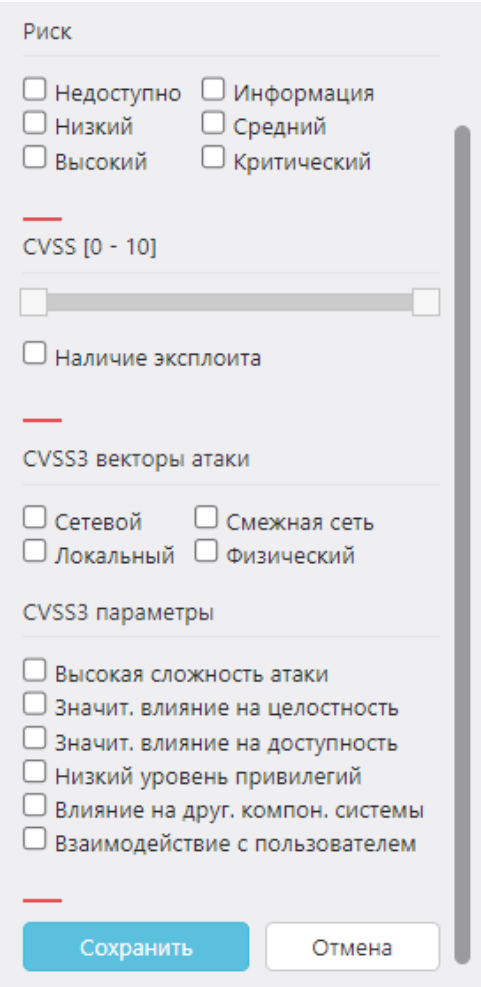
Сохраните профиль, нажав соответствующую кнопку.

Динамический профиль

Шаг 3. Укажите параметры для поиска OVAL-определений, воспользовавшись фильтром → **Сохранить**;

> При изменении настроек фильтрации в таблице будут отображаться OVAL-определения, которые попадут в профиль.


Новый профиль
Динамический профиль, содержит набор аудитов, удовлетворяющих фильтрам.
Имя
Описание
Семейство
Windows
Класс
Уязвимость
Фильтр по названию
Фильтр по описанию
CVE
ФСТЭК
НКЦКИ
Дата публикации (начало)
Не учитывать
Начиная с 01/30/2023
Начиная с 20 дней назад
Дата публикации (конец)
Не учитывать
Заканчивая 01/30/2023
Заканчивая 20 дней назад

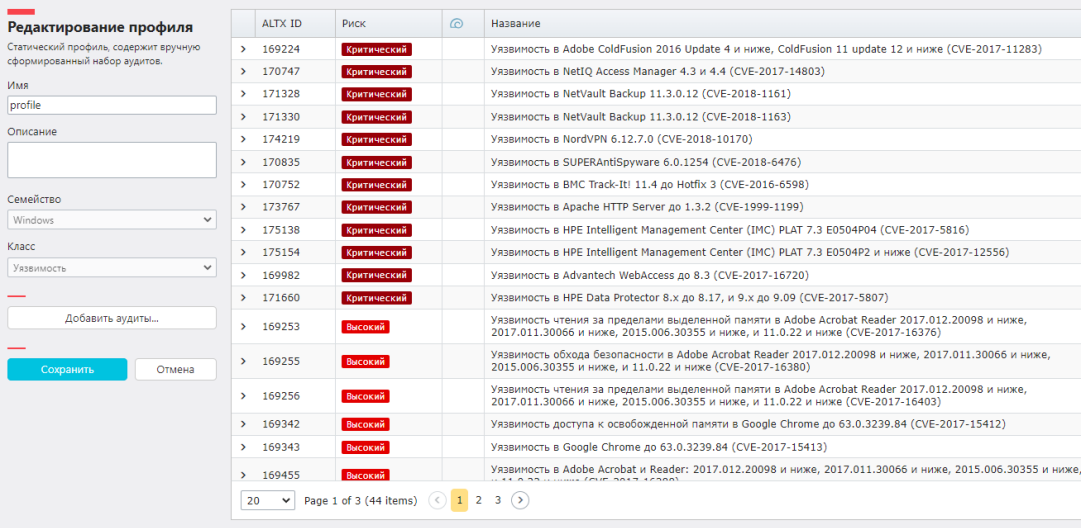


Редактирование профиля аудитов

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Для того, чтобы отредактировать созданный ранее профиль аудитов, выполните следующие шаги.

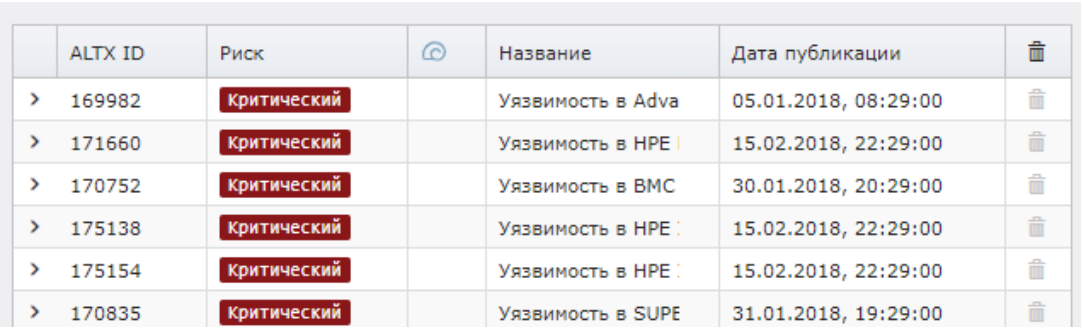
Откройте **Инструменты** → **Менеджер профилей** → ⚙ → **Редактировать**;



При редактировании профиля аудитов есть возможность изменить имя профиля и добавить / убрать OVAL-определения.

Добавление: Для добавления OVAL-определений в профиль аудитов нажмите **Добавить аудиты** → отметьте в списке нужные определения, воспользовавшись фильтром при необходимости → **Выбрать аудиты**.

Удаление: Для удаления уже добавленных определений нажмите  ;

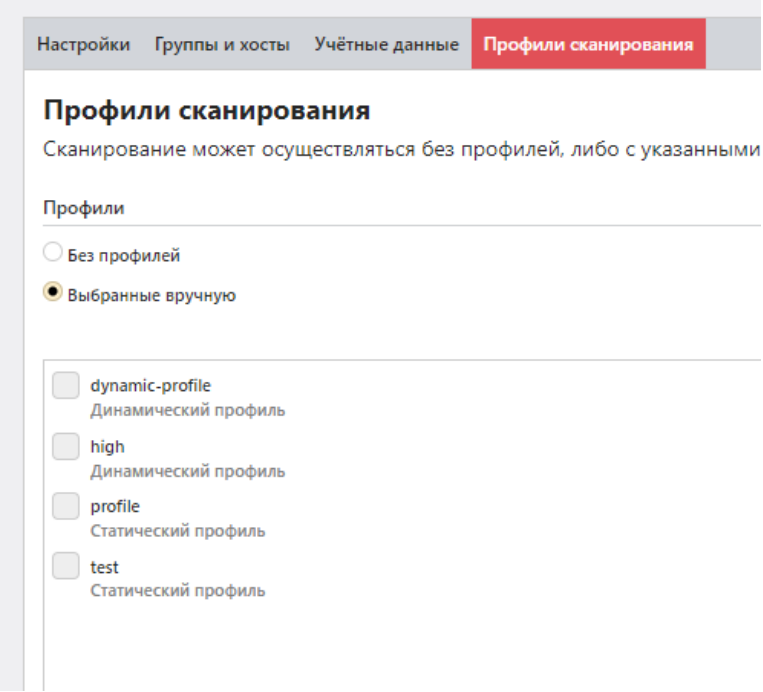


После внесения изменений нажмите **Сохранить**.

Применение профилей аудитов при создании задания

При создании заданий типа Аудит уязвимостей / обновлений (4.1 Аудит уязвимостей, 4.2 Аудит обновлений) есть возможность указать профиль аудитов.

Для этого на шаге 5 (Профили сканирования) выберите **Выбранные вручную** → отметьте необходимые профили → **Далее**;



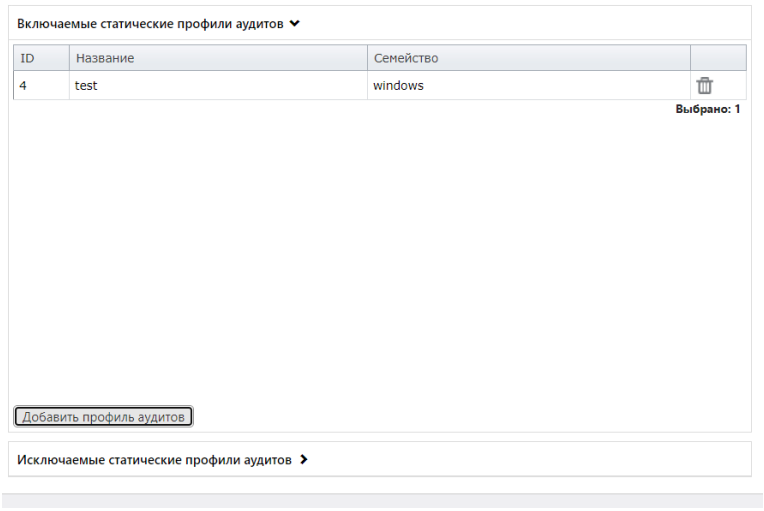
Применение статических профилей аудитов к отчетам

> При создании отчета (7.1 Создание простого отчета) типа Уязвимости / Обновления есть возможность указать **только** статические профили аудитов.

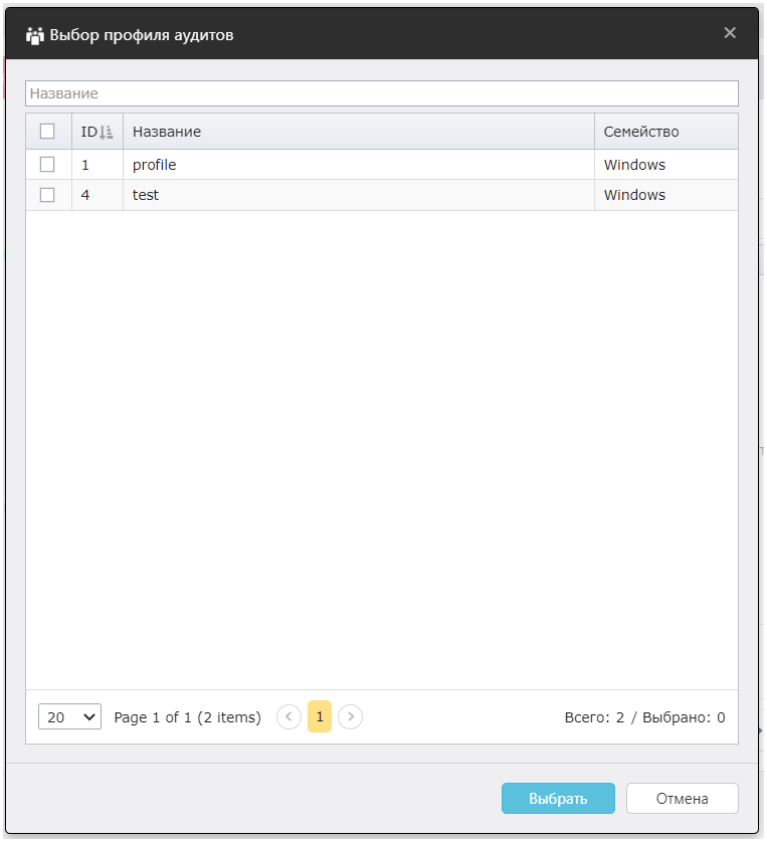
RedCheck позволяет включить и исключить профиль из отчета. При включенном профиле в отчет попадут только те OVAL-определения, которые указаны в выбранном профиле. При исключении указанные в профиле определения не попадут в отчет.

Для добавления / удаления профиля в отчет выполните следующие шаги.

Шаг 1. При создании отчета в разделе **Фильтрация результатов сканирования** раскройте список **Включаемые / Исключаемые статические профили аудитов** → **Добавить профиль аудитов**;



Шаг 2. Отметьте нужные профили аудитов → **Выбрать**.



5.2 Конфигурации

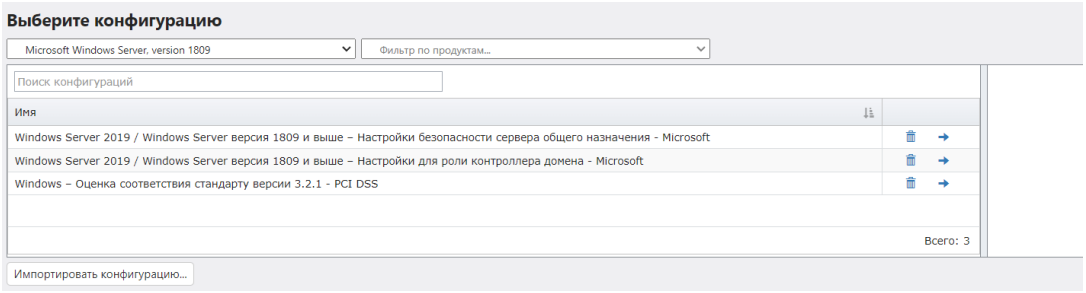
RedCheck предоставляет возможность изменять конфигурации, имеющиеся в базе данных, для проведения Аудита конфигураций согласно собственных настройкам правил проверки. Работа с конфигурациями происходит в Менеджере конфигураций.

Пример использования

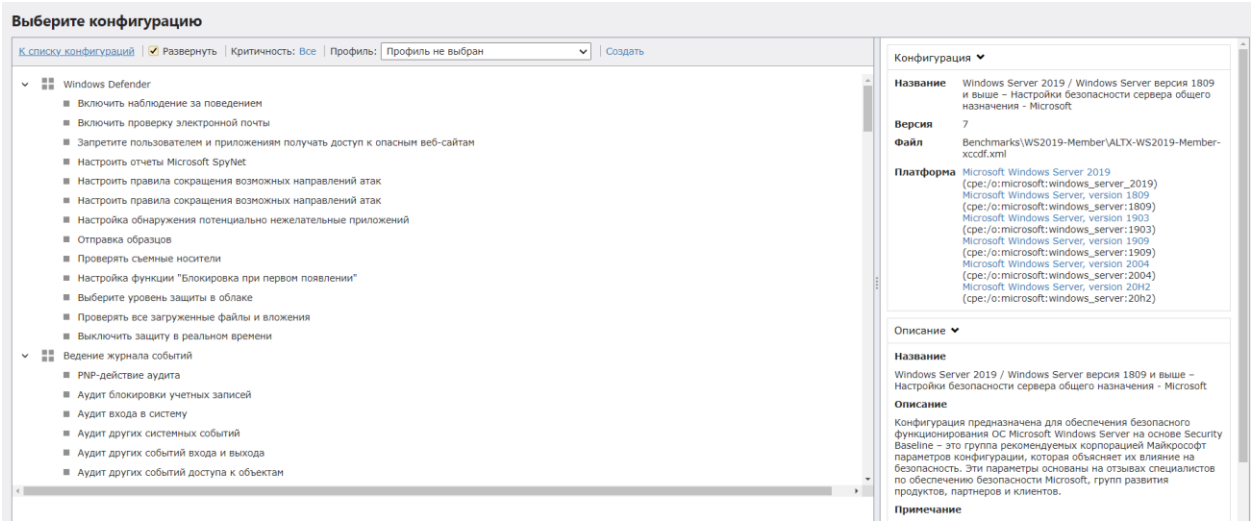
Отредактируем конфигурацию «Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения - Microsoft».

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

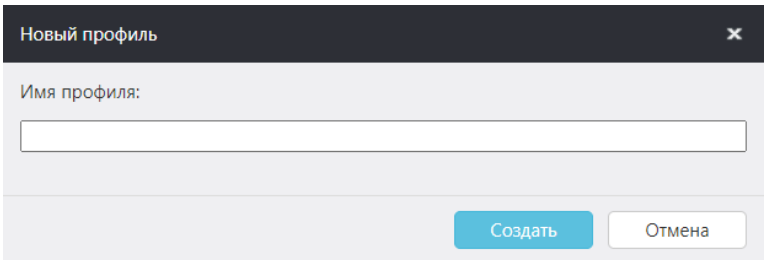
Раскроем **Инструменты** → **Менеджер конфигураций** → выберем в фильтре по платформам **Microsoft Windows Server, version 1809**;



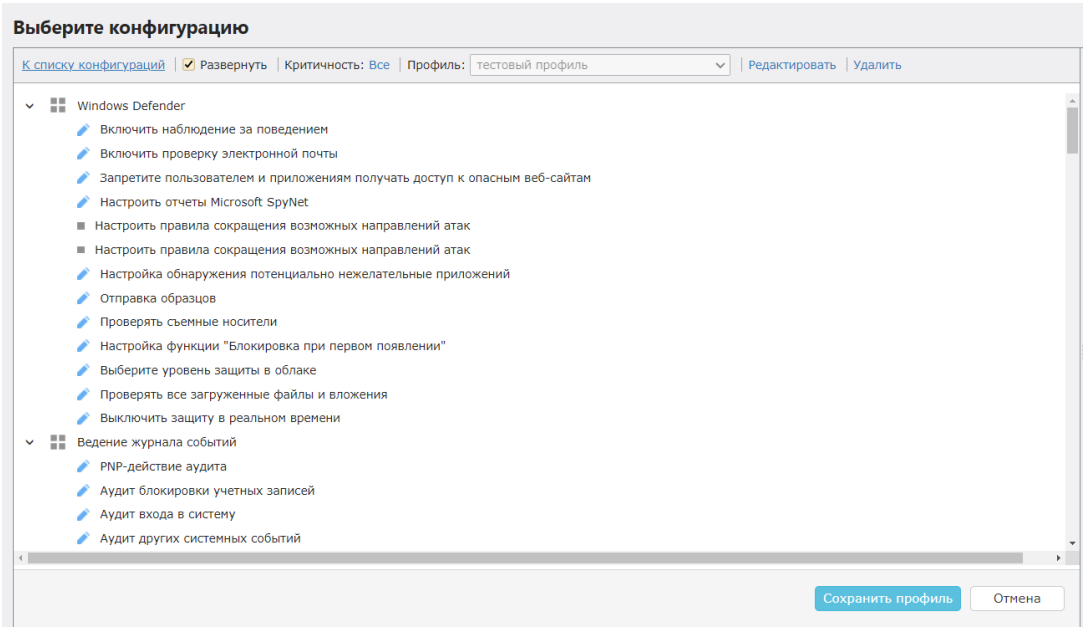
Для редактирования конфигурации для сервера общего назначения нажмем



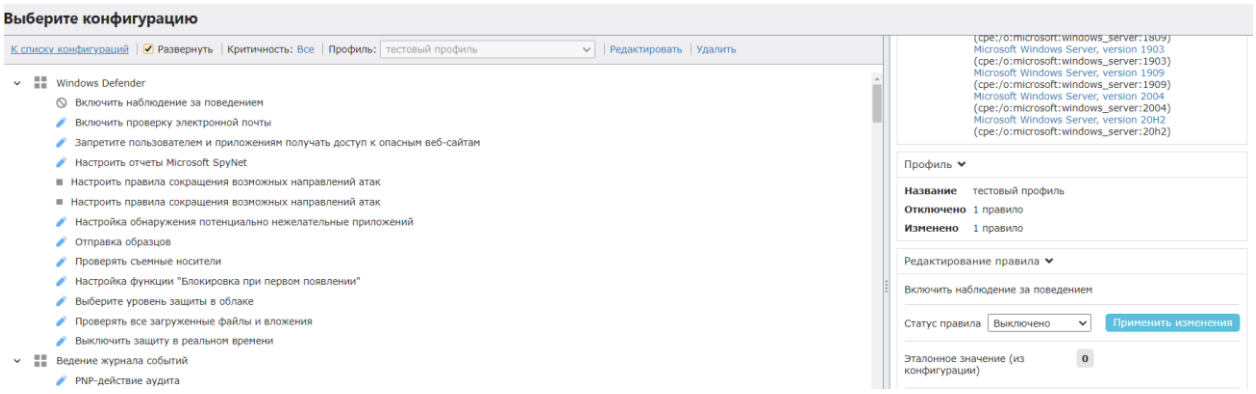
Создадим собственный профиль для изменения правил в конфигурации. Для этого нажмем **Создать** → введем имя для профиля → **Создать**.



После создания профиля можно изменять нужные нам правила.



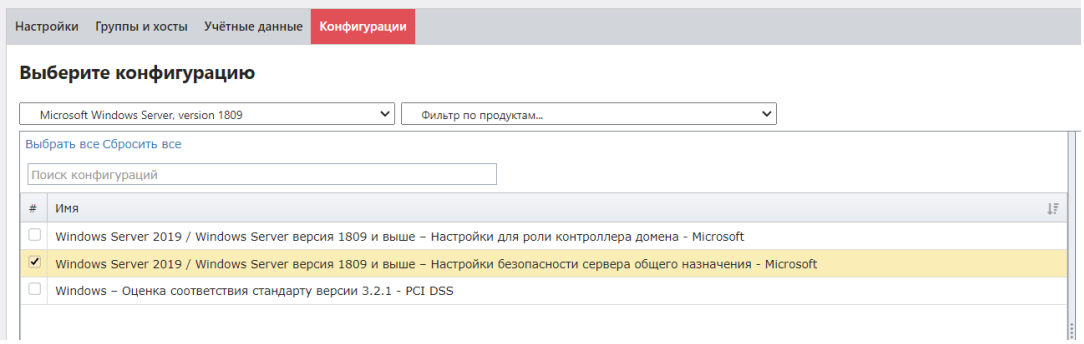
Отключим правило Включить наблюдение за поведением. В списке **Статус правила** выберем **Выключено** → **Применить изменения**. Возле правила изменится иконка, уведомляющая, что правило неактивно.



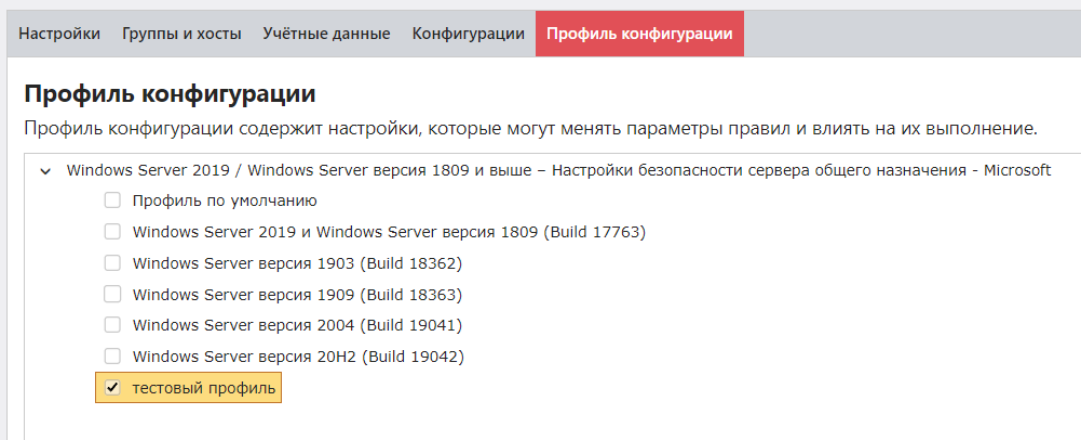
Изменим эталонное значение для правила **Проверять съемные носители**. Отметим **Переопределить эталонное значение** и изменим в списке значение с **Enabled (0)** на **Disabled (1)** → **Применить изменения**. Возле правила изменится иконка, уведомляющая, что эталонное значение правила было переопределено.

Сохраним созданный нами профиль, нажав **Сохранить профиль**.

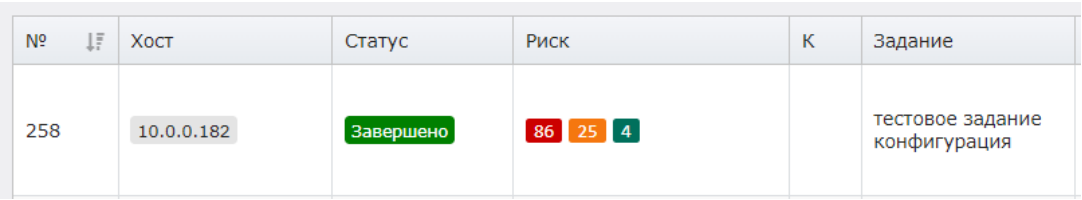
Создадим задание Аудит конфигураций → на шаге **Конфигурация** выберем отредактированную конфигурацию → **Далее**.



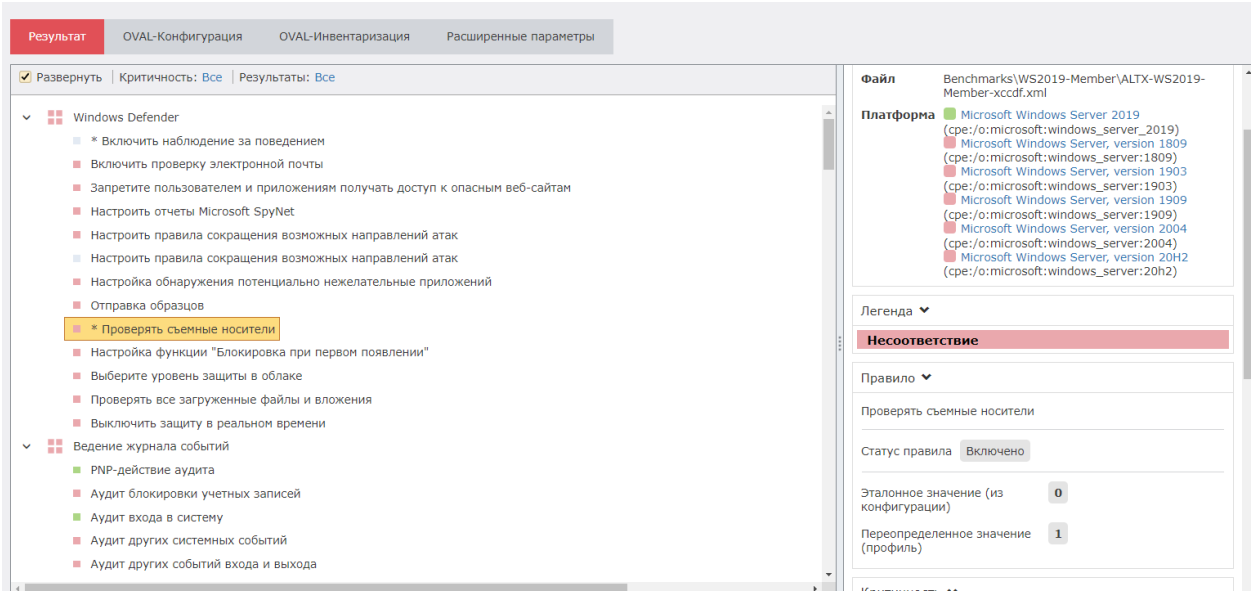
Отметим созданный нами профиль → **Далее**.



Перейдем в **История** и посмотрим результат сканирования, нажав **Завершено**.



Видим, что измененные правила помечаются перед своим названием знаком *****. Для правил, в которых было переопределено эталонное значение, пишется стандартное и переопределенное значение.



В RedCheck есть возможность импортировать собственные конфигурации (5.2.1 Импорт конфигураций). Конфигурация должна быть написана с использованием открытого стандарта OVAL. ALTX-SOFT предоставляет услуги написания конфигураций. За подробностями обращайтесь в службу тех. поддержки (контакты указаны на странице вендора).

5.2.1 Импорт конфигураций

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

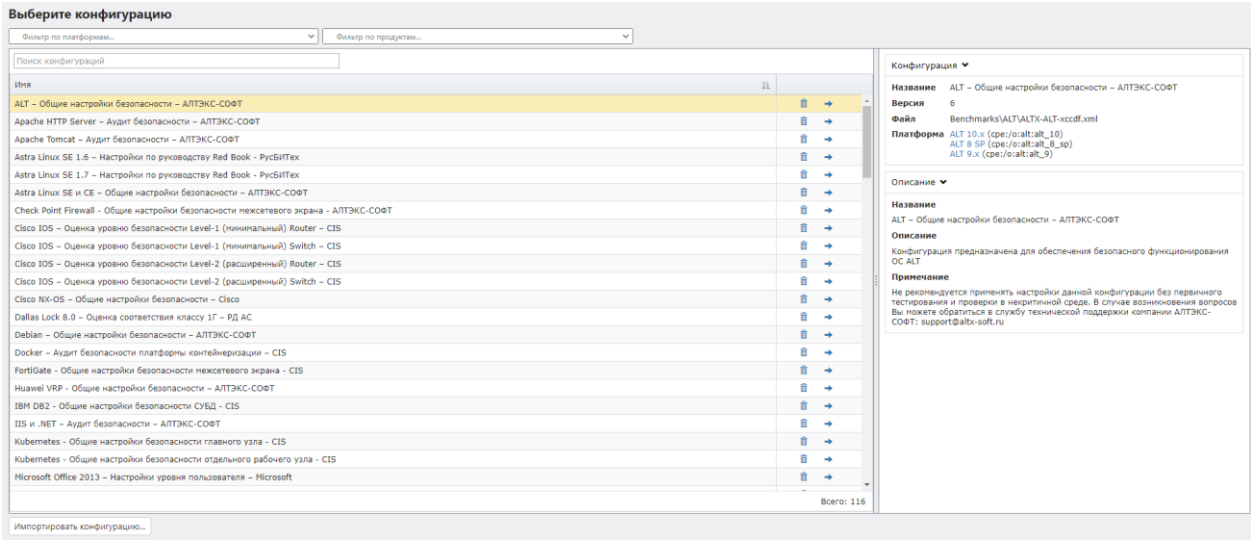
Чтобы импортировать конфигурацию в базу данных, выполните следующие шаги.

Шаг 1. Откройте **Инструменты** → **Менеджер конфигураций**;

Шаг 2. В менеджере можно просматривать имеющиеся в Системе конфигурации. Нажмите **Импортировать конфигурацию** → выберите необходимые файлы;

Конфигурация состоит из 4-х файлов:

- NAME-cpe-dictionary.xml
- NAME-cpe-oval.xml
- NAME-oval.xml
- NAME-xccdf.xml



5.3 OVAL-определения

RedCheck предоставляет возможность добавлять собственные OVAL-определения для проведения Аудита уязвимостей, обновлений, конфигураций и Инвентаризации.

Классы OVAL-определений

Все OVAL-определения делятся на 4 класса:

- Соответствие (compliance) – правило для конфигураций;
- Инвентарь – определения для Инвентаризации;
- Уязвимость;
- Обновление;

Уровни критичности

OVAL-определения имеют разный уровень критичности:

Недоступно – вендор не предоставил значение уровня критичности;

Информация – OVAL-определение для инвентаря (ПО).

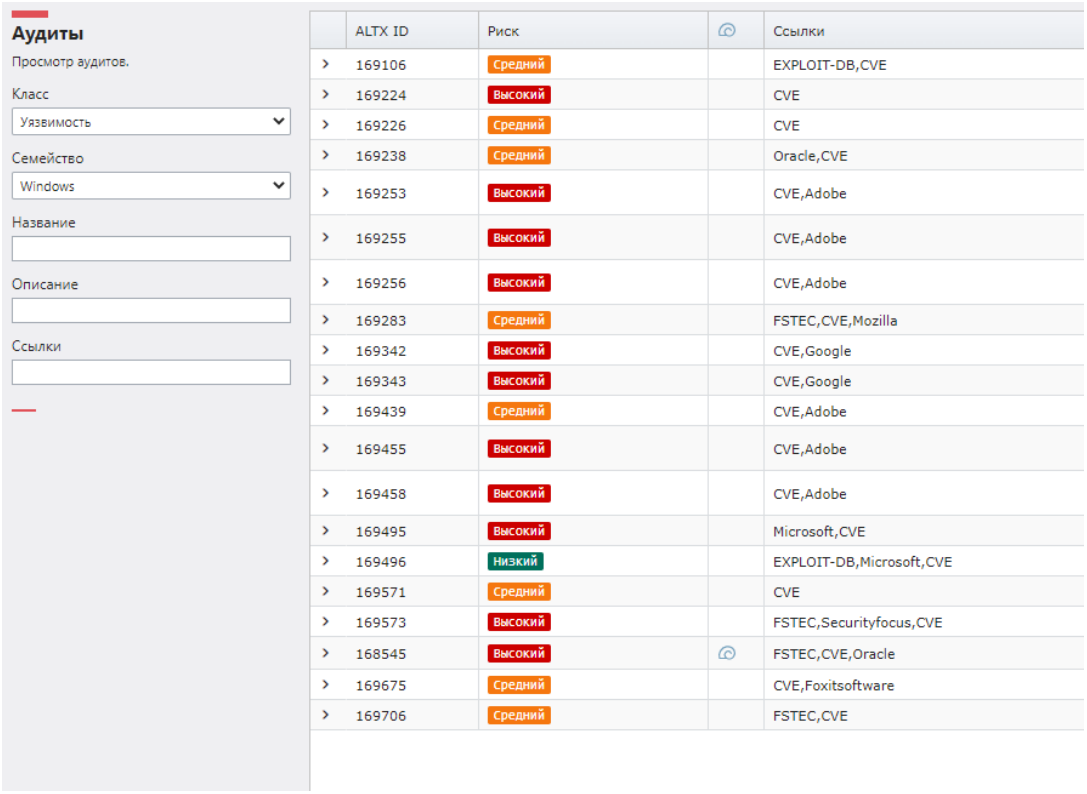
Низкий, Средний, Высокий и Критический – стандартные определения уровня критичности.

Просмотр OVAL-определений

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Раскройте **Инструменты** → **Менеджер аудитов**;

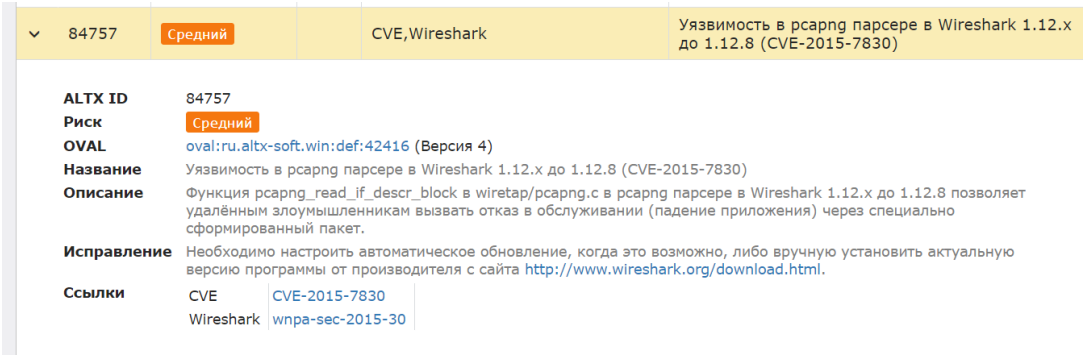
В менеджере можно посмотреть OVAL-определения, находящиеся в используемой базе данных.



	ALTX ID	Риск		Ссылки
›	169106	Средний		EXPLOIT-DB,CVE
›	169224	Высокий		CVE
›	169226	Средний		CVE
›	169238	Средний		Oracle,CVE
›	169253	Высокий		CVE,Adobe
›	169255	Высокий		CVE,Adobe
›	169256	Высокий		CVE,Adobe
›	169283	Средний		FSTEC,CVE,Mozilla
›	169342	Высокий		CVE,Google
›	169343	Высокий		CVE,Google
›	169439	Средний		CVE,Adobe
›	169455	Высокий		CVE,Adobe
›	169458	Высокий		CVE,Adobe
›	169495	Высокий		Microsoft,CVE
›	169496	Низкий		EXPLOIT-DB,Microsoft,CVE
›	169571	Средний		CVE
›	169573	Высокий		FSTEC,Securityfocus,CVE
›	168545	Высокий		FSTEC,CVE,Oracle
›	169675	Средний		CVE,Foxitsoftware
›	169706	Средний		FSTEC,CVE

Информация об уязвимости состоит из:

- ALTX ID – внутренний идентификатор уязвимости;
- Риск – уровень критичности. Расчет критичности производится с учетом базовых и временных метрик CVSS на основании данных вендора сканера, вендора ПО, экспертных организаций;
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Исправление – информация по устранению уязвимости;
- Ссылки – страницы уязвимости в различных базах данных уязвимостей;



⌄	84757	Средний		CVE,Wireshark	Уязвимость в pcapng парсере в Wireshark 1.12.x до 1.12.8 (CVE-2015-7830)

ALTX ID 84757
Риск Средний
OVAL oval:ru.altx-soft.win:def:42416 (Версия 4)
Название Уязвимость в pcapng парсере в Wireshark 1.12.x до 1.12.8 (CVE-2015-7830)
Описание Функция pcapng_read_if_descr_block в wiretap/pcapng.c в pcapng парсере в Wireshark 1.12.x до 1.12.8 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (падение приложения) через специально сформированный пакет.
Исправление Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта http://www.wireshark.org/download.html.
Ссылки

CVE	CVE-2015-7830
Wireshark	wnpa-sec-2015-30

Импортирование OVAL-определения

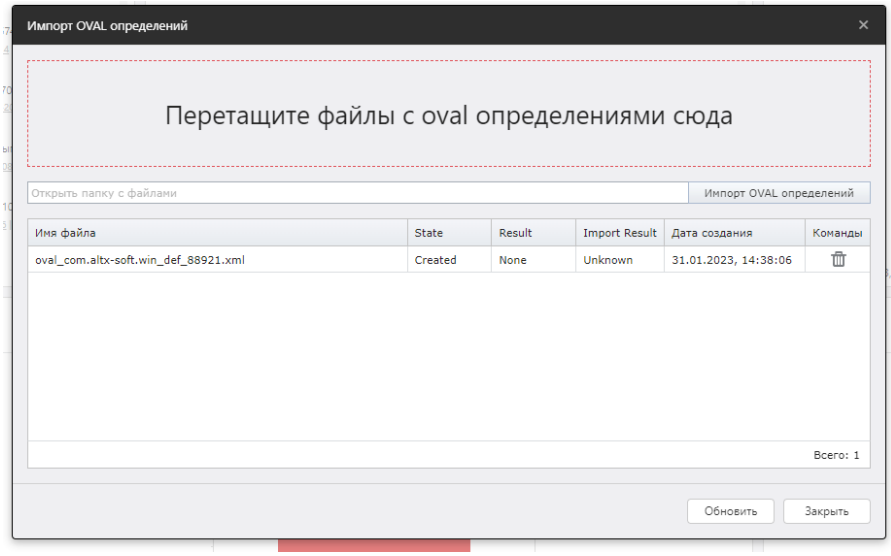
Необходимая роль: RedCheck_Admins / RedCheck_Adminis

> Размер файла OVAL-определения не должен превышать 10 МБ.

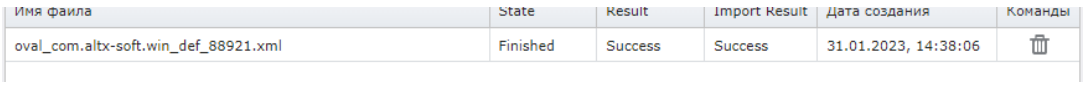
Чтобы импортировать свое собственное OVAL-определение, выполните следующие шаги.

Шаг 1. Раскройте **Инструменты** → **Импорт OVAL определений**;

Шаг 2. Перетащите / выберите в проводнике XML-файл, нажав **Импорт OVAL определений**;



Шаг 3. Через некоторое время нажмите **Обновить**. При успешном добавлении столбец **State** поменяет значение на **Finished**, а столбцы **Result** и **Import Result** на **Success**.



Добавленное определение будет доступно для просмотра в Менеджере аудитов.

5.4 Отслеживание изменений результатов сканирования (Контроль)

Для того, чтобы следить за изменениями на хосте, в RedCheck существует функция Контроль. Данная функция позволяет назначить один из результатов сканирования выбранного задания эталоном для сравнения. При дальнейших выполнениях задания результат будет автоматически сравниваться с эталоном и уведомлять о несоответствиях.

Доступные типы заданий

Функция контроль доступна только для следующих типов заданий:

- Аудит уязвимостей;
- Аудит конфигураций;
- Инвентаризация;
- Фиксация.

Результат контроля

Статус контроля может иметь следующие значения:

Соответствие – вся информация текущего результата сканирования совпадает с эталоном;

Несоответствие – текущий результат сканирования не совпадает с эталоном;

Не проведен – после назначения эталона сканирований не проводилось.

Типы статуса

Добавлен – в результате сканирования появилось новое OVAL-определение, отсутствующее в эталоне;

Удален – OVAL-определение, имеющееся в эталоне, не было обнаружено в результате сканирования;

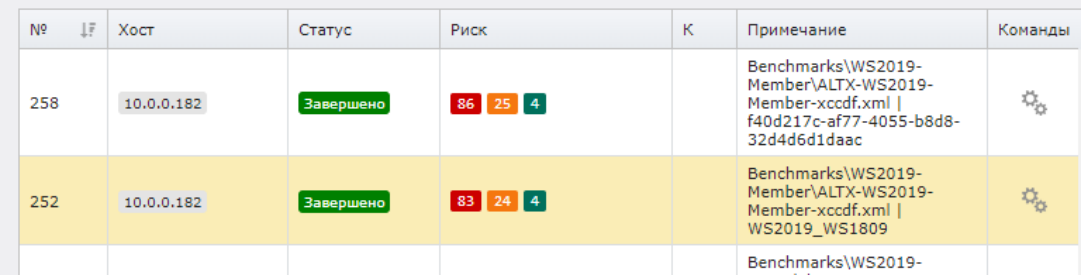
Изменен – какой-либо параметр был изменен.

Пример использования

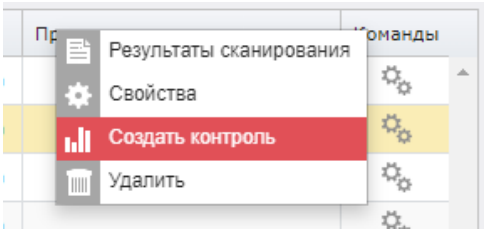
Необходимая роль: любая

Воспользуемся функцией Контроль, чтобы следить за тем, какие изменения вносятся на хосте для устранения уязвимостей.

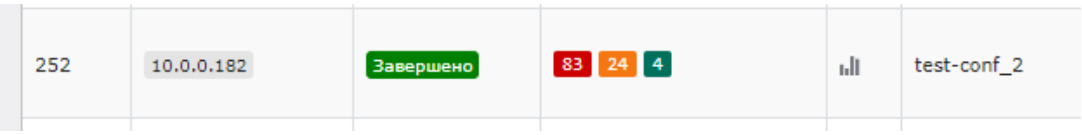
У нас есть результат сканирования хоста заданием Аудит конфигураций.



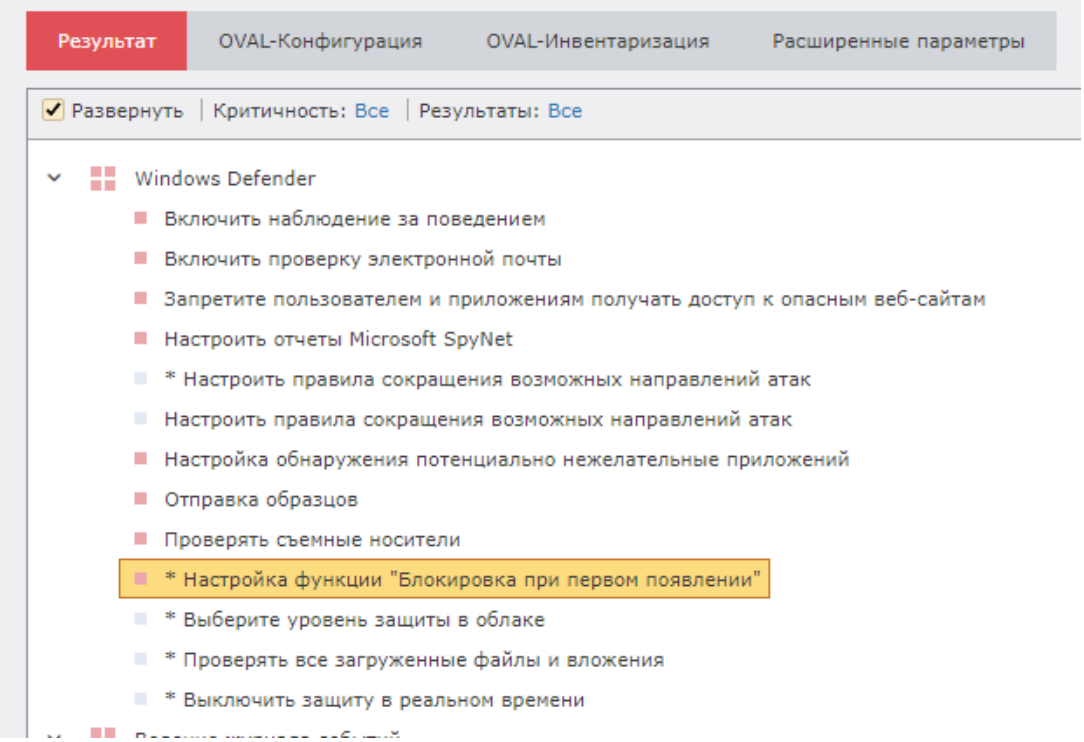
Нажмем → **Создать контроль**;



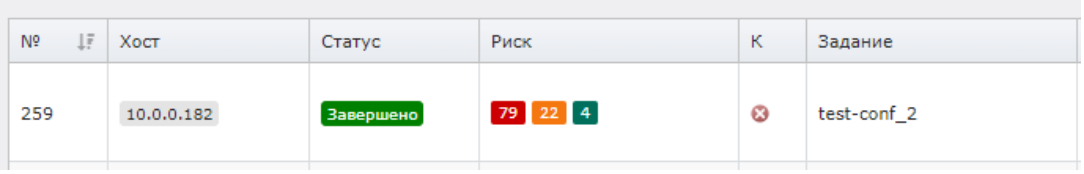
После этого данный результат сканирования будет помечен как **Эталон** ( )



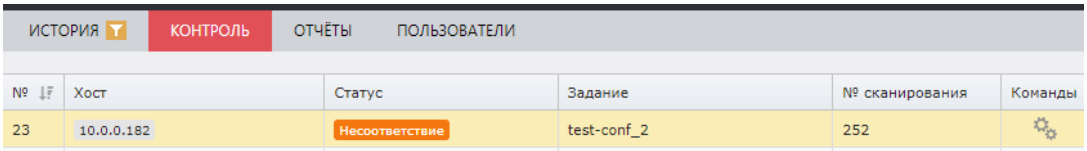
Исправим несоответствие некоторых правил конфигурации на хосте.



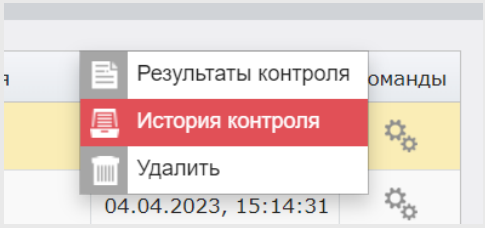
Проведем повторное сканирование. Видим, что в столбце К (Статус или результат Контроля) появился знак несоответствия с эталоном.



Перейдем в **Контроль** → откроем результат, нажав **Несоответствие** в столбце **Статус**.

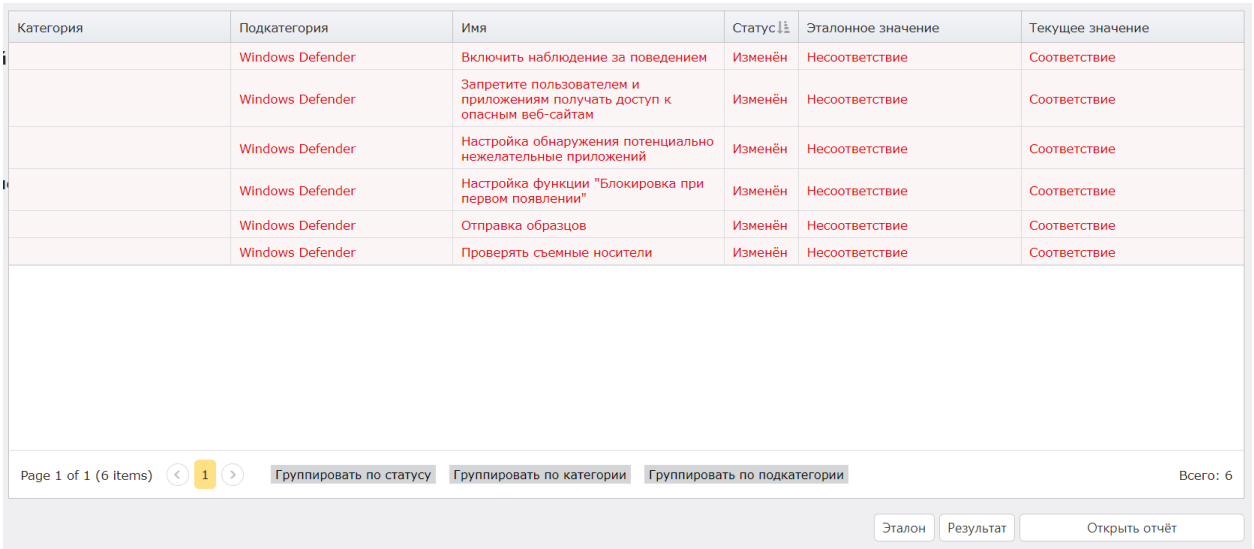


Чтобы посмотреть историю контроля, нажмите → **История контроля**.



Видим, что было изменено 6 правил.

Эталонное значение – значение, которое было в эталонном результате сканирования.



Категория	Подкатегория	Имя	Статус	Эталонное значение	Текущее значение
	Windows Defender	Включить наблюдение за поведением	Изменён	Несоответствие	Соответствие
	Windows Defender	Запретите пользователем и приложениям получать доступ к опасным веб-сайтам	Изменён	Несоответствие	Соответствие
	Windows Defender	Настройка обнаружения потенциально нежелательные приложений	Изменён	Несоответствие	Соответствие
	Windows Defender	Настройка функции "Блокировка при первом появлении"	Изменён	Несоответствие	Соответствие
	Windows Defender	Отправка образцов	Изменён	Несоответствие	Соответствие
	Windows Defender	Проверять съемные носители	Изменён	Несоответствие	Соответствие

Page 1 of 1 (6 items) 1 Группировать по статусу Группировать по категории Группировать по подкатегории Всего: 6

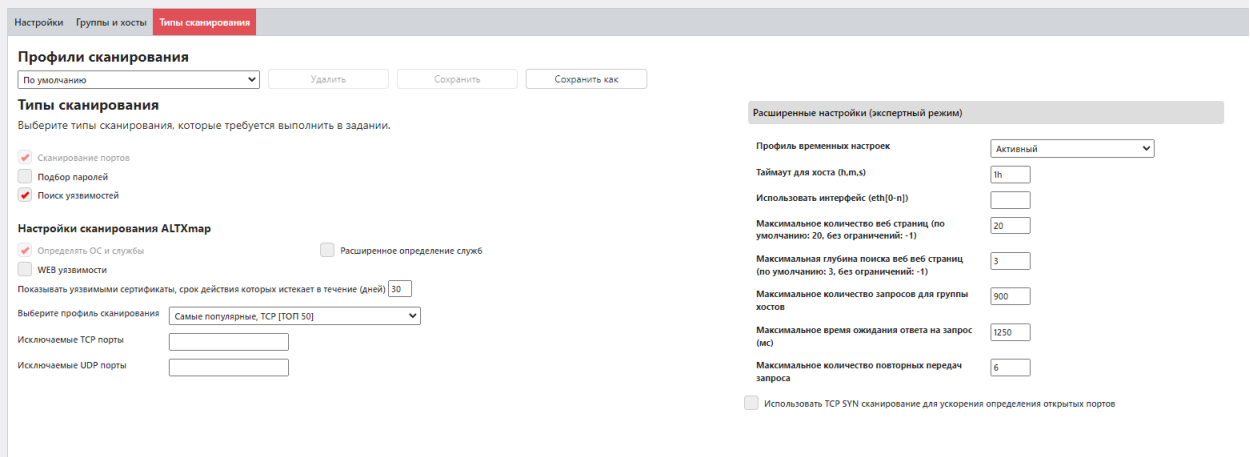
Эталон Результат Открыть отчёт

Чтобы посмотреть эталонный результат сканирования или текущий, нажмите **Эталон** или **Результат** соответственно.

5.5 Профили сканирования Altxmap

RedCheck позволяет сохранять настройки для Altxmap и затем использовать их в других заданиях типа Аудит в режиме «Пентест».

Создать профиль сканирования можно на вкладке **Типы сканирования** при создании задания **Аудит в режиме «Пентест»**.



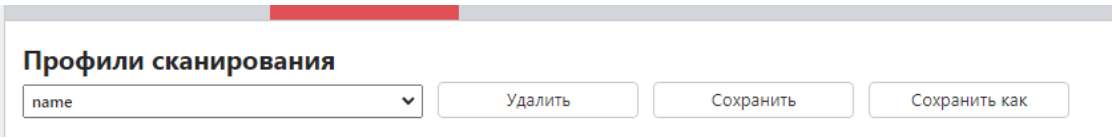
Шаг 1. Укажите новые значения для нужных параметров;

Шаг 2. Нажмите **Сохранить как** → укажите имя → **Сохранить**;

Профиль будет создан.

Чтобы внести изменения в профиль, нажмите на **Сохранить**;

Для удаления профиля нажмите **Удалить**;



6 Результаты сканирований

Результат сканирования каждого хоста является отдельной записью в базе данных RedCheck. Каждая запись может состоять из списка OVAL-определений (уязвимостей, найденных на хосте; установленного ПО и ОС), отображать соответствие конфигурации, предоставлять информацию о зафиксированных файлах и ключах реестра и другой информации.

Уровни критичности

OVAL-определения подразделяются по уровню критичности:

Недоступно – вендор не предоставил значение уровня критичности;

Информация – OVAL-определение для инвентаря (ПО).

Низкий, Средний, Высокий, Критический – стандартные определения уровня критичности.

> Расчет критичности производится с учетом базовых и временных метрик CVSS на основании данных вендора сканера, вендора ПО, экспертных организаций;

Статус сканирования

Сканирование хоста может завершиться с одним из трех статусов:

Завершено – выполнение аудита для указанного хоста завершено успешно;

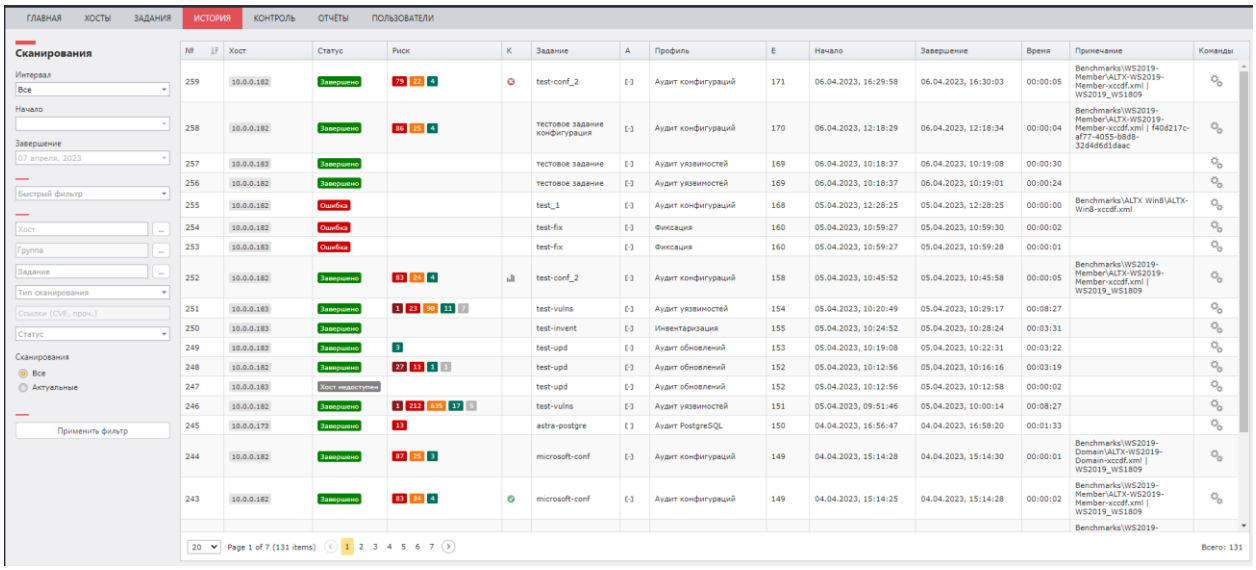
Ошибка – при сканировании произошла ошибка;

Хост недоступен – служба сканирования не смогла подключиться указанным транспортом к хосту;

Просмотр результатов сканирований

Необходимая роль: любая

Чтобы посмотреть результаты сканирований, перейдите в История.



В таблице будет содержаться следующая информация:

- ID задания;
- Хост – IP-адрес или имя хоста;
- Статус – показатель, уведомляющий о результате, с которым завершилось сканирование;
- Риск – количество уязвимостей, найденных на хосте;
- К – статус или результат контроля;
- Задание – название задания;
- А – использовался или нет Agent RedCheck для сканирования хоста;
- Профиль – тип задания;
- Е – идентификатор выполненного задания;
- Время начала и окончания сканирования, общее время выполнения задания.
- Примение – название конфигурации, которая использовалась при сканировании (Аудит конфигураций, Аудит СУБД).

Для просмотра информации о результате сканирования хоста нажмите на значение в столбце **Статус**, или → **Результат сканирования**.

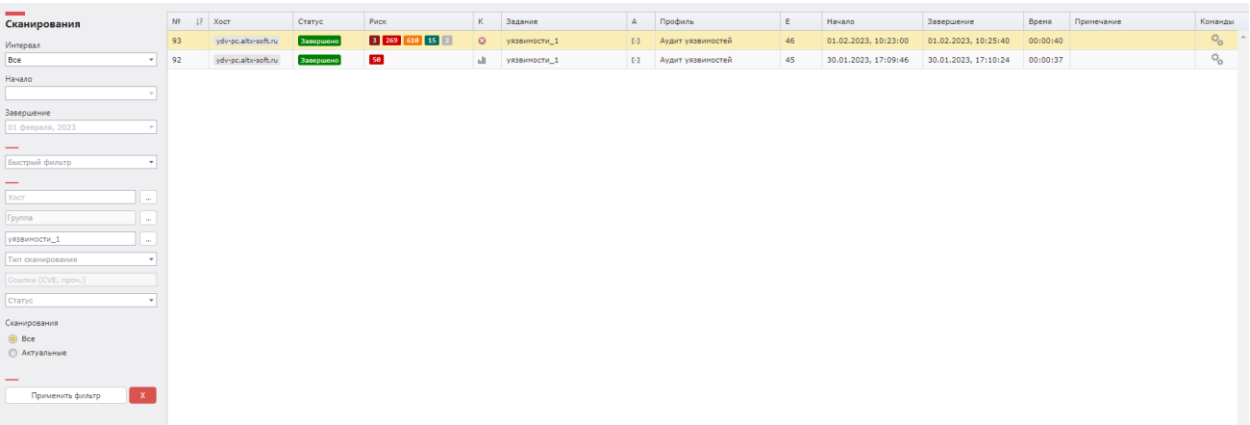
Каждый тип задания предоставляет отличную от других информацию о выполненном сканировании.

- 6.1 Аудит уязвимостей
- 6.2 Аудит обновлений
- 6.3 Аудит конфигураций
- 6.4 Инвентаризация
- 6.5 Фиксация (контроль целостности)
- 6.6 Аудит уязвимостей АСУ ТП
- 6.7 Аудит СУБД
- 6.8 Проверка доступности
- 6.9 Обнаружение хостов
- 6.10 Аудит в режиме "Пентест"
- 6.11 Статистика выполненных заданий

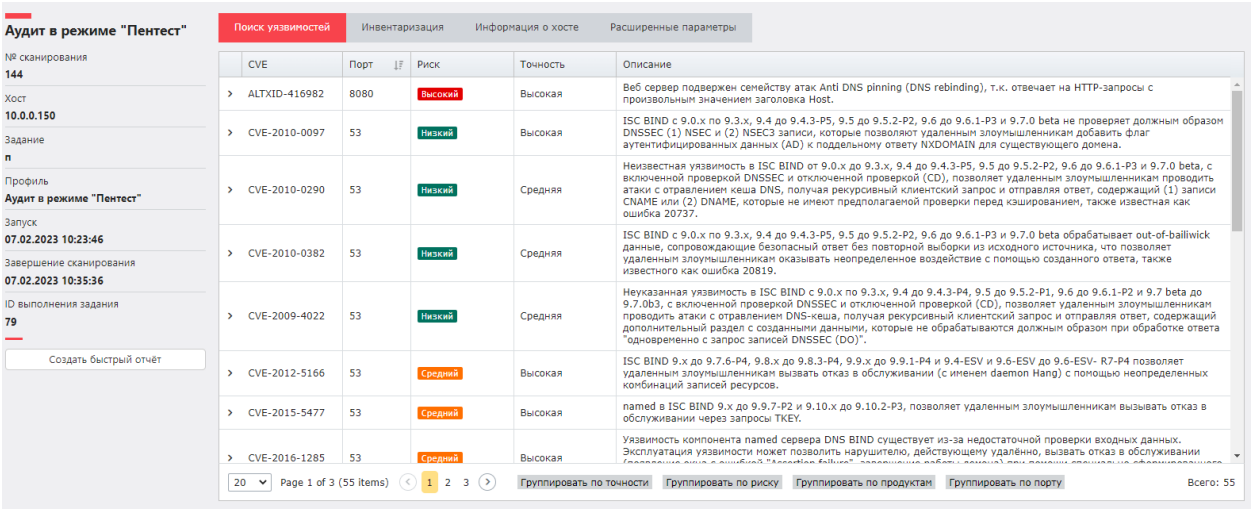
Просмотр истории сканирования определенного задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Шаг 1. Перейдите в **Задания** → ⚙ → **История**;



Шаг 2. Нажмите ⚙ → **Результаты сканирования**;

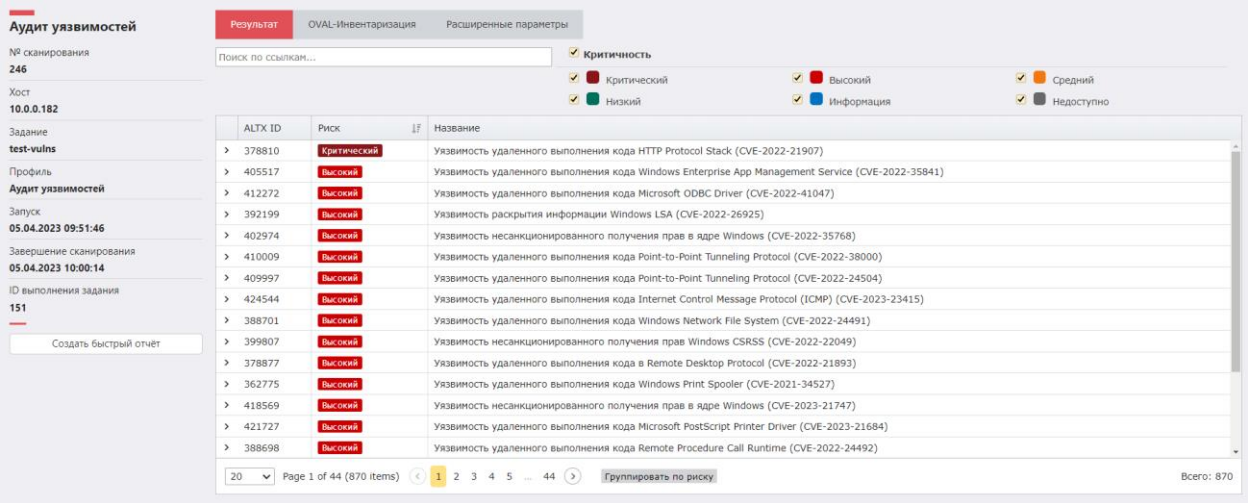

Аудит в режиме "Пентест"
№ сканирования
144
Хост
10.0.0.150
Задание
п
Профиль
Аудит в режиме "Пентест"
Запуск
07.02.2023 10:23:46
Завершение сканирования
07.02.2023 10:35:36
ID выполнения задания
79
Создать быстрый отчёт
Поиск уязвимостей
Инвентаризация
Информация о хосте
Расширенные параметры
CVE
Порт
Риск
Точность
Описание
ALTXID-416982 8080 Высокий Высокая Веб сервер подвержен семейству атак Anti DNS pinning (DNS rebinding), т.к. отвечает на HTTP-запросы с произвольным значением заголовка Host.
CVE-2010-0097 53 Низкий Высокая ISC BIND с 9.0.x по 9.3.x, 9.4 до 9.4.3-P5, 9.5 до 9.5.2-P2, 9.6 до 9.6.1-P3 и 9.7.0 beta не проверяет должным образом DNSSEC (1) NSEC и (2) NSEC3 записи, которые позволяют удаленным злоумышленникам добавить флаг аутентифицированных данных (AD) к поддельному ответу NXDOMAIN для существующего домена.
CVE-2010-0290 53 Низкий Средняя Неизвестная уязвимость в ISC BIND от 9.0.x до 9.3.x, 9.4 до 9.4.3-P5, 9.5 до 9.5.2-P2, 9.6 до 9.6.1-P3 и 9.7.0 beta, с включенной проверкой DNSSEC и отключенной проверкой (CD), позволяет удаленным злоумышленникам проводить атаки с отравлением кеша DNS, получая рекурсивный клиентский запрос и отправляя ответ, содержащий (1) записи CNAME или (2) DNAME, которые не имеют предполагаемой проверки перед кэшированием, также известная как ошибка 20737.
CVE-2010-0382 53 Низкий Средняя ISC BIND с 9.0.x по 9.3.x, 9.4 до 9.4.3-P5, 9.5 до 9.5.2-P2, 9.6 до 9.6.1-P3 и 9.7.0 beta обрабатывает out-of-bailiwick данные, сопровождающие безопасный ответ без повторной выборки из исходного источника, что позволяет удаленным злоумышленникам оказывать неопределенное воздействие с помощью созданного ответа, также известного как ошибка 20819.
CVE-2009-4022 53 Низкий Средняя Неуказанная уязвимость в ISC BIND с 9.0.x по 9.3.x, 9.4 до 9.4.3-P4, 9.5 до 9.5.2-P1, 9.6 до 9.6.1-P2 и 9.7 beta до 9.7.0b3, с включенной проверкой DNSSEC и отключенной проверкой (CD), позволяет удаленным злоумышленникам проводить атаки с отравлением DNS-кеша, получая рекурсивный клиентский запрос и отправляя ответ, содержащий дополнительный раздел с созданными данными, которые не обрабатываются должным образом при обработке ответа "одновременно с запрос записей DNSSEC (DO)".
CVE-2012-5166 53 Средний Высокая ISC BIND 9.x до 9.7.6-P4, 9.8.x до 9.8.3-P4, 9.9.x до 9.9.1-P4 и 9.4-ESV и 9.6-ESV до 9.6-ESV- R7-P4 позволяет удаленным злоумышленникам вызвать отказ в обслуживании (с именем daemon Hang) с помощью неопределенных комбинаций записей ресурсов.
CVE-2015-5477 53 Средний Высокая named в ISC BIND 9.x до 9.9.7-P2 и 9.10.x до 9.10.2-P3, позволяет удаленным злоумышленникам вызывать отказ в обслуживании через запросы TKEY.
CVE-2016-1285 53 Средний Высокая Уязвимость компонента named сервера DNS BIND существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании
20 Page 1 of 3 (55 items) 1 2 3
Группировать по точности
Группировать по риску
Группировать по продуктам
Группировать по порту
Всего: 55

6.1 Аудит уязвимостей

Описание результатов сканирования задания Аудит уязвимостей.

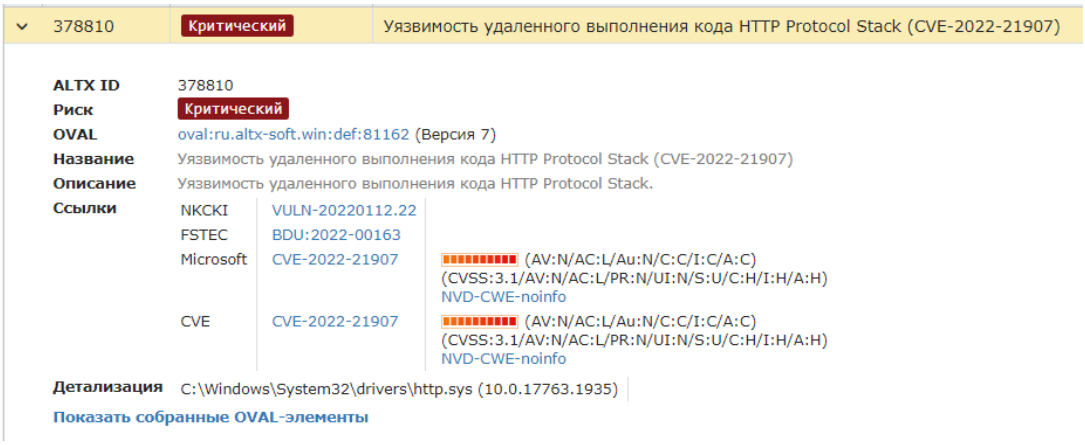
Результат

Вкладка отображает список найденных на хосте уязвимостей. Каждое OVAL-определение можно раскрыть и просмотреть информацию из OVALdb.



OVAL-определение состоит из:

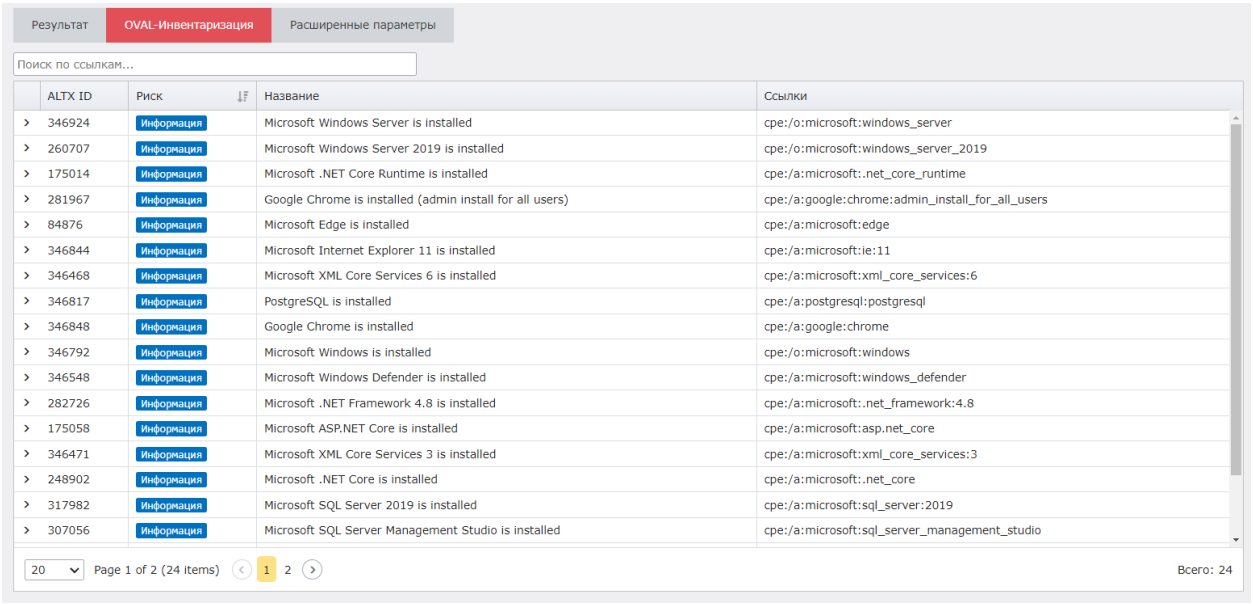
- ALTX ID – внутренний идентификатор уязвимости;
- Риск – уровень критичности; (Сведения об интегральной оценке по базовым метрикам CVSS)
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Ссылки – страницы уязвимости в различных базах данных уязвимостей;
- Детализация – файлы, подверженные уязвимости;



OVAL-Инвентаризация

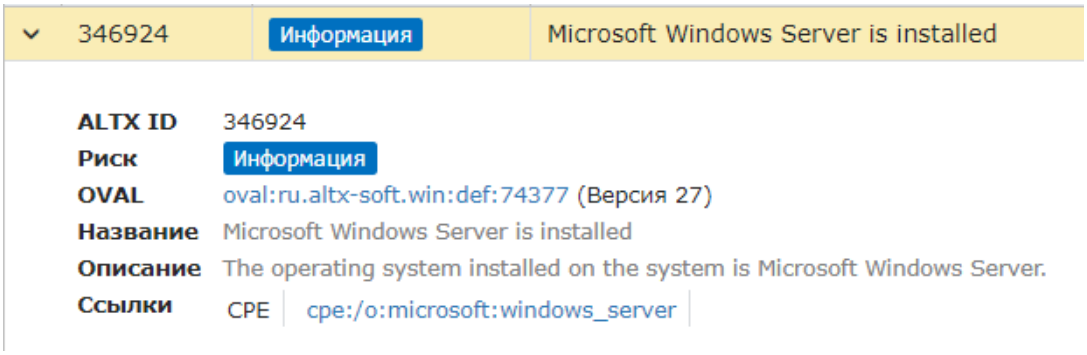
Вкладка отображает список с OVAL-определениями класса Информация.

> Информация – OVAL-определение для инвентаря (ПО).



Информация о найденном ПО включает в себя:

- ALTX ID – внутренний идентификатор уязвимости;
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Ссылки – CPE продукта;
- Продукты – название ПО.



Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

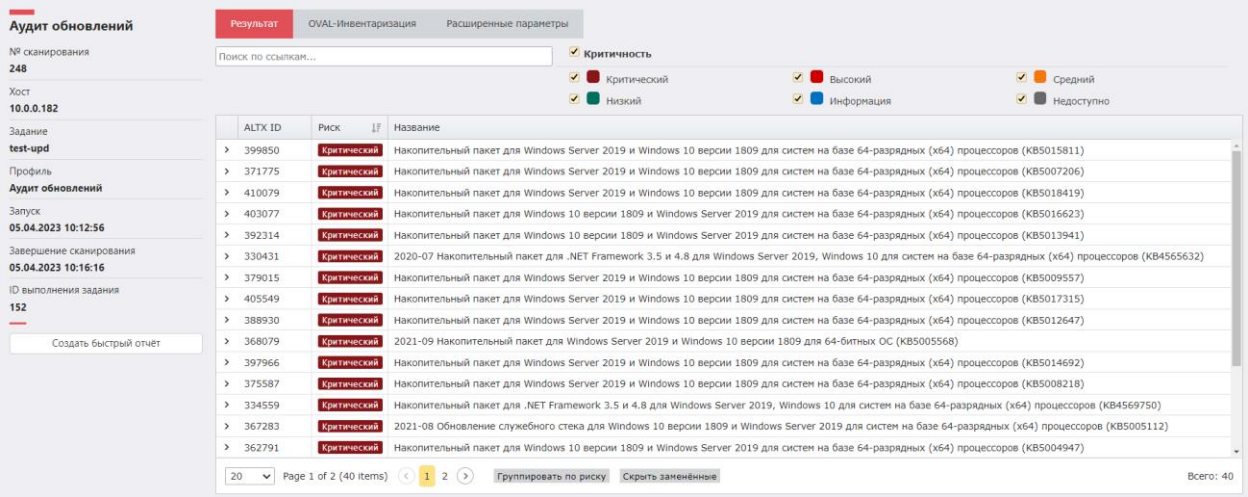
Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.2 Аудит обновлений

Описание результатов сканирования задания Аудит обновлений.

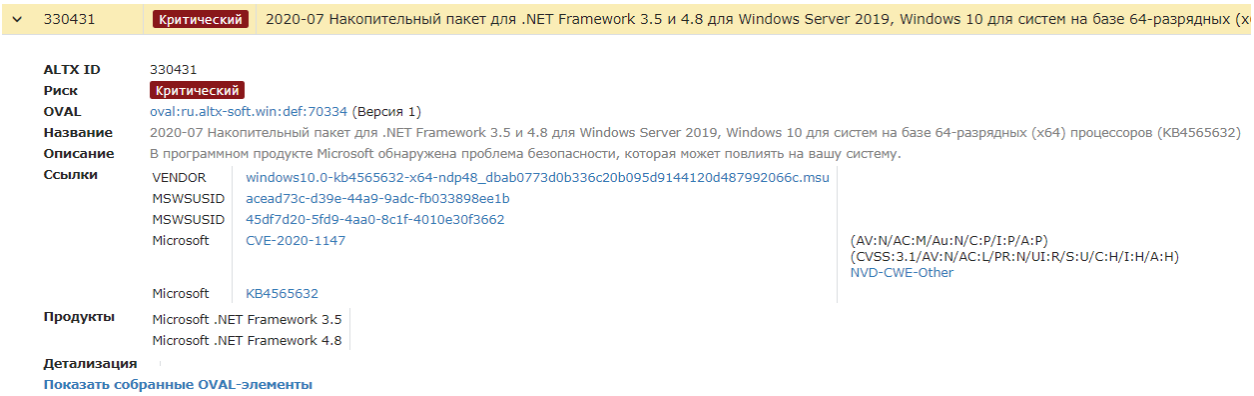
Результат

Вкладка отображает список неустановленных на хосте обновлений. Каждое OVAL-определение можно раскрыть и просмотреть информацию из OVALdb.



OVAL-определение состоит из:

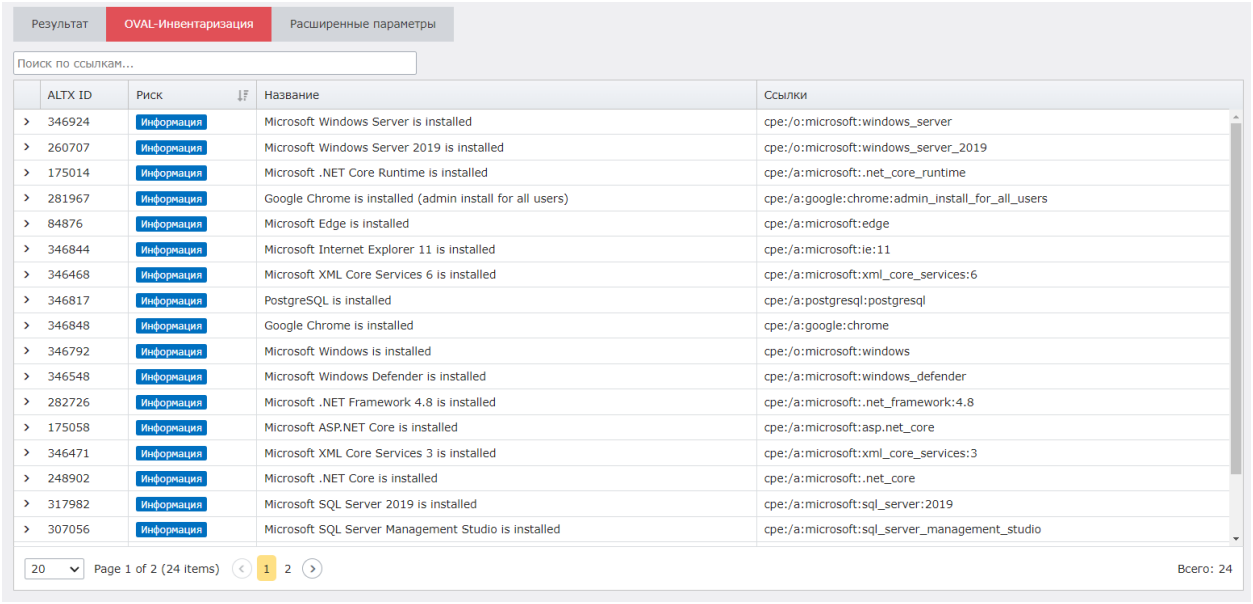
- ALTX ID – внутренний идентификатор уязвимости;
- Риск – уровень критичности; (Сведения об интегральной оценке по базовым метрикам CVSS)
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Ссылки – страницы уязвимости в различных базах данных уязвимостей;
- Продукты – название продукта;



OVAL-Инвентаризация

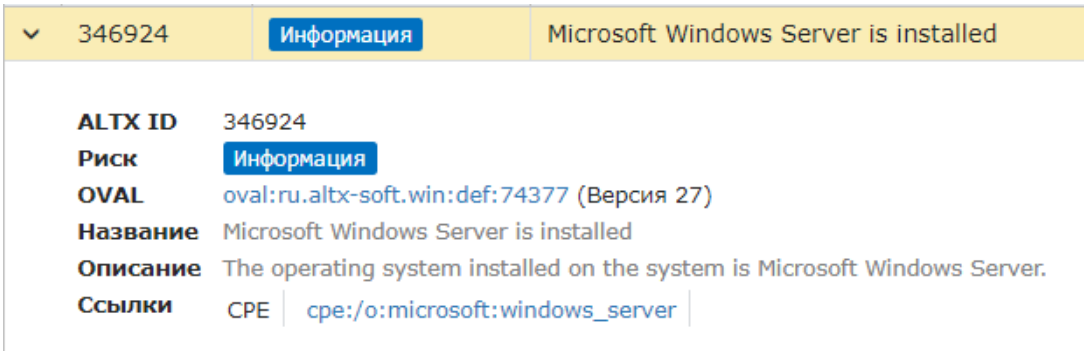
Вкладка отображает список с OVAL-определениями класса Информация.

> Информация – OVAL-определение для инвентаря (ПО).



Информация о найденном ПО включает в себя:

- ALTX ID – внутренний идентификатор уязвимости;
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Ссылки – CPE продукта;
- Продукты – название ПО.



Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.3 Аудит конфигураций

Описание результатов сканирования задания Аудит конфигураций.

Статус проверки правила

Соответствие – значение параметра на хосте соответствует эталонному значению в конфигурации;

Несоответствие – значение параметра на хосте не соответствует эталонному значению в конфигурации;

Ошибка – критическая ошибка при выполнении проверки. При возникновении обратитесь в службу тех. поддержки;

Не проверено – в конфигурации нет информации для правила (эталонного значения, исправления и т.д.);

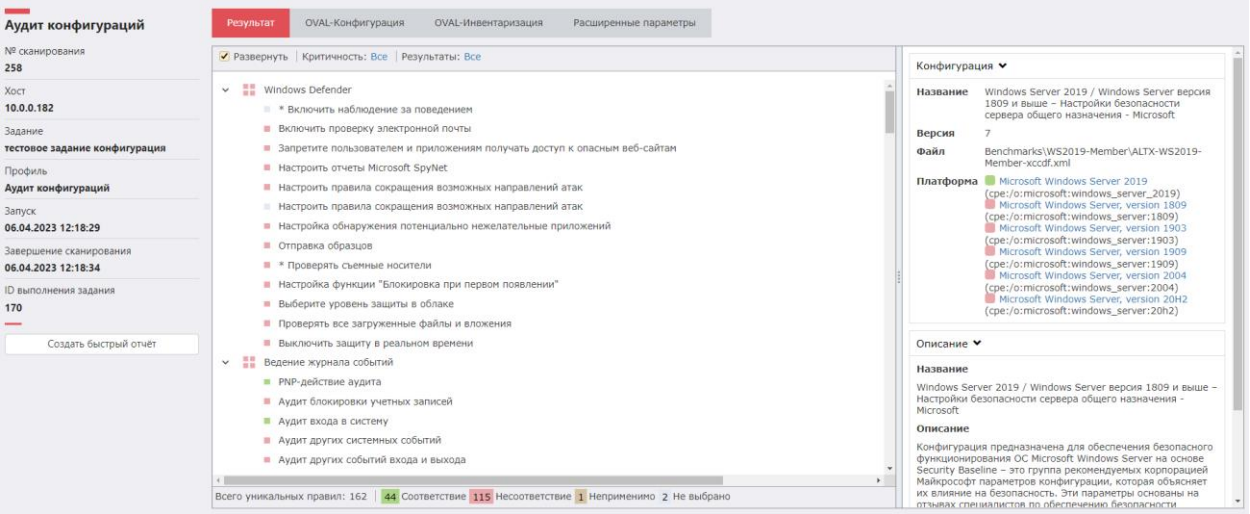
Не выбрано – правило отключено в профиле конфигурации;

Неизвестно – ошибка при проверке правила. Убедитесь, что используемая для сканирования учетная запись обладает нужными правами, а примененные на хосте групповые политики позволяют проводить необходимые проверки;

Неприменимо – данное правило неприменимо для проверяемой платформы;

Результат

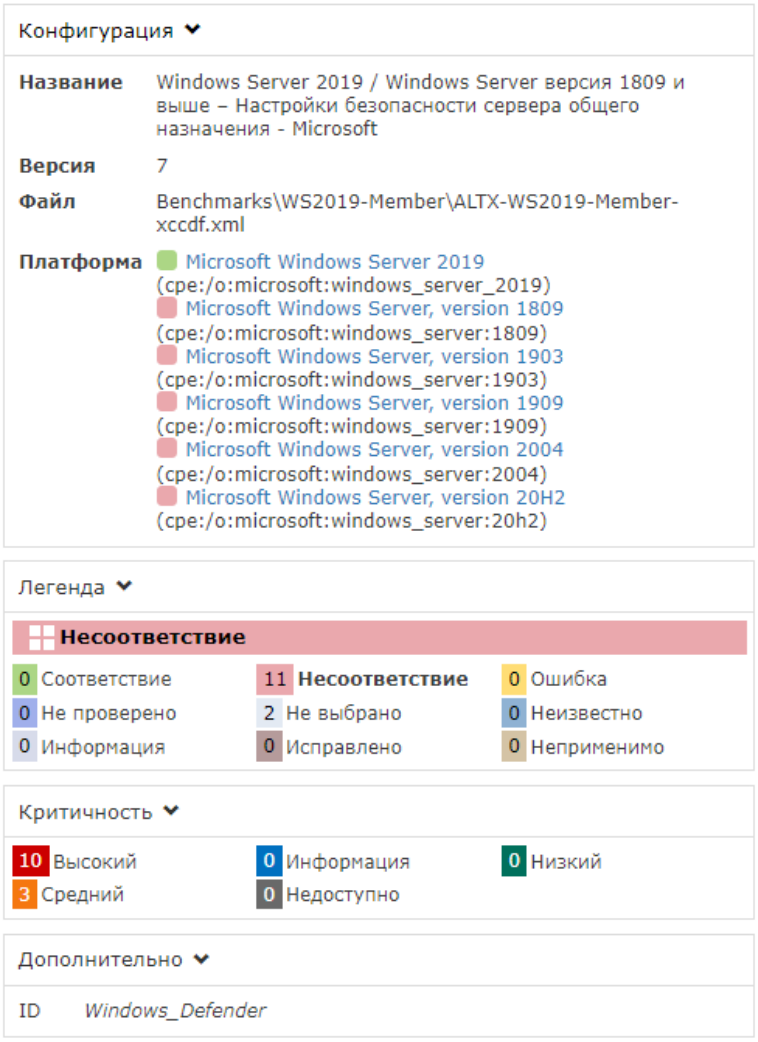
Вкладка содержит список проверенных правил конфигурации.



Правила входят в группы, которые обозначаются иконкой

Информация о группе

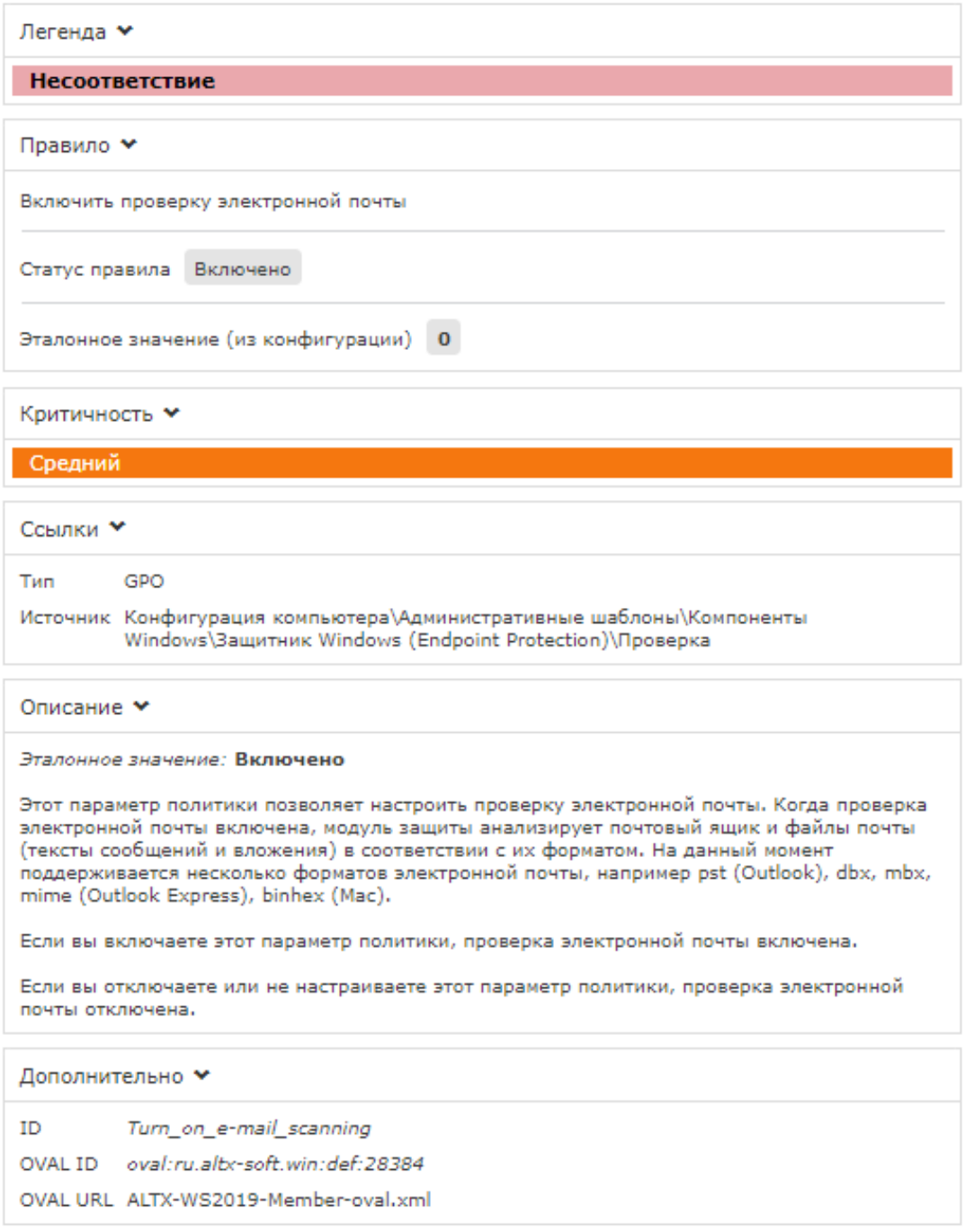
- Конфигурация – информация о конфигурации:
  - Версия конфигурации;
  - Путь к файлу конфигурации;
  - Платформы, для которых применима конфигурация. Платформа, установленная на хосте, отображается иконкой
- Легенда – итоговый статус проверки и количественная статистика. Итоговый статус определяется следующим образом: если в группе есть хоть одно правило со статусом Несоответствие, то группа будет иметь такой же статус.
- Критичность – информация о уровнях критичности правил группы; (Сведения об интегральной оценке по базовым метрикам CVSS)
- Дополнительно – дополнительная информация о группе.



Информация о правиле

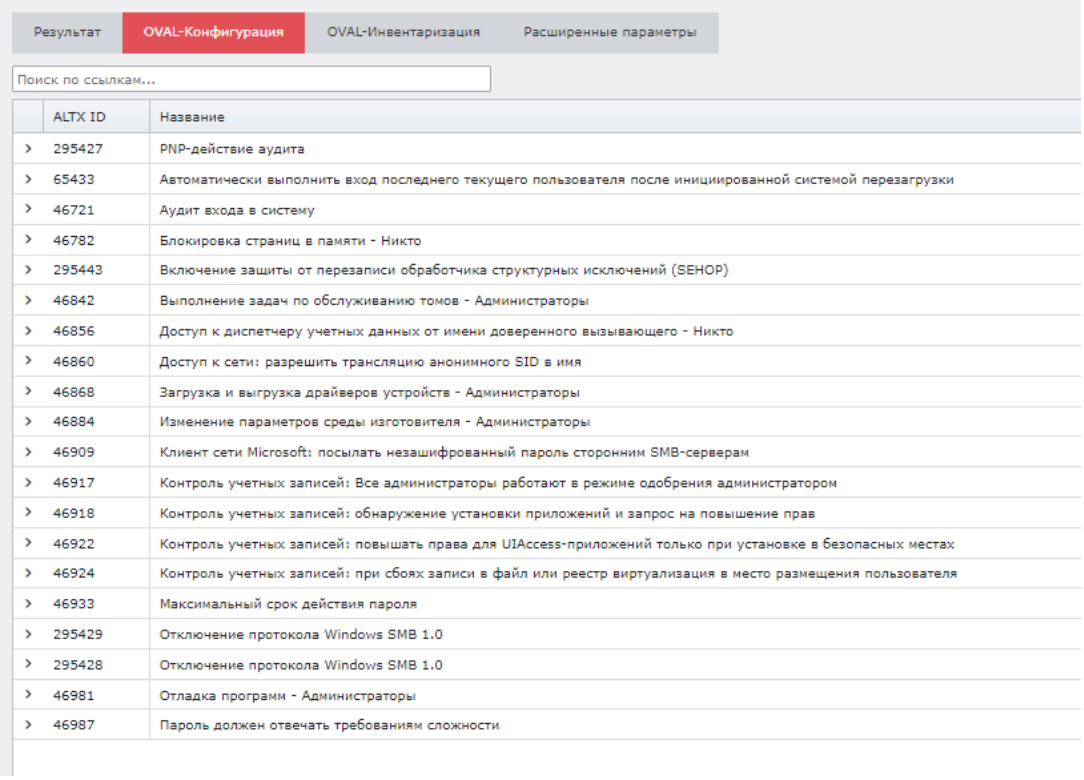
- Легенда – статус проверки;
- Правило – название правила;
- Статус правила – включено или нет правило в используемом профиле конфигурации;
    - Эталонное значение – значение из конфигурации, с которым происходит сравнение.
- Критичность – информация о уровне критичности правила; (Сведения об интегральной оценке по базовым метрикам CVSS)
- Ссылки – расположение параметра безопасности;
- Описание – описание правила;

- Фактическое значение – значение параметра, которое было обнаружено на хосте;
- Дополнительно – дополнительная информация о правиле.



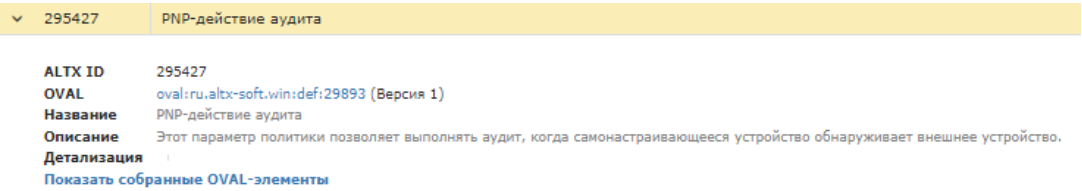
OVAL-Конфигурация

Вкладка содержит детализацию проверок правил конфигурации.



OVAL-определение состоит из:

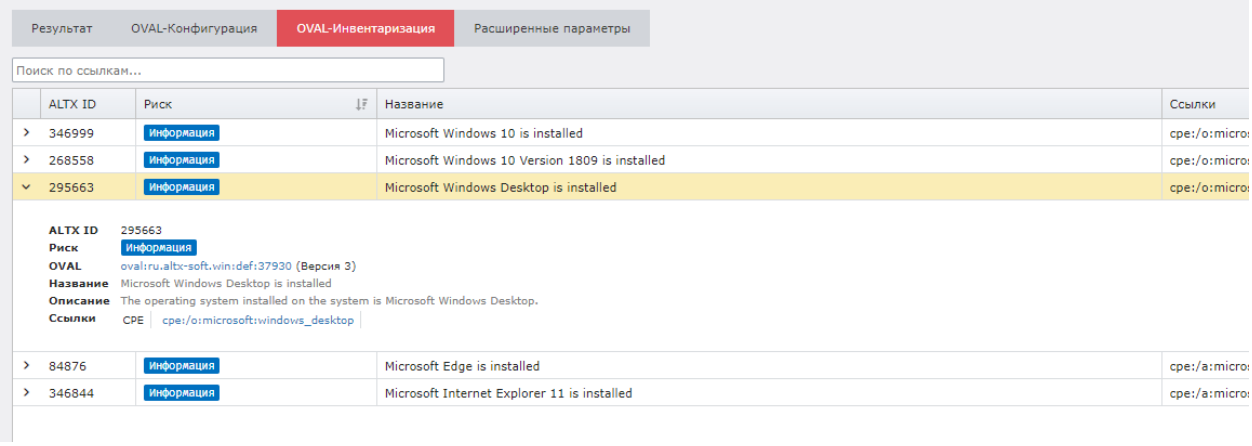
- ALTX ID – внутренний идентификатор уязвимости;
- OVAL – ссылка на страницу уязвимости в OVALdb;



OVAL-Инвентаризация

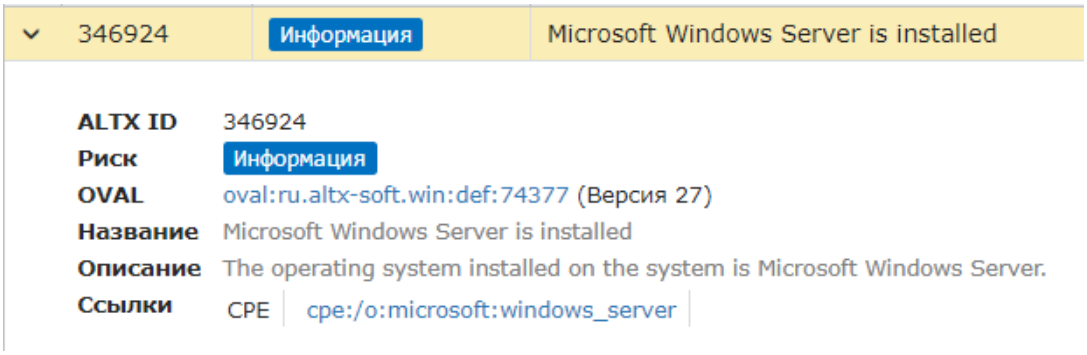
Вкладка отображает список с OVAL-определениями класса Информация.

> Информация – OVAL-определение для инвентаря (ПО).



Информация о найденном ПО включает в себя:

- ALTX ID – внутренний идентификатор уязвимости;
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Ссылки – CPE продукта;
- Продукты – название ПО.



Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

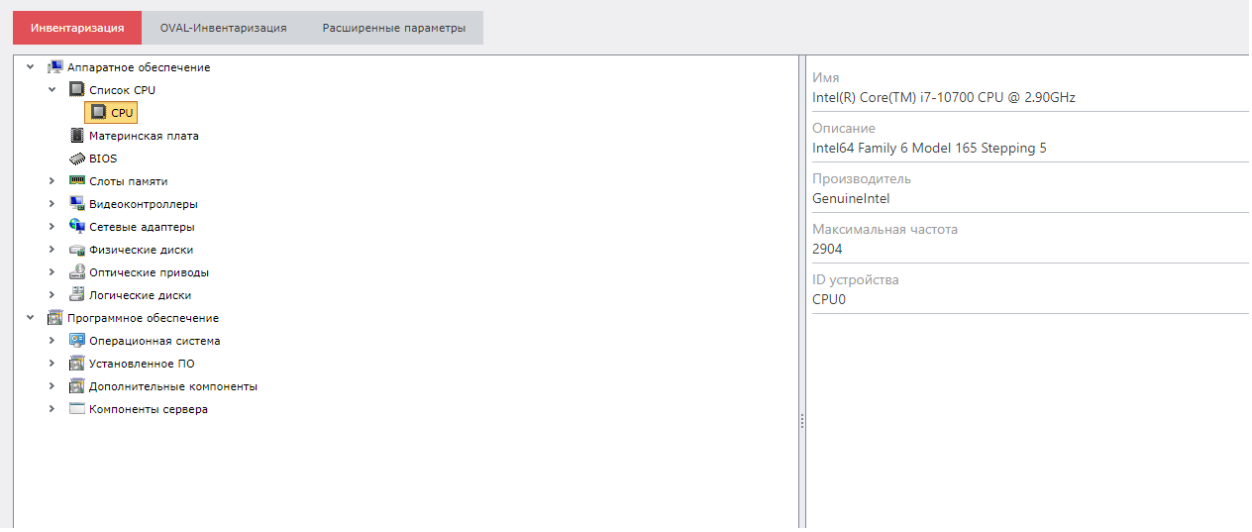
Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.4 Инвентаризация

Описание результата сканирования задания Инвентаризация.

Инвентаризация

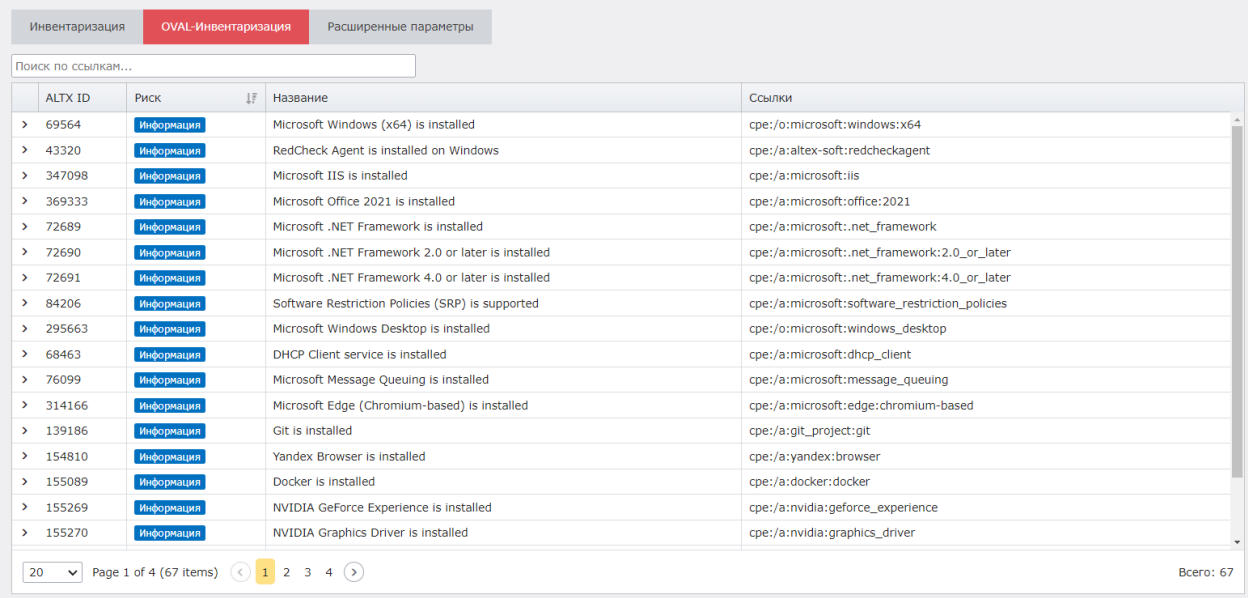
Вкладка содержит информацию о аппаратном и программном обеспечении, обнаруженном на хосте.



OVAL-Инвентаризация

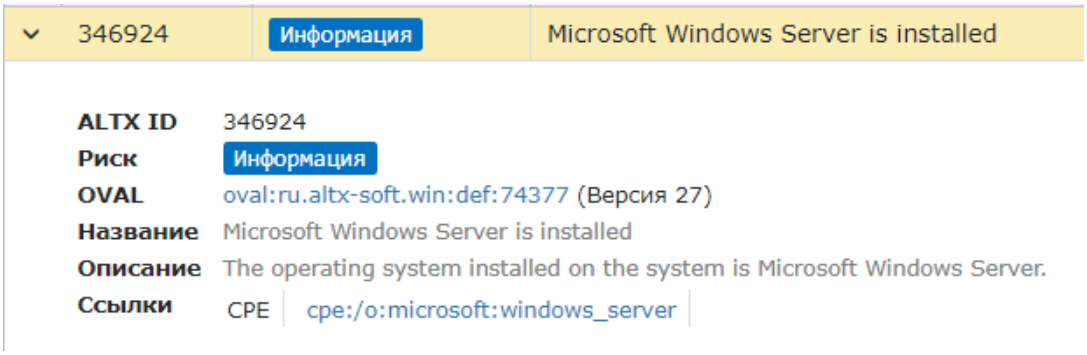
Вкладка отображает список с OVAL-определениями класса Информация.

> Информация – OVAL-определение для инвентаря (ПО).



Информация о найденном ПО включает в себя:

- ALTX ID – внутренний идентификатор уязвимости;
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Ссылки – CPE продукта;
- Продукты – название ПО.



Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

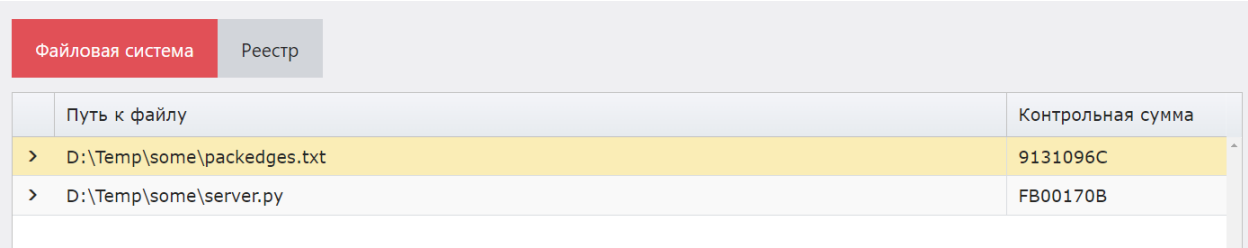
Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.5 Фиксация (контроль целостности)

Описание результата сканирования задания Фиксация.

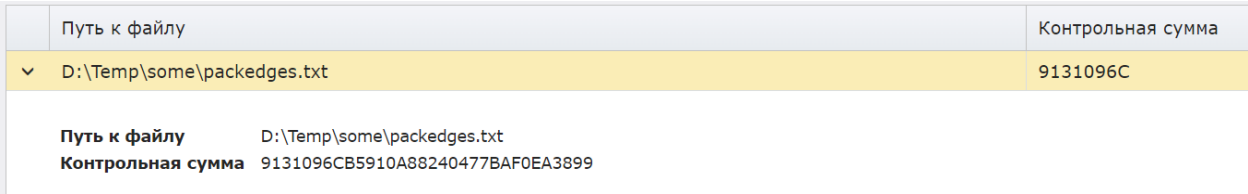
Файловая система

Вкладка отображает список зафиксированных файлов на хосте.



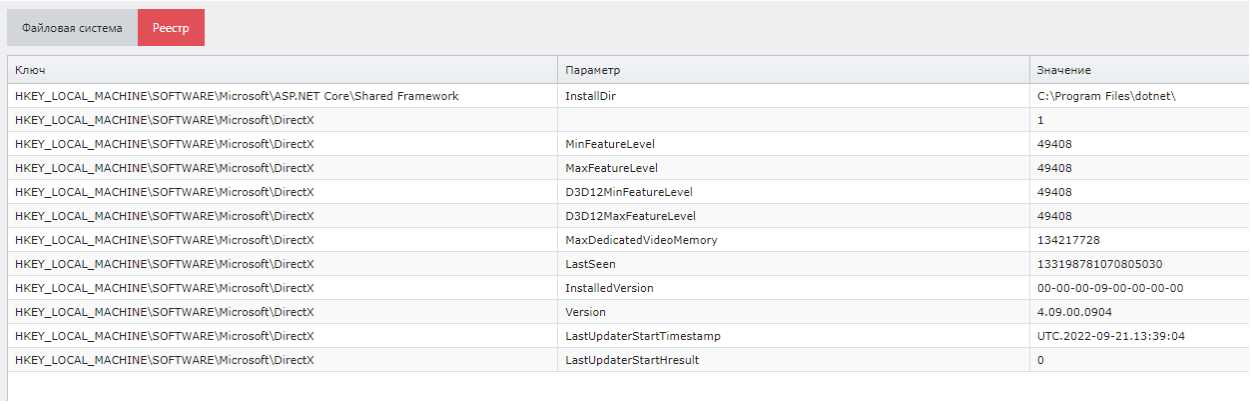
Каждая запись содержит следующую информацию о файле:

- Путь к файлу;
- Контрольная сумма.



Реестр

Вкладка отображает зафиксированные ключи и параметры реестра.

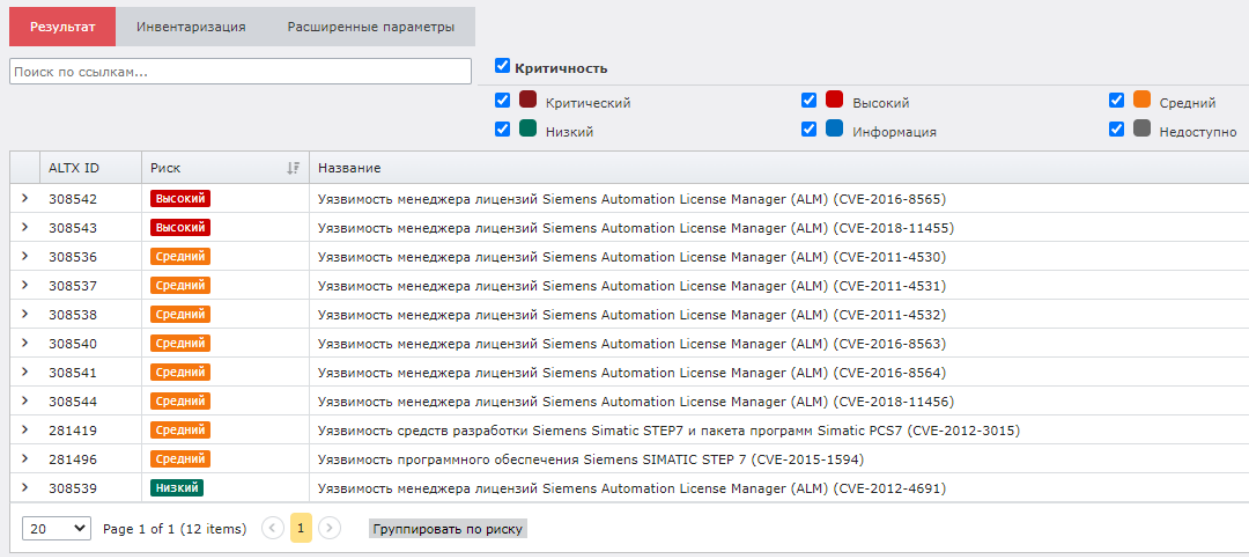


6.6 Аудит уязвимостей АСУ ТП

Описание результатов сканирования задания Аудит уязвимостей АСУ ТП.

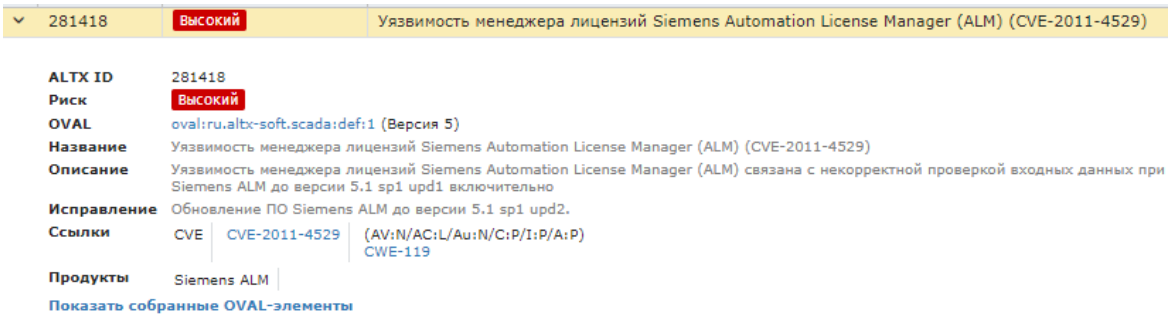
Результат

Вкладка отображает список найденных на хосте уязвимостей. Каждое OVAL-определение можно раскрыть и просмотреть информацию из OVALdb.



Информация об уязвимости состоит из:

- ALTX ID – внутренний идентификатор уязвимости;
- Риск – уровень критичности; (Сведения об интегральной оценке по базовым метрикам CVSS)
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Исправление – способ устранения уязвимости;
- Ссылки – страницы уязвимости в различных базах данных уязвимостей;
- Детализация – файлы, подверженные уязвимости;
- Продукты – название ПО.

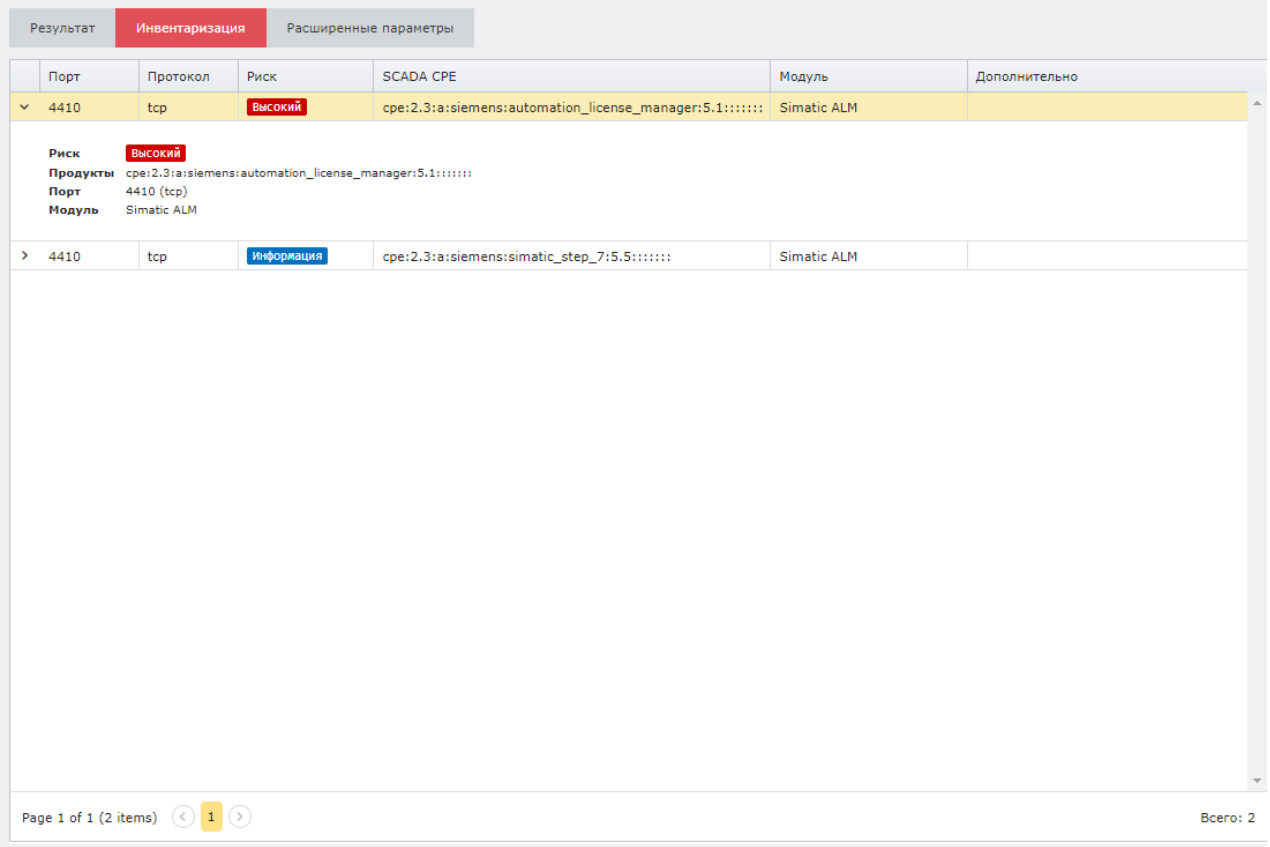


Инвентаризация

Вкладка содержит OVAL-определения для контроллеров, протоколов или ПО, обнаруженных на сканируемом хосте.

Информация о найденном ПО включает в себя:

- Риск – уровень критичности;
- Продукты – CPE найденного модуля;
- Порт – порт и протокол определения;
- Модуль – название найденного продукта.



Справа отображается список с информацией о найденном ПО (раскрывающийся список с необнаруженных ПО будет пустой).

Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.7 Аудит СУБД

Описание результата сканирования задания Аудит СУБД.

Статус проверки правила

Соответствие – значение параметра на хосте соответствует эталонному значению в конфигурации;

Несоответствие – значение параметра на хосте не соответствует эталонному значению в конфигурации;

Ошибка – критическая ошибка при выполнении проверки. При возникновении обратитесь в службу тех. поддержки;

Не проверено – в конфигурации нет информации для правила (эталонного значения, исправления и т.д.);

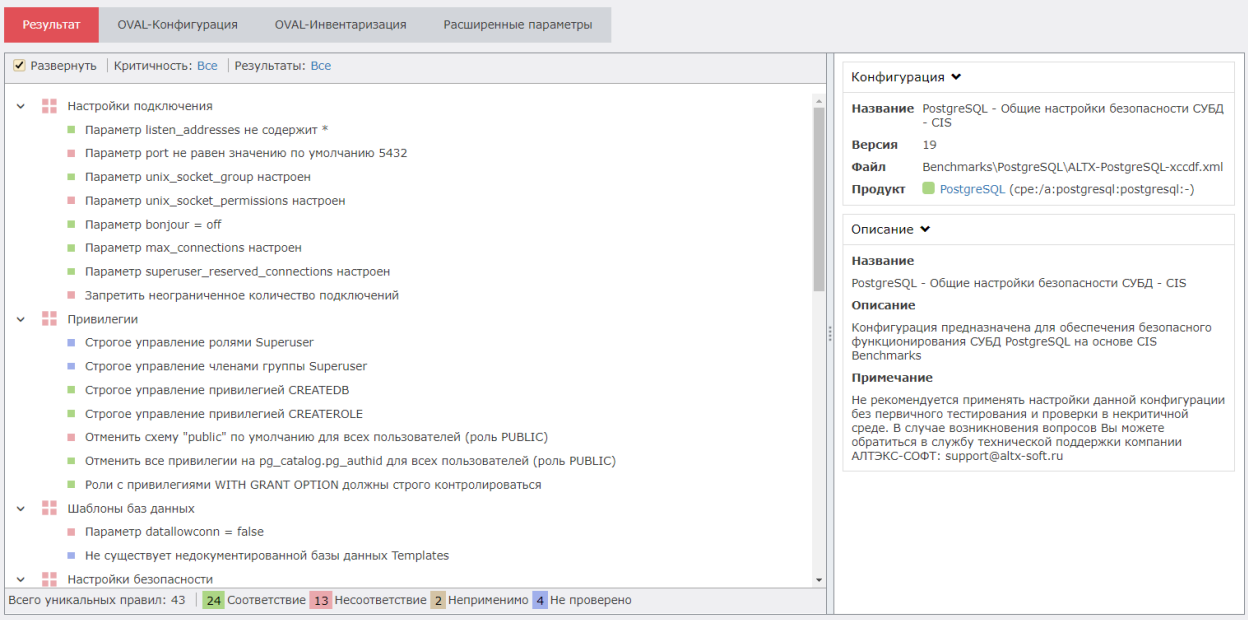
Не выбрано – правило отключено в профиле конфигурации;

Неизвестно – ошибка при проверке правила. Убедитесь, что используемая для сканирования учетная запись обладает нужными правами, а примененные на хосте групповые политики позволяют проводить необходимые проверки;

Неприменимо – данное правило неприменимо для проверяемой платформы;

Результат

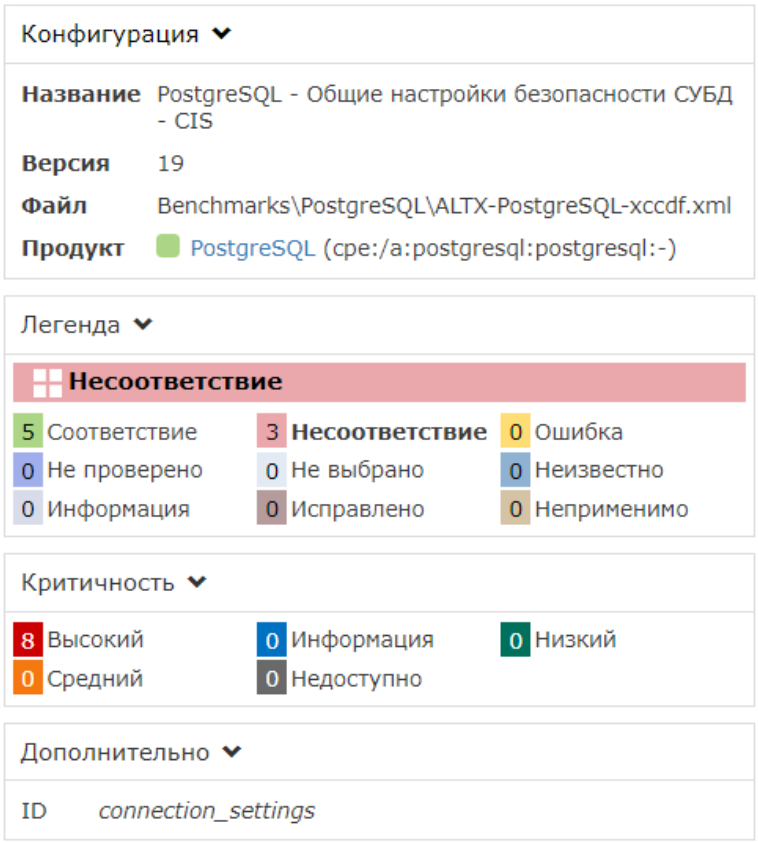
Вкладка содержит список проверенных правил конфигурации.



Правила входят в группы, которые обозначаются иконкой 

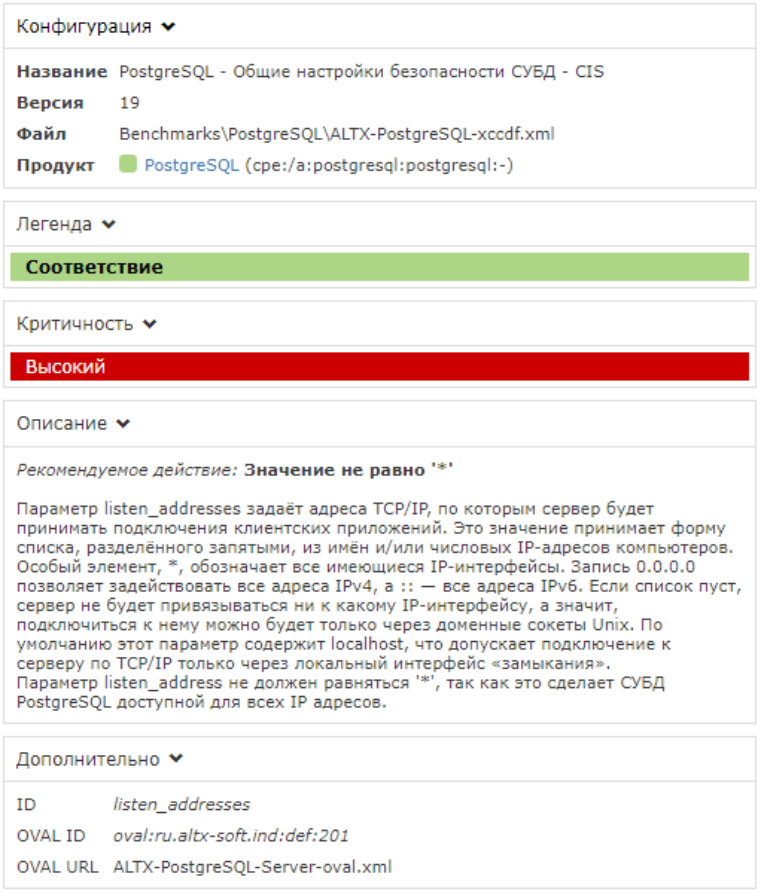
Информация о группе

- Конфигурация – информация о конфигурации:
  - Версия конфигурации;
  - Путь к файлу конфигурации;
  - Платформы, для которых применима конфигурация. Платформа, установленная на хосте, отображается иконкой 
- Легенда – итоговый статус проверки и количественная статистика. Итоговый статус определяется следующим образом: если в группе есть хоть одно правило со статусом Несоответствие, то группа будет иметь такой же статус.
- Критичность – информация о уровнях критичности правил группы; (Сведения об интегральной оценке по базовым метрикам CVSS)
- Дополнительно – дополнительная информация о группе.



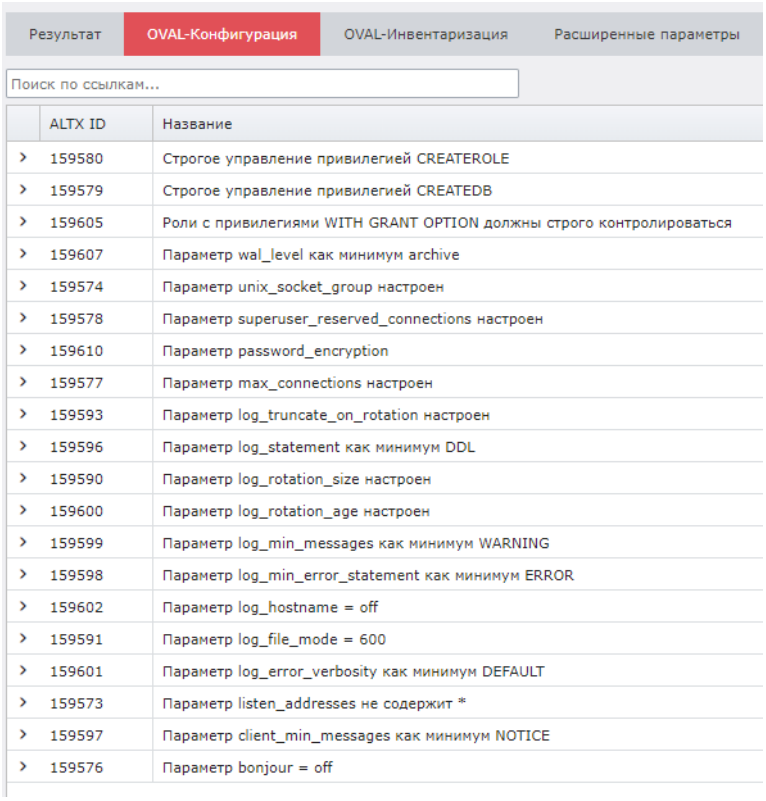
Информация о правиле

- Легенда – статус проверки;
- Правило – название правила;
- Статус правила – включено или нет правило в используемом профиле конфигурации;
    - Эталонное значение – значение из конфигурации, с которым происходит сравнение.
- Критичность – информация о уровне критичности правила; (Сведения об интегральной оценке по базовым метрикам CVSS)
- Ссылки – расположение параметра безопасности;
- Описание – описание правила;
- Фактическое значение – значение параметра, которое было обнаружено на хосте;
- Дополнительно – дополнительная информация о правиле.



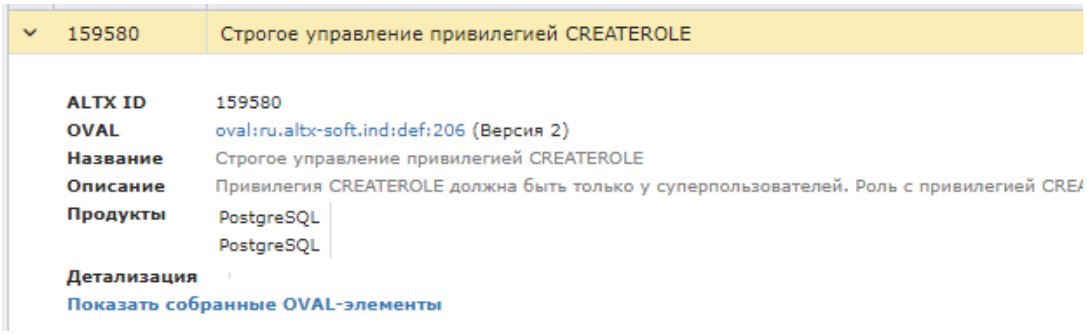
OVAL-Конфигурация

Вкладка содержит детализацию проверок правил конфигурации.



OVAL-определение состоит из:

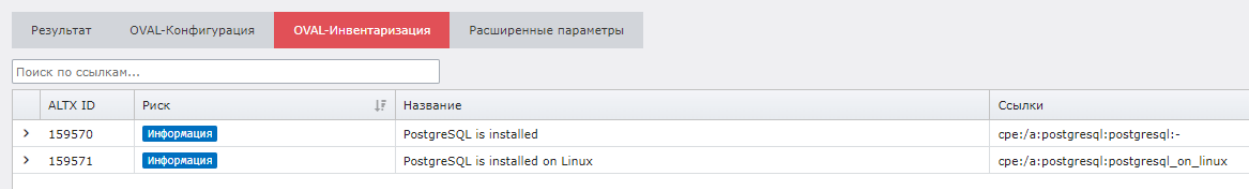
- ALTX ID – внутренний идентификатор уязвимости;
- OVAL – ссылка на страницу уязвимости в OVALdb;



OVAL-Инвентаризация

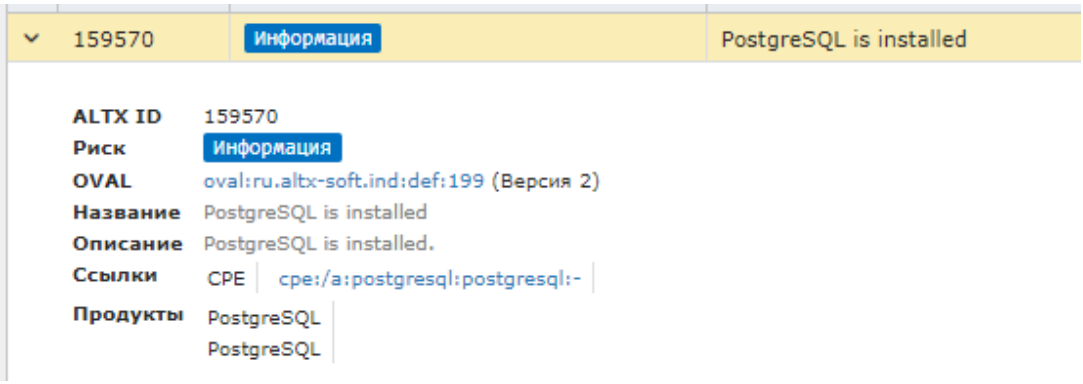
Вкладка отображает список с OVAL-определениями класса Информация.

> Информация – OVAL-определение для инвентаря (ПО).



Информация о найденном СУБД включает в себя:

- ALTX ID – внутренний идентификатор уязвимости;
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Ссылки – CPE продукта;
- Продукты – название СУБД.



Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.8 Проверка доступности

Описание результата сканирования задания Проверка доступности. Данный тип задания также предоставляет дополнительную статистику.

Результат

Вкладка содержит список хостов, проверенных на доступность.

Запись о хосте содержит следующую информацию:

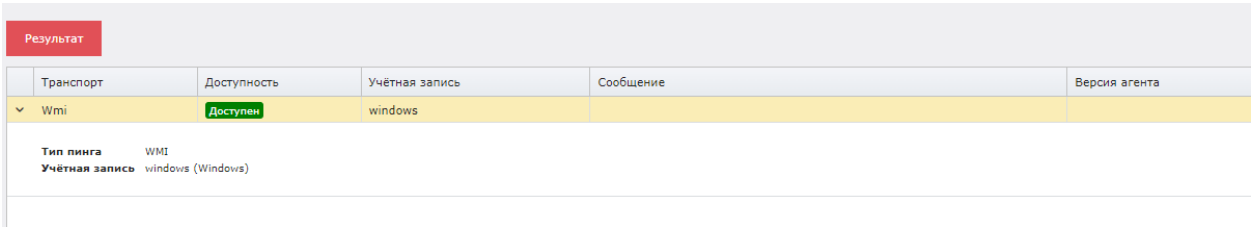
- Транспорт (Тип пинга) – способ подключения к хосту, который был выбран для проверки;
- Доступность – статус проверки:

Доступен – выполнение проверки для указанного хоста завершено успешно;

Ошибка – при проверке произошла ошибка;

Хост недоступен – служба сканирования не смогла подключиться указанным транспортом к хосту;

- Учетная запись для сканирования, с помощью которой выполнялось задание;
- Сообщение об ошибке;
- Версия агента RedCheck, если он установлен на хосте.

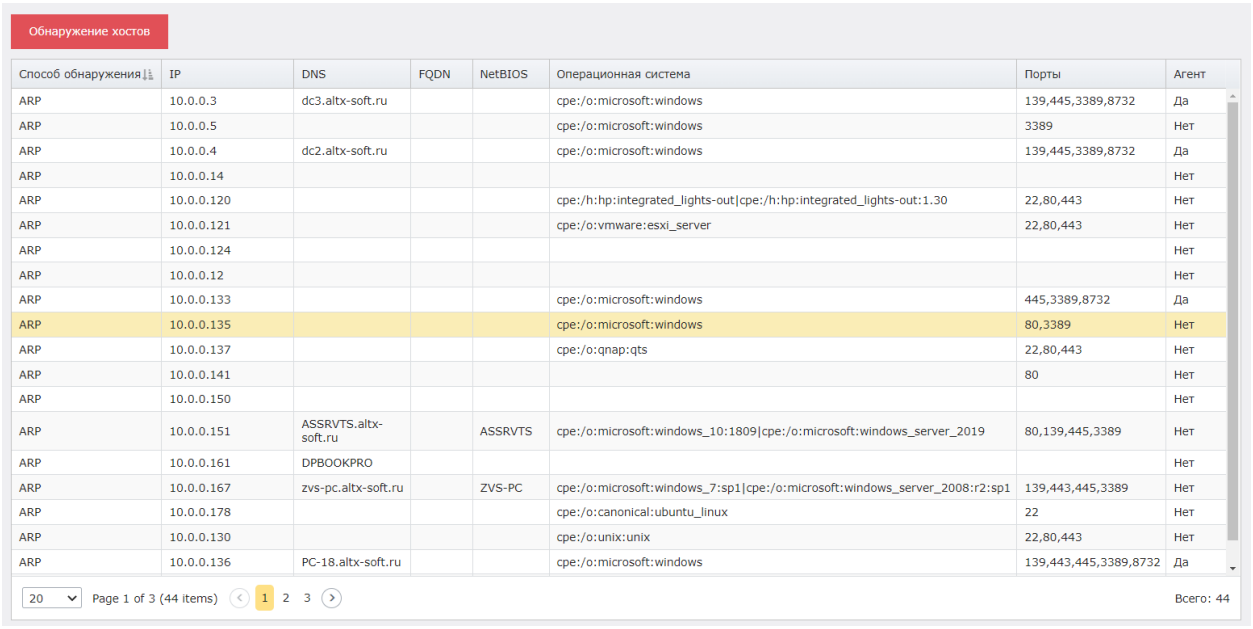


6.9 Обнаружение хостов

Описание результата сканирования задания Обнаружение хостов. Данный тип задания также предоставляет дополнительную статистику, по результатам которой можно добавить обнаруженные хосты в базу данных.

Обнаружение хостов

Вкладка содержит записи хостов, обнаруженных во время выполнения задания.



Способ обнаружения	IP	DNS	FQDN	NetBIOS	Операционная система	Порты	Агент
ARP	10.0.0.3	dc3.altx-soft.ru			cpe:/o:microsoft:windows	139,445,3389,8732	Да
ARP	10.0.0.5				cpe:/o:microsoft:windows	3389	Нет
ARP	10.0.0.4	dc2.altx-soft.ru			cpe:/o:microsoft:windows	139,445,3389,8732	Да
ARP	10.0.0.14						Нет
ARP	10.0.0.120				cpe:/h:hp:integrated_lights-out|cpe:/h:hp:integrated_lights-out:1.30	22,80,443	Нет
ARP	10.0.0.121				cpe:/o:vmware:esxi_server	22,80,443	Нет
ARP	10.0.0.124						Нет
ARP	10.0.0.12						Нет
ARP	10.0.0.133				cpe:/o:microsoft:windows	445,3389,8732	Да
ARP	10.0.0.135				cpe:/o:microsoft:windows	80,3389	Нет
ARP	10.0.0.137				cpe:/o:qnap:qts	22,80,443	Нет
ARP	10.0.0.141					80	Нет
ARP	10.0.0.150						Нет
ARP	10.0.0.151	ASSRVTS.altx-soft.ru		ASSRVTS	cpe:/o:microsoft:windows_10:1809|cpe:/o:microsoft:windows_server_2019	80,139,445,3389	Нет
ARP	10.0.0.161	DPBOOKPRO					Нет
ARP	10.0.0.167	zvs-pc.altx-soft.ru		ZVS-PC	cpe:/o:microsoft:windows_7:sp1|cpe:/o:microsoft:windows_server_2008:r2:sp1	139,443,445,3389	Нет
ARP	10.0.0.178				cpe:/o:canonical:ubuntu_linux	22	Нет
ARP	10.0.0.130				cpe:/o:unix:unix	22,80,443	Нет
ARP	10.0.0.136	PC-18.altx-soft.ru			cpe:/o:microsoft:windows	139,443,445,3389,8732	Да

Информация о хосте состоит из:

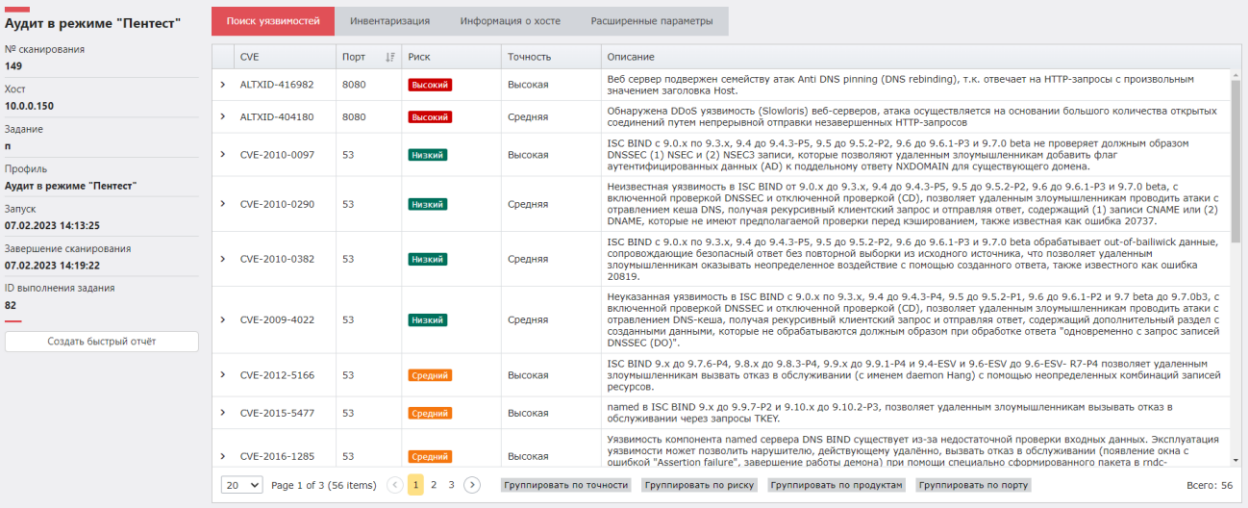
- Способа обнаружения (ARP, TCP, UDP и т.д.);
- IP-адреса, DNS-имени, FQDN, NetBIOS;
- Тип ОС – CPE операционной системы;
- Порты – открытые порты на хосте;
- Агент – статус наличия агента RedCheck на хосте.

6.10 Аудит в режиме "Пентест"

Описание результата сканирования задания Аудит в режиме «Пентест».

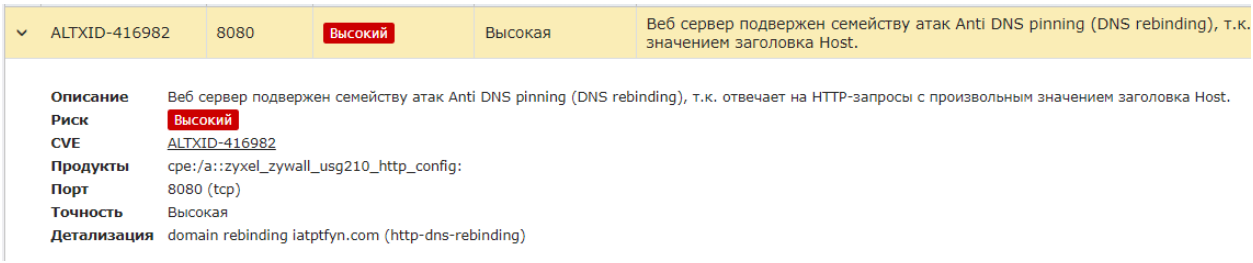
Поиск уязвимостей

Вкладка отображает список найденных методом черного ящика уязвимостей на хосте.



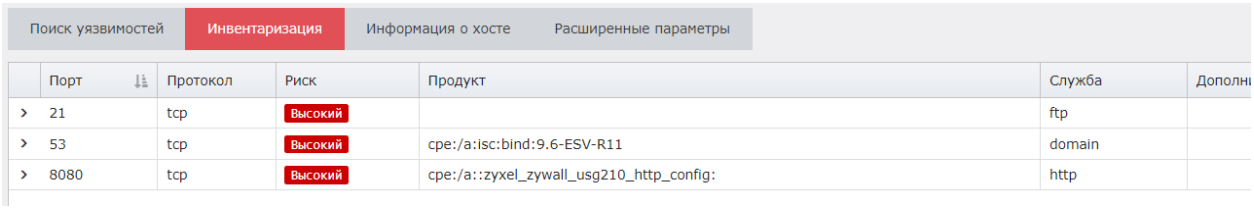
Информация об уязвимости состоит из:

- Ссылки – страницы уязвимости в различных базах данных уязвимостей;
- Риск – уровень критичности; (Сведения об интегральной оценке по базовым метрикам CVSS)
- CVE – ссылка-идентификатор CVE;
- Продукты – CPE продукта;
- CWE – ссылка-идентификатор CWE;
- CVSSv2 – показатели метрики в CVSS v2;
- Порт – на котором работает продукт;
- Точность – достоверность определенной уязвимости;
- Детализация – версия продукта.



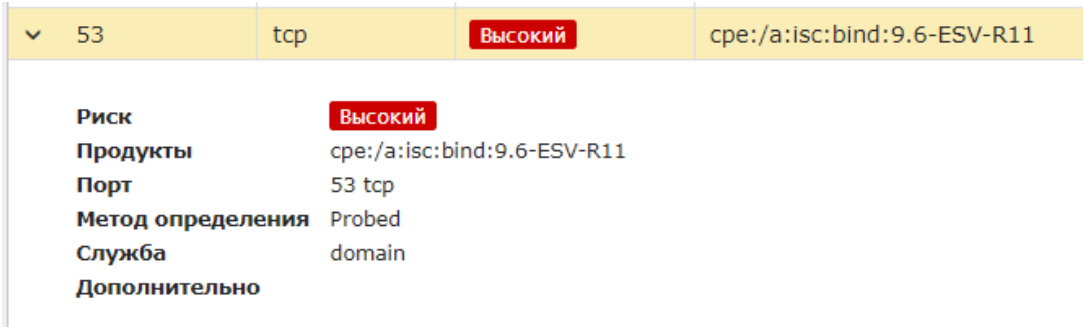
Инвентаризация

Вкладка отображает список служб, которые работают на открытых портах.



Информация о службе включает в себя:

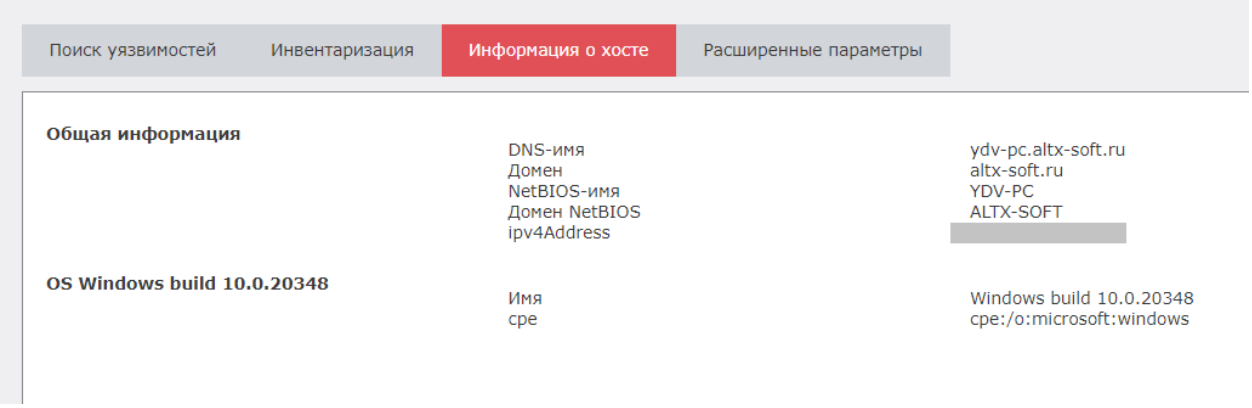
- Риск – уровень критичности; (Сведения об интегральной оценке по базовым метрикам CVSS)
- Продукты – CPE продукта;
- Порт – порт, на котором работает служба;
- Служба – название службы;



> Количество информации может изменяться в зависимости от службы.

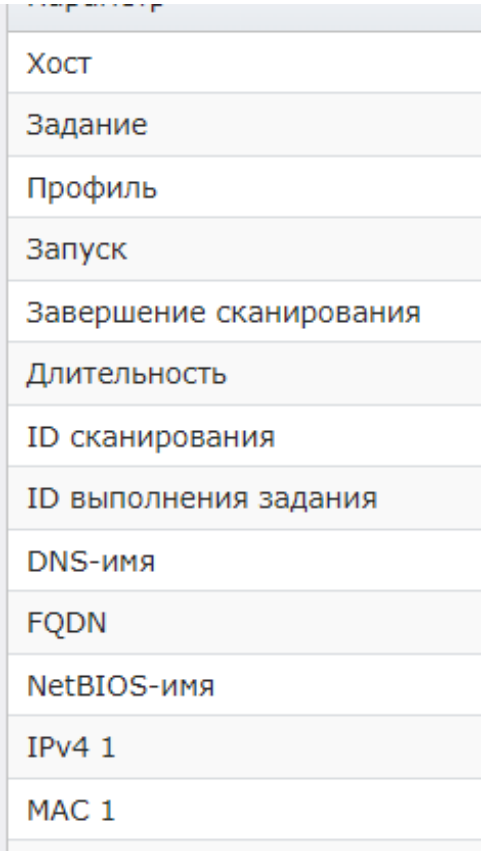
Информация о хосте

Вкладка содержит информацию о хосте, которую определил RedCheck методом черного ящика.



Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:



6.11 Статистика выполненных заданий

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Некоторые типы заданий имеют дополнительную информацию (статистику), которую можно экспортировать в CSV-файл. Такая возможность есть для:

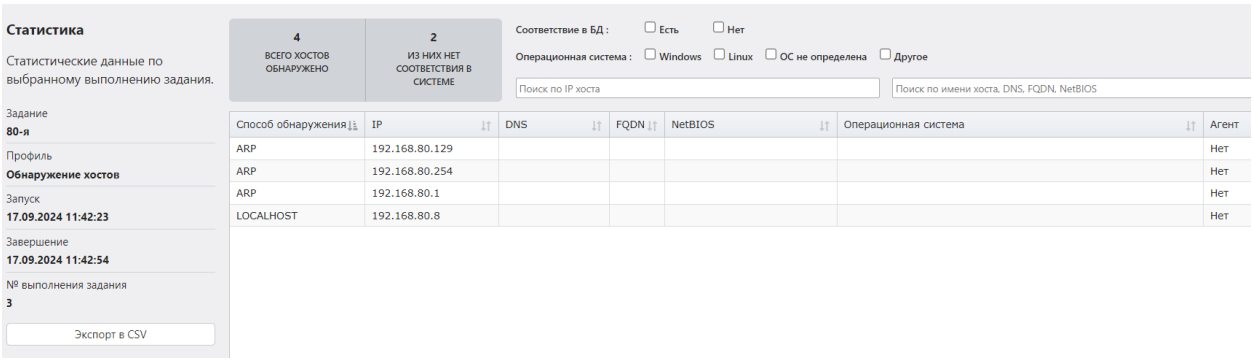
- Обнаружение хостов;
- Проверка доступности;

Перейдите в **Задания** → нажмите ⚙ → **Свойства** → **Дополнительно** → **Статистика**;

Статистика «Обнаружение хостов»

Запись об обнаруженном хосте содержит следующую информацию:

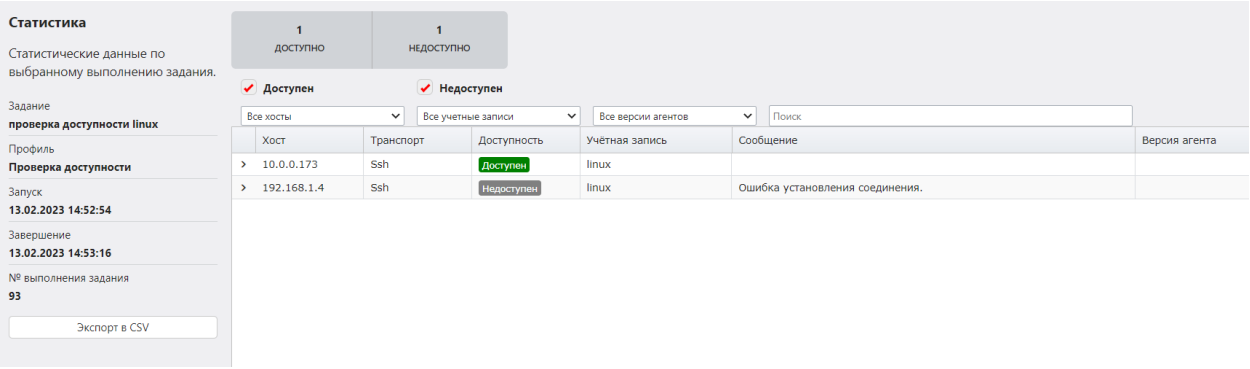
- Способ обнаружения – протокол, которым удалось обнаружить хост;
- IP-адрес;
- DNS-имя;
- FQDN-имя;
- NetBIOS-имя;
- Операционная система – CPE хоста;
- Агент – установлен Агент сканирования на хосте или нет;



Статистика «Проверки доступности»

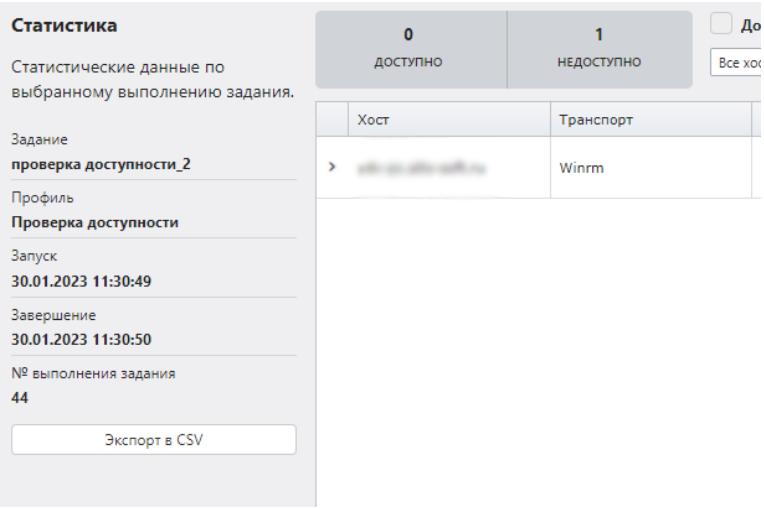
Запись о доступном хосте содержит следующую информацию:

- IP-адрес (имя) хоста;
- Проверяемый транспорт;
- Статус проверки;
- Учетная запись для сканирования, которая использовалась при сканировании;
- Сообщение об ошибке;
- Версия агента RedCheck, если он установлен на хосте.



Экспорт в CSV

В окне статистики нажмите **Экспорт в CSV**;



1. Обнаружение хостов. Файл будет иметь название **HostDiscovery-N-statistics.csv**, где N – ID итерации запуска.

Структура CSV файла

Ip	IP-адрес хоста
Reason	Протокол, которым удалось обнаружить хост
Dns	DNS-имя хоста
Fqdn	FQDN-имя хоста
NetBIOS	NetBIOS-имя хоста
Os	CPE
OpenPorts	Открытые порты, по которым удалось обнаружить хост
IsAgent	Установлен агент на хосте или нет
IdExistingHost	ID хоста, существующего в базе данных RedCheck

Пример:

Код

```
Ip,Reason,Dns,Fqdn,NetBIOS,Os,OpenPorts,IsAgent,IdExistingHost
192.168.80.129,ARP,,,,,,False,67
192.168.80.8,LOCALHOST,,,,,,False,69
```

2. Проверка доступности. Файл будет иметь название **Ping-N-statistics.csv**, где N – ID итерации запуска.

Структура CSV файла

ConnectionAddress	IP-адрес или DNS-имя хоста
PingType	Проверяемый протокол

Result	Результат проверки: False или True
Credential	Название учетной записи, используемой для проверки
Message	Сообщение об ошибке. если хост недоступен
AgentVersion	Версия Агента сканирования, если он установлен на хосте

Пример:

Код

```
ConnectionAddress,PingType,Result,Credential,Message,AgentVersion
192.168.80.210,Winrm,False,winrm
test,HTTPConnectionPool(host='192.168.100.210', port=5985): Max
retries exceeded with url: /wsman (Caused by
NewConnectionError('<urllib3.connection.HTTPConnection object at
0x701ef5a13550>: Failed to establish a new connection: [Errno 111]
Connection refused')),
```

7 Отчеты

RedCheck обладает инструментом создания отчетов. Отчет – файл с информацией о проведенном сканировании. В отчет могут входить результаты сканирования множества хостов одновременно. Возможность использовать профили аудитов (5.1 Профили аудитов) позволяет выбирать / исключать из результатов сканирования конкретные OVAL-определения.

RedCheck предлагает пять форматов отчета: html, pdf, mht, csv, xml.

> Если необходимо автоматически доставлять отчеты после завершения сканирований, настройте сервис доставки отчетов.

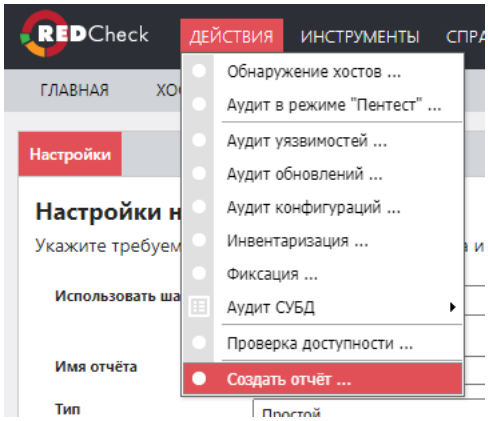
Типы отчетов

В Системе есть две разновидности отчетов: простой и дифференциальный.

- Простой – это собранные в один документ результаты сканирований по указанным хостам (7.1 Создание простого отчета);
- Дифференциальный – документ, в котором происходит сравнение двух результатов сканирования между собой. Отчет будет состоять из разницы между результатами сканирования (7.2 Создание дифференциального отчета).

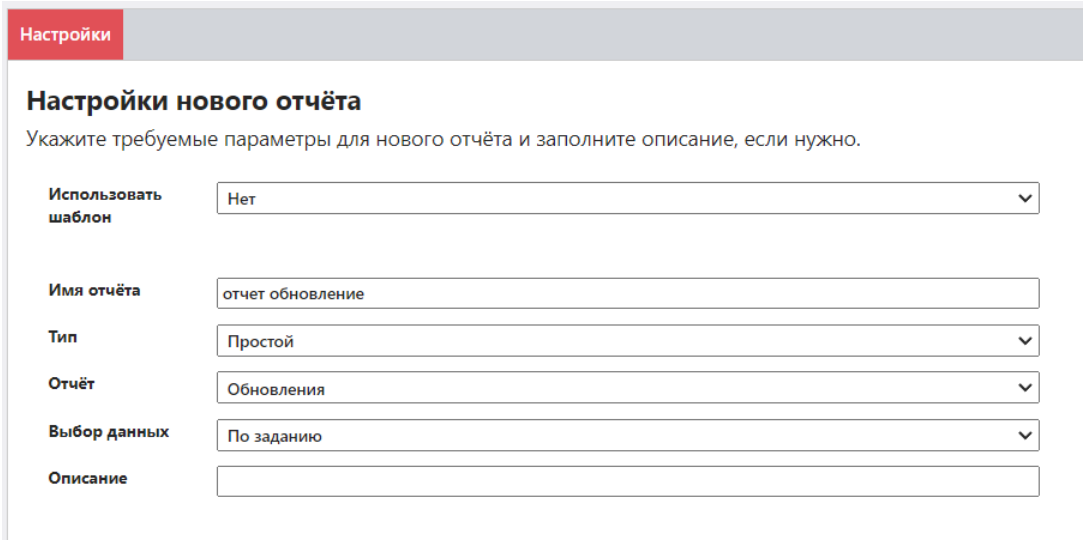
Пример создания простого отчета

Раскроем **Действия** → **Создать отчет**;

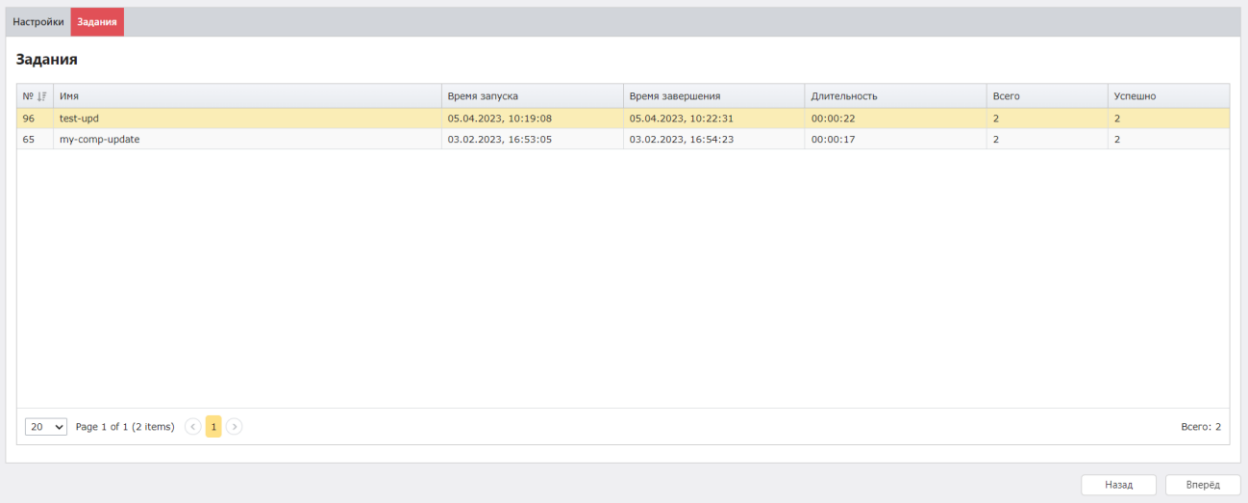


Укажем следующие настройки для отчета:

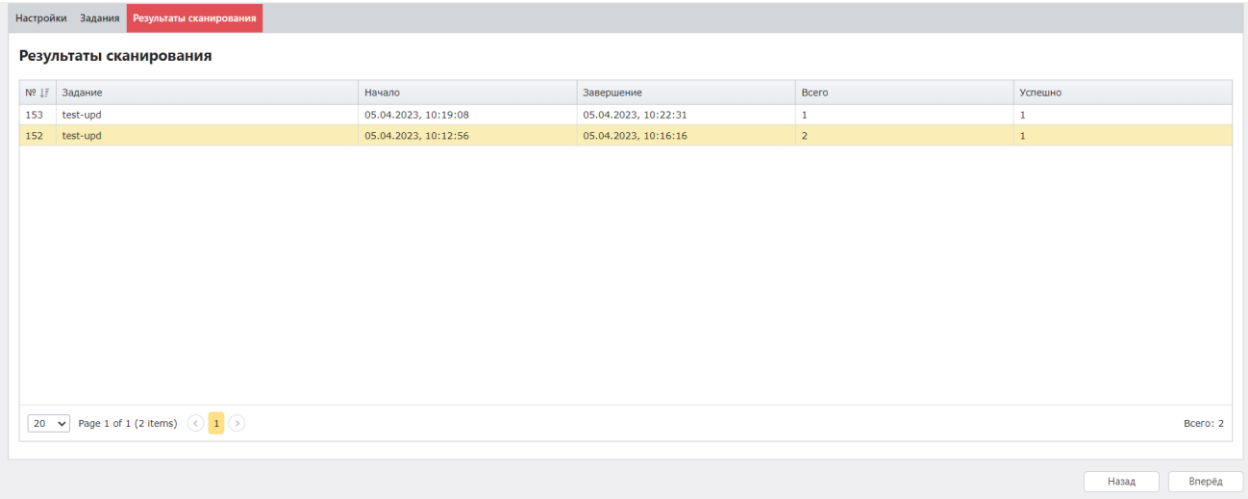
- Тип – Простой;
- Отчет – Обновления, т. е. отчет для задания Аудит обновлений.
- Выбор данных – по заданию, т.е. отчет по результатам сканирования одного задания.



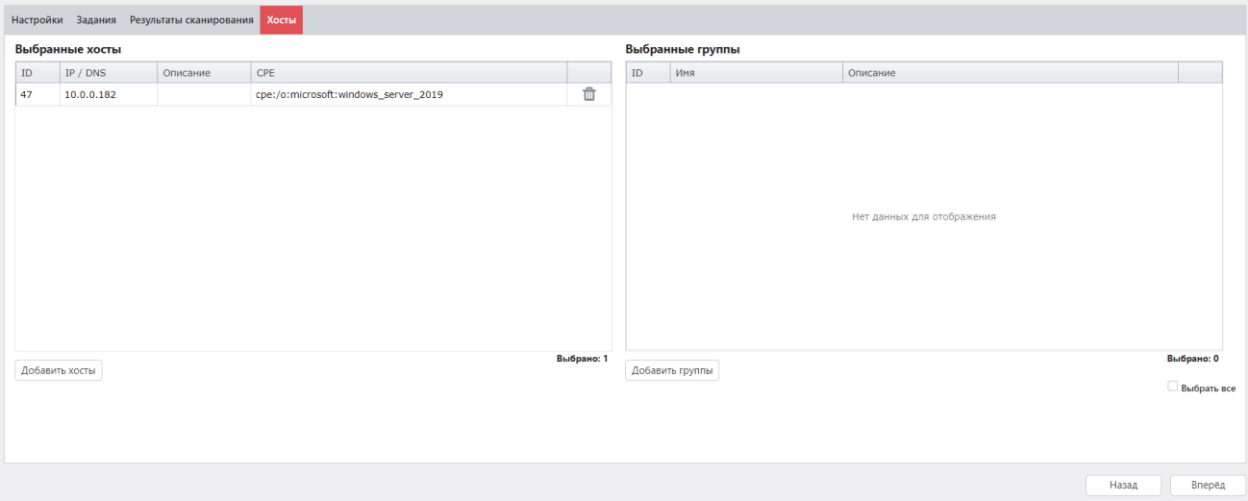
Выберем задание → **Вперед**;



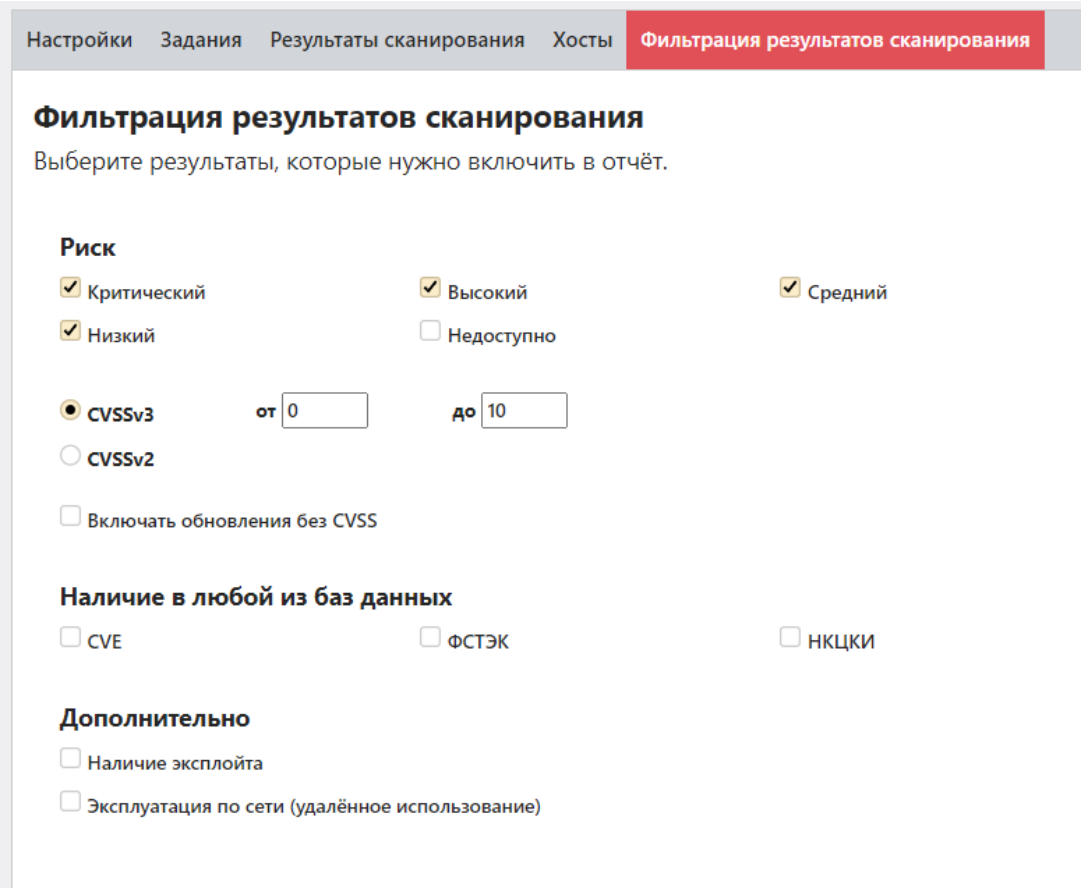
Выберем результат сканирования → **Вперед**;



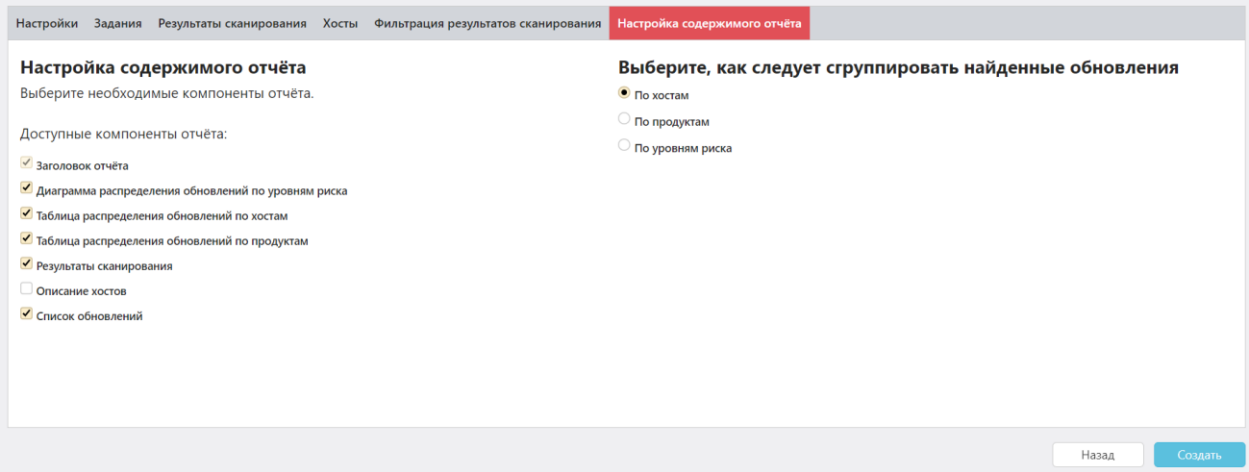
Добавим хосты. В данном случае только один хост, так как второй был недоступен в момент выполнения задания → **Вперед**;



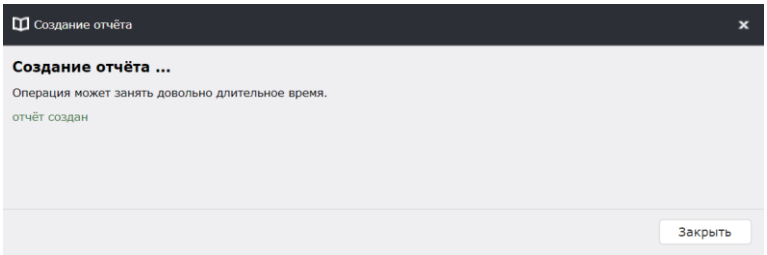
Укажем следующие настройки фильтрации результатов сканирования: исключим из отчета OVAL-определения с уровнем критичности Недоступно и без CVSS.



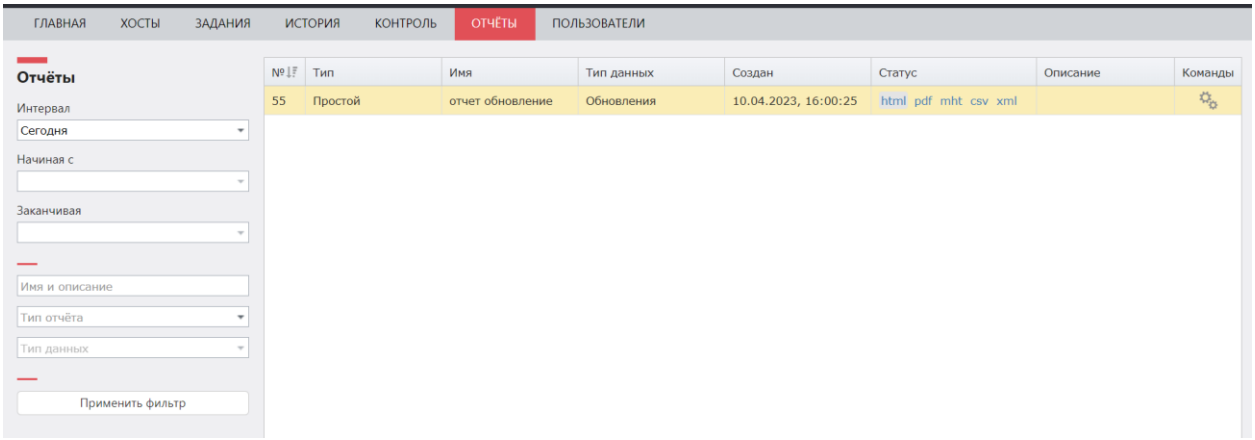
Оставим стандартные настройки содержимого отчета → **Создать**;



Дождемся окончания процесса создания отчета.



Перейдем в **Отчеты** → выберем html формат.

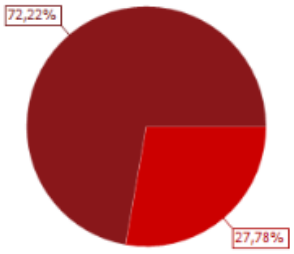


Отчет имеет следующий вид.

RED Check ОТЧЁТ

№ отчёта	4a161f62-cb43-4df7-804c-96adcbd22ac6
Профиль	Обновления
Задание	test-upd
Начало/завершение сканирования	05.04.2023 10:12:56 / 05.04.2023 10:16:16
Формирование отчёта	10.04.2023 16:00:25
Имя	отчет обновление
Хосты [1]	10.0.0.182

Диаграмма распределения обновлений по уровням риска



Риск	Количество
Критический	26
Высокий	10
Средний	0
Низкий	0
Всего	36

Фильтрация результатов сканирования	
Уровни риска	Критический, Высокий, Средний, Низкий
CVSSv3, от	0
CVSSv3, до	10
CVSSv2 (при отсутствии CVSSv3), от	0
CVSSv2 (при отсутствии CVSSv3), до	10
Включать обновления без CVSS	Нет

Таблица распределения обновлений по хостам

Хост / Риск	Критический	Высокий	Средний	Низкий	Всего
10.0.0.182	26	10	0	0	36
Всего	**26**	**10**	**0**	**0**	**36**

1

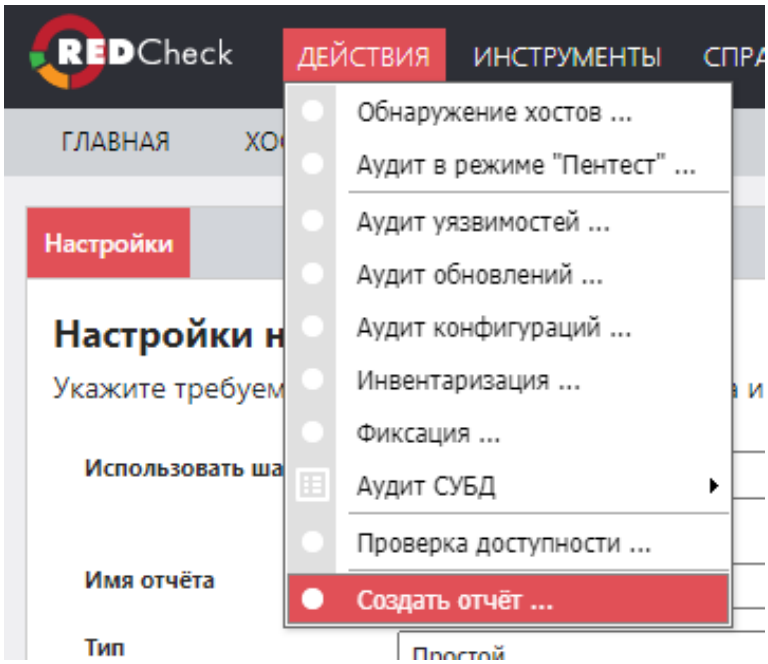
Более подробное описание создания отчета находится в разделе 7.1 Создание простого отчета.

7.1 Создание простого отчета

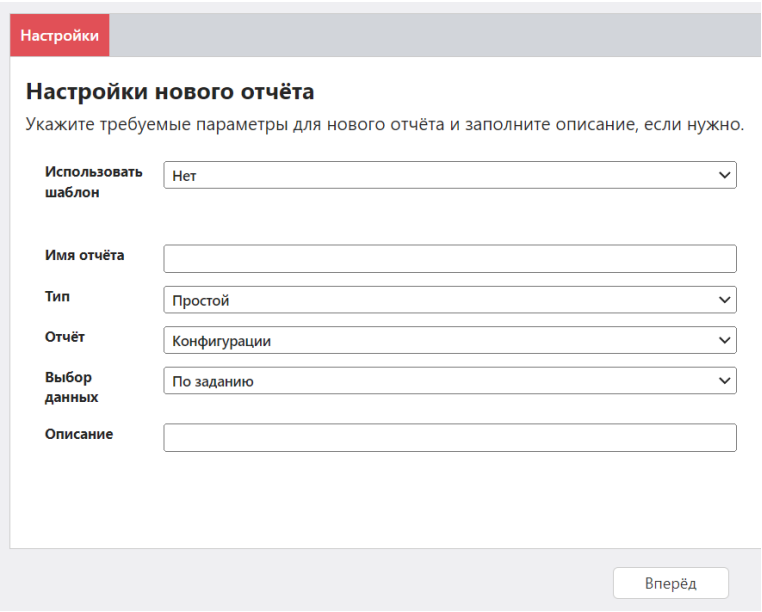
Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Чтобы создать простой отчет, выполните следующие шаги.

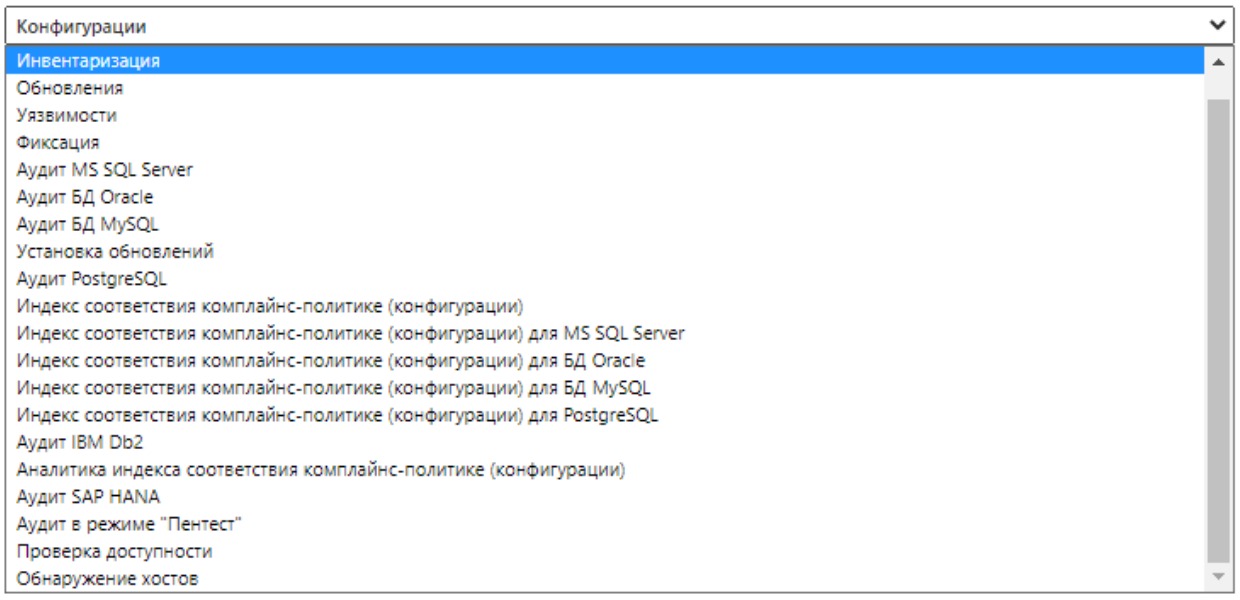
Шаг 1. Раскройте **Действия** → **Создать отчет**;



Шаг 2. Заполните начальную страницу мастера → **Вперед**:



Параметр **Отчет** – тип данных, их которых будет создаваться отчет. В зависимости от выбранного значения последовательность создания отчета может измениться из-за дополнительных параметров;



Параметр **Выбор данных:**

По заданию: отчет по одному результату сканирования выбранного задания для

нескольких хостов;

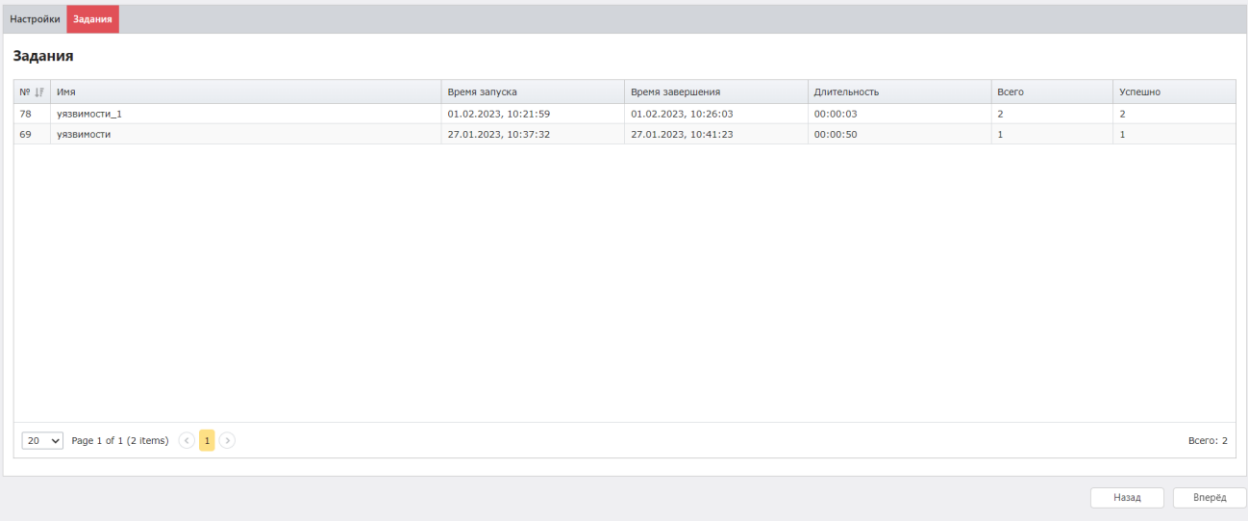
По хостам (актуальные сканирования): отчет по актуальным результатам сканирования выбранных заданий для указанных хостов;

По единичному хосту (с выбором сканирования): отчет по одному результату сканирования для одного хоста;

Выбор данных: По заданию

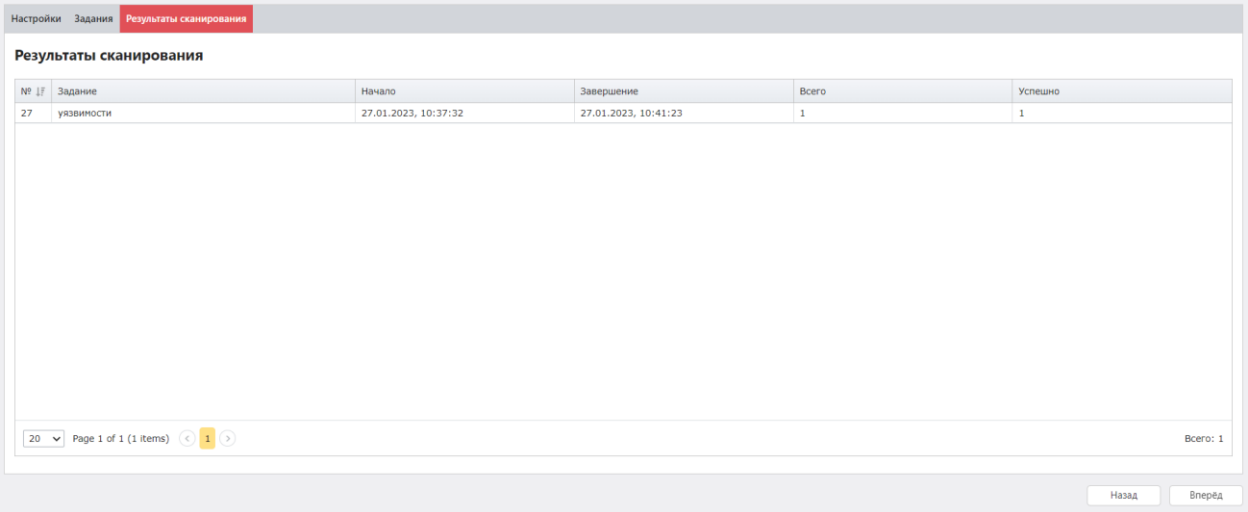
Шаг 3. Выберите задание, по результатам которого будет строиться отчет

→ **Вперед**:

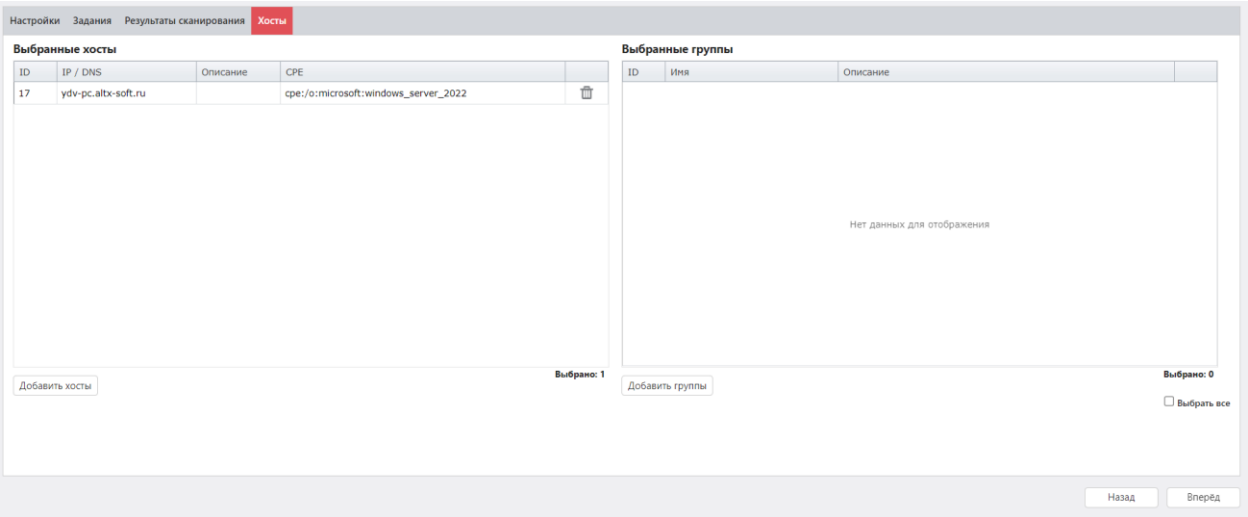


Шаг 4. Выберите результат сканирования, по которому будет строиться отчет

→ **Вперед**:



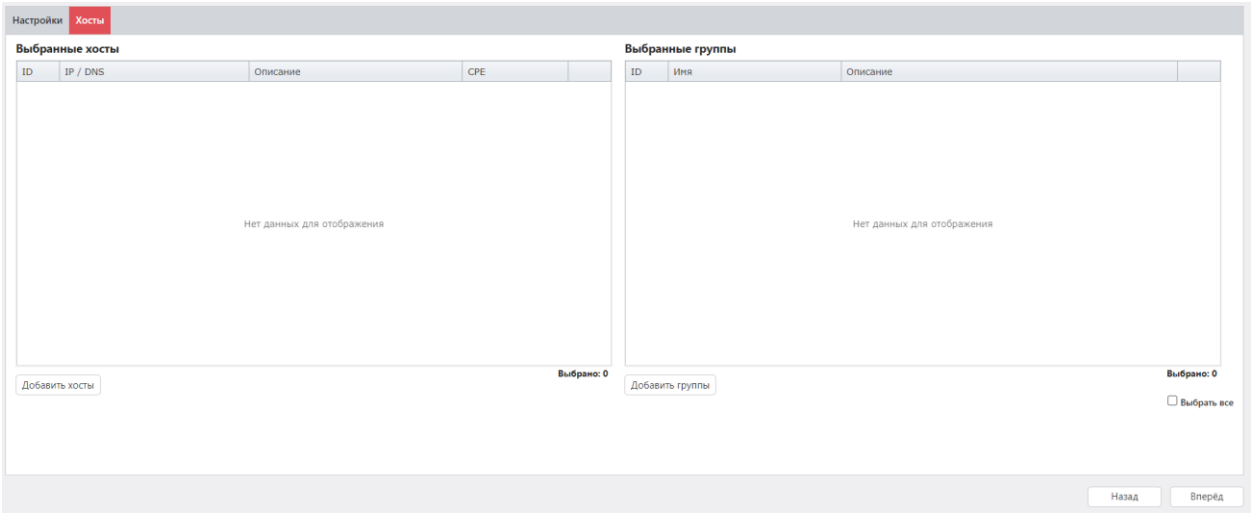
Шаг 5. Добавьте хосты (**Добавить хосты**) / группы (**Добавить группы**) из результата сканирования, которые хотите видеть в отчете → **Вперед**:



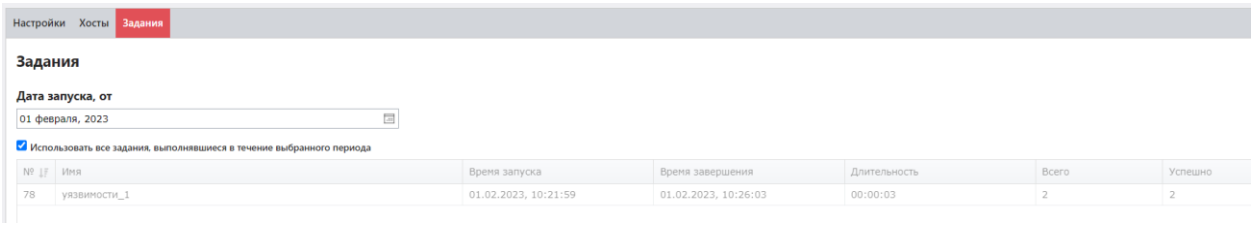
Шаг 6. Укажите дополнительные настройки для отчета (7.1.1 Настройки для разных типов заданий)

Выбор данных: По хостам

Шаг 3. Добавьте хосты (**Добавить хосты**) / группы (**Добавить группы**), которые хотите видеть в отчете → **Вперед**:



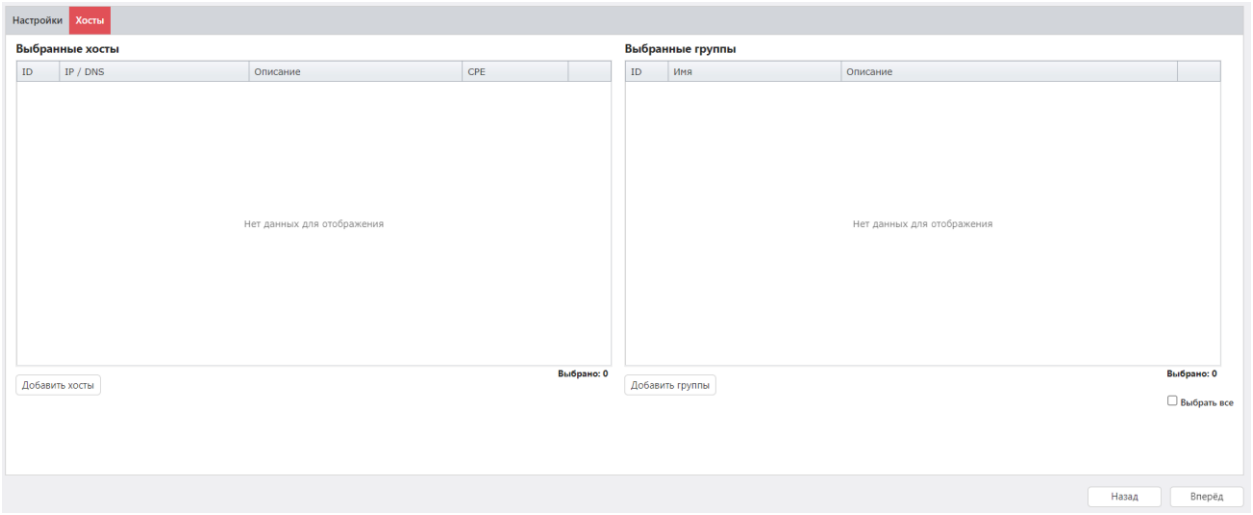
Шаг 4. Выберите задания, которые хотите видеть в отчете, или воспользуйтесь фильтром по дате запуска → **Вперед**:



Шаг 5. Укажите дополнительные настройки для отчета (7.1.1 Настройки для разных типов заданий)

Выбор данных: По единичному хосту

Шаг 3. Добавьте хост (**Добавить хосты**), который хотите видеть в отчете → **Вперед**:



Шаг 4. Выберите результат сканирования → **Вперед**:

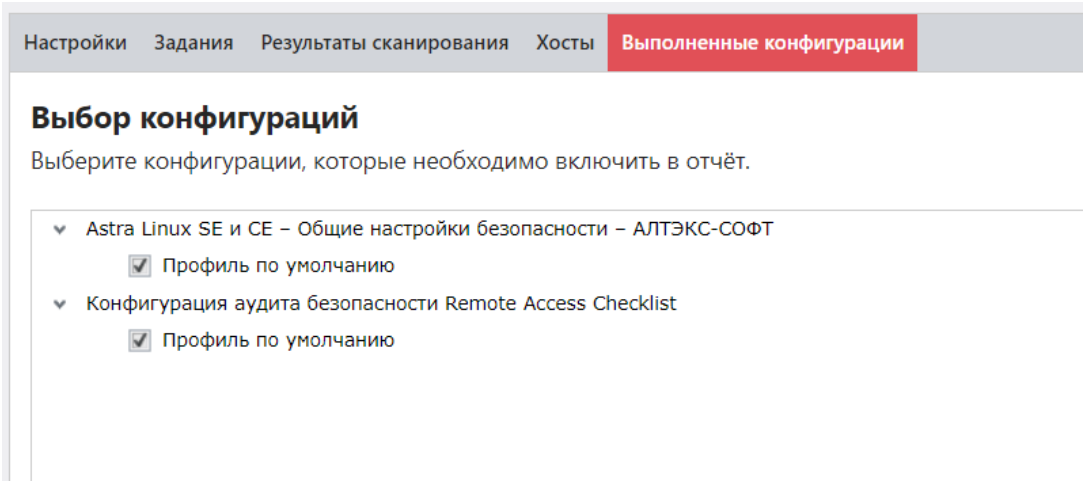
Шаг 5. Укажите дополнительные настройки для отчета (7.1.1 Настройки для разных типов заданий)

7.1.1 Настройки для разных типов задания

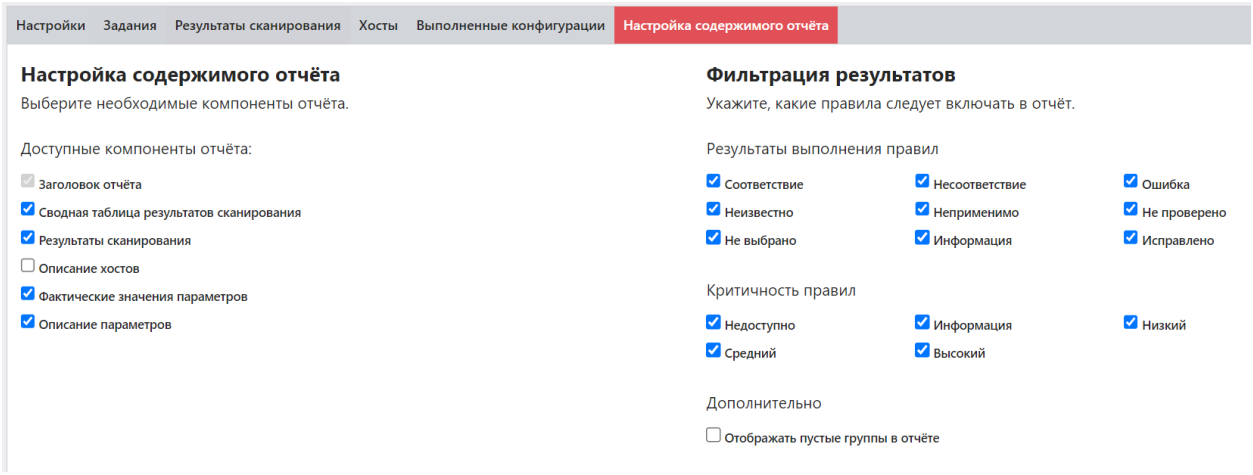
Содержание

Конфигурации

Выберите конфигурации, сведения о которых хотите включить в отчет → **Вперед**:

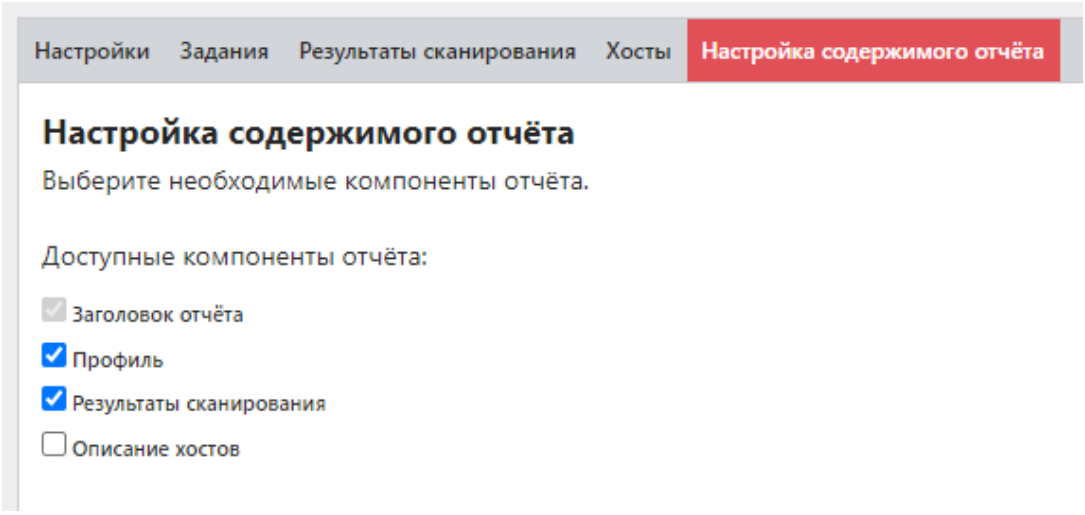


Укажите настройки содержимого отчета и фильтрации результатов → **Создать**:



Инвентаризация

Укажите настройки содержимого отчета → **Создать**:

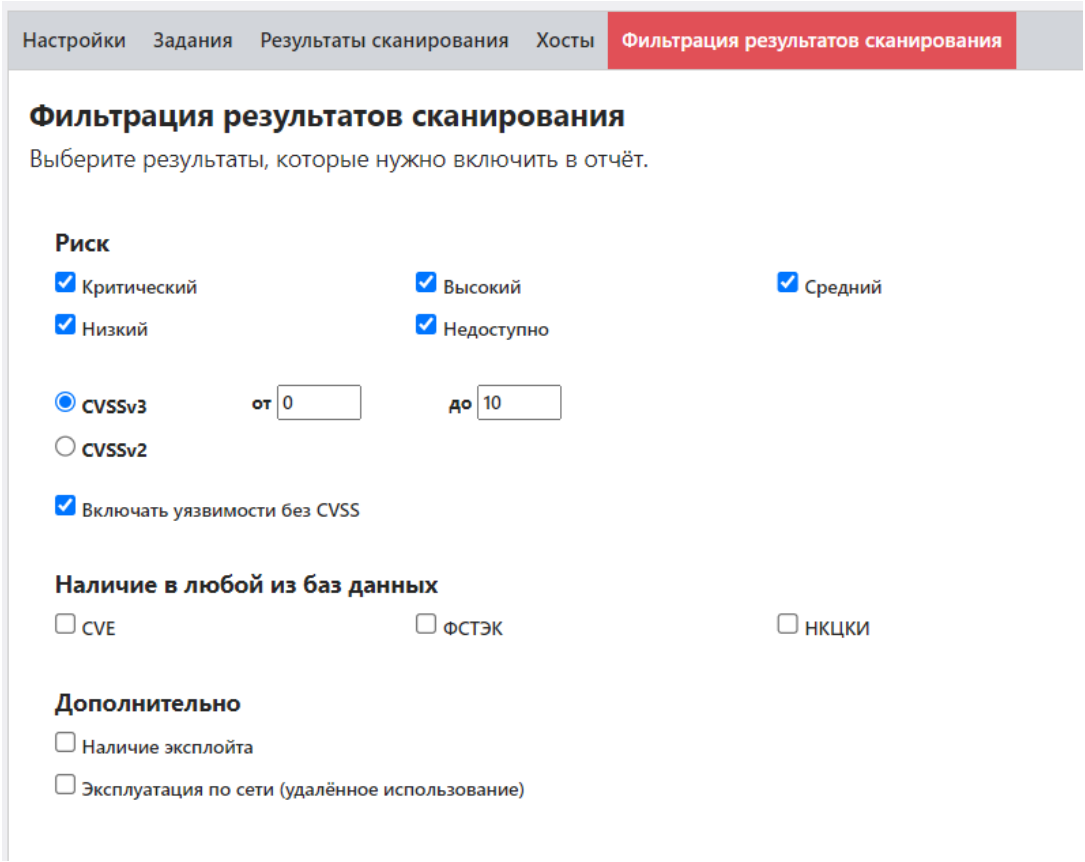


Уязвимости

Укажите настройки для фильтрации результата сканирования → **Вперед**:

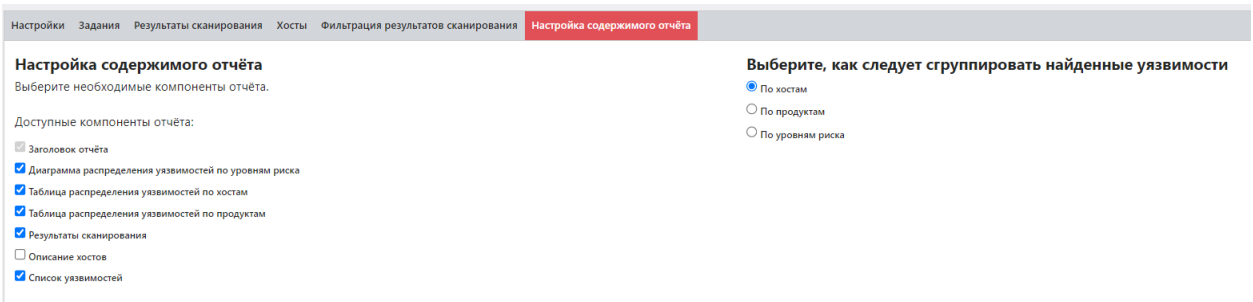
- Риск – фильтрация по категориям риска;
- В отчет попадут только те уязвимости, метрика CVSS которых будет в указанном интервале;
- Включать уязвимости без CVSS – в отчете будут уязимости, CVSS для которых не было определено;
- Дополнительно:
  - Наличие эксплойта – OVAL-определение имеет эксплойт;

- Эксплуатация по сети – эксплойт можно воспроизвести удаленно;



К отчету можно применить профиль сканирования (5.1 Профили сканирования).

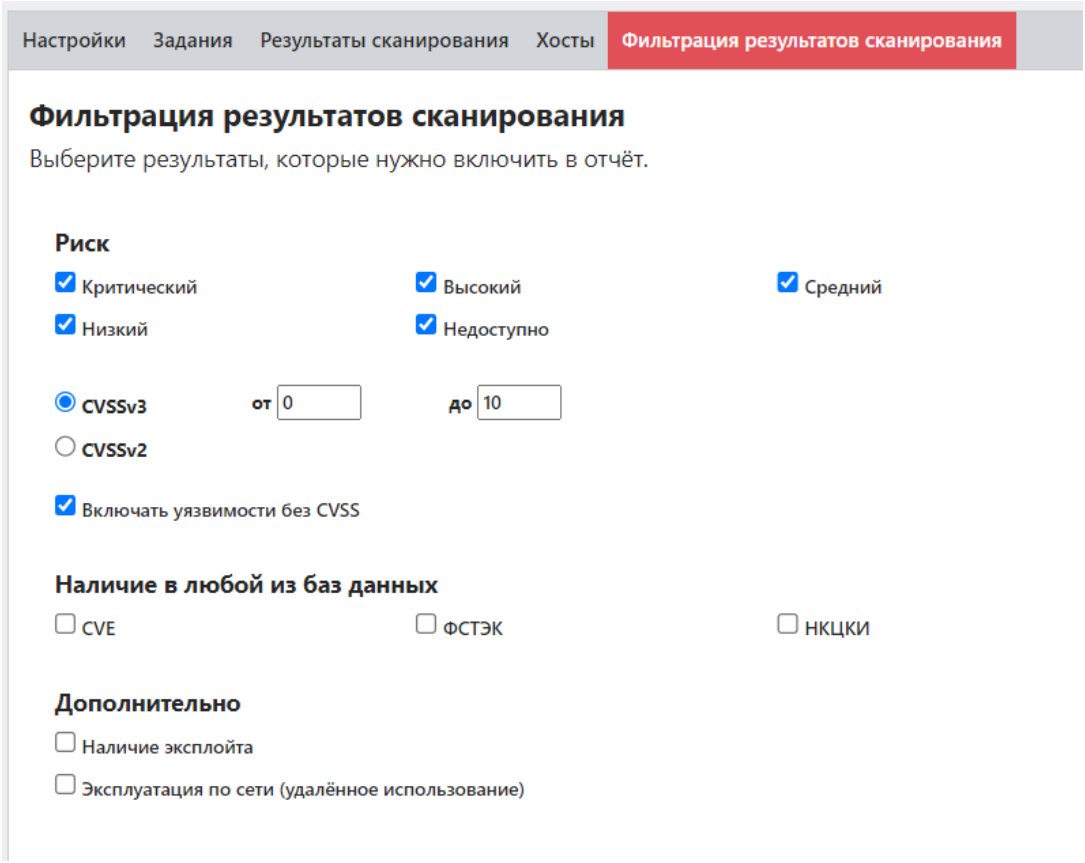
Укажите, что будет содержаться в отчете и варианты группировки уязвимостей → **Создать**:



Обновления

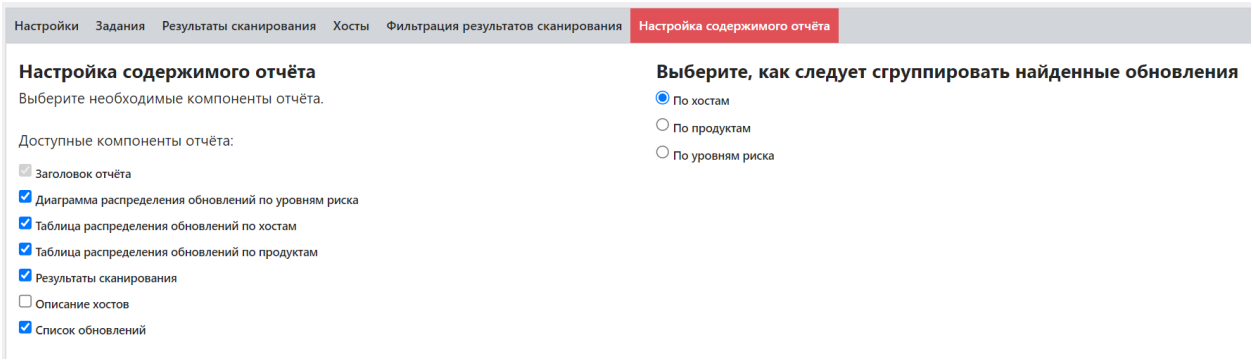
Укажите настройки для фильтрации результата сканирования → **Вперед**:

- Риск – фильтрация по категориям риска;
- В отчет попадут только те уязвимости, метрика CVSS которых будет в указанном интервале;
- Включать уязвимости без CVSS – в отчете будут уязимости, CVSS для которых не было определено;
- Дополнительно:
  - Наличие эксплойта – OVAL-определение имеет эксплойт;
  - Эксплуатация по сети – эксплойт можно воспроизвести удаленно;



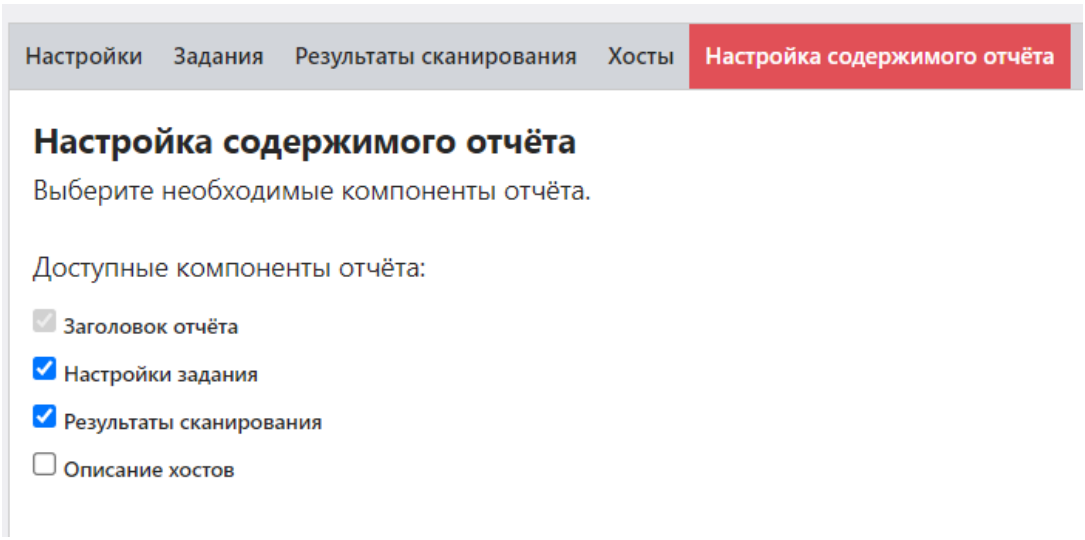
К отчету можно применить профиль сканирования (5.1 Профили сканирования).

Укажите, что будет содержаться в отчете и вариант группировки найденных обновлений → **Создать**:



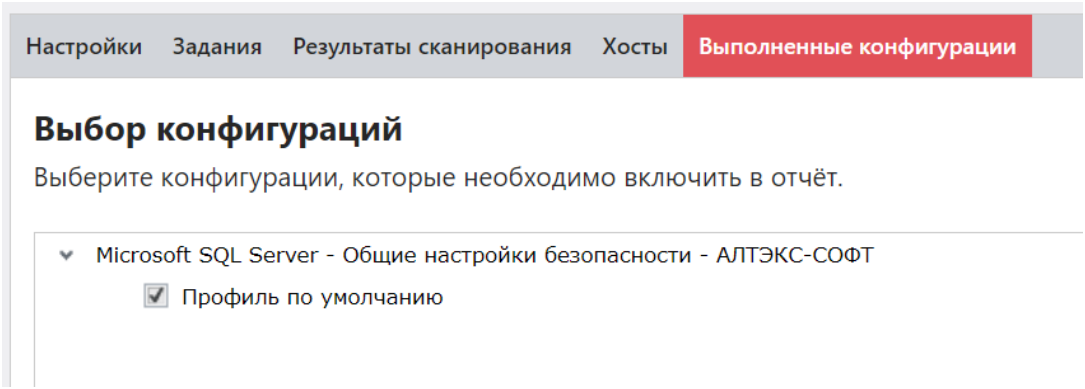
Фиксация

Укажите, что будет содержаться в отчете → **Создать**:

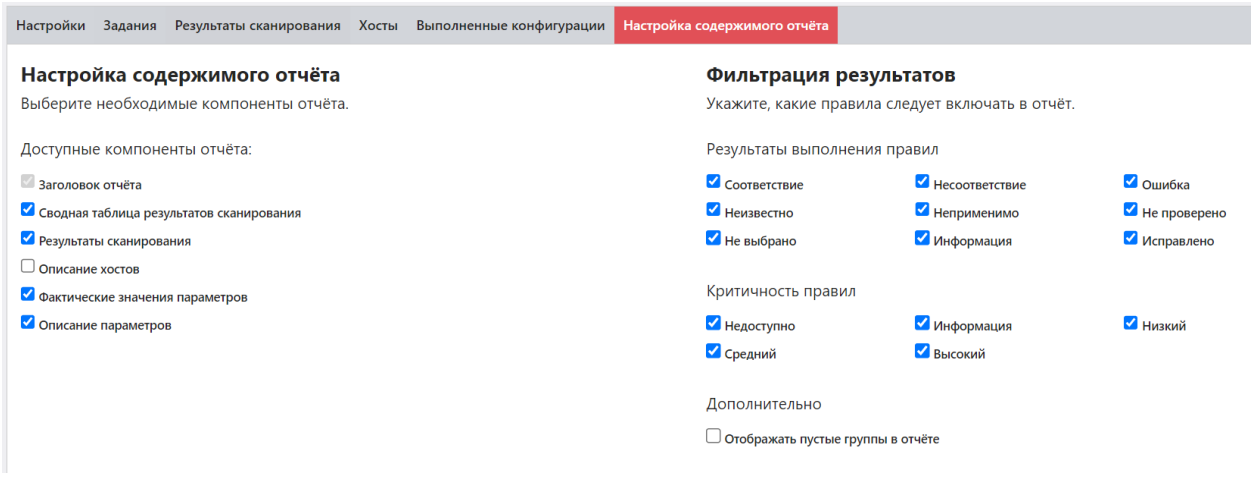


Аудит СУБД

Выберите профиль конфигурации, проверку с которым хотите увидеть в отчете → **Вперед**:



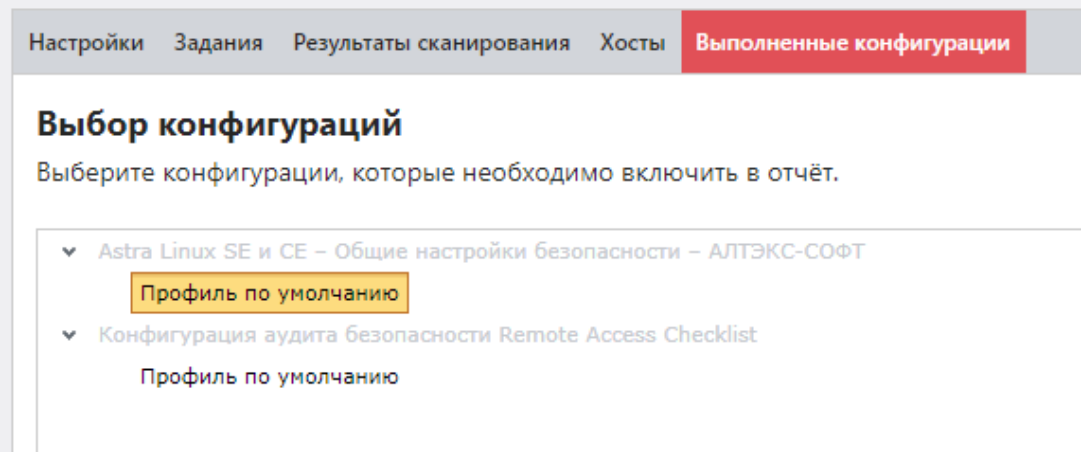
Укажите настройки содержимого отчета и фильтрации результатов → **Создать**:



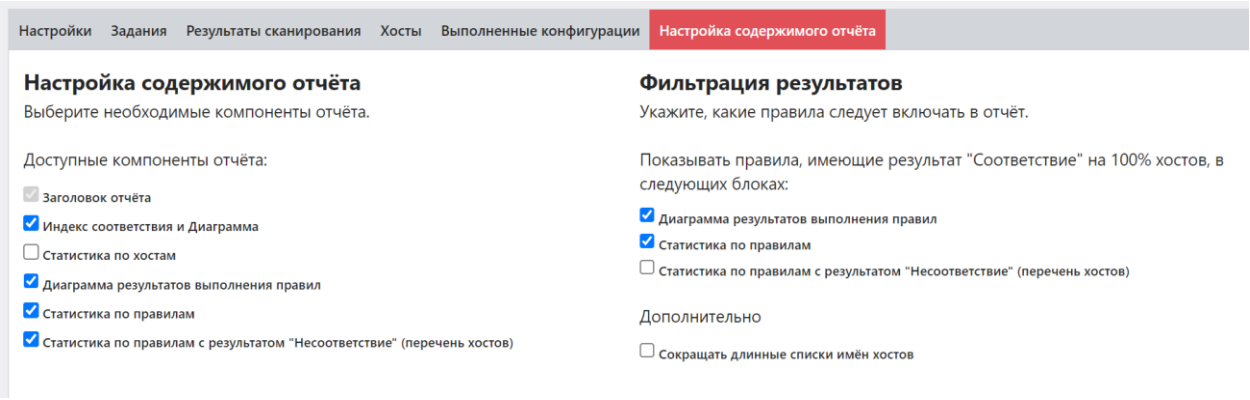
Индекс соответствия комплайнс-политике (конфигурации)

Отчет показывает, насколько хосты соответствуют выбранной конфигурации, детально информируя о каждом правиле.

Выберите конфигурацию, соответствие с которой хотите увидеть в отчете → **Вперед**:



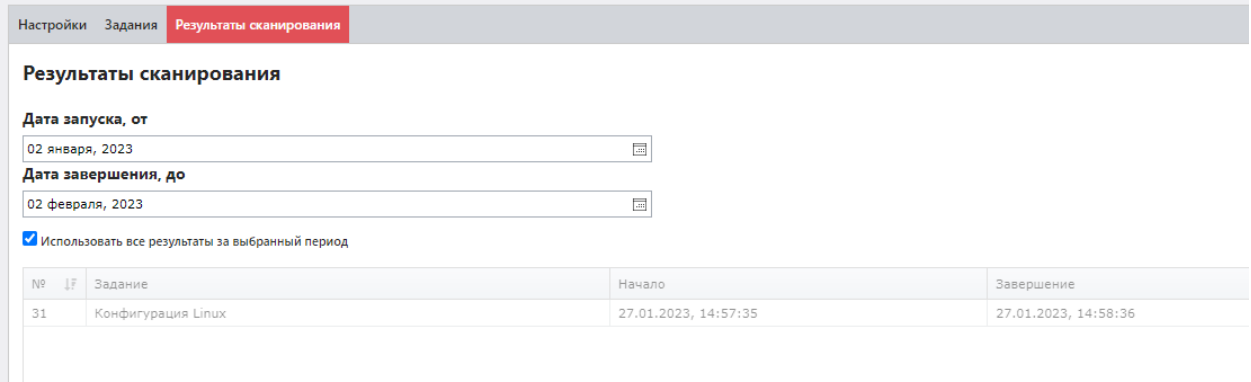
Укажите настройки содержимого отчета и фильтрации результатов → **Создать**:



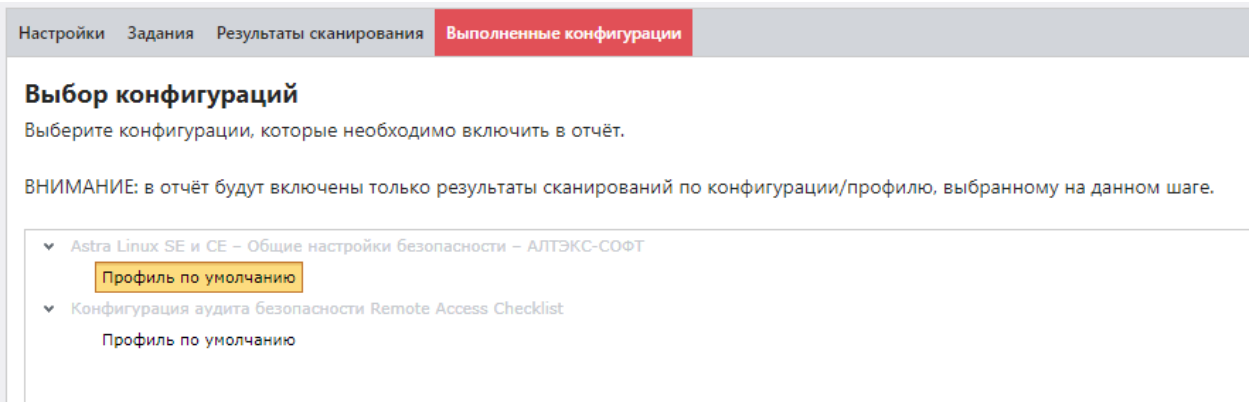
Аналитика индекса соответствия комплайнс-политике (конфигурации)

Отчет будет содержать данные о количестве успешно просканированных хостах и их соответствии выбранной конфигурации. Отчет не показывает соответствие с каждым правилом конфигурации.

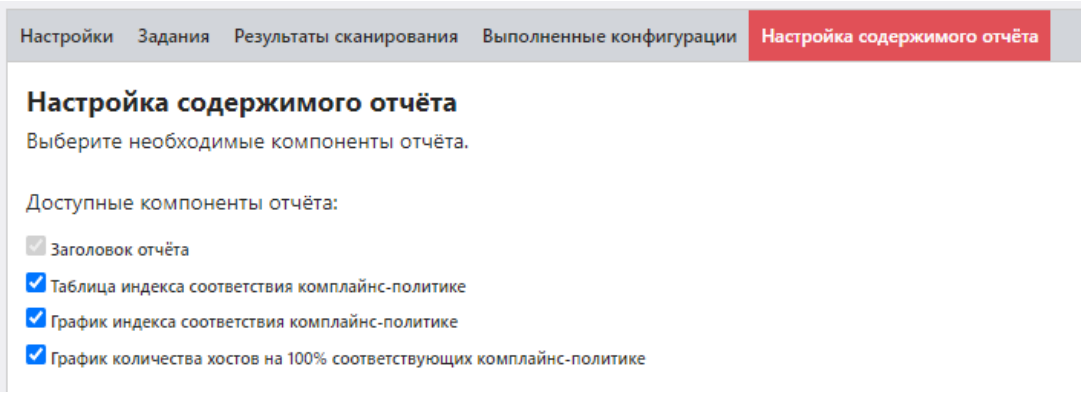
Укажите результаты сканирования или воспользуйтесь фильтром по дате запуска и завершения



Выберите конфигурацию, аналитику которой хотите включить в отчет → **Вперед**:

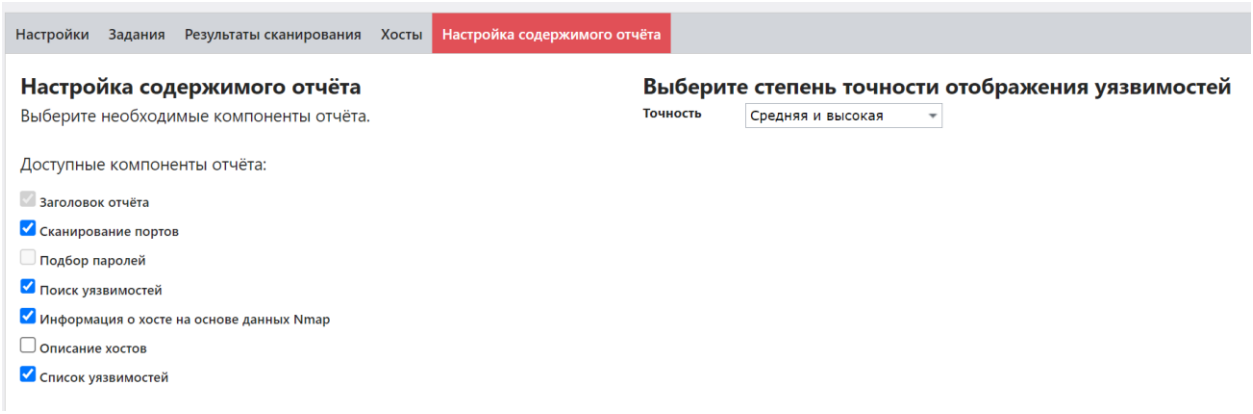


Укажите, что будет содержаться в отчете → **Создать**:



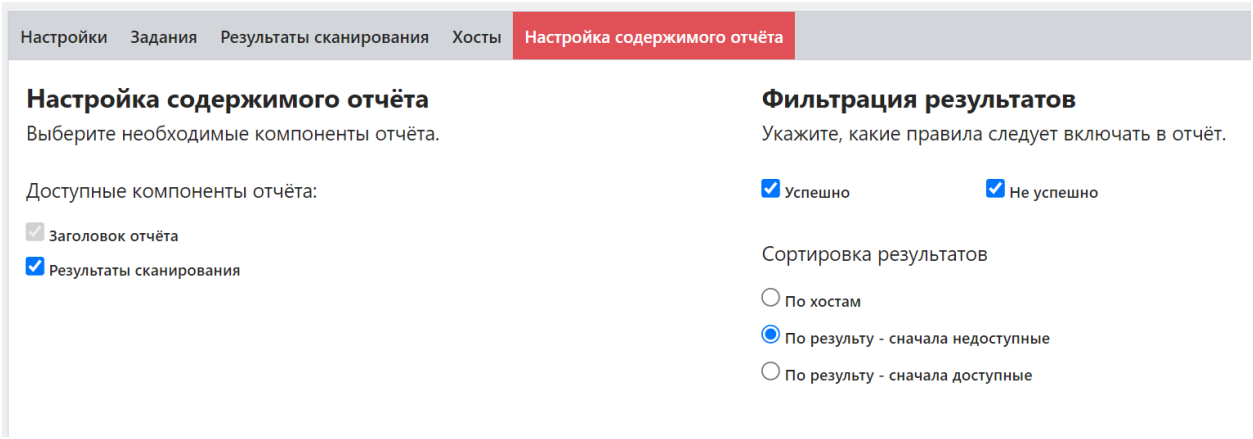
Аудит в режиме «Пентест»

Укажите, что будет содержаться в отчете → **Создать**:



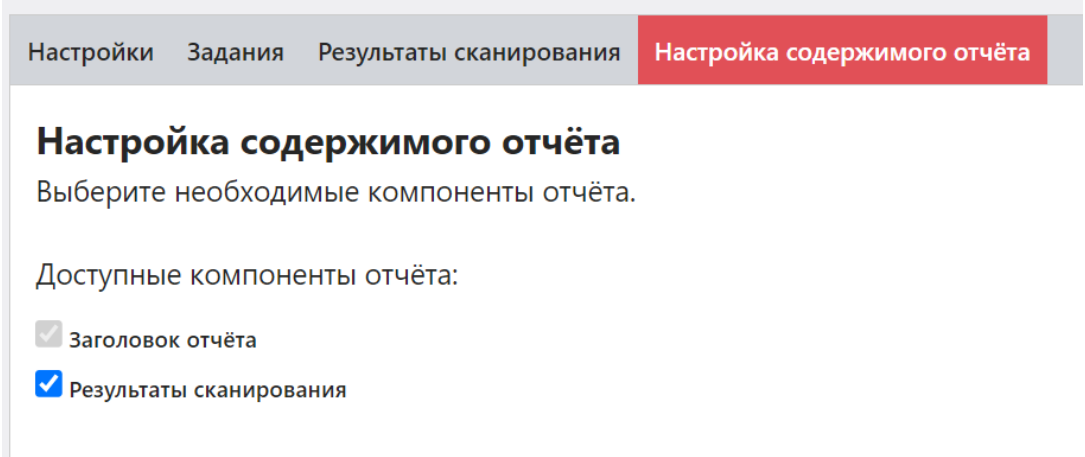
Проверка доступности

Укажите, что будет содержаться в отчете → **Создать**:



Обнаружение хостов

Укажите, что будет содержаться в отчете → **Создать**:

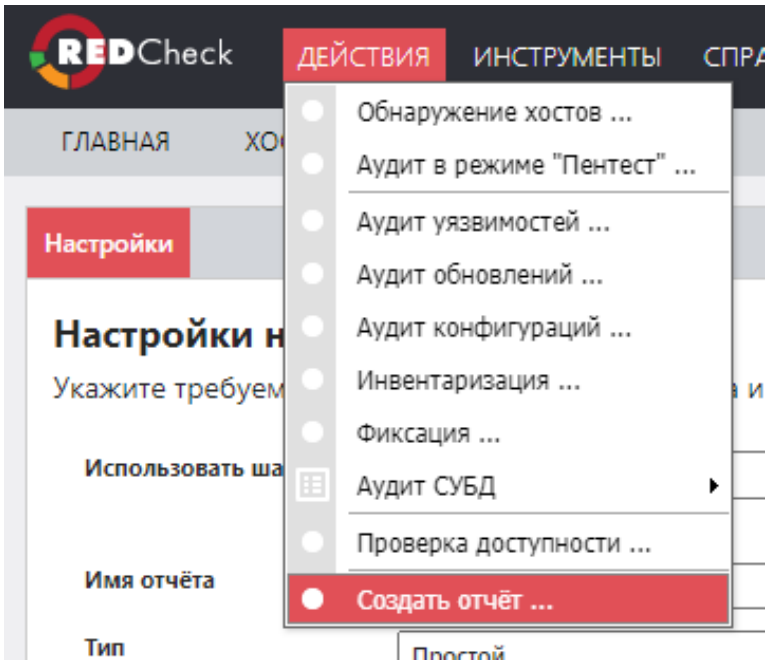


7.2 Создание дифференциального отчета

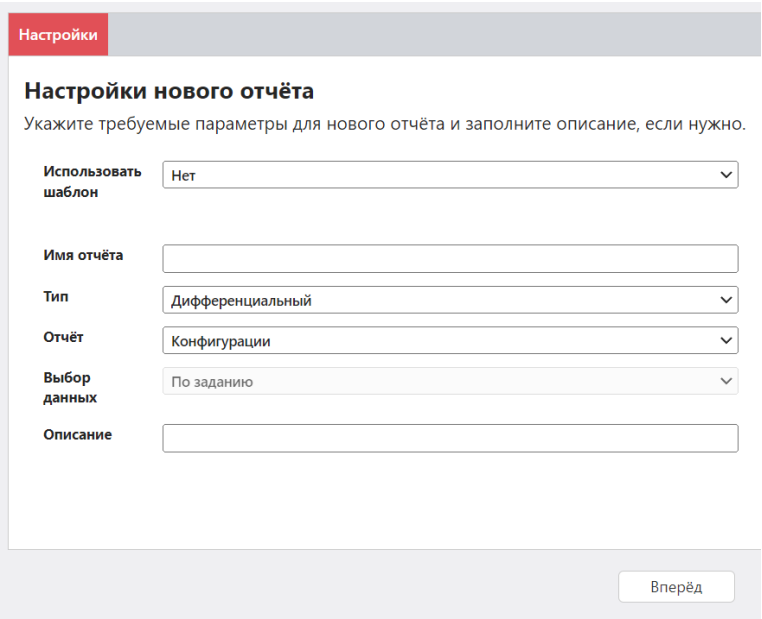
Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Чтобы создать дифференциальный отчет, выполните следующие шаги.

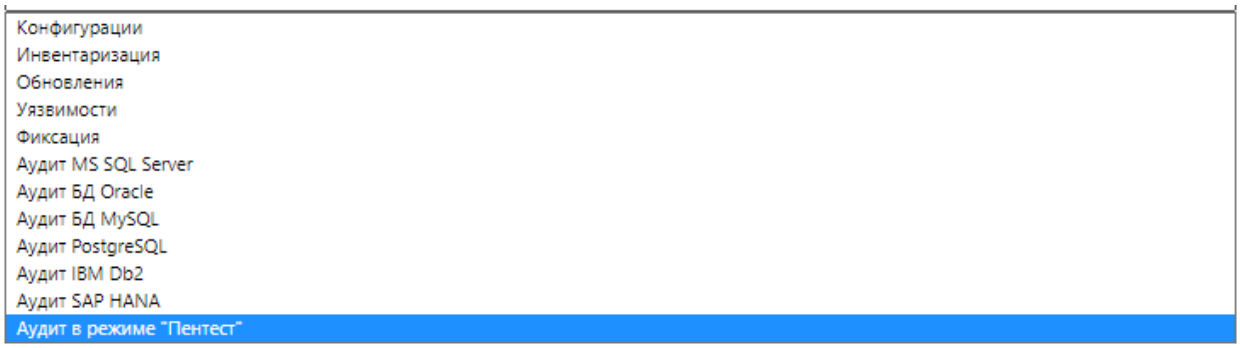
Шаг 1. Раскройте **Действия** → **Создать отчет**;



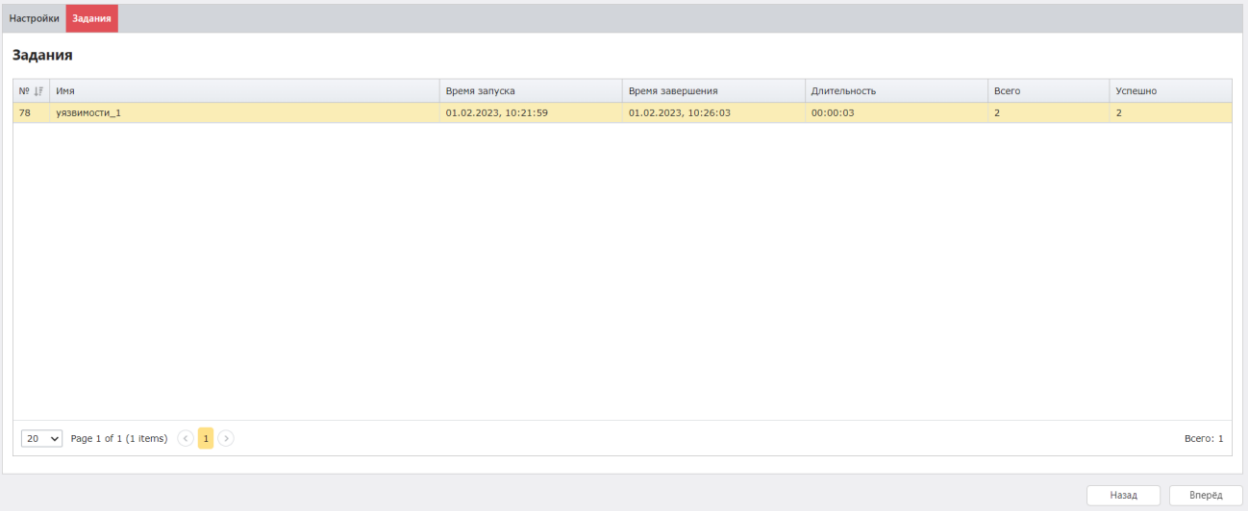
Шаг 2. Заполните начальную страницу мастера → **Вперед**:



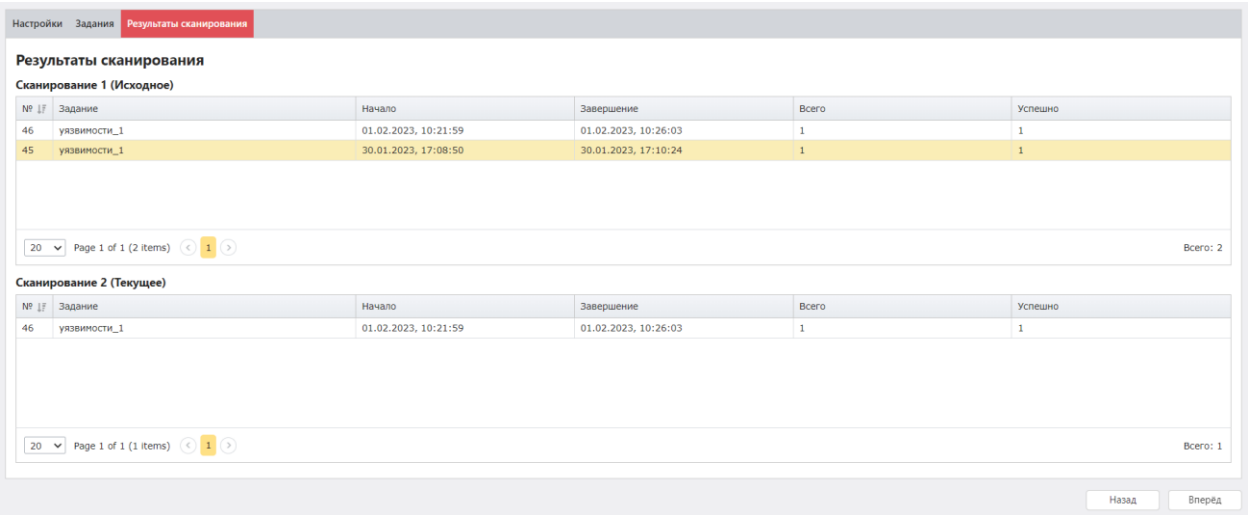
Отчет – тип данных, их которых будет создаваться отчет. В зависимости от выбранного значения последовательность создания отчета может измениться из-за дополнительных параметров;



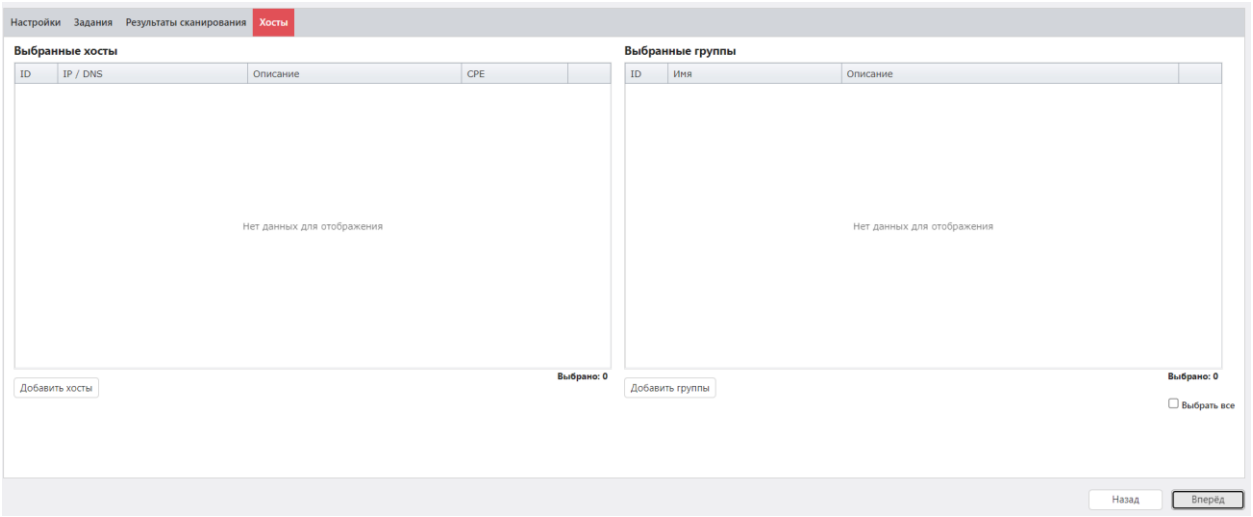
Шаг 3. Выберите задание → **Вперед**:



Шаг 4. Выберите в верхней таблице более ранний результат сканирования, после чего выберите в нижней таблице один из появившихся более поздних результатов → **Вперед**:



Шаг 5. Добавьте хосты (**Добавить хосты**) / группы (**Добавить группы**) из результата сканирования, которые хотите видеть в отчете → **Вперед**:



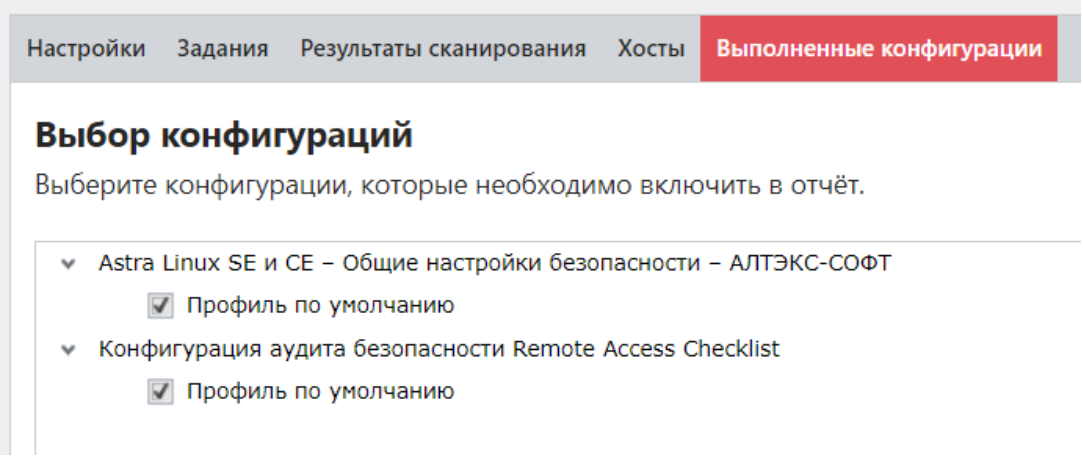
Шаг 6. Укажите дополнительные настройки для отчета (7.2.1 Настройки для разных типов заданий)

7.2.1 Настройки для разных типов задания

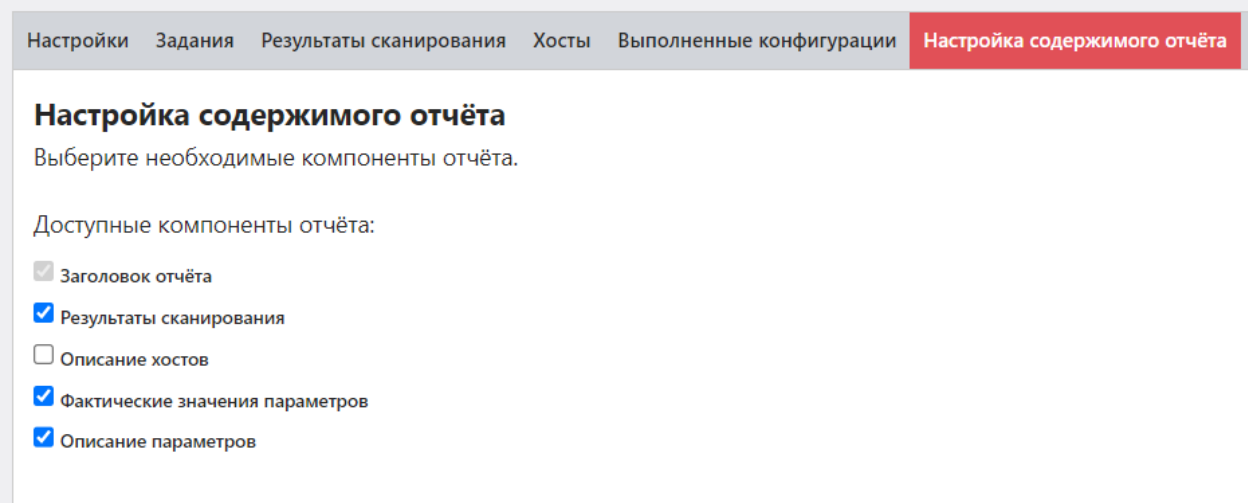
Содержание

Конфигурации

Выберите конфигурации, сравнение которых будет в отчете → **Вперед**;

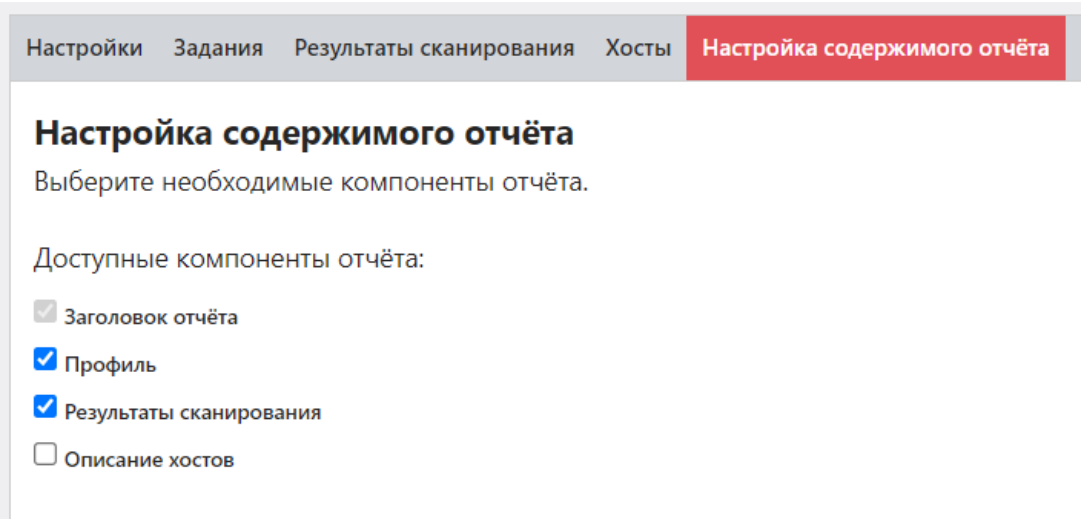


Укажите, что будет содержать отчет → **Создать**;



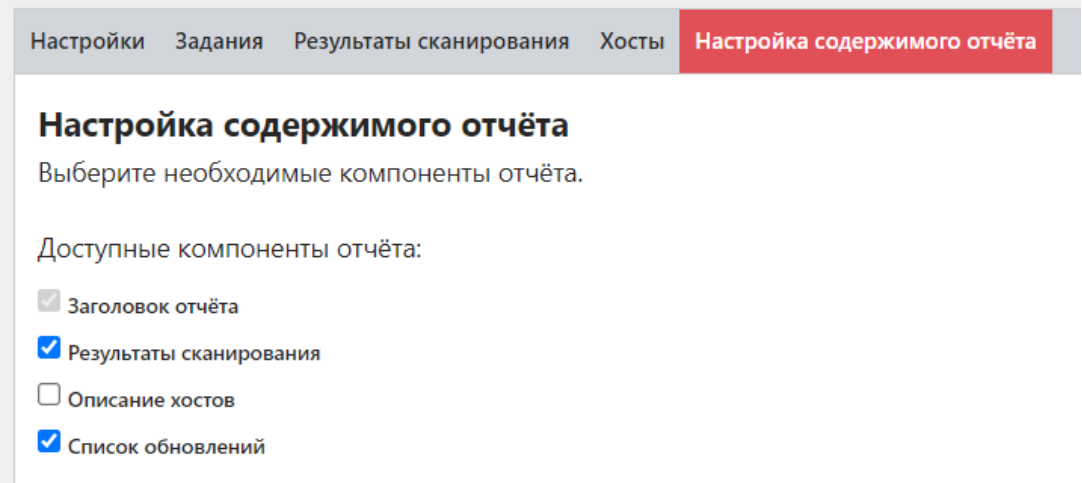
Инвентаризация

Укажите, что будет содержать отчет → **Создать**;



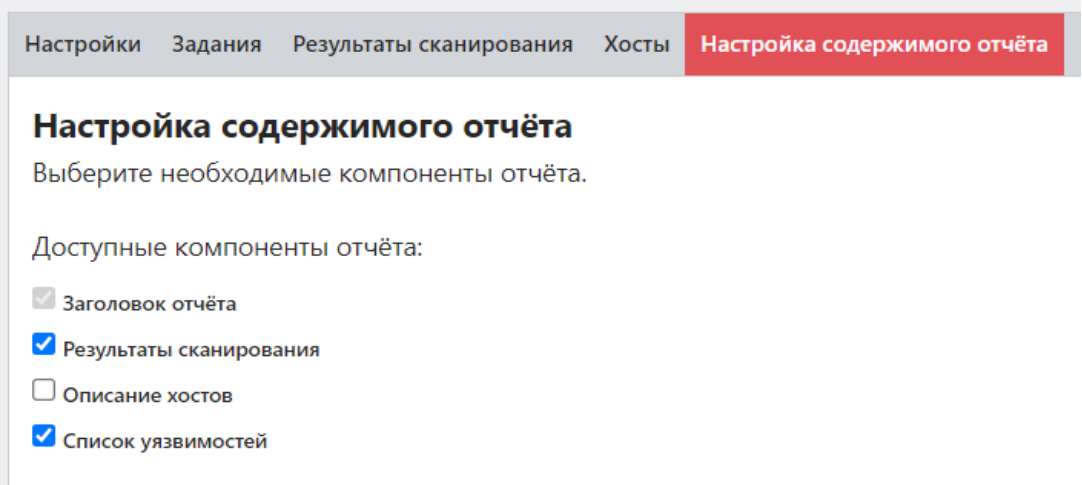
Обновления

Укажите, что будет содержать отчет → **Создать**;



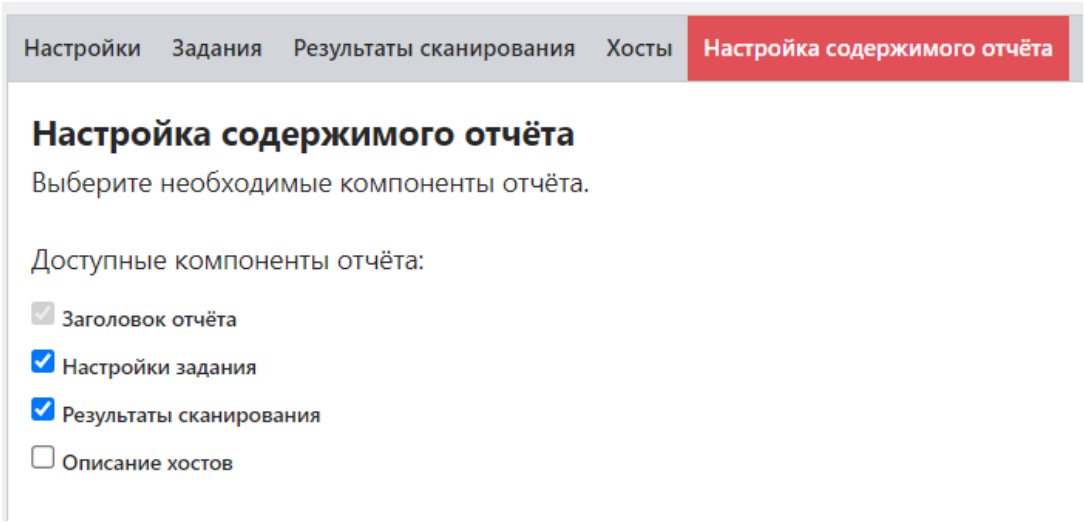
Уязвимости

Укажите, что будет содержать отчет → **Создать**;



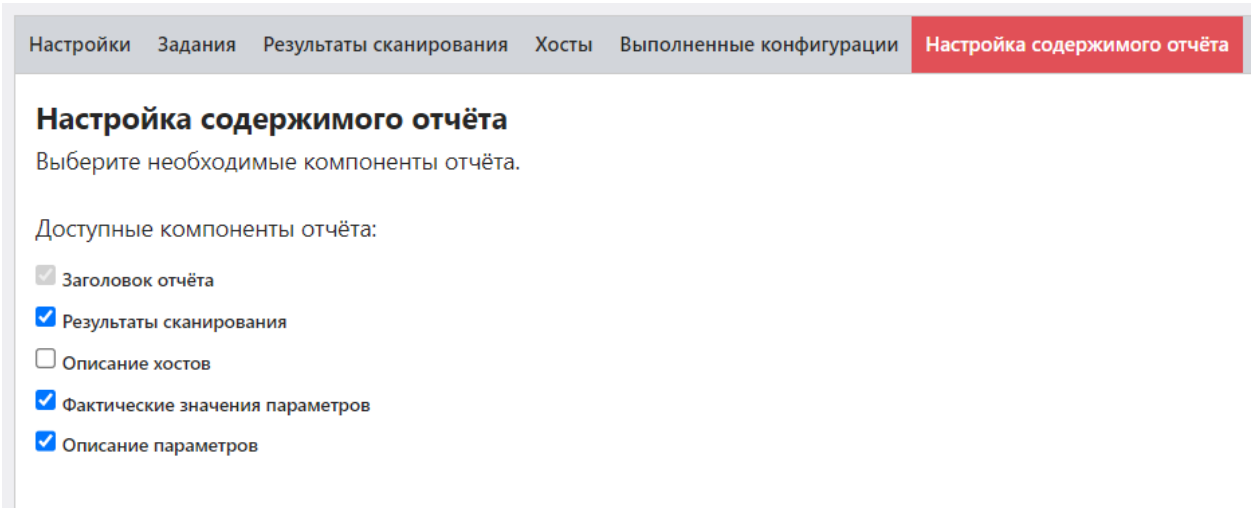
Фиксация

Укажите, что будет содержать отчет → **Создать**;



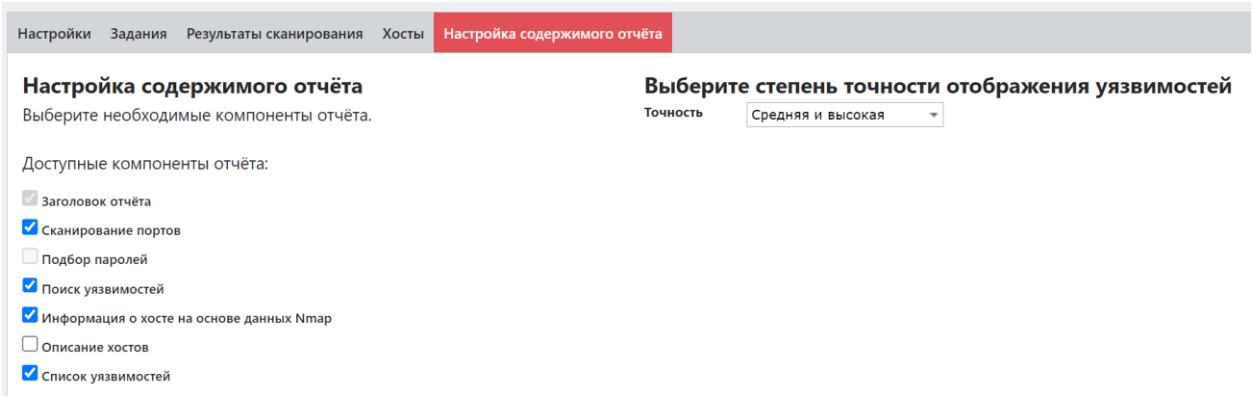
Аудит СУБД

Укажите, что будет содержать отчет → **Создать**;



Аудит в режиме «Пентест»

Укажите, что будет содержать отчет → **Создать**;


Настройки
Задания
Результаты сканирования
Хосты
Настройка содержимого отчёта
Настройка содержимого отчёта
Выберите необходимые компоненты отчёта.
Доступные компоненты отчёта:
Заголовок отчёта
Сканирование портов
Подбор паролей
Поиск уязвимостей
Информация о хосте на основе данных Nmap
Описание хостов
Список уязвимостей
Выберите степень точности отображения уязвимостей
Точность
Средняя и высокая

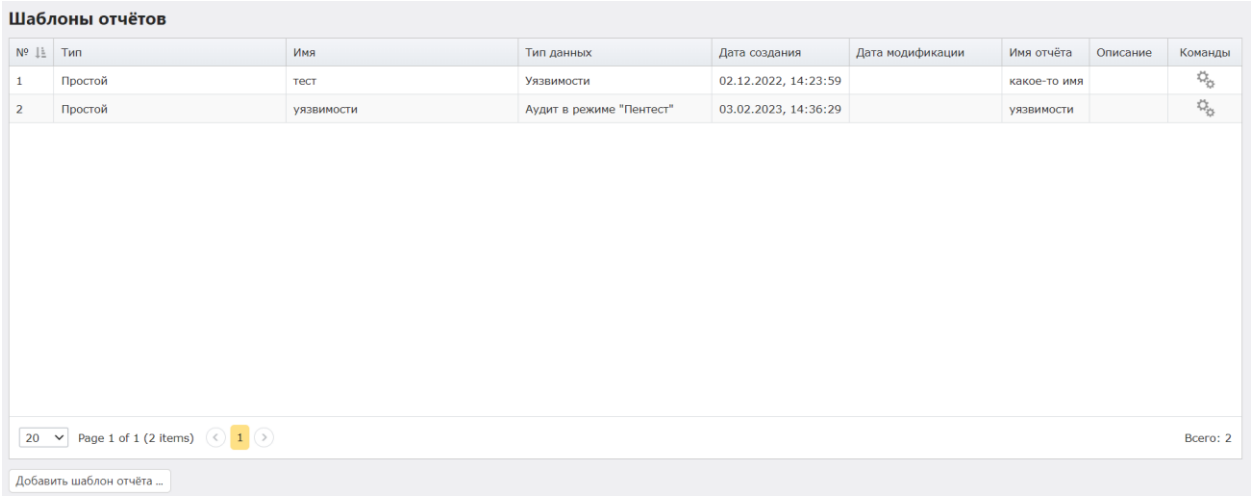
7.3 Шаблоны отчетов

Шаблоны отчетов позволяют автоматизировать создание отчетов, а также предоставляют гибкую настройку того, что будет включено в отчет.

> Шаблон отчетов может быть создан только для простых отчетов.

Пример создания и использования

Раскроем **Инструменты** → **Менеджер шаблонов отчетов** → нажмем **Добавить шаблон отчета**;

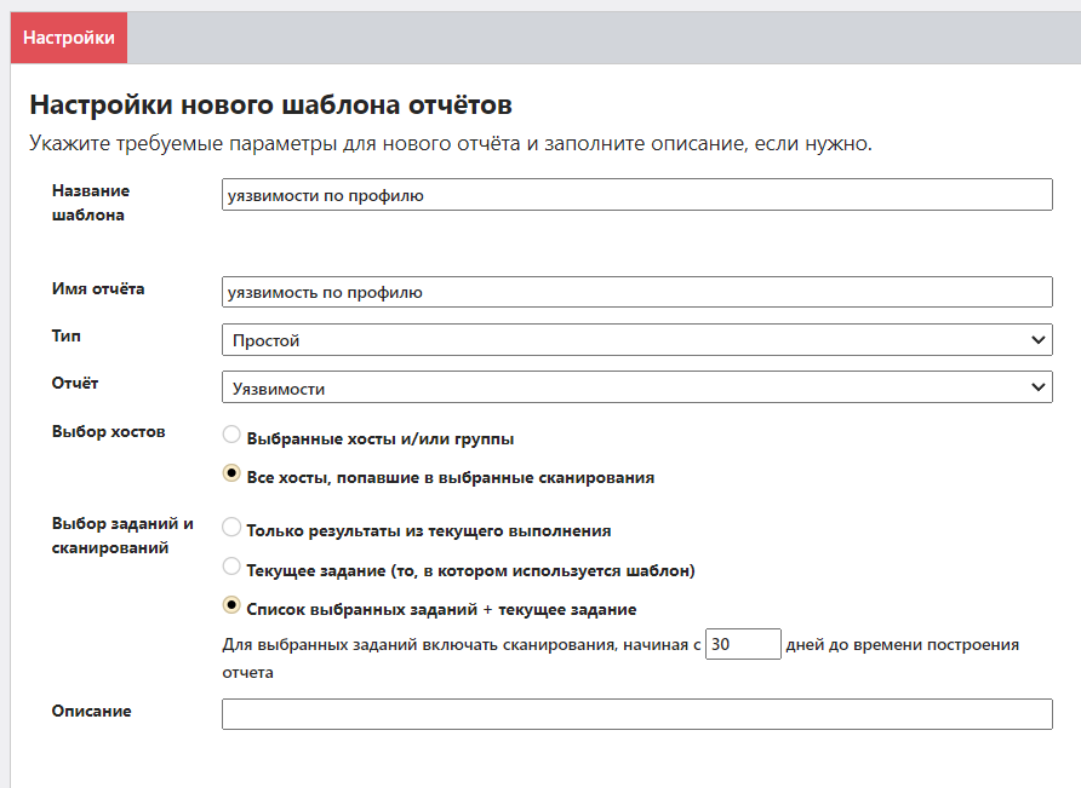


Заполним начальную форму в мастере → **Вперед**;

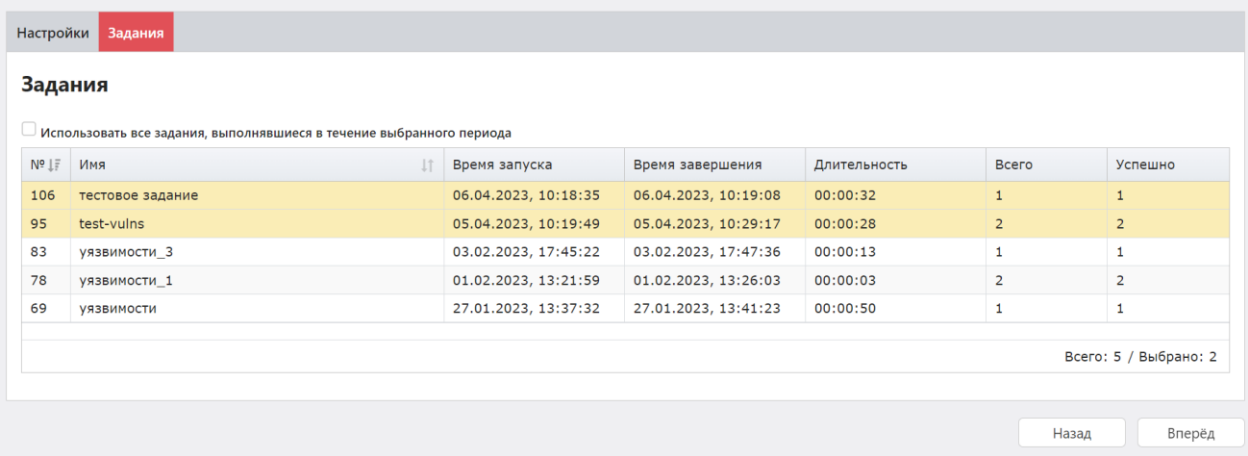
> **Выбор хостов:**
>
> - Выбранные хосты и/или группы – в отчет попадут выбранные хосты / группы;
> - Все хосты, попавшие в выбранные сканирования – в отчет будут включены хосты в соответствии со значением следующего параметра;
>
> **Выбор заданий и сканирований:**
>
> - Только результаты из текущего выполнения – в отчете будут результаты

выполнения задания, в котором используется шаблон;

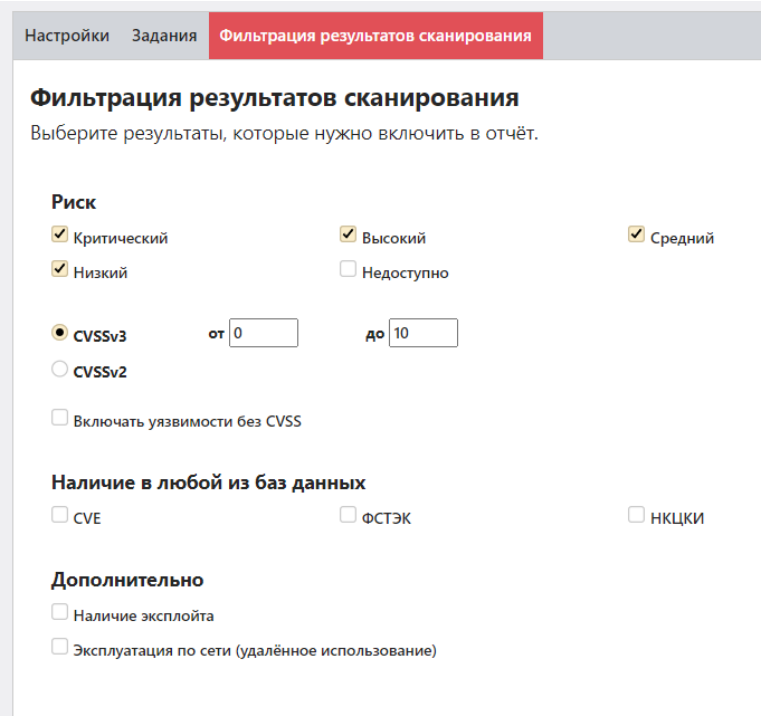
- Текущее задание (то, в котором используется шаблон) – в отчет будут добавлены актуальные результаты сканирования задания, в котором используется шаблон, начиная с N (указывается число) дней до текущего времени построения отчета;
- Список выбранных заданий + текущее задание – в отчет будут добавлены актуальные результаты сканирования выбранных заданий, начиная с N (указывается число) дней до текущего времени построения отчета;



Выберем задания, которые будут попадать в отчет → **Вперед**;

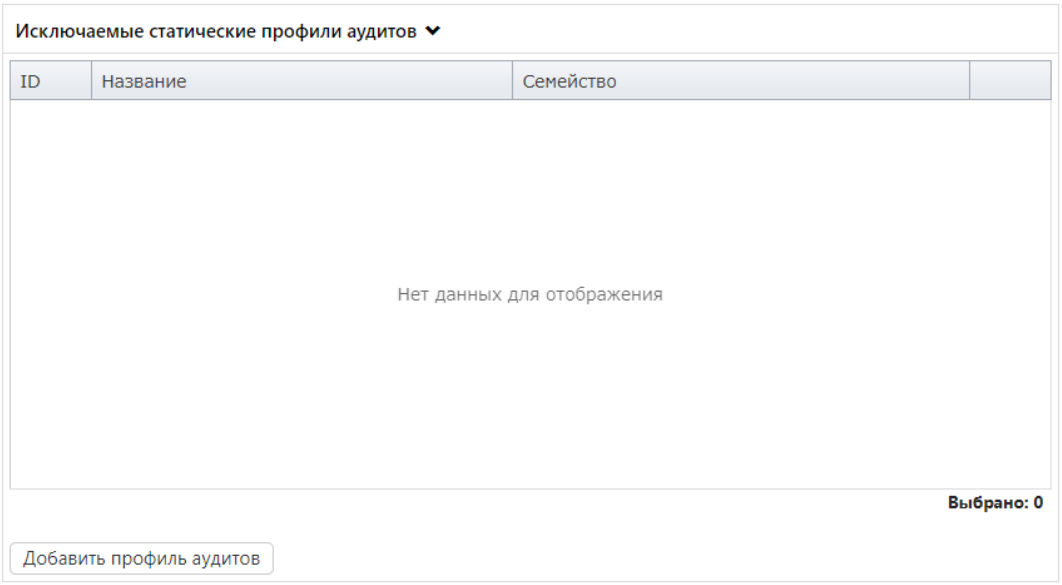


Укажем следующие параметры для фильтрации результатов сканирования.

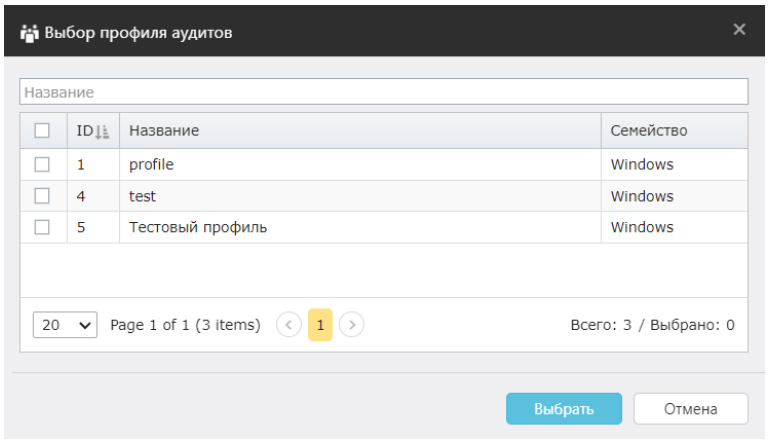


Укажем профиль аудитов для исключения некоторых уязвимостей из отчета.

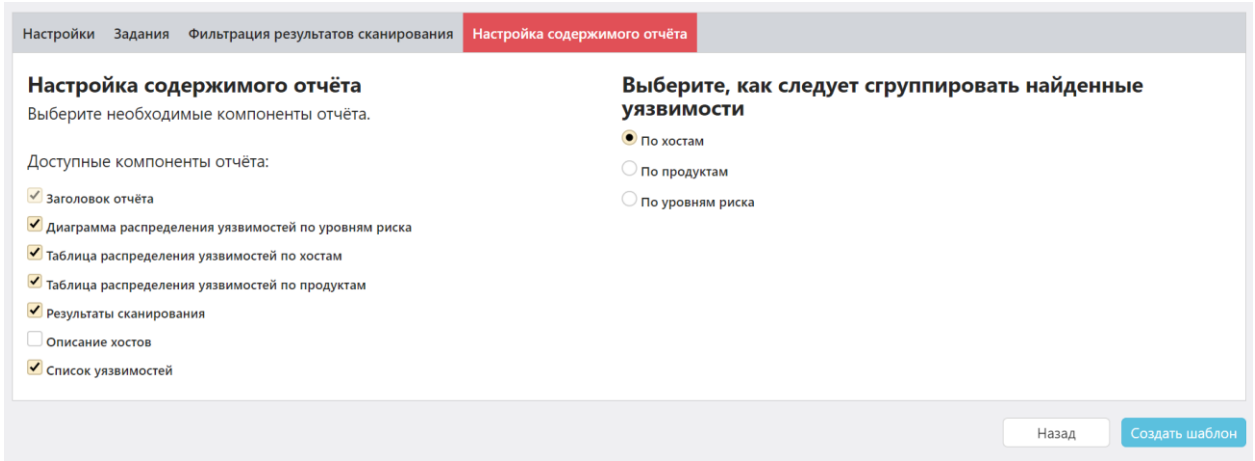
Раскроем список **Исключаемые статические профили аудитов → Добавить профиль аудитов**;



Выберем профиль → **Выбрать** → **Вперед**;

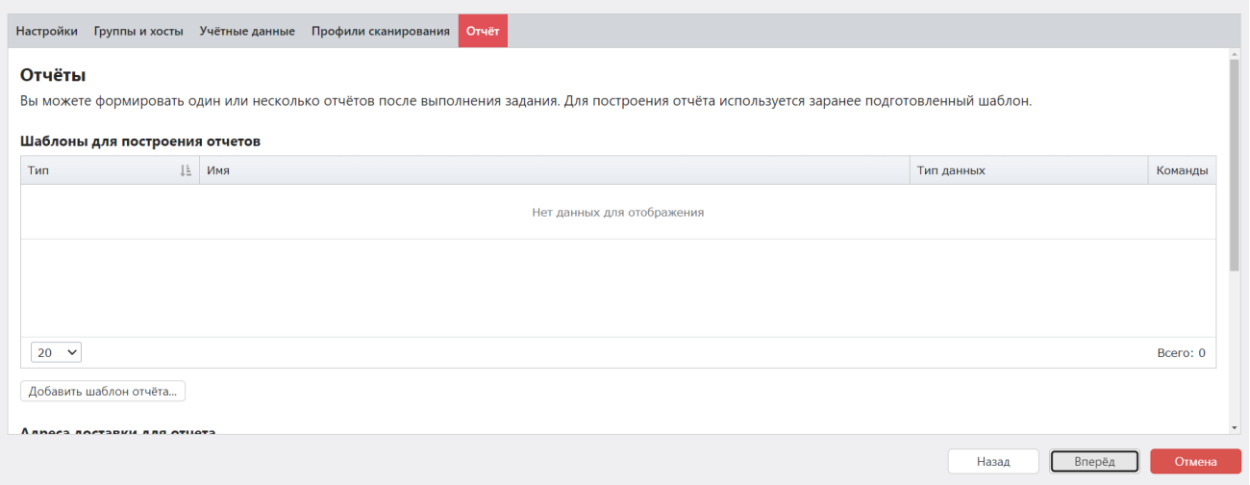


Укажем настройки содержимого отчета и группировки → **Создать шаблон**.



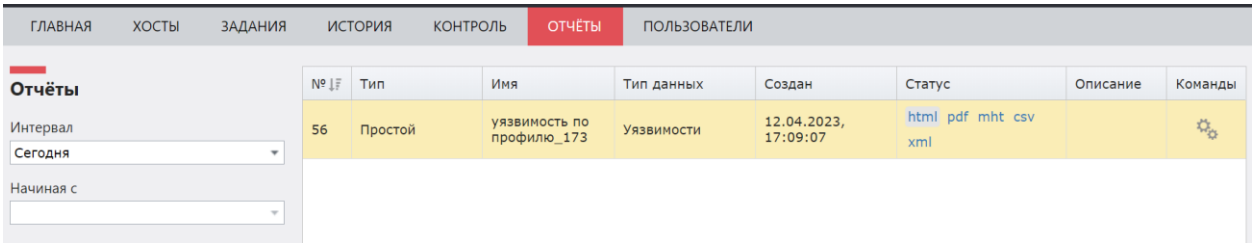
Настройки шаблона отличаются друг от друга в зависимости от выбранного типа задания (7.3.1 Настройки для разных типов задания).

Создадим задание Аудит уязвимостей. На шаге Отчет → **Добавить шаблон отчета** → выберем шаблон → **Выбрать** → **Вперед**;



После завершения сканирования посмотрим созданный по шаблону отчет.

Перейдем в **Отчеты** и скачаем в формате html отчет.



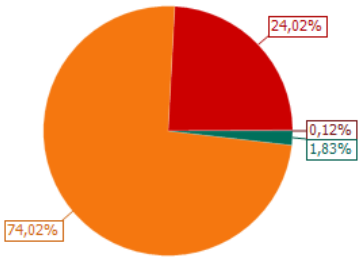
Отчет был создан и в него попали все результаты сканирования, полученные в течении прошедших 30 дней для указанных заданий в шаблоне отчета.

RED Check

ОТЧЁТ

№ отчёта	*dcd4f077-69c8-4c63-98d9-0248742510d5*
Профиль	*Уязвимости*
Задания	*тест шаблона, тестовое задание*
Начало/завершение сканирования	*06.04.2023 10:18:37 / 12.04.2023 17:08:58*
Формирование отчёта	*12.04.2023 17:09:07*
Имя	*уязвимость по профилю_173*
Хосты [3]	*10.0.0.182, 10.0.0.175, 10.0.0.183*

Диаграмма распределения уязвимостей по уровням риска



Риск	Количество
Критический	*2*
Высокий	*393*
Средний	*1211*
Низкий	*30*
Всего	*1636*

Фильтрация результатов сканирования	
Уровни риска	*Критический, Высокий, Средний, Низкий*
CVSSv3, от	*0*
CVSSv3, до	*10*
CVSSv2 (при отсутствии CVSSv3), от	*0*
CVSSv2 (при отсутствии CVSSv3), до	*10*
Включать уязвимости без CVSS	*Нет*
Исключаемые статические профили аудитов	*profile (windows)*

Таблица распределения уязвимостей по хостам

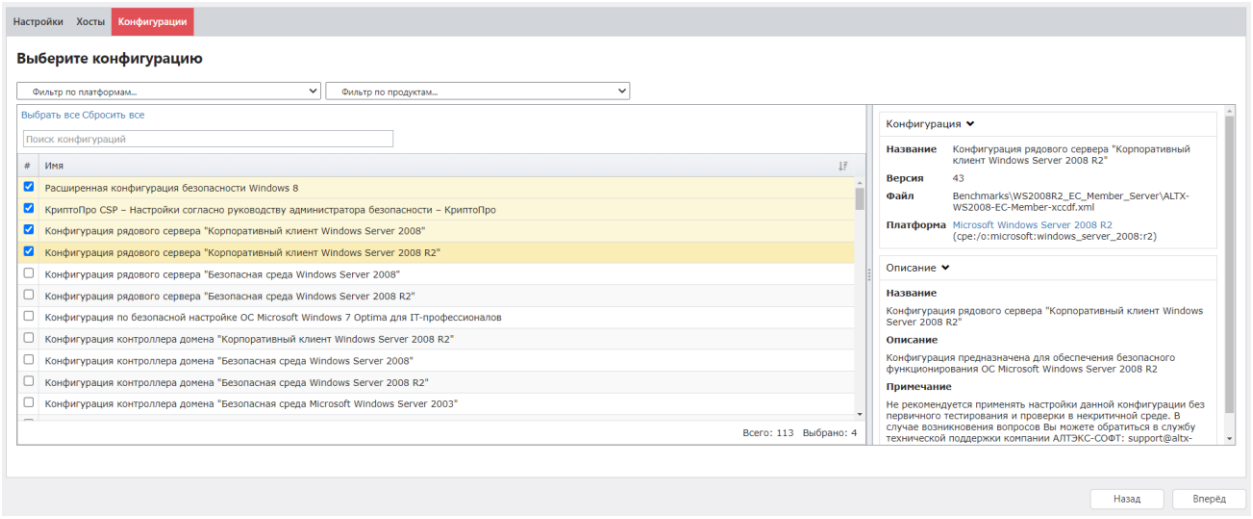
Хост / Риск	Критический	Высокий	Средний	Низкий	Всего

7.3.1 Настройки для разных типов задания

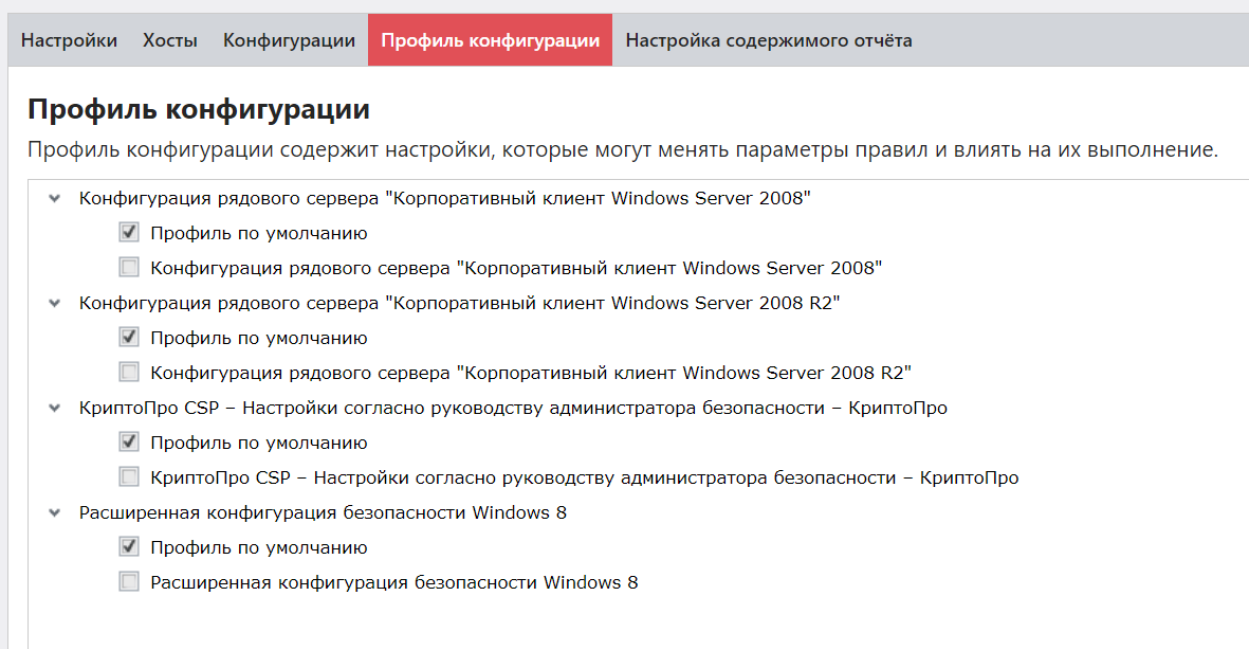
Содержание

Конфигурации

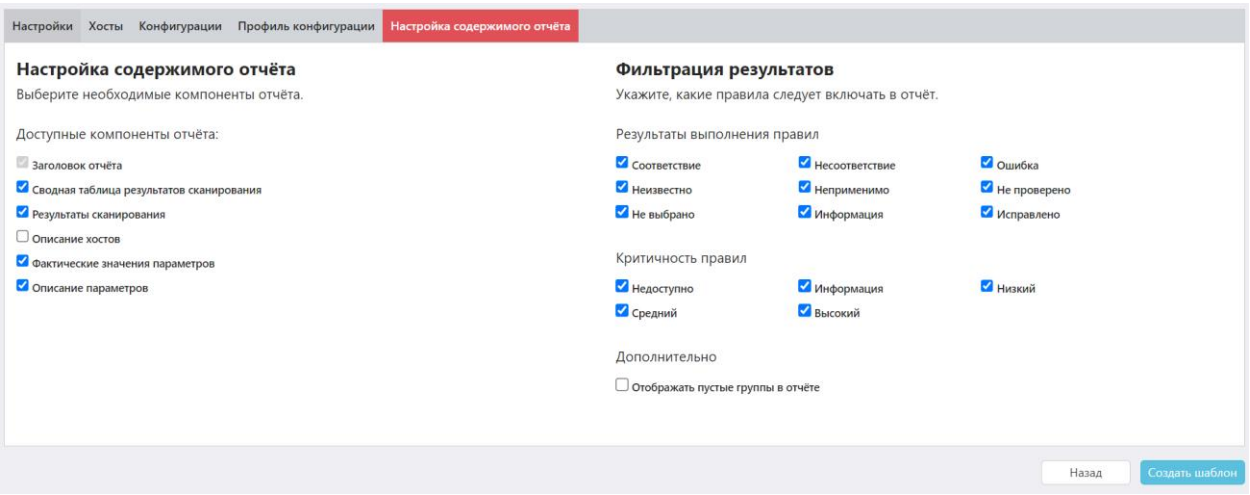
Выберите конфигурации из общего списка, которые попадут в отчет, если будут в результате сканирования → **Вперед**;



Отметьте профили конфигурации для отчетов, использующих шаблон → **Вперед**;

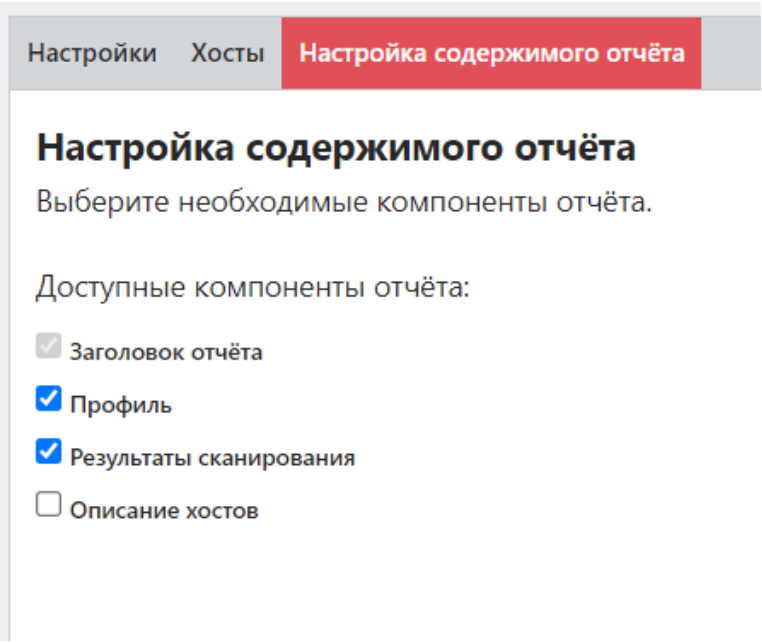


Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;



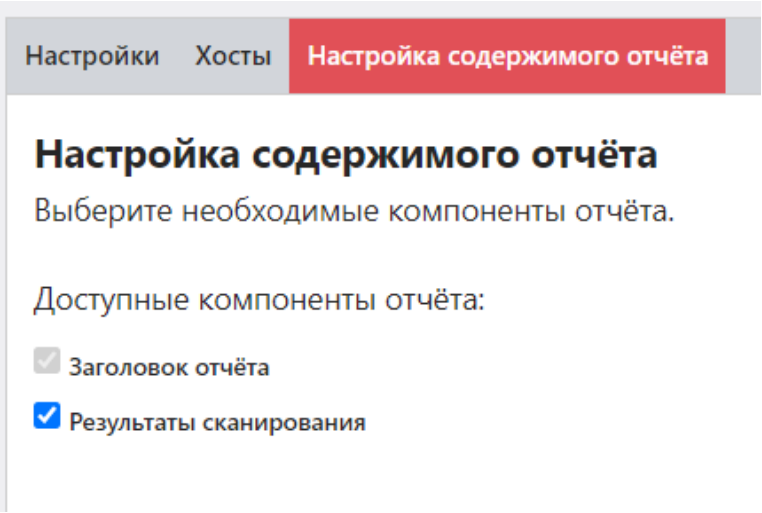
Инвентаризация

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;



Обновления

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;

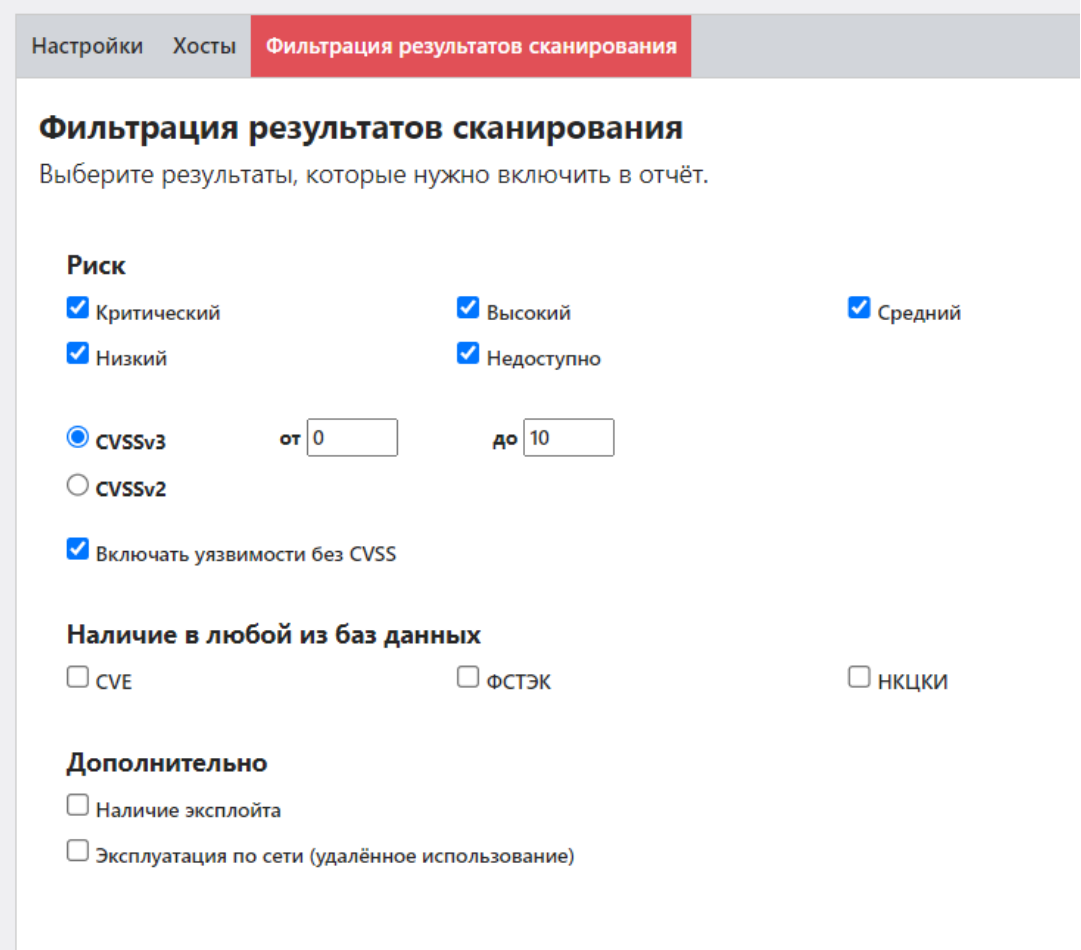


Уязвимости

Укажите настройки для фильтрации результата сканирования → **Вперед**:

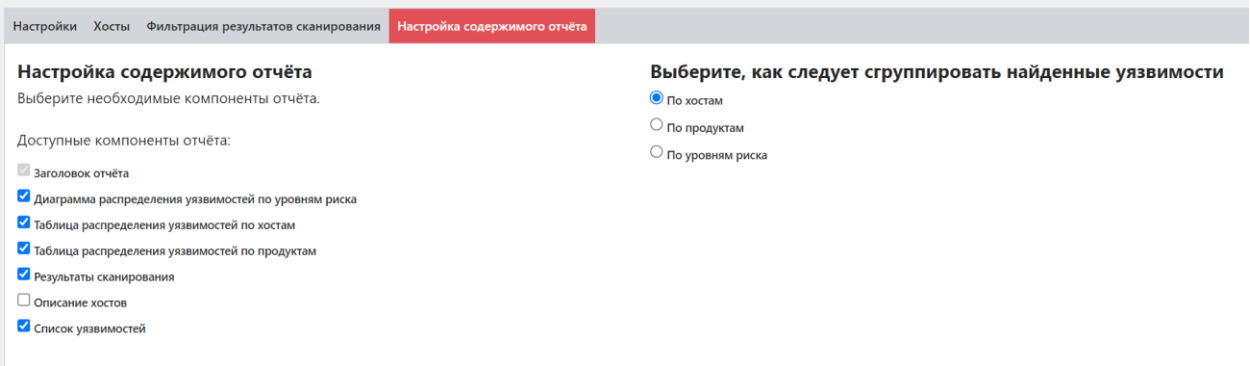
- Риск – фильтрация по категориям риска;
- В отчет попадут только те уязвимости, метрика CVSS которых будет в указанном интервале;

- Включать уязвимости без CVSS – в отчете будут уязвимости, CVSS для которых не было определено;
- Дополнительно:
  - Наличие эксплойта – OVAL-определение имеет эксплойт;
  - Эксплуатация по сети – эксплойт можно воспроизвести удаленно;



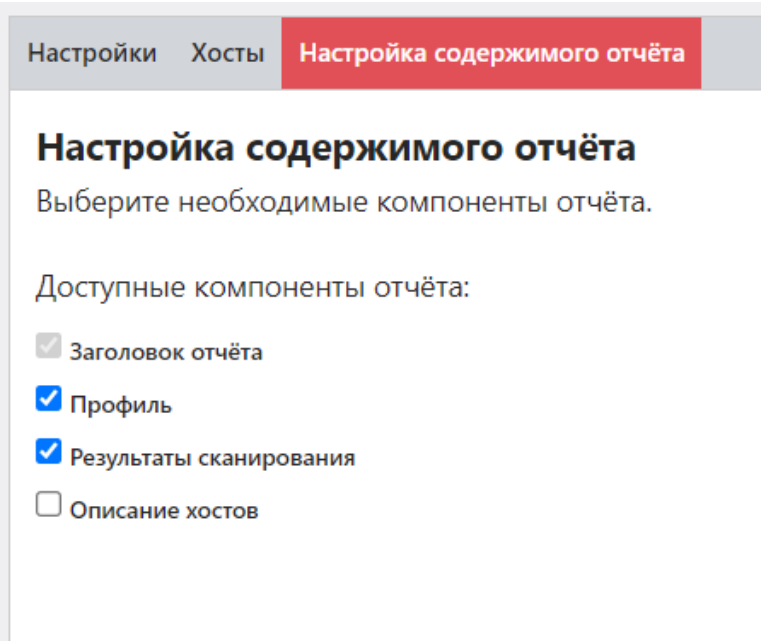
К отчету можно применить профиль сканирования (5.1 Профили сканирования).

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;



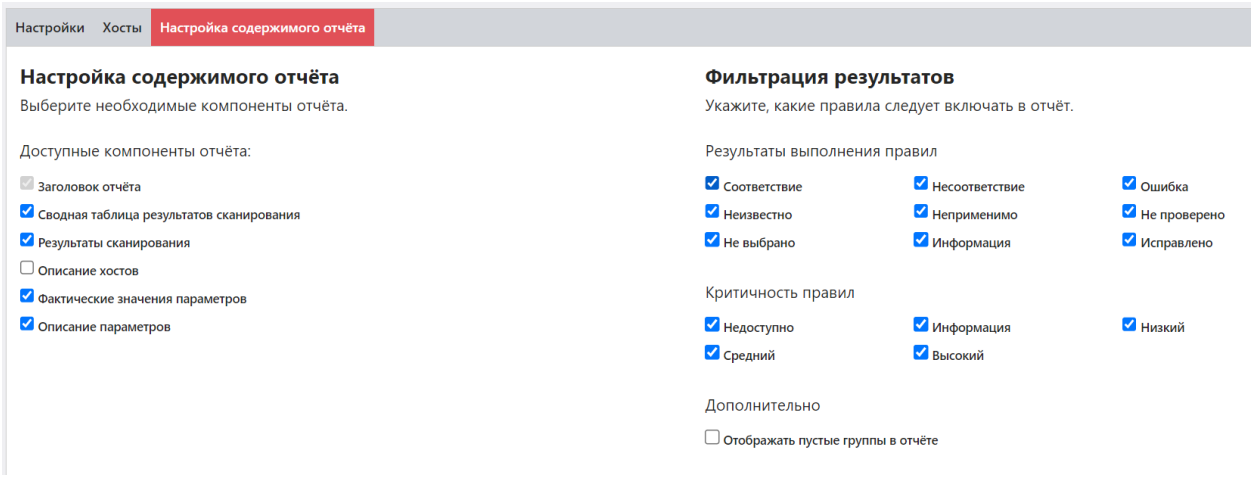
Фиксация

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;



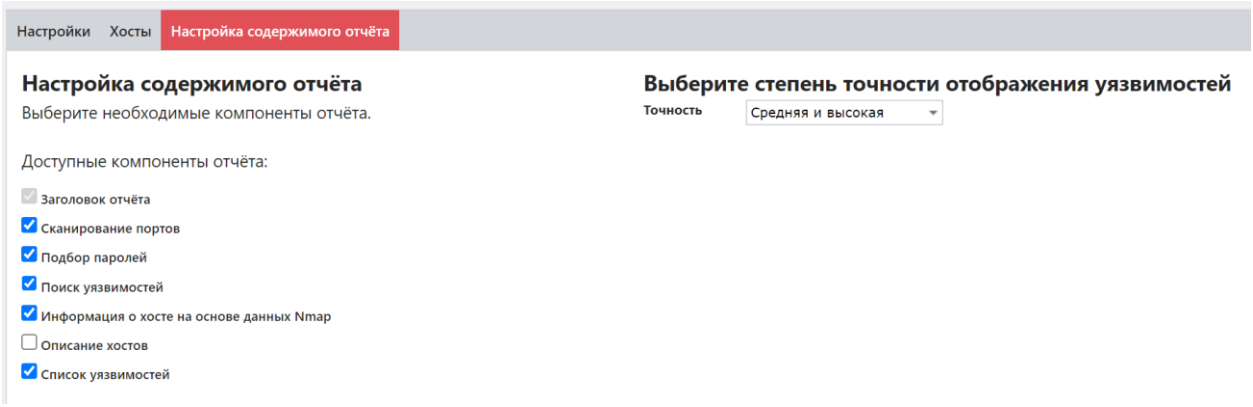
Аудит СУБД

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;



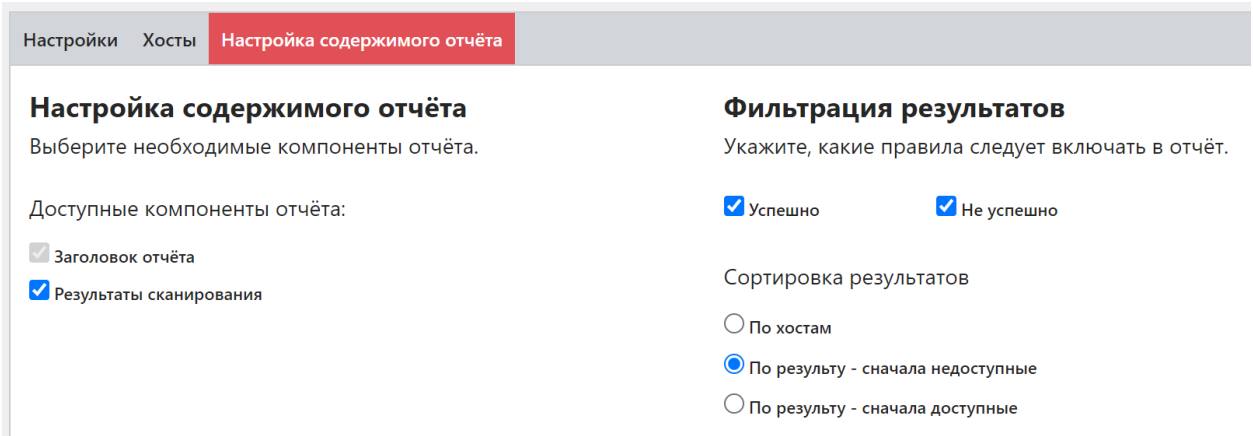
Аудит в режиме «Пентест»

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;



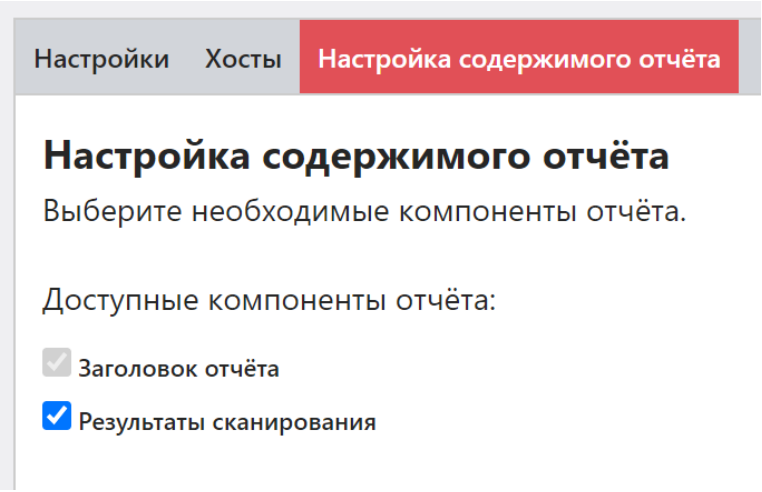
Проверка доступности

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;



Обнаружение хостов

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;



7.4 Просмотр CSV отчетов

В RedCheck отчет в формате csv соответствует стандарту RFC 4180. Это означает, что разделителем между столбцами является запятая.

Разные офисные пакеты открывают отчет в формате csv по-разному. Это приводит к ошибкам отображения. Ниже предлагаются инструкции правильного открытия csv отчетов для следующих офисных пакетов:

- Microsoft Excel;
- R7 Офис;
- Libre Office / Open Office;

Microsoft Excel

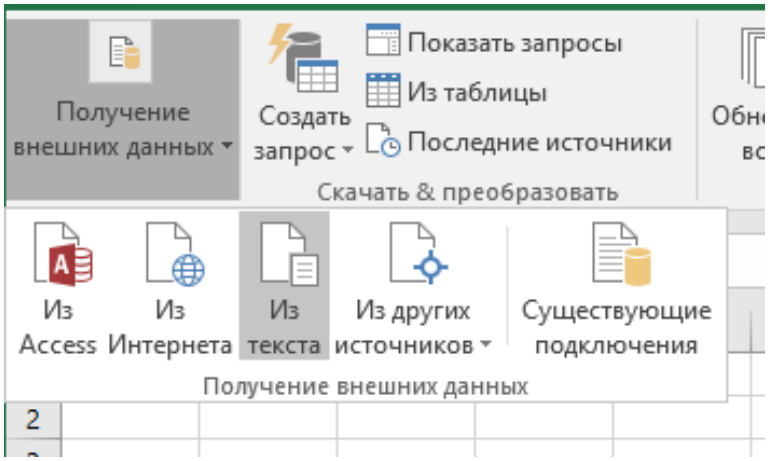
> В примере используется Excel 2016. Для других версий шаги идентичны.

1-й способ

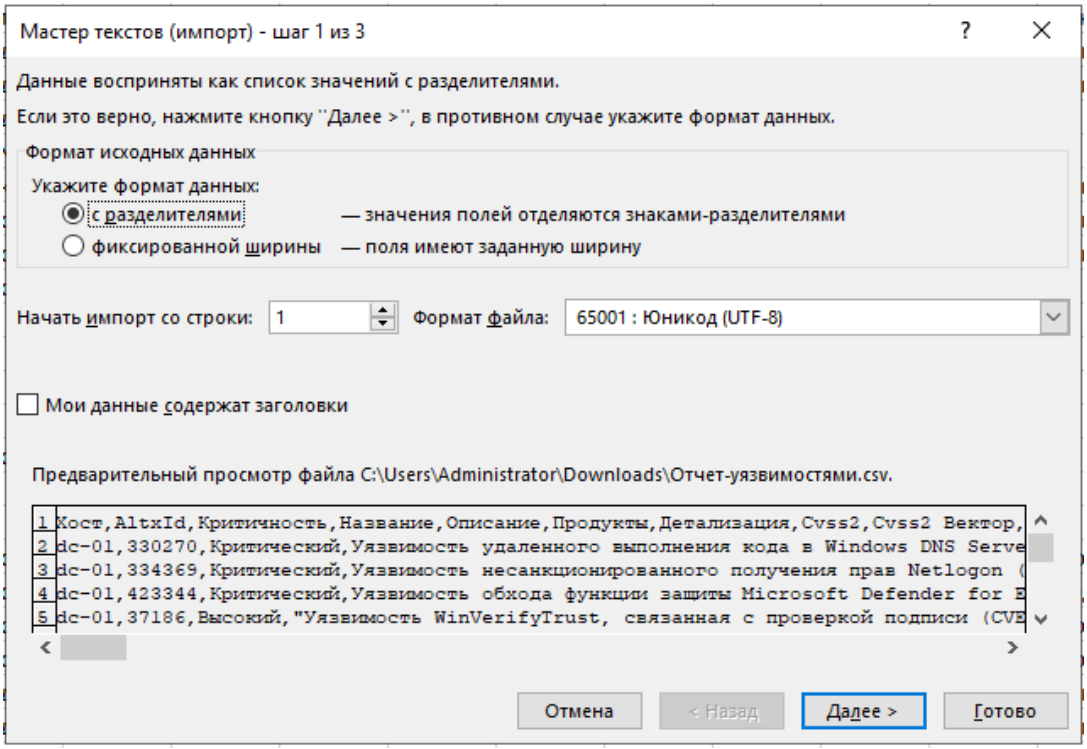
Нажмите **Файл** → **Открыть** → выберите отчет в формате csv;

2-й способ

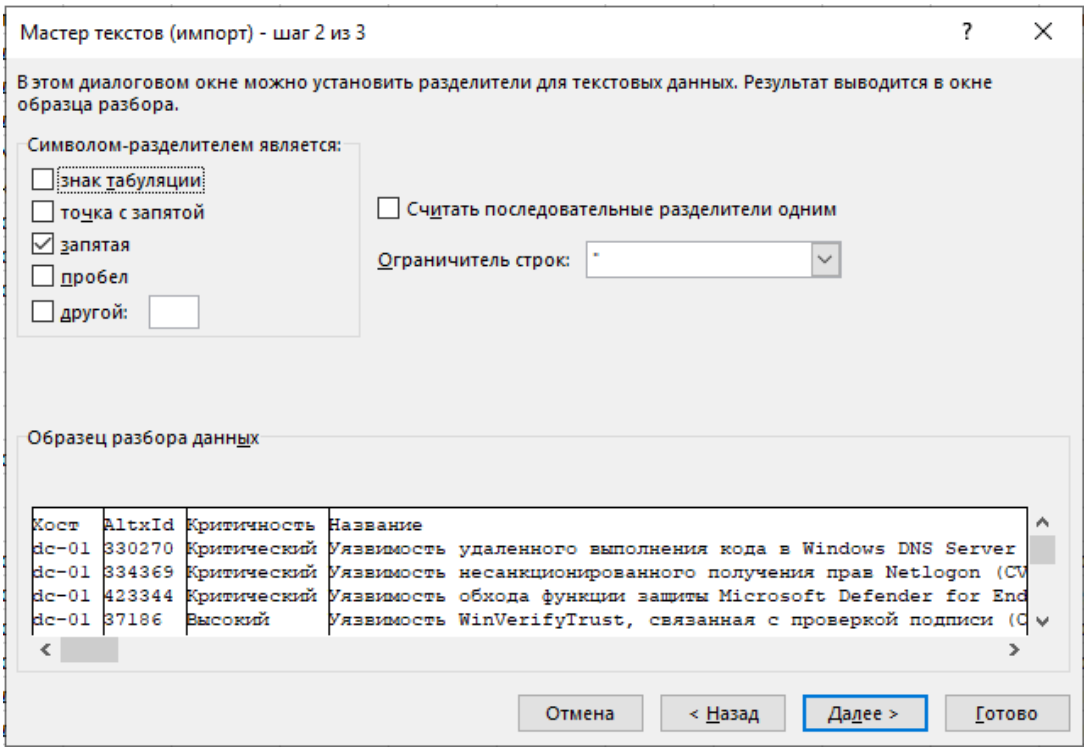
Нажмите **Данные** → **Получение внешних данных** → **Из текста** → выберите отчет в формате csv;



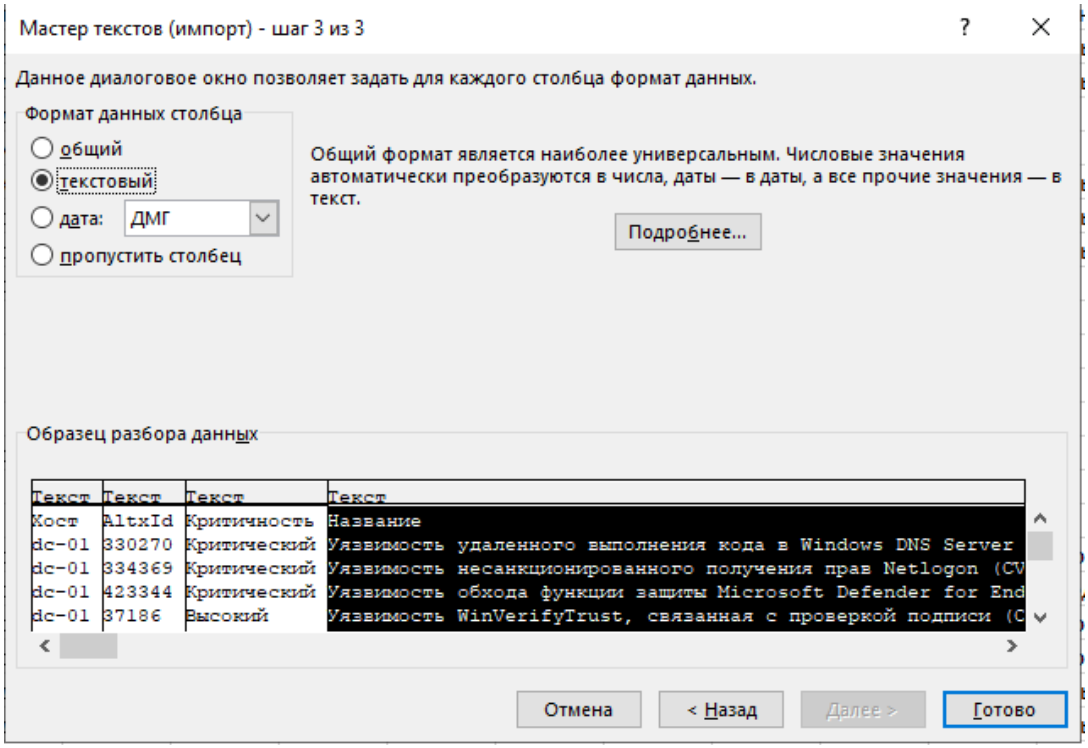
Шаг 1. В появившемся окне укажите формат данных **с разделителями** → **Далее**;



Шаг 2. Отметьте **запятая** в списке **Символом-разделителем является** → **Далее**;



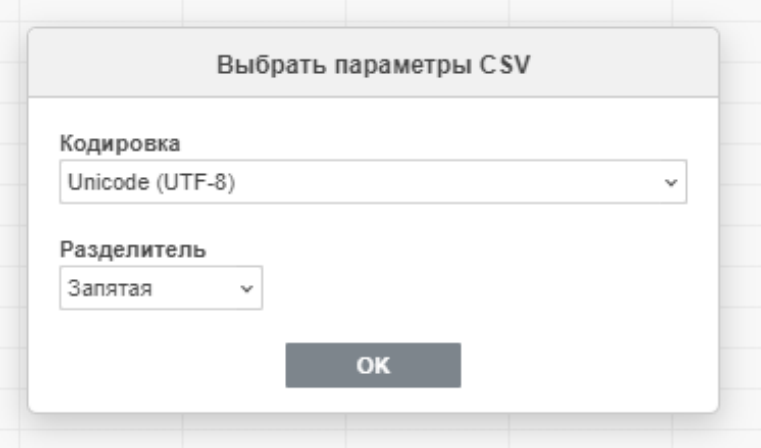
Шаг 3. Для каждого столбца укажите **текстовый** формат данных → **Готово**;



Это необходимо для корректного отображения вещественных чисел, которые Microsoft Excel по умолчанию пытается представить в виде даты.

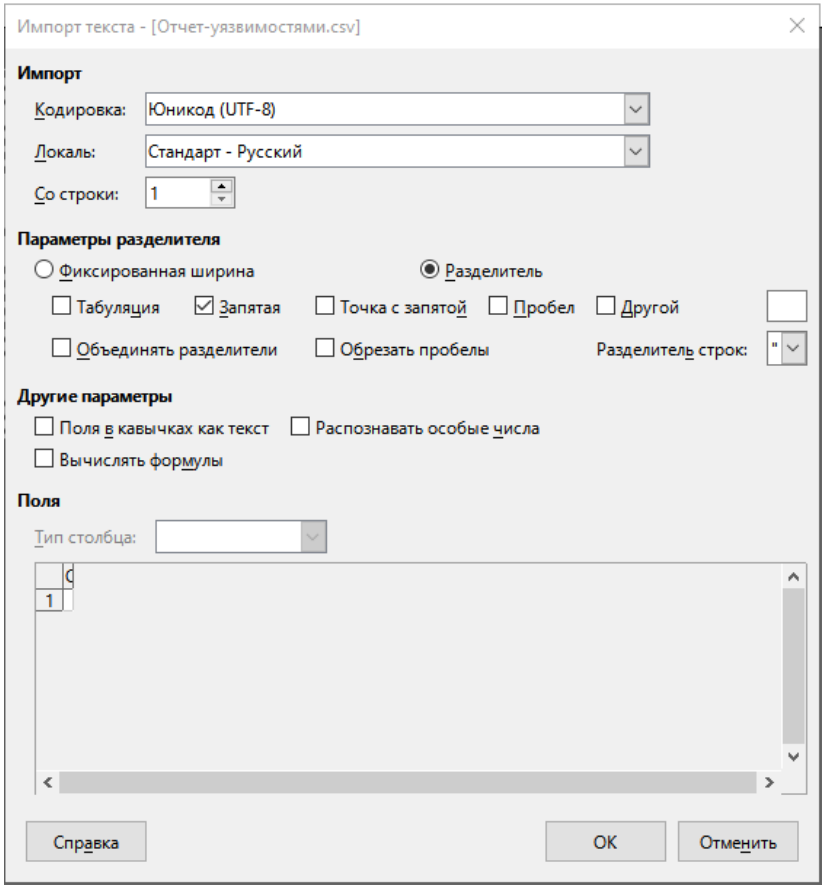
R7 Офис

Откройте csv отчет с помощью R7 Офиса → в появившемся окне выберите **Запятая** из списка **Разделитель** → **ОК**;



Libre Office / Open Office

Откройте csv отчет с помощью Libre Office → в появившемся окне выберите **Разделитель** в **Параметры разделителя** → отметьте **Запятая** → **ОК**;


Импорт текста - [Отчет-уязвимостями.csv]
Импорт
Кодировка:
Юникод (UTF-8)
Локаль:
Стандарт - Русский
Со строки:
1
Параметры разделителя
Фиксированная ширина
Разделитель
Табуляция
Запятая
Точка с запятой
Пробел
Другой
Объединять разделители
Обрезать пробелы
Разделитель строк:
Другие параметры
Поля в кавычках как текст
Распознавать особые числа
Вычислять формулы
Поля
Тип столбца:
1
Справка
OK
Отменить

8 Аналитика

Модуль Аналитики необходим для контроля сканирования инфраструктуры, анализа и устранения уязвимостей и соответствия конфигурациям безопасности. Инструмент позволяет точно определить как проблемы доступа к хостам, так и анализ их сканирования в регламент.

Анализ уязвимостей позволяет определить появление новых угроз, количество не устраненных, а также отдельный список по закрытым проблемам безопасности, в указанный пользователем регламент (срок анализа в днях).

Данный функционал приближает классический сканер безопасности RedCheck к возможностям мощных VM-решений без необходимости проводить интеграции и управлять уязвимостями по результатам сканирования в едином интерфейсе.

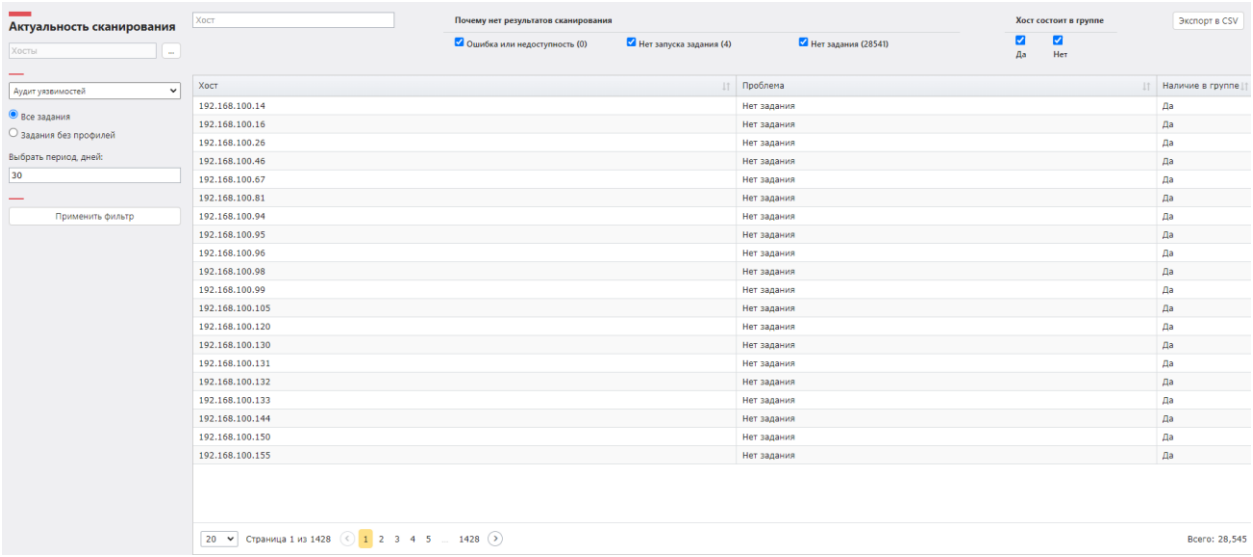
> Доступно только для редакций Expert и Enterprise

Содержание

8.1 Актуальность сканирования

Данная форма аналитики позволяет определить, какие хосты и по какой причине не были успешно просканированы за указанный период.

Для перехода на форму нажмите **Аналитика** → **Актуальность сканирования**



Поддерживается 4 типа сканирования:

- Аудит уязвимостей;
- Аудит обновлений;
- Аудит конфигураций;
- Аудит в режиме «Пентест».

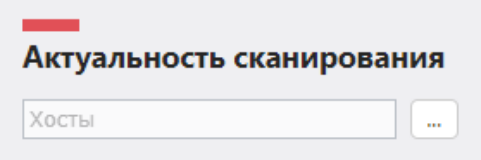
Информация об актуальности сканирования включает в себя:

- Хост – IP-адрес или DNS-имя хоста;
- Проблема – отображает информацию о том, почему нет результата сканирования. Может принимать 3 значения:
  - Ошибка или недоступность – сканирование хоста завершилось с ошибкой, или хост оказался недоступен;
  - Нет запуска задания – хост входит в список целей какого-либо задания, но задание ни разу не было запущено;
  - Нет задания – хост не входит в список целей ни для одного задания;

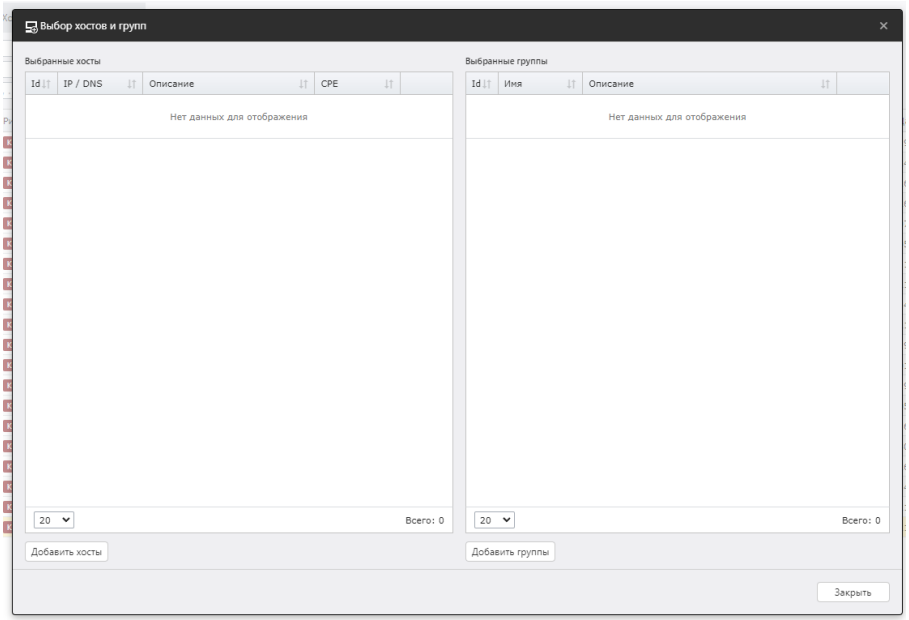
- Наличие в группе – находится ли хост в какой-либо группе.

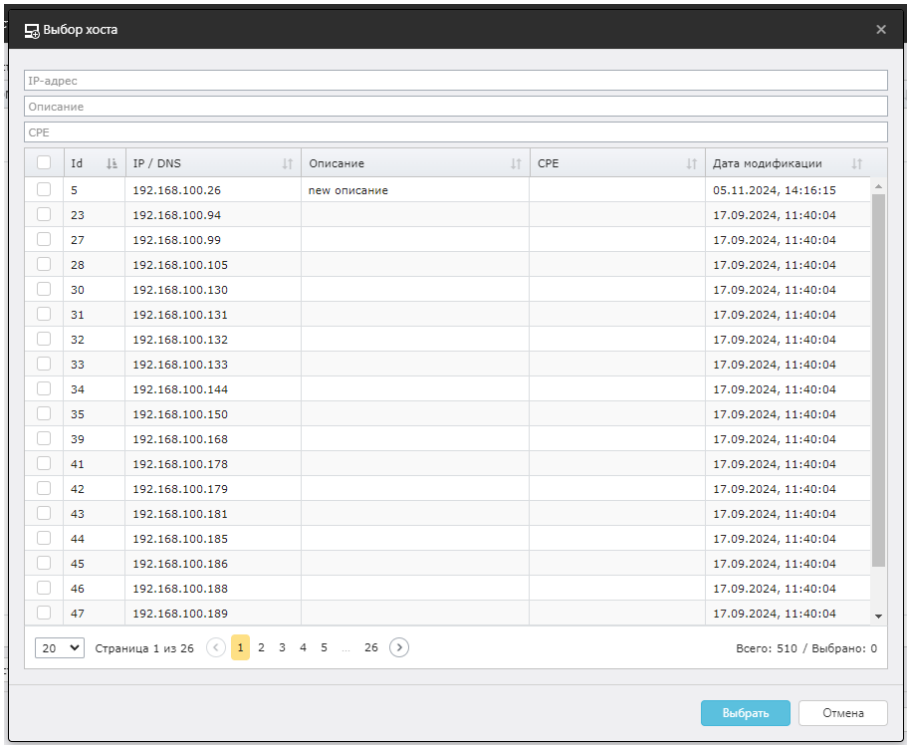
Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

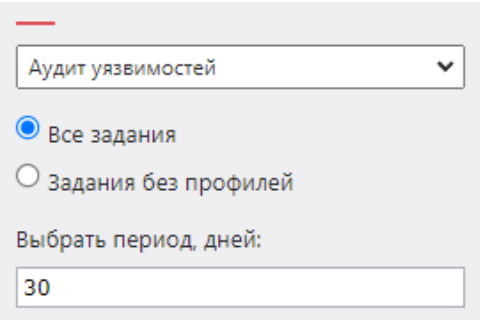


- Хосты – можно выбрать хосты, уязвимости для которых будут отображаться. Нажмите на ..., после чего откроется окно выбора групп и хостов:

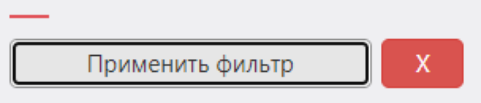




- Тип сканирования – для какого типа сканирования проверять результаты сканирования хостов;
    - Для аудита уязвимостей / обновлений – учитывать или нет задания с профилями сканирования (5.1 Профили аудитов);
- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для поиска проблем;



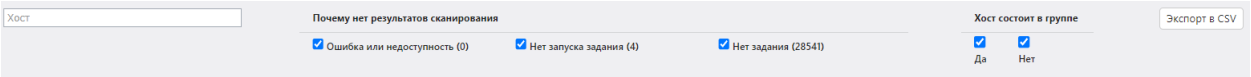
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра.

- Хост – IP-адрес или DNS-имя хоста. Можно указывать как полное значение, так и часть;
- Почему нет результатов сканирования – отображать только те хосты, у которых Проблема совпадает с отмеченными. Также показывает количество хостов для каждого типа Проблемы. Можно фильтровать по трем значениям:
  - Ошибка или недоступность – сканирование хоста завершилось с ошибкой, или хост оказался недоступен;
  - Нет запуска задания – хост входит в список целей (в том числе в составе группы) какого-либо задания, но задание ни разу не было запущено;
  - Нет задания – хост не входит в список целей (в том числе в составе группы) ни для одного задания;
- Хост состоит в группе – отображать хосты согласно тому, состоят они в какой-либо группе или нет.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая находится в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **ScanningRelevance-dd-mm-yyyy.csv**.

Структура CSV файла

Id хоста	ID хоста

Имя хоста	IP-адрес или DNS-имя хоста
Наличие в группе	Состоит хост в какой-либо группе или нет. Принимает 2 значения: True и False
Проблема	Почему нет результатов сканирования. Принимает 3 значения: Нет задания, Нет запуска задания, Ошибка или недоступность
Id заданий	ID заданий, которые не были запущены. Указываются через точку с запятой
"Id заданий, в которых сканируется группа, включающая данный хост"	Указываются через точку с запятой
ID сканирований	ID результата сканирования, который завершился ошибкой или недоступностью хоста

Пример:

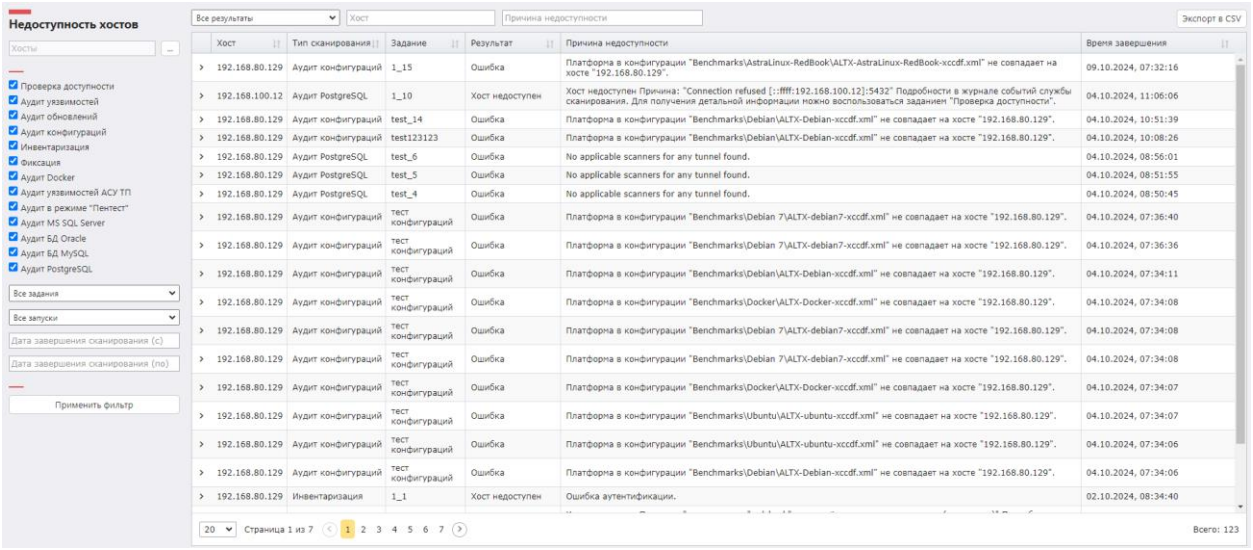
Bash (оболочка Unix)

```
Id хоста,Имя хоста,Наличие в группе,Проблема,Id заданий,"Id заданий,
в которых сканируется группа, включающая данный хост",ID сканирований
5,192.168.80.26,True,Нет запуска задания,111;112;113,4,
```

8.2 Недоступность хостов

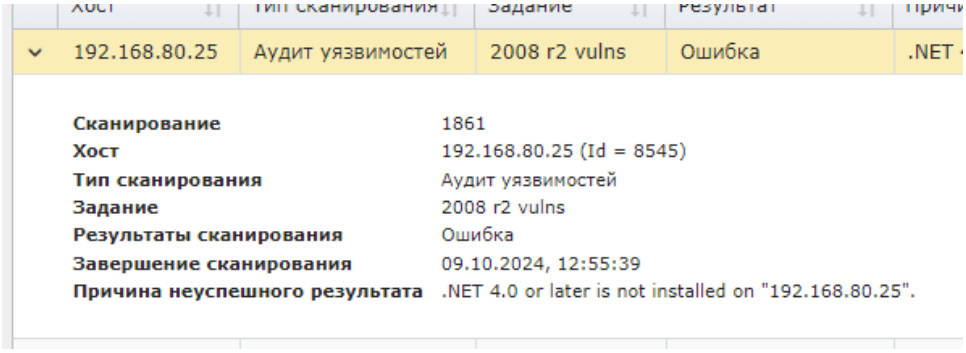
Данная форма аналитики позволяет определить, сколько хостов оказываются недоступными при сканировании, а также причины недоступности или завершения сканирования ошибкой.

Для перехода на форму нажмите **Аналитика** → **Недоступность хостов**



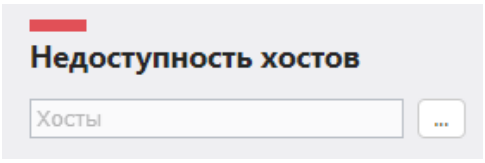
Информация о недоступности хоста включает в себя:

- Сканирование – ID результата сканирования;
- Хост – IP-адрес или DNS-имя хоста (ID хоста);
- Тип сканирования задания;
- Задание – название задания;
- Результат сканирования – результат актуального (последнего) сканирования указанного задания для хоста;
- Время завершения сканирования;
- Причина неуспешного результата – описание причины недоступности или ошибки;

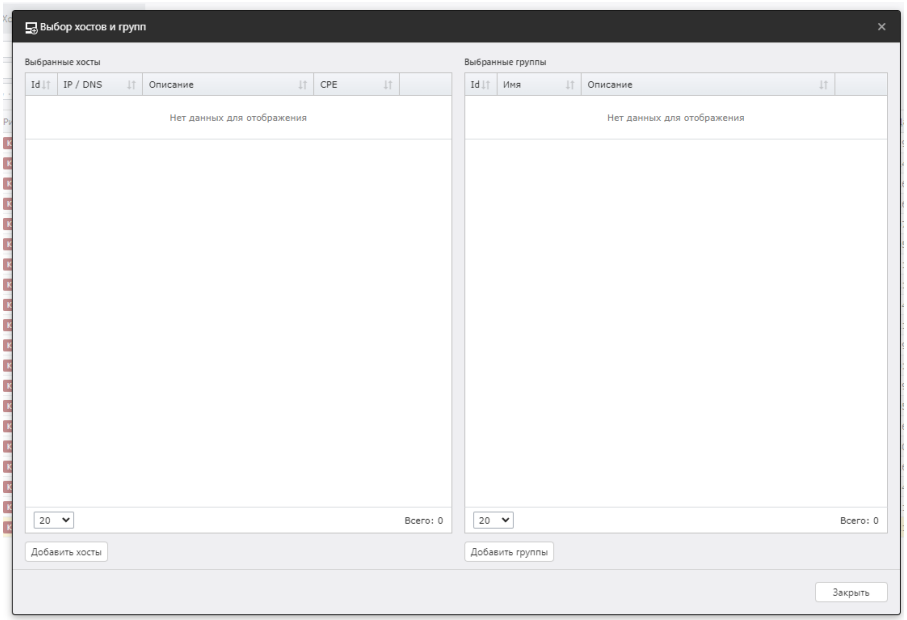


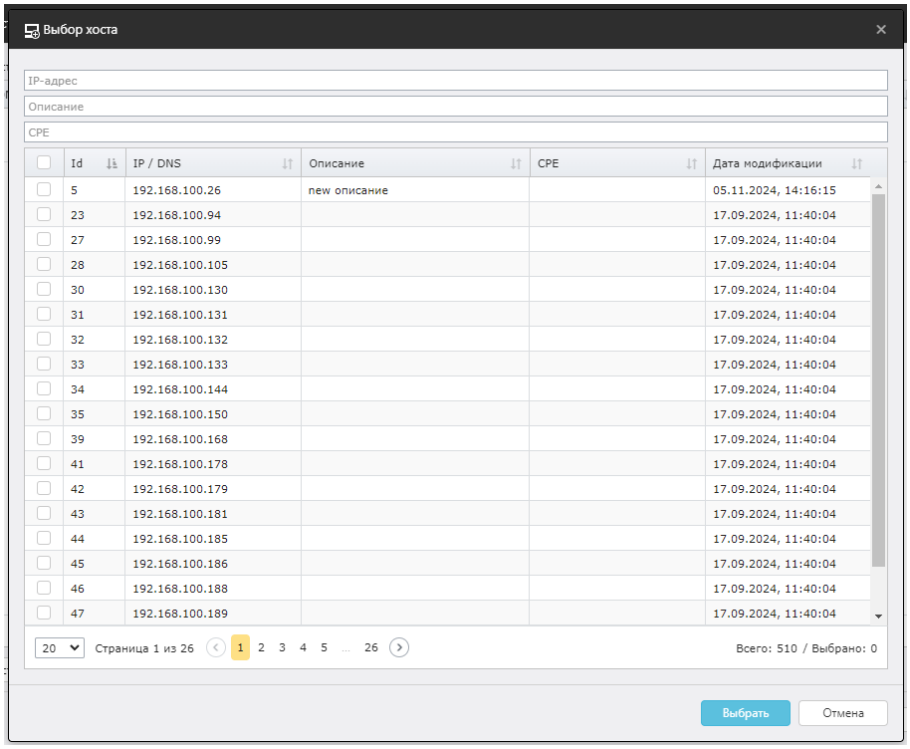
Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

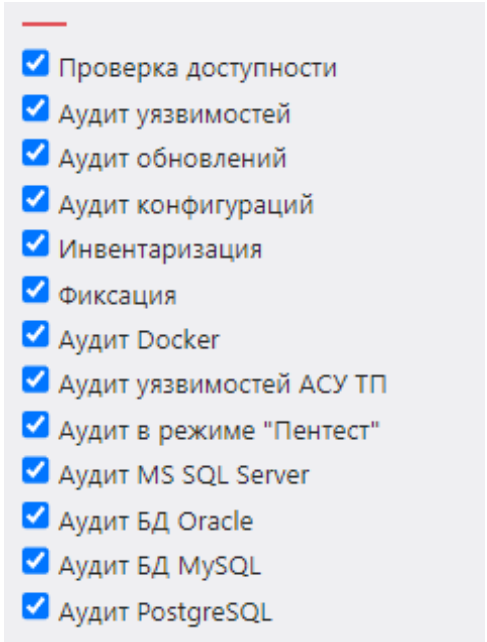


- Хосты – можно выбрать хосты, которые будут отображаться. Нажмите на ..., после чего откроется окно выбора групп и хостов:



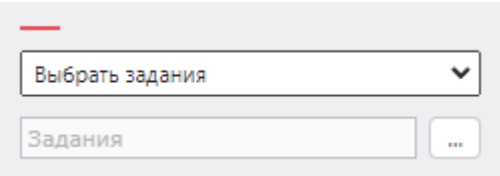


- Типы сканирований, по которым будет производиться поиск причины недоступности хостов;



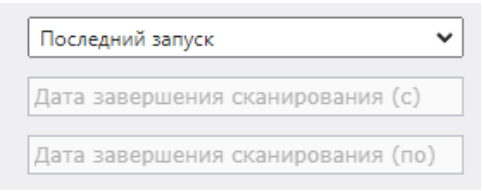
- Задания – можно выбрать задания, из результатов сканирования которых будет производиться поиск причин недоступности хостов. Из выпадающего списка можно выбрать два варианта: **Все задания** и

Выбрать задания. Если указать **Выбрать задания**, появится дополнительное поле:

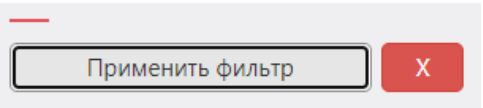


Нажмите на , после чего откроется окно выбора заданий;

- Запуски задания – из выпадающего списка можно выбрать какие результаты сканирования попадут в результирующую таблицу: Все запуски или Последний (актуальный) запуск:
- Дата завершения сканирования (с / по) – учитывать результаты сканирования, которые завершились в указанный период.



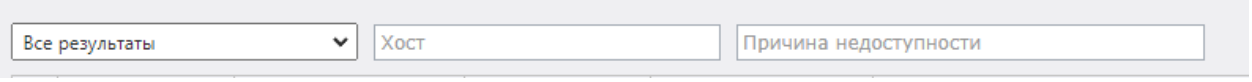
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Тип результатов сканирования – Ошибка или Хост недоступен;
- Хост – IP-адрес или DNS-имя хоста;
- Причина недоступности – описание причины недоступности или ошибки. Можно указывать часть причины доступности или ошибки.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая находится в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **UnavailabilityReasons-dd-mm-yyyy.csv**.

Структура CSV файла

ID сканирования	ID результата сканирования
Id хоста	ID хоста
Имя хоста	IP-адрес или DNS-имя хоста
Тип сканирования	Тип сканирования задания
Задание	Название задания
Результаты сканирования	Статус, которым завершилось сканирование: Ошибка или Хост недоступен
Причина недоступности	Описание ошибки или недоступности хоста
Время завершения	Время завершения сканирования
Детализация	Описание для некоторых ошибок в формате xml (для заданий типа **Проверка доступности**): "<exception name=""TypeException""><prop name=""Message""></prop></exception>"

Пример:

Bash (оболочка Unix)

```
ID сканирования,Id хоста,Имя хоста,Тип
сканирования,Задание,Результаты сканирования,Причина
недоступности,Время завершения,Детализация
1638,5,192.168.1.26,Проверка доступности,w,Хост недоступен,Failed to
authenticate the user name_user with negotiate,17.09.2024
13:11:00,"<exception name=""PythonException"">  <prop
name=""Message"">Failed to authenticate the user name_user with
negotiate</prop></exception>"
```

8.3 Анализ уязвимостей

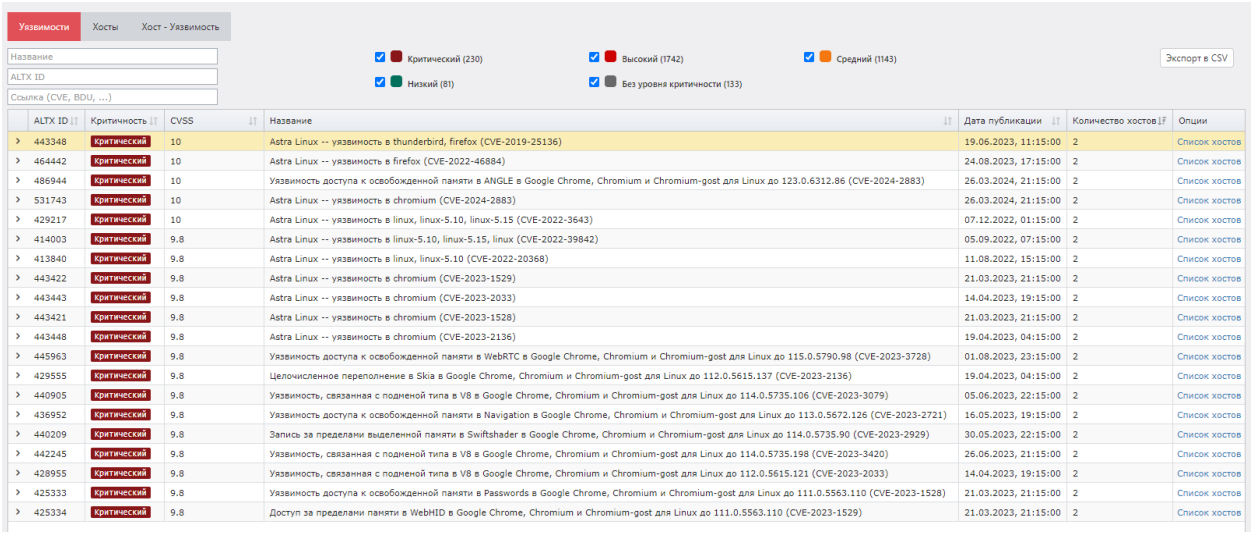
Данная форма аналитики позволяет проводить анализ инфраструктуры на предмет наличия любых или конкретных уязвимостей на хостах за последние N дней.

Для перехода на форму нажмите **Аналитика → Анализ уязвимостей**

Содержание

8.3.1 Вкладка Уязвимости

В данной вкладке отображается информация об уязвимостях, обнаруженных во время сканирований инфраструктуры, согласно общему фильтру.

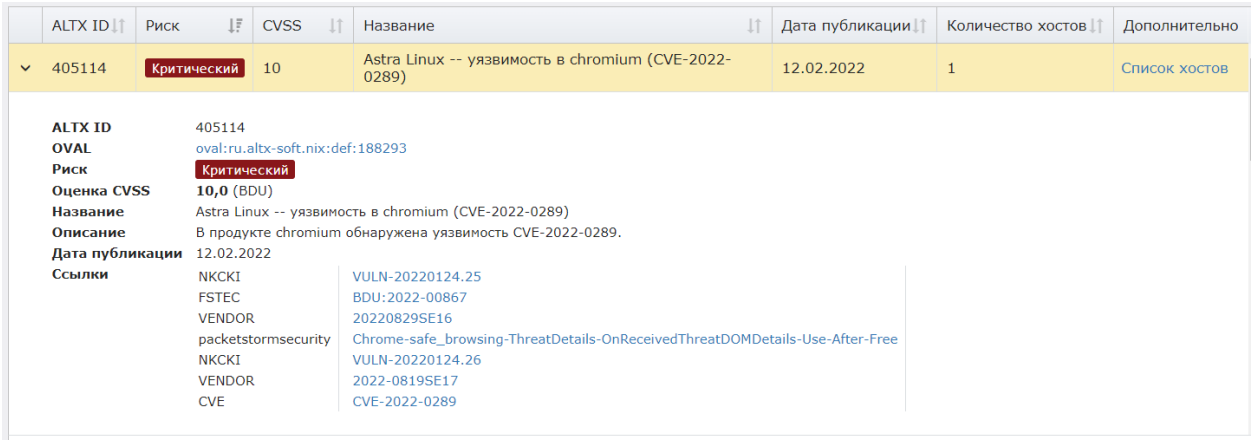


ALTX ID	Критичность	CVSS	Название	Дата публикации	Количество хостов	Опции
443348	Критический	10	Astra Linux -- уязвимость в thunderbird, firefox (CVE-2019-25136)	19.06.2023, 11:15:00	2	Список хостов
464442	Критический	10	Astra Linux -- уязвимость в firefox (CVE-2022-46884)	24.08.2023, 17:15:00	2	Список хостов
486944	Критический	10	Уязвимость доступа к освобожденной памяти в ANGLE в Google Chrome, Chromium и Chromium-gost для Linux до 123.0.6312.86 (CVE-2024-2883)	26.03.2024, 21:15:00	2	Список хостов
531743	Критический	10	Astra Linux -- уязвимость в chromium (CVE-2024-2883)	26.03.2024, 21:15:00	2	Список хостов
429217	Критический	10	Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)	07.12.2022, 01:15:00	2	Список хостов
414003	Критический	9.8	Astra Linux -- уязвимость в linux-5.10, linux-5.15, linux (CVE-2022-39842)	05.09.2022, 07:15:00	2	Список хостов
413840	Критический	9.8	Astra Linux -- уязвимость в linux, linux-5.10 (CVE-2022-20368)	11.08.2022, 15:15:00	2	Список хостов
443422	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-1529)	21.03.2023, 21:15:00	2	Список хостов
443443	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-2033)	14.04.2023, 19:15:00	2	Список хостов
443421	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-1528)	21.03.2023, 21:15:00	2	Список хостов
443448	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-2136)	19.04.2023, 04:15:00	2	Список хостов
445963	Критический	9.8	Уязвимость доступа к освобожденной памяти в WebRTC в Google Chrome, Chromium и Chromium-gost для Linux до 115.0.5790.98 (CVE-2023-3728)	01.08.2023, 23:15:00	2	Список хостов
429555	Критический	9.8	Целочисленное переполнение в Skia в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.137 (CVE-2023-2136)	19.04.2023, 04:15:00	2	Список хостов
440905	Критический	9.8	Уязвимость, связанная с подменой типа в V8 в Google Chrome, Chromium и Chromium-gost для Linux до 114.0.5735.106 (CVE-2023-3079)	05.06.2023, 22:15:00	2	Список хостов
436952	Критический	9.8	Уязвимость доступа к освобожденной памяти в Navigation в Google Chrome, Chromium и Chromium-gost для Linux до 113.0.5672.126 (CVE-2023-2721)	16.05.2023, 19:15:00	2	Список хостов
440209	Критический	9.8	Запись за пределами выделенной памяти в Swiftshader в Google Chrome, Chromium и Chromium-gost для Linux до 114.0.5735.90 (CVE-2023-2929)	30.05.2023, 22:15:00	2	Список хостов
442245	Критический	9.8	Уязвимость, связанная с подменой типа в V8 в Google Chrome, Chromium и Chromium-gost для Linux до 114.0.5735.198 (CVE-2023-3420)	26.06.2023, 21:15:00	2	Список хостов
428955	Критический	9.8	Уязвимость, связанная с подменой типа в V8 в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.121 (CVE-2023-2033)	14.04.2023, 19:15:00	2	Список хостов
425333	Критический	9.8	Уязвимость доступа к освобожденной памяти в Passwords в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1528)	21.03.2023, 21:15:00	2	Список хостов
425334	Критический	9.8	Доступ за пределами памяти в WebHID в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1529)	21.03.2023, 21:15:00	2	Список хостов

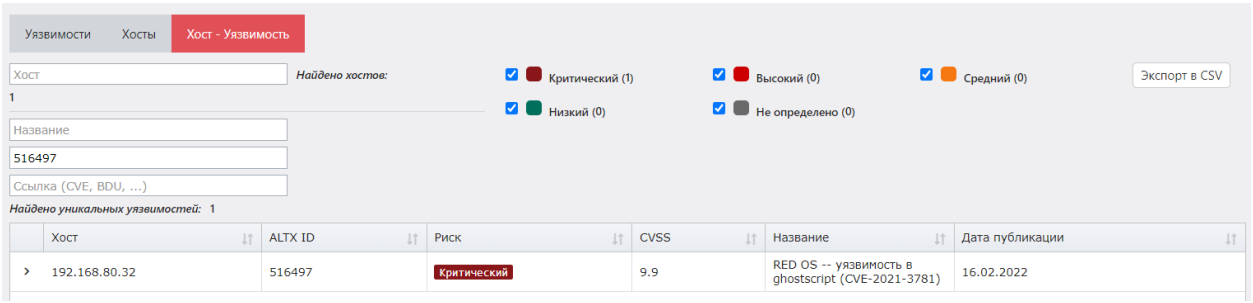
По умолчанию уязвимости отсортированы по количеству хостов, на которых они обнаружены, от большего к меньшему.

Информация об уязвимости включает в себя:

- Уникальный идентификатор ALTX ID;
- Ссылка на страницу уязвимостей в OVALdb;
- Риск и CVSS – Сведения об интегральной оценке по базовым метрикам CVSS;
- Имя уязвимости, описание, дата публикации вендором;
- Ссылки на бюллетени по данной уязвимости;
- Количество хостов, на которых была обнаружена данная уязвимость;

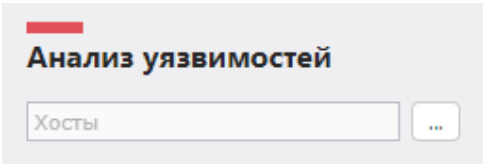


Нажав **Список хостов**, вы перейдете на вкладку **«Хост – Уязвимость»**, где в фильтре для результирующей таблицы уже будет указан ALTX ID выбранной уязвимости.

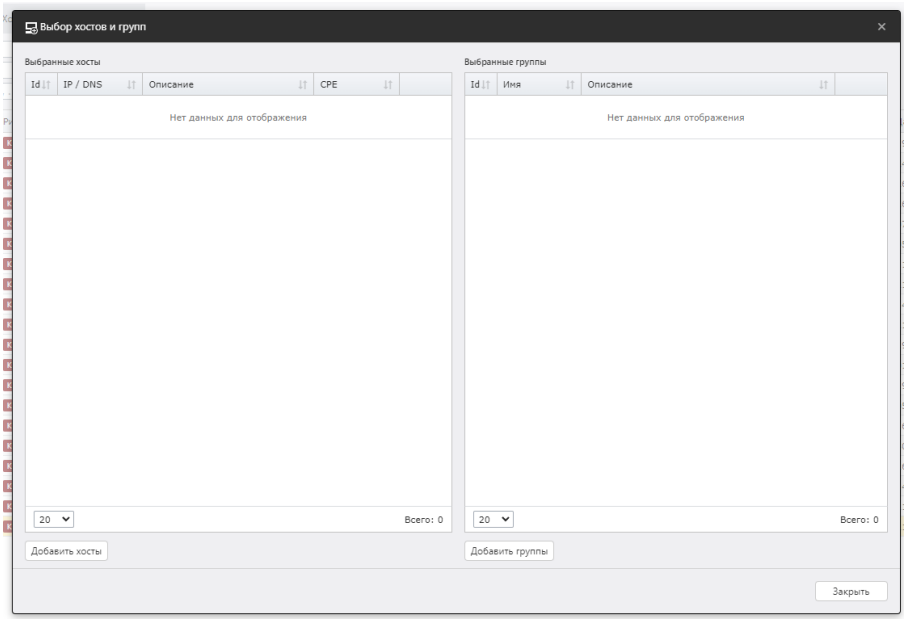


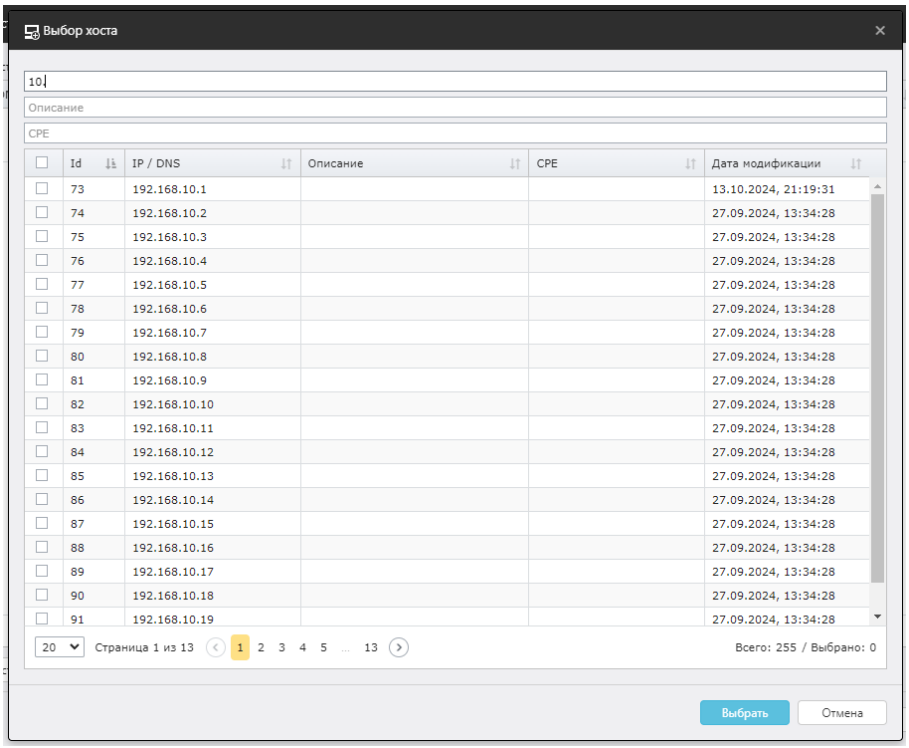
Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

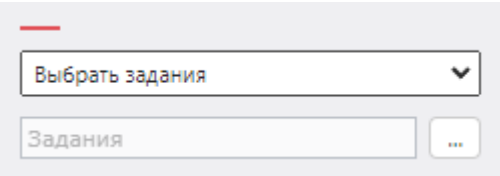


- Хосты – можно выбрать хосты, уязвимости для которых будут отображаться. Нажмите на ..., после чего откроется окно выбора групп и хостов:



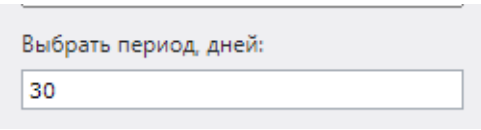


- Задания – можно выбрать задания, из результатов сканирования которых будет производиться поиск уязвимостей. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

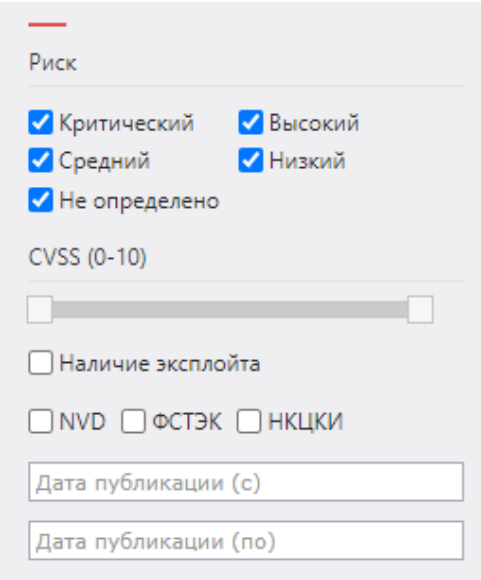


Нажмите на ... , после чего откроется окно выбора заданий;

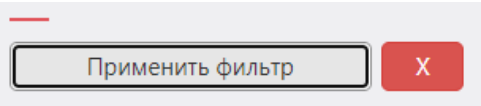
- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для поиска уязвимостей;



- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; Сведения об интегральной оценке по базовым метрикам CVSS;
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;
- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.



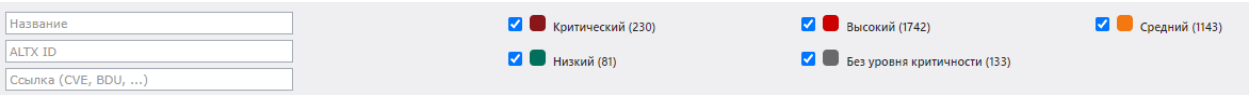
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Название – название уязвимости;
- ALTX ID – уникальный идентификатор уязвимости, состоящий из цифр;
- Ссылка – идентификатор бюллетеня по данной уязвимости;
- Риск – в таблице будут отображаться уязвимости с отмеченными вариантами риска.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **VulnerabilityAnalysis-Vulnerabilities-dd-mm-yyyy.csv**.

Структура CSV файла

ALTX ID	Уникальный идентификатор уязвимости
Количество хостов	Количество хостов, на которых обнаружена уязвимость
Хосты	Список ID хостов, на которых обнаружена уязвимость. Если значений больше одного, то они указываются в двойных кавычках через запятую. Например, "67,69"

OVAL определение	Ссылка на страницу уязвимости в OVALdb
Риск	Принимает значения: Критический, Высокий, Средний, Низкий
Оценка CVSS	Значение указывается в двойных кавычках. Сведения об интегральной оценке по базовым метрикам CVSS
Источник CVSS	Название вендора или базы данных уязвимостей, откуда взято значение для оценки CVSS
Уязвимость	Имя уязвимости
Описание	Описание уязвимости
Дата публикации	Дата публикации бюллетеня вендором

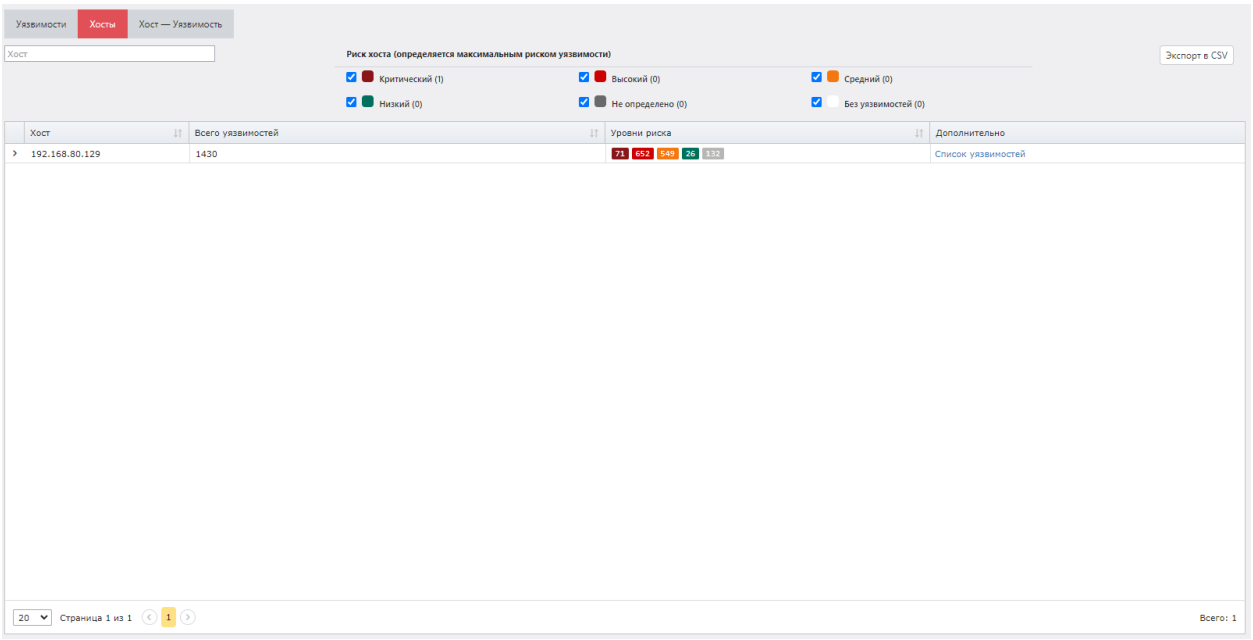
Пример:

Код

```
ALTX ID,Количество хостов,Хосты,OVAL определение,Уровень
критичности,Оценка CVSS,Источник CVSS,Уязвимость,Описание,Дата
публикации
362408,1,69,oval:ru.altx-soft.nix:def:156895,Высокий,"8,8",BDU,Astra
Linux -- уязвимость в openjpeg2 (CVE-2020-27814),В продукте openjpeg2
обнаружена уязвимость CVE-2020-27814.,26.01.2021
```

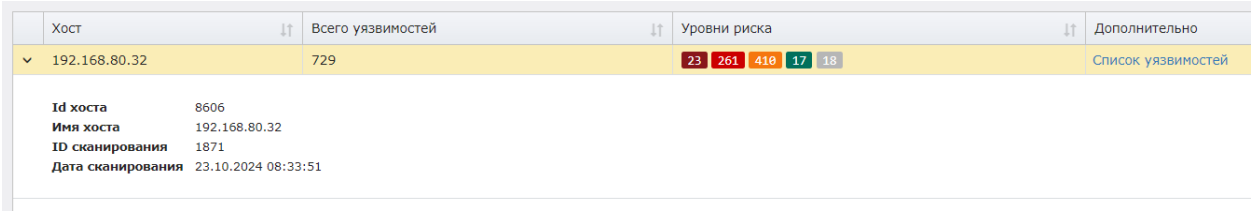
8.3.2 Вкладка Хосты

В данной вкладке отображается информация об уязвимостях на конкретных хостах, которые были обнаруженных во время сканирований инфраструктуры, согласно общему фильтру.

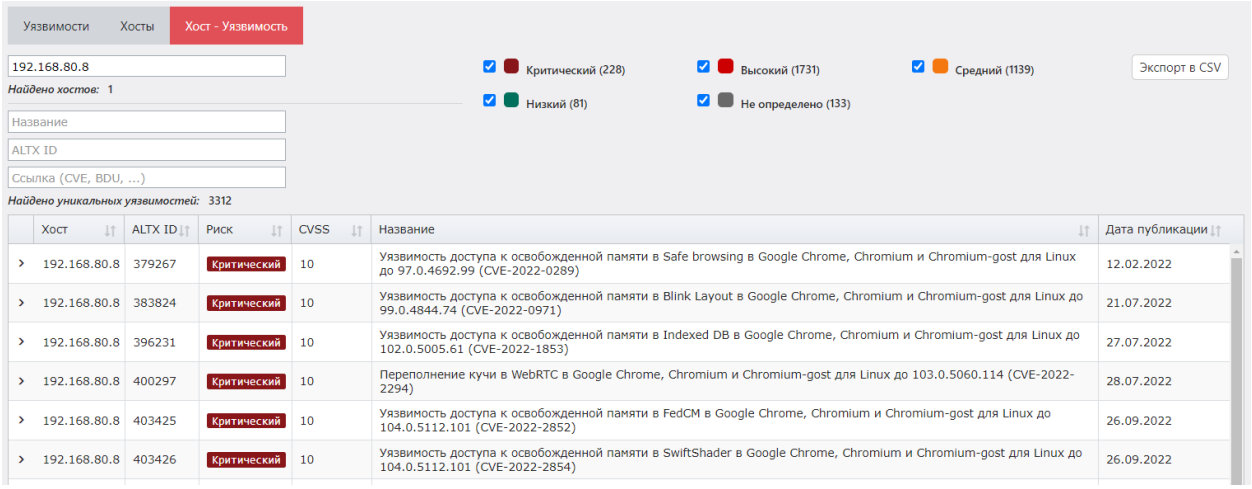


В данной вкладке отображается информация о хостах:

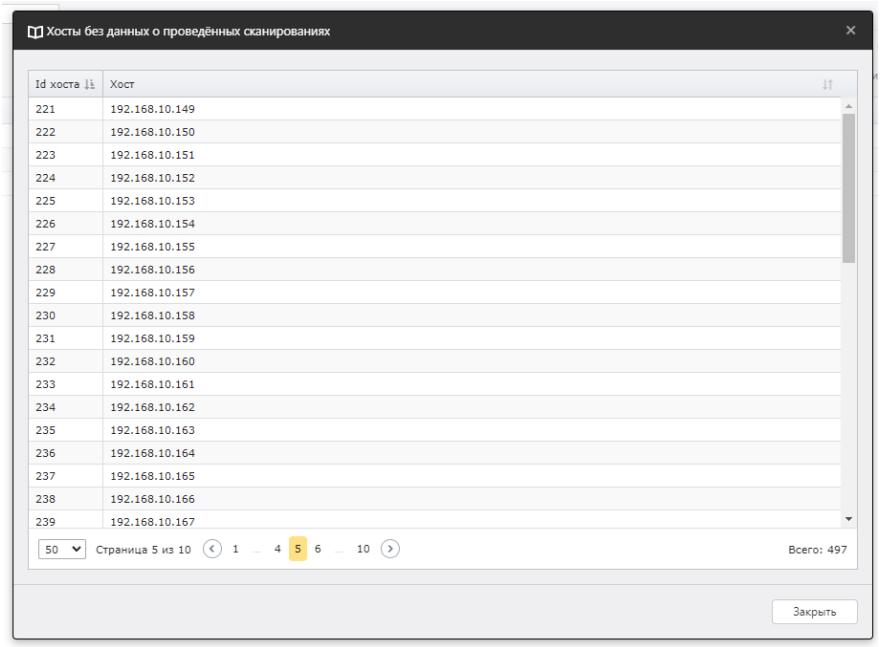
- ID хоста;
- IP-адрес или DNS имя хоста;
- Описание хоста;
- ID актуального (последнего) сканирования со статусом **Завершено**;
- Дата актуального сканирования;
- Общее количество уязвимостей на хосте;
- Количество найденных уязвимостей, сгруппированных по уровню риска;



Нажав **Список уязвимостей** возле хоста, вы перейдете на вкладку **«Хост – Уязвимость»**, где в фильтре для результирующей таблицы уже будет указан выбранный хост.

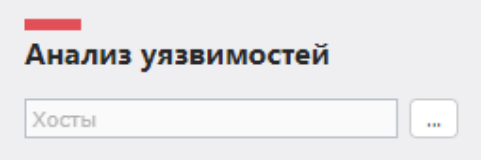


Под таблицей располагается кнопка **Хосты без успешных результатов сканирования** со списком хостов, для которых в рамках выбранных заданий все сканирования завершились со статусом **Ошибка** или **Хост недоступен**. Данное окно является информационным.

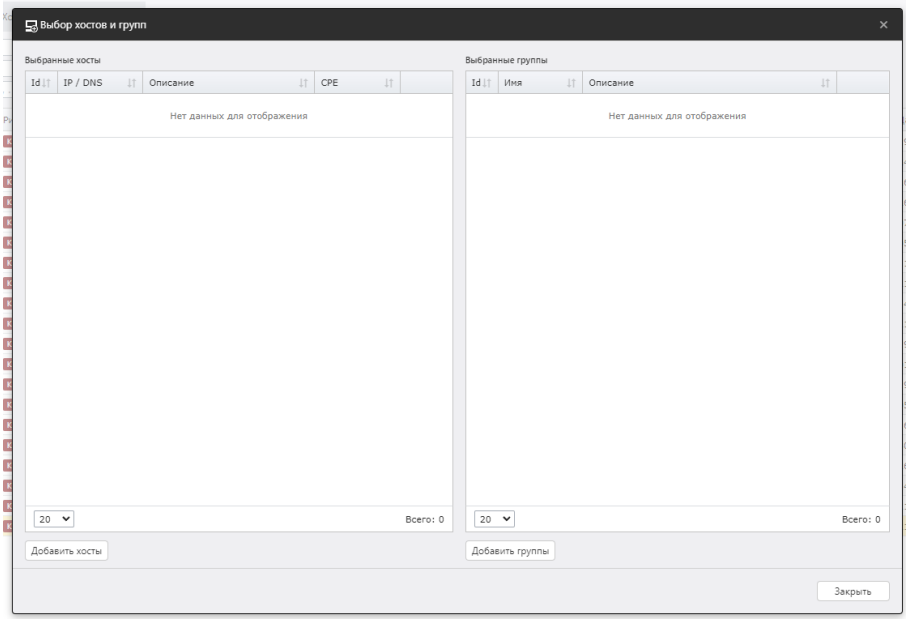


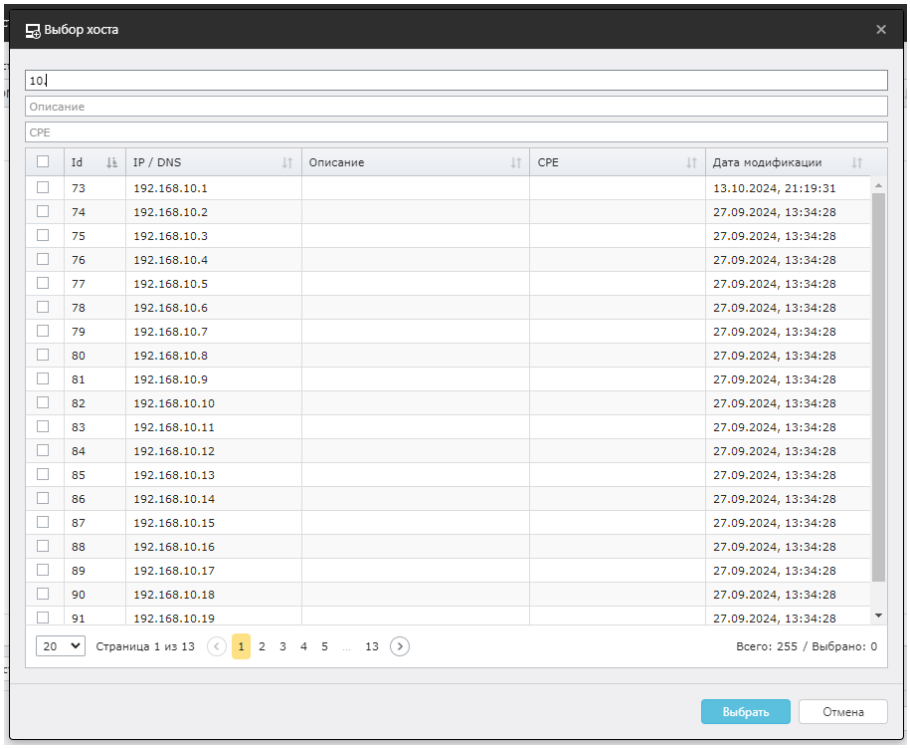
Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

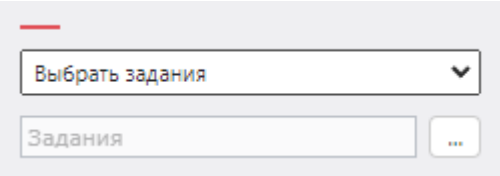


- Хосты – можно выбрать хосты, уязвимости для которых будут отображаться. Нажмите на ..., после чего откроется окно выбора групп и хостов;





- Задания – можно выбрать задания, из результатов сканирования которых будет производиться поиск уязвимостей. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

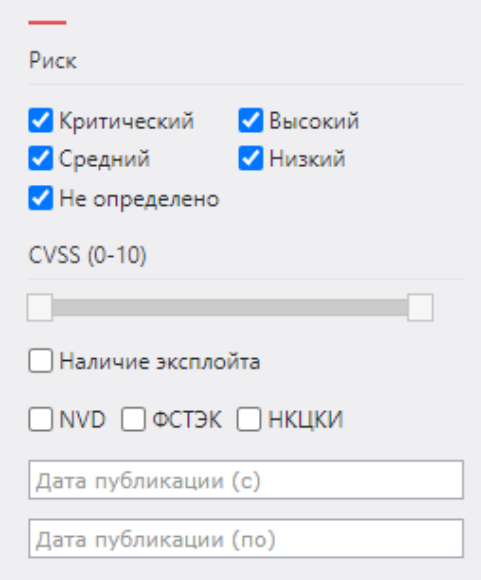


Нажмите на

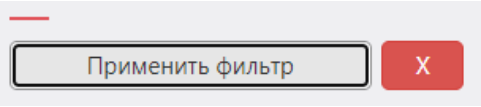
, после чего откроется окно выбора заданий;

- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для поиска уязвимостей;
- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; Сведения об интегральной оценке по базовым метрикам CVSS;
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;

- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.



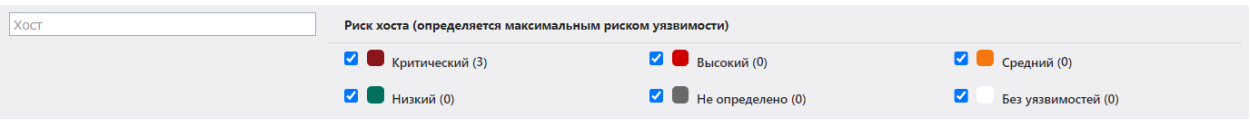
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



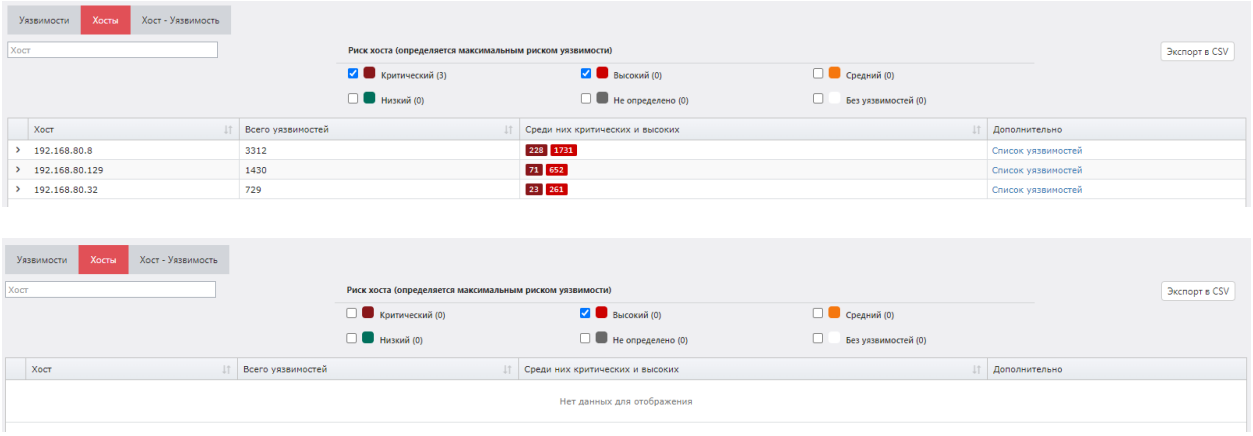
Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра.

- Хост – IP-адрес или DNS-имя хоста. Можно указывать как полное значение, так и часть;
- Риск хоста (определяется максимальным риском уязвимости) – будет отображаться хосты, на которых есть хоть одна уязвимость выбранного риска и этот риск является максимальным для хоста.



Например, при фильтрации только по Высокому риску в результирующую таблицу не попадут хосты, у которых обнаружены уязвимости критического уровня.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **VulnerabilityAnalysis-Hosts-dd-mm-yyyy.csv**.

Структура CSV файла

Id хоста	ID хоста, на котором найдены уязвимости
Имя хоста	IP-адрес или DNS-имя хоста
Описание хоста	Описание хоста
CPE	CPE хоста
Всего уязвимостей	Количество всех уязвимостей, найденных на хосте
Уязвимостей с	Количество уязвимостей на хосте с Критическим риском

критичным риском	
Уязвимостей с высоким риском	Количество уязвимостей на хосте с Высоким риском
Уязвимостей с средним риском	Количество уязвимостей на хосте со Средним риском
Уязвимостей с низким риском	Количество уязвимостей на хосте с Низким риском
Уязвимостей с неопределенным риском	Количество уязвимостей на хосте с Неопределенным риском
ID сканирования	ID актуального (последнего) результата сканирования со статусом **Завершено**
Время завершения	Время завершения актуального результата сканирования

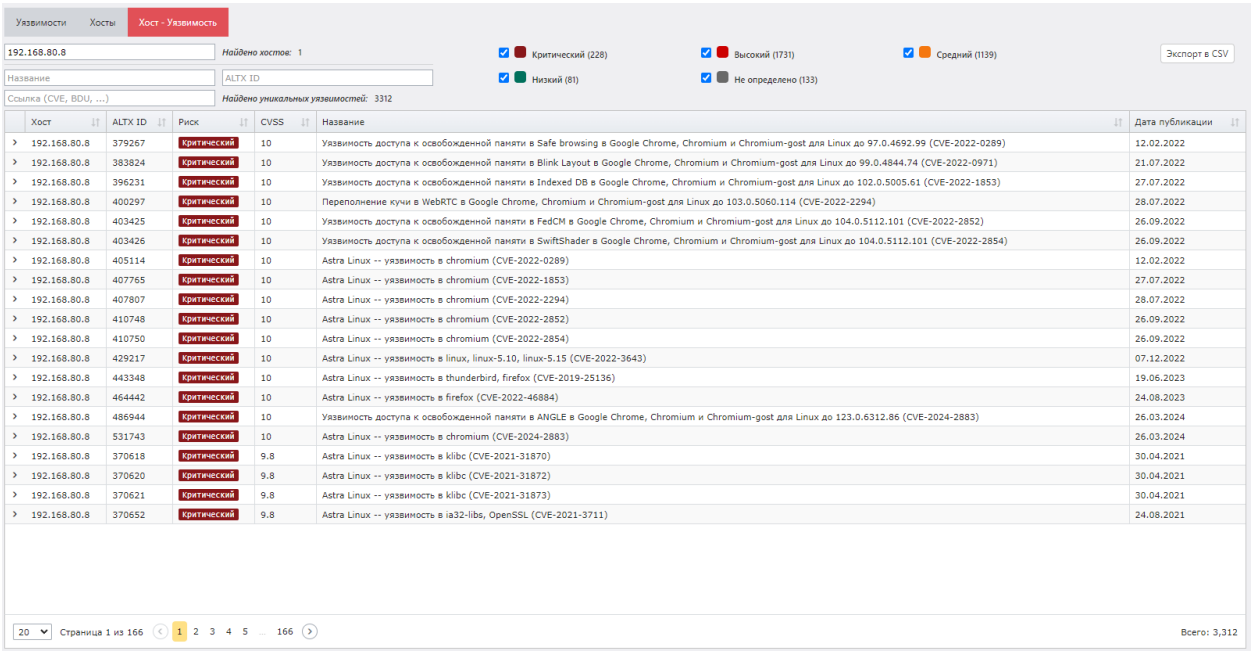
Пример:

Код

```
Id хоста,Имя хоста,Описание хоста,CPE,Всего уязвимостей,Уязвимостей с критичным риском,Уязвимостей с высоким риском,Уязвимостей с средним риском,Уязвимостей с низким риском,Уязвимостей с неопределенным риском,ID сканирования,Время завершения
67,192.168.80.129,123,,1430,71,652,549,26,132,1862,14.10.2024 12:45:37
```

8.3.3 Вкладка Хост – Уязвимость

В данной вкладке отображается информация об уязвимостях с указанием к какому хосту они относятся.



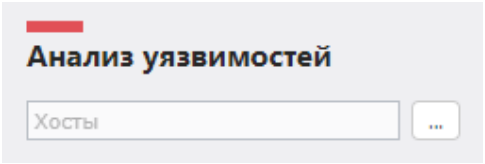
Хост	ALTX ID	Риск	CVSS	Название	Дата публикации
192.168.80.8	379267	Критический	10	Уязвимость доступа к освобожденной памяти в Safe browsing в Google Chrome, Chromium и Chromium-gost для Linux до 97.0.4692.99 (CVE-2022-0289)	12.02.2022
192.168.80.8	383824	Критический	10	Уязвимость доступа к освобожденной памяти в Blink Layout в Google Chrome, Chromium и Chromium-gost для Linux до 99.0.4844.74 (CVE-2022-0971)	21.07.2022
192.168.80.8	396231	Критический	10	Уязвимость доступа к освобожденной памяти в Indexed DB в Google Chrome, Chromium и Chromium-gost для Linux до 102.0.5005.61 (CVE-2022-1853)	27.07.2022
192.168.80.8	400297	Критический	10	Переполнение кучи в WebRTC в Google Chrome, Chromium и Chromium-gost для Linux до 103.0.5060.114 (CVE-2022-2294)	28.07.2022
192.168.80.8	403425	Критический	10	Уязвимость доступа к освобожденной памяти в FedCM в Google Chrome, Chromium и Chromium-gost для Linux до 104.0.5112.101 (CVE-2022-2852)	26.09.2022
192.168.80.8	403426	Критический	10	Уязвимость доступа к освобожденной памяти в SwiftShader в Google Chrome, Chromium и Chromium-gost для Linux до 104.0.5112.101 (CVE-2022-2854)	26.09.2022
192.168.80.8	405114	Критический	10	Astra Linux -- уязвимость в chromium (CVE-2022-0289)	12.02.2022
192.168.80.8	407765	Критический	10	Astra Linux -- уязвимость в chromium (CVE-2022-1853)	27.07.2022
192.168.80.8	407807	Критический	10	Astra Linux -- уязвимость в chromium (CVE-2022-2294)	28.07.2022
192.168.80.8	410748	Критический	10	Astra Linux -- уязвимость в chromium (CVE-2022-2852)	26.09.2022
192.168.80.8	410750	Критический	10	Astra Linux -- уязвимость в chromium (CVE-2022-2854)	26.09.2022
192.168.80.8	429217	Критический	10	Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)	07.12.2022
192.168.80.8	443348	Критический	10	Astra Linux -- уязвимость в thunderbird, firefox (CVE-2019-25136)	19.06.2023
192.168.80.8	464442	Критический	10	Astra Linux -- уязвимость в firefox (CVE-2022-46884)	24.08.2023
192.168.80.8	486944	Критический	10	Уязвимость доступа к освобожденной памяти в ANGLE в Google Chrome, Chromium и Chromium-gost для Linux до 123.0.6312.86 (CVE-2024-2883)	26.03.2024
192.168.80.8	531743	Критический	10	Astra Linux -- уязвимость в chromium (CVE-2024-2883)	26.03.2024
192.168.80.8	370618	Критический	9.8	Astra Linux -- уязвимость в klibc (CVE-2021-31870)	30.04.2021
192.168.80.8	370620	Критический	9.8	Astra Linux -- уязвимость в klibc (CVE-2021-31872)	30.04.2021
192.168.80.8	370621	Критический	9.8	Astra Linux -- уязвимость в klibc (CVE-2021-31873)	30.04.2021
192.168.80.8	370652	Критический	9.8	Astra Linux -- уязвимость в ia32-libs, OpenSSL (CVE-2021-3711)	24.08.2021

Информация об уязвимости включает в себя:

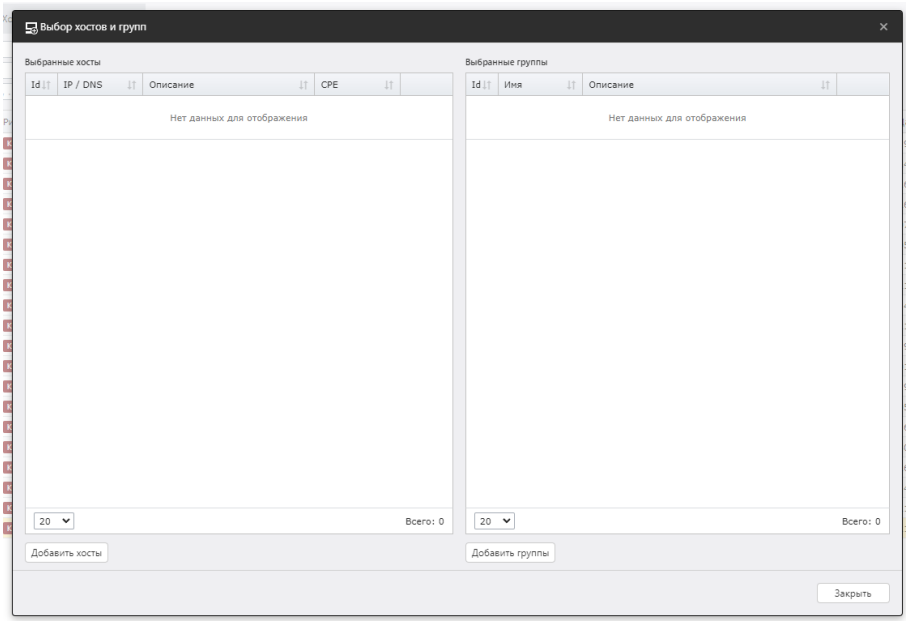
- ID последнего сканирования со статусом Завершено, в котором была обнаружена данная уязвимость;
- IP-адрес или DNS имя хоста и ID хоста, на котором обнаружена уязвимость;
- Уникальный идентификатор ALTX ID;
- Ссылка на страницу уязвимости в OVALdb;
- Риск и CVSS – Сведения об интегральной оценке по базовым метрикам CVSS;
- Имя уязвимости, описание, дата публикации вендором;
- Ссылки на бюллетени по данной уязвимости;
- Детализация – какие пакеты или файлы уязвимы;

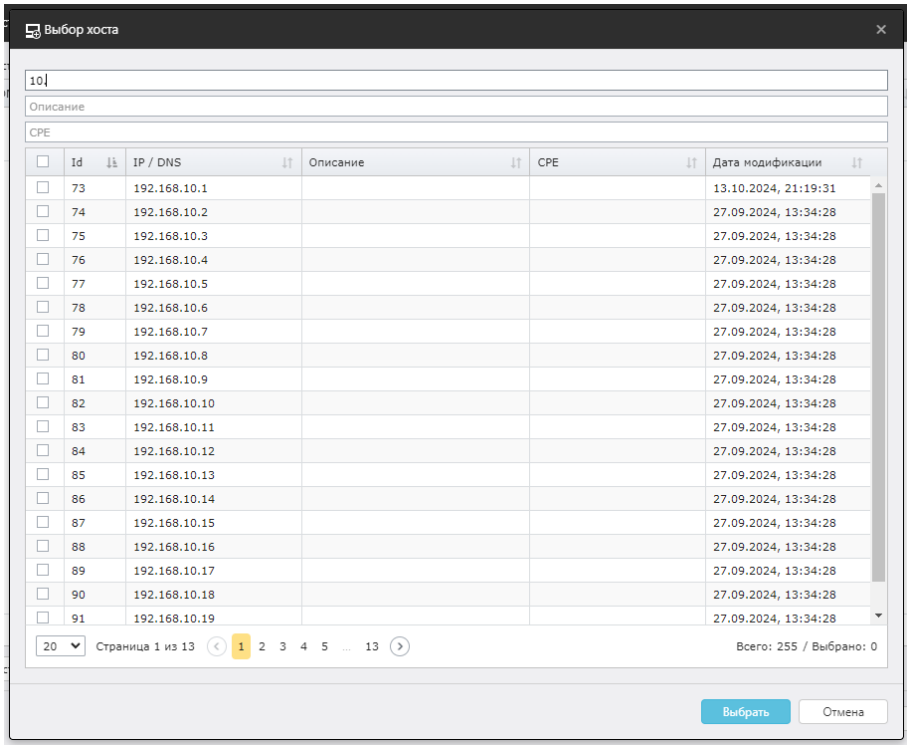
Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

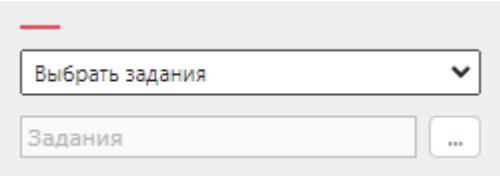


- Хосты – можно выбрать хосты, уязвимости для которых будут отображаться. Нажмите на ..., после чего откроется окно выбора групп и хостов;





- Задания – можно выбрать задания, из результатов сканирования которых будет производиться поиск уязвимостей. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

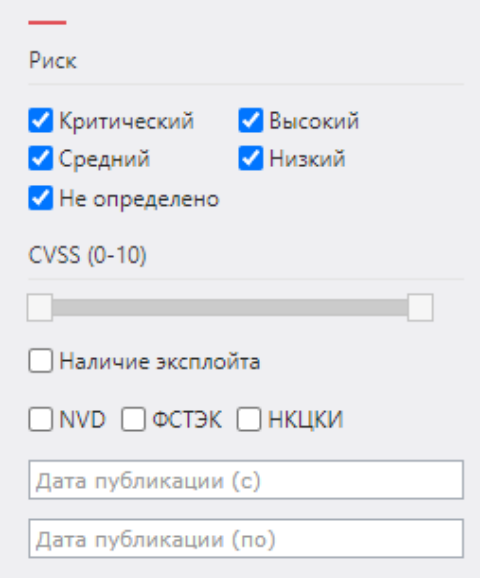


Нажмите на

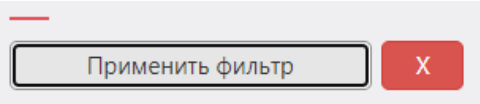
, после чего откроется окно выбора заданий;

- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для поиска уязвимостей;
- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; Сведения об интегральной оценке по базовым метрикам CVSS;
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;

- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.



Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.

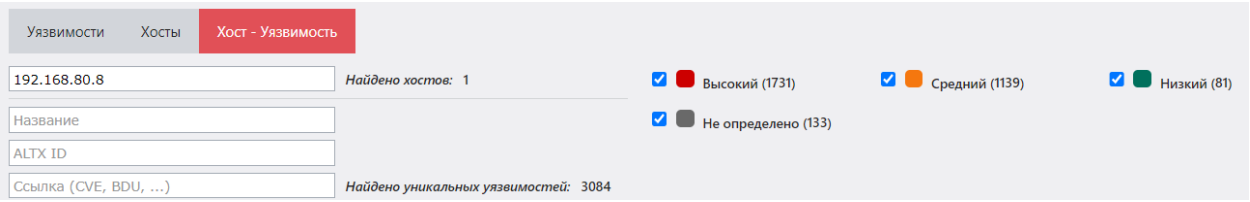


Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Хост – IP-адрес или DNS-имя хоста;
- Название – имя уязвимости;
- ALTX ID – уникальный идентификатор уязвимости;
- Ссылка (CVE, BDU, ...) – идентификатор бюллетеня по данной уязвимости;
- Найдено хостов – количество хостов, отображаемых в таблице согласно данному фильтру;

- Найдено уникальных уязвимостей – количество уязвимостей без дублирования согласно данному фильтру. Уязвимости с одним и тем же ALTX ID могут встречаться несколько раз, если уязвимыми оказались несколько пакетов или файлов (строка Детализация из подробной информации о найденной уязвимости);
- Риск – в таблице будут отображаться уязвимости с отмеченными уровнями риска.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **VulnerabilityAnalysis-VulnerabilitiesForHosts-dd-mm-yyyy.csv**.

Структура CSV файла

ID сканирования	ID актуального (последнего) результата сканирования со статусом **Завершено**
Id хоста	ID хоста, на котором найдены уязвимости
Имя хоста	IP-адрес или DNS-имя хоста
ALTX ID	Уникальный идентификатор уязвимости
OVAL определение	Ссылка на страницу уязвимости в OVALdb
Риск	Принимает значения: Критический, Высокий, Средний, Низкий

Оценка CVSS	Значение указывается в двойных кавычках. Сведения об интегральной оценке по базовым метрикам CVSS
Источник CVSS	Название вендора или базы данных уязвимостей, откуда взято значение для оценки CVSS
Уязвимость	Имя уязвимости. Указывается в двойных кавычках
Описание	Описание уязвимости
Дата публикации	Дата публикации бюллетени вендором
Детализация	Уязвимые пакеты или файлы. Если значений несколько, разделяется точкой с запятой

Пример:

Код

```
ID сканирования,Id хоста,Имя хоста,ALTX ID,OVAL
определение,Риск,Оценка CVSS,Источник CVSS,Уязвимость,Описание,Дата
публикации,Детализация
1866,69,192.168.80.8,343423,oval:ru.altx-
soft.nix:def:144841,Высокий,"8,8",BDU,"Уязвимость доступа к
освобожденной памяти в clipboard в Google Chrome, Chromium и
Chromium-gost для Linux до 87.0.4280.88 (CVE-2020-16037)",Уязвимость
доступа к освобожденной памяти в clipboard в Google
Chrome.,08.01.2021,chromium (0:87.0.4280.66-0astragost1)
```

8.4 Контроль устранения уязвимостей

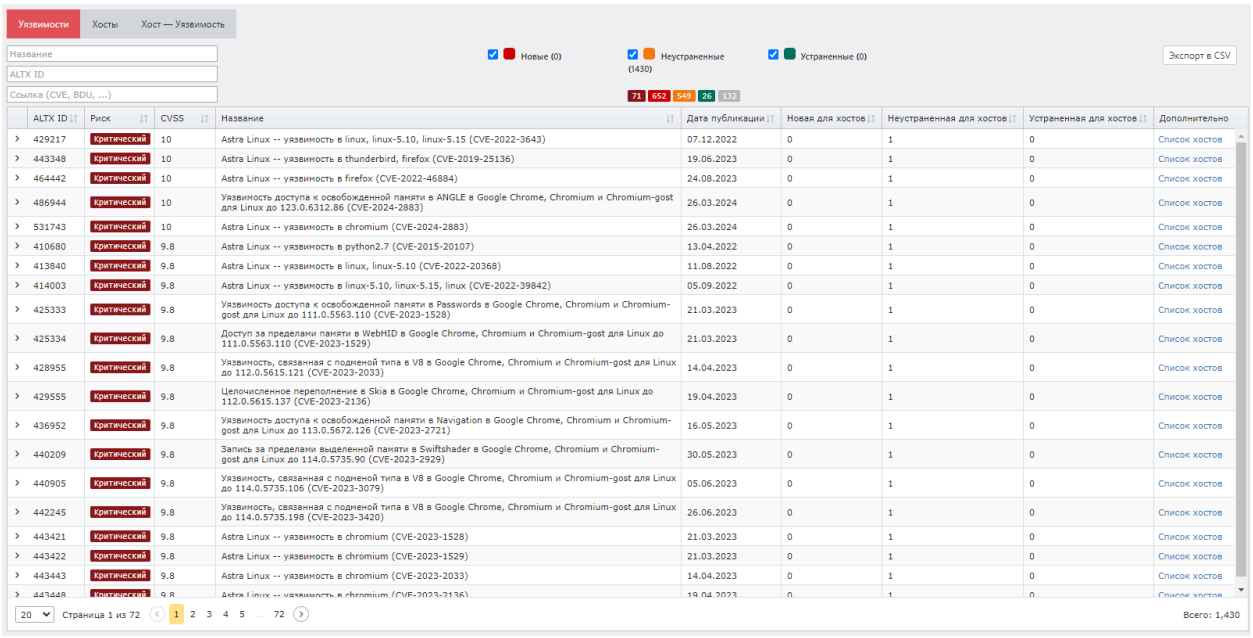
Данная форма аналитики позволяет проводить сравнение состояния инфраструктуры на предмет наличия уязвимостей в двух временных отметках.

Для перехода на форму нажмите **Аналитика** → **Контроль устранения уязвимостей**

Содержание

8.4.1 Вкладка Уязвимости

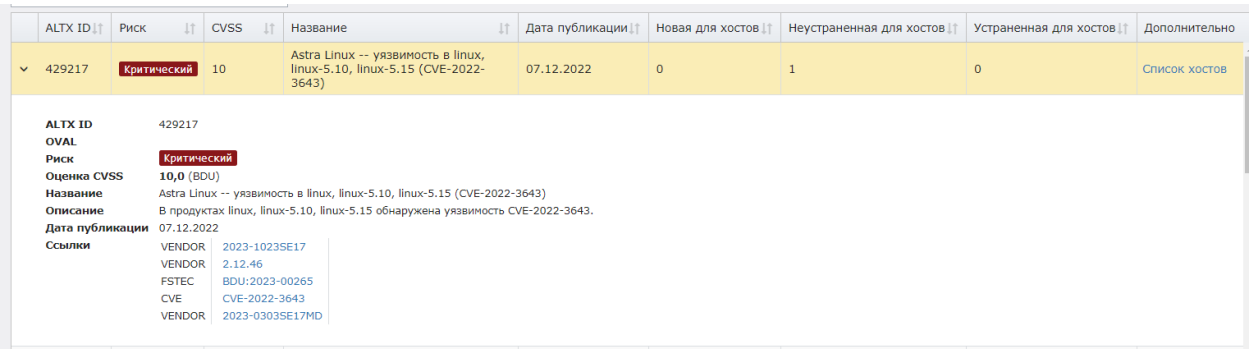
В данной вкладке отображается информация о наличии уязвимостей и их устранении на хостах, согласно выбранному заданию и итерации запуска в сравнении с предыдущими итерациями.



> Уязвимости в таблице сгруппированы по ALTX ID. Если уязвимость была обнаружена на одном хосте / нескольких хостах в разных файлах / пакетах, то на этой вкладке сведения по ней будут показаны в рамках одной строки.

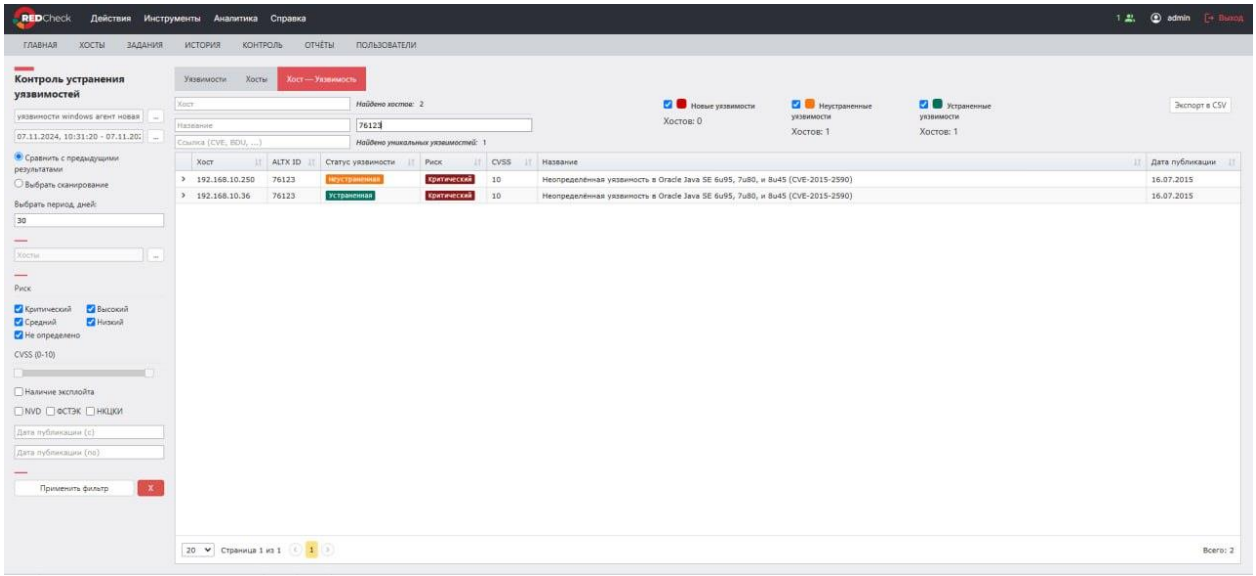
Информация об уязвимости включает в себя:

- Уникальный идентификатор ALTX ID;
- Ссылка на страницу уязвимости в OVALdb;
- Риск и CVSS – Сведения об интегральной оценке по базовым метрикам CVSS;
- Имя уязвимости, описание, дата публикации вендором;
- Ссылки на бюллетени по данной уязвимости;
- Информация о появлении и устранении данной уязвимости на хостах;



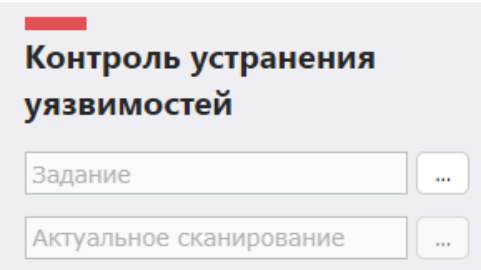
Нажав **Список хостов**, вы перейдете на вкладку **«Хост – Уязвимость»**, где в фильтре для результирующей таблицы уже будет указан ALTX ID выбранной уязвимости. В случае, если одна и та же уязвимость была найдена в разных файлах / пакетах, то для каждого случая в таблице будет собственная строка с информацией.

Если анализируется одна уникальная уязвимость, то под чекбоксами фильтра «по Статусу уязвимости» будет указано количество хостов для каждого статуса.



Общий фильтр

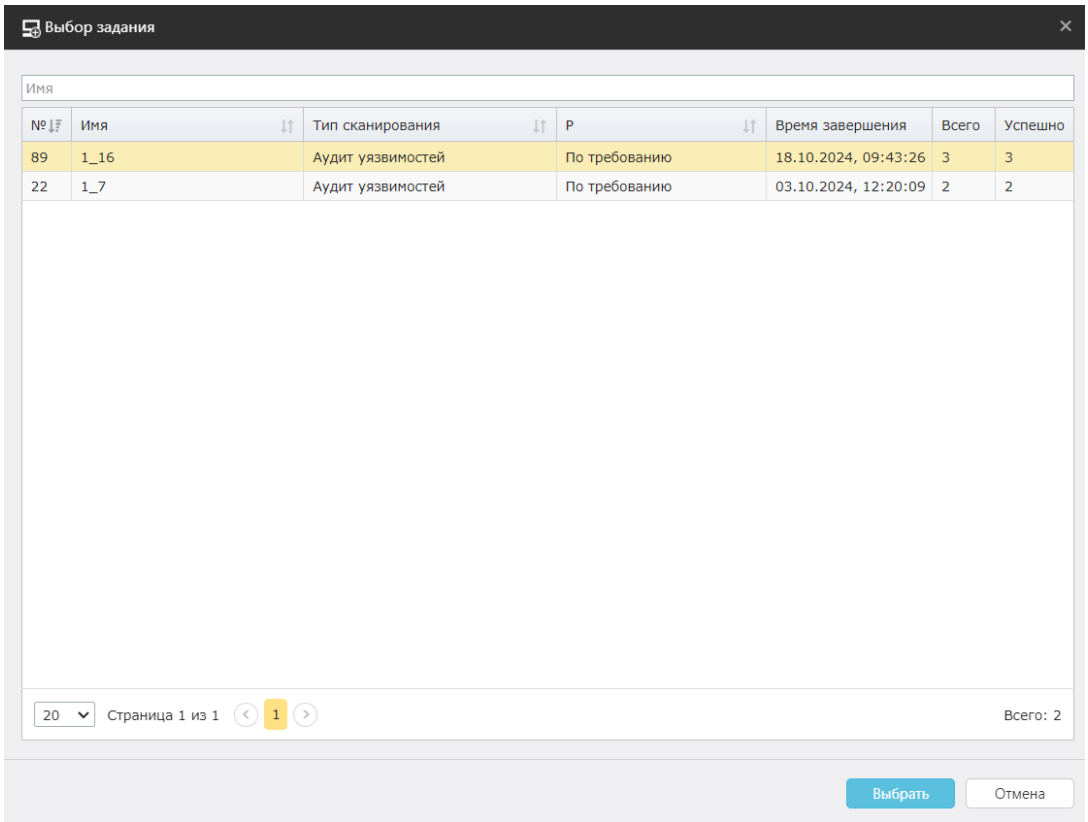
Общий фильтр располагается слева от результирующей таблицы.



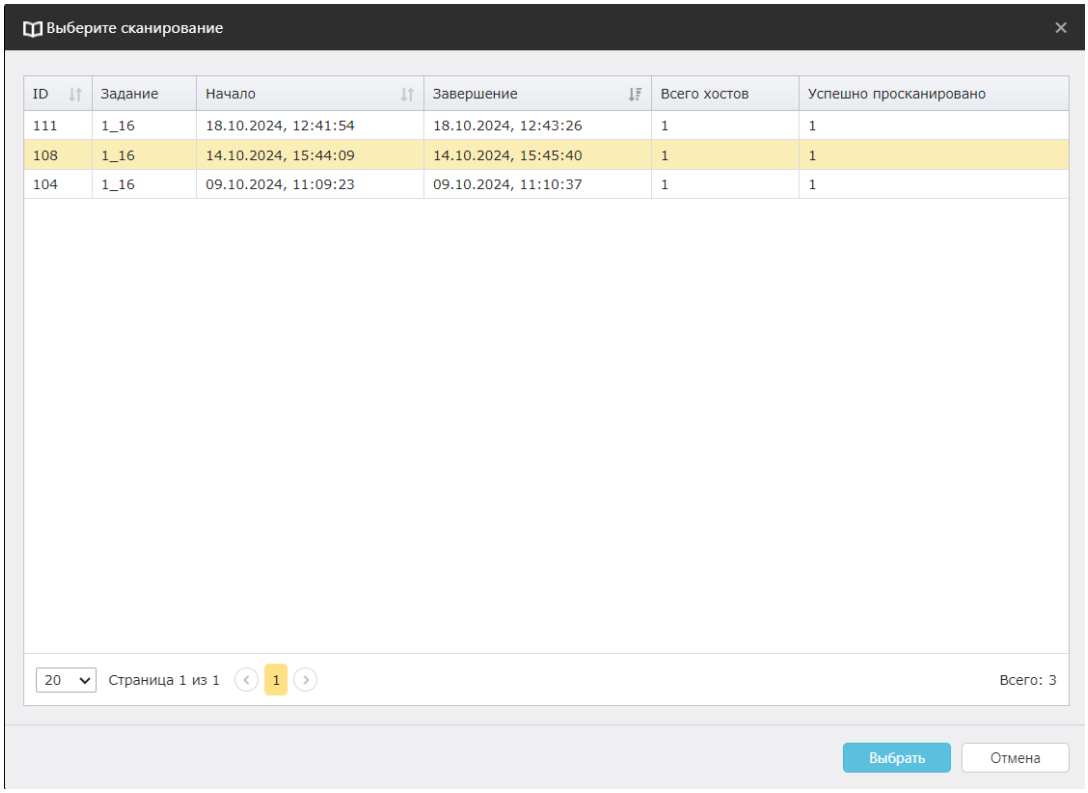
- Задание – необходимо выбрать задание типа Аудит уязвимостей.

  Нажмите на ..., после чего откроется окно выбора:

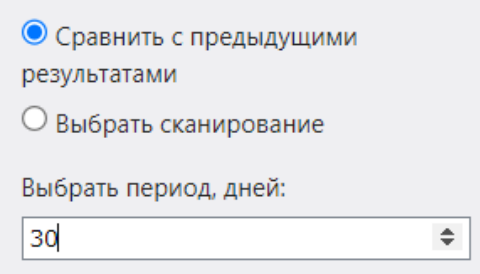
  - Всего – сколько было запусков задания;
  - Успешно – сколько из них выполнились успешно (хотя бы одно сканирование имеет статус **Завершено**);



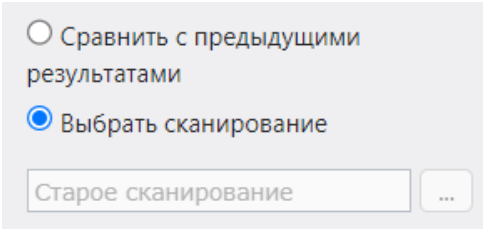
- Актуальное сканирование – необходимо выбрать итерацию запуска, с которой будут сравниваться предыдущие запуски. В такой итерации запуска должно быть хотя бы одно успешное сканирование;



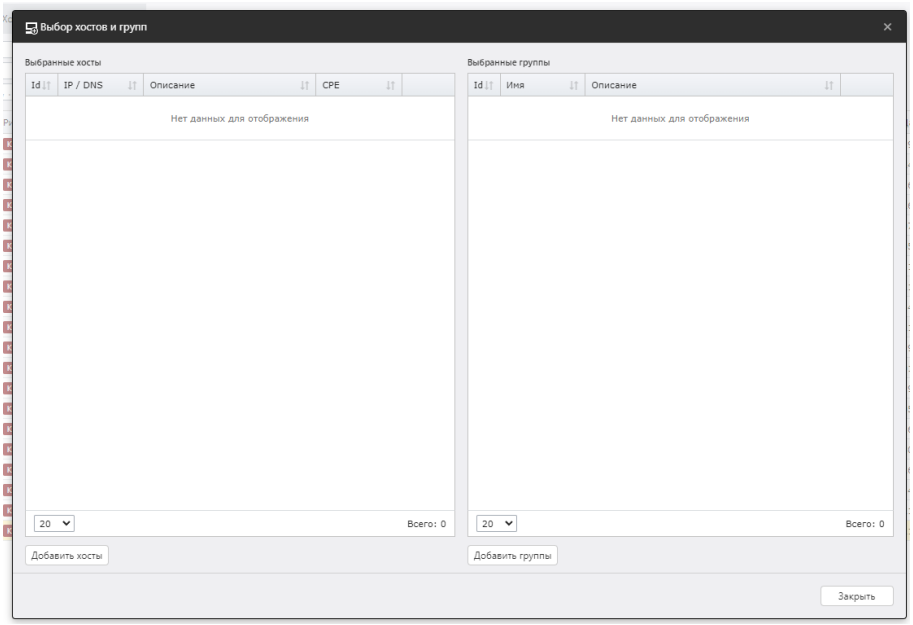
- Сравнивать с предыдущими результатами – сравнить с предыдущим успешным сканированием. Для каждого хоста предыдущее успешное сканирование подбирается индивидуально и может быть взято из разных итерацией запуска. Фильтр по времени позволяет ограничить период, за который подбирается предыдущее успешное сканирование;

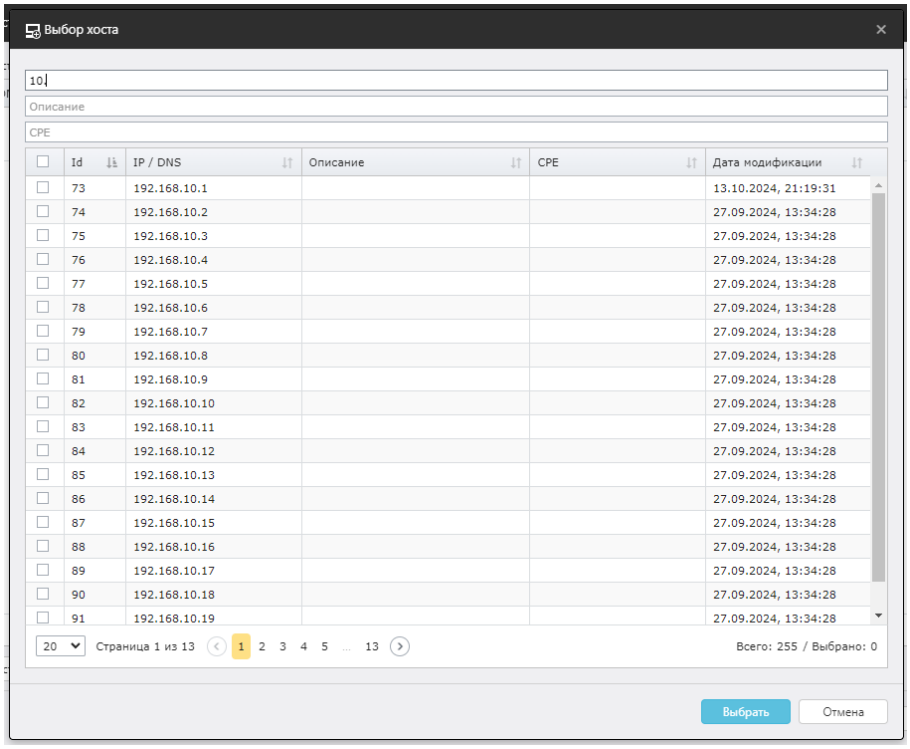


- Выбрать сканирование – сравнение выбранной выше итерации будет проходить с одной конкретной итерацией запуска для выбранного задания;

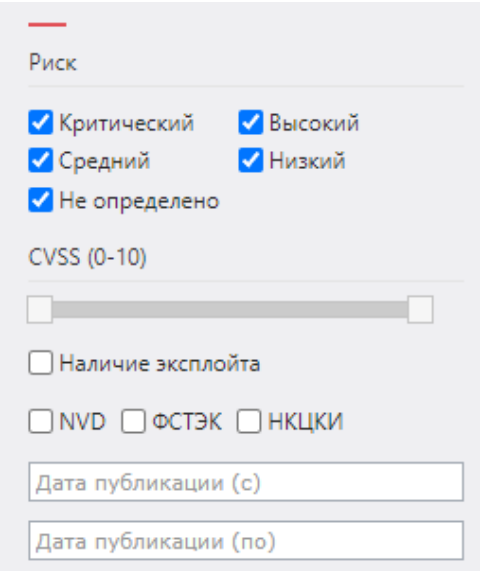


- Хосты – можно выбрать хосты, для которых будет проведен контроль устранения уязвимостей. Нажмите на ..., после чего откроется окно выбора групп и хостов:

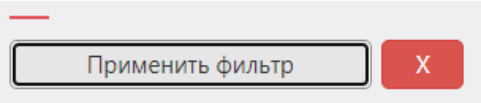




- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; Сведения об интегральной оценке по базовым метрикам CVSS;
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;
- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.



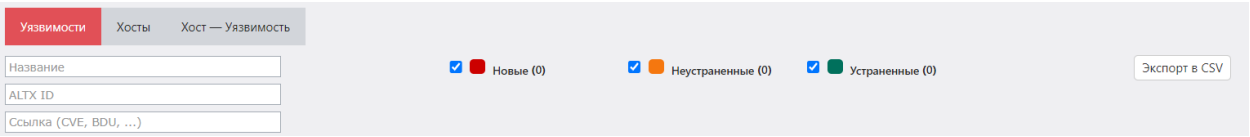
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Название – название уязвимости;
- ALTX ID – уникальный идентификатор уязвимости, состоящий из цифр;
- Ссылка – идентификатор бюллетеня по данной уязвимости;
- Статус уязвимости – в таблице будут отображаться уязвимости с отмеченными статусами. Если хотя бы на одном хосте уязвимость имеет выбранный статус, она попадёт в данную таблицу.
    - Новые – уязвимости, появившиеся в актуальном сканировании (итерации запуска);
    - Неустраненные – уязвимости, которые были найдены в предыдущих сканированиях и остались неустраненными в актуальном сканировании;
    - Устраненные – уязвимости, которые были найдены в предыдущих сканированиях и устранены в актуальном сканировании;



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы.

Полученный файл будет называться **VulnerabilityRemediationControl-Vulnerabilities-dd-mm-yyyy.csv**.

Структура CSV файла

ALTX ID	Уникальный идентификатор уязвимости
Риск	Принимает значения: Критический, Высокий, Средний, Низкий
Оценка CVSS	Значение указывается в двойных кавычках. Сведения об интегральной оценке по базовым метрикам CVSS
Источник CVSS	Название вендора или базы данных уязвимостей, откуда взято значение для оценки CVSS
Уязвимость	Имя уязвимости
Описание	Описание уязвимости
Дата публикации	Дата публикации бюллетеня вендором
Новая для хостов	Количество хостов, для которых данная уязвимость новая, т.е. появилась в актуальном сканировании (итерации запуска)
Неустраненная для хостов	Количество хостов, для которых данная уязвимость была найдены в предыдущих сканированиях и осталась неустраненной в актуальном сканировании
Устраненная для хостов	Количество хостов, для которых данная уязвимость была найдены в предыдущих сканированиях и устранена в актуальном сканировании

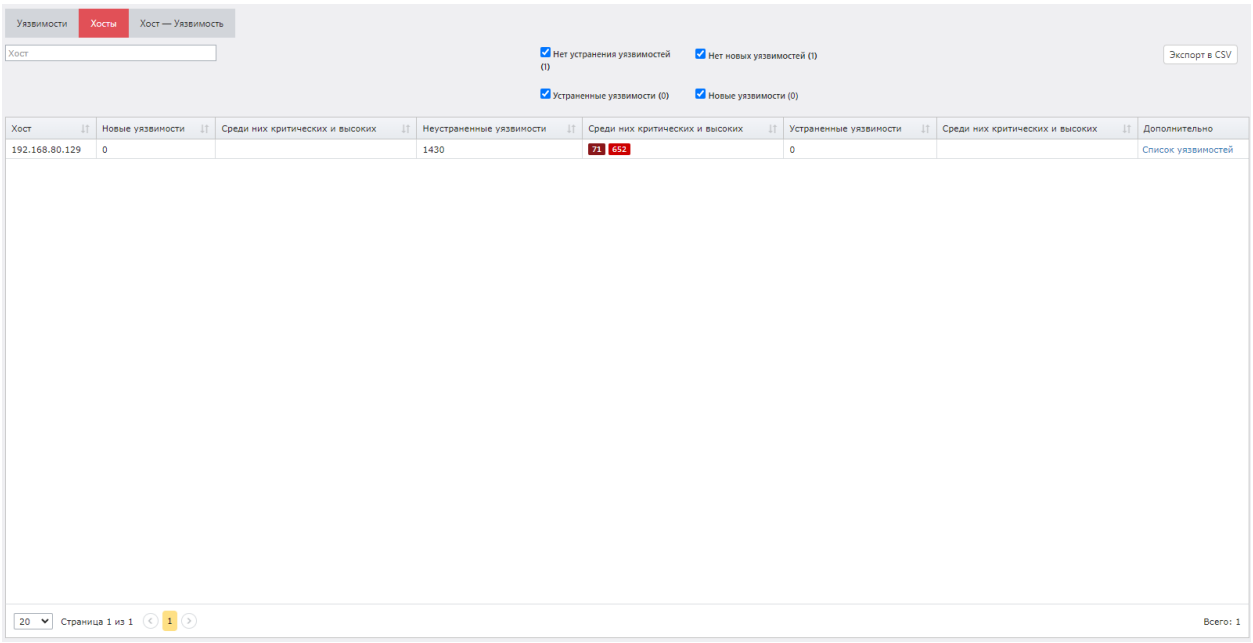
Пример:

Bash (оболочка Unix)

```
ALTX ID,Риск,Оценка CVSS,Источник CVSS,Уязвимость,Описание,Дата
публикации,Новая для хостов,Неустраненная для хостов,Устраненная для
хостов
404856,Средний,"6,5",BDU,"Astra Linux -- уязвимость в thunderbird,
icu (CVE-2020-21913)","В продуктах thunderbird, icu обнаружена
уязвимость CVE-2020-21913.",20.09.2021,0,1,0
```

8.4.2 Вкладка Хосты

В данной вкладке отображается информация о наличии или устранении уязвимостей на хостах, согласно выбранному заданию и итерации запуска в сравнении с предыдущими итерациями.

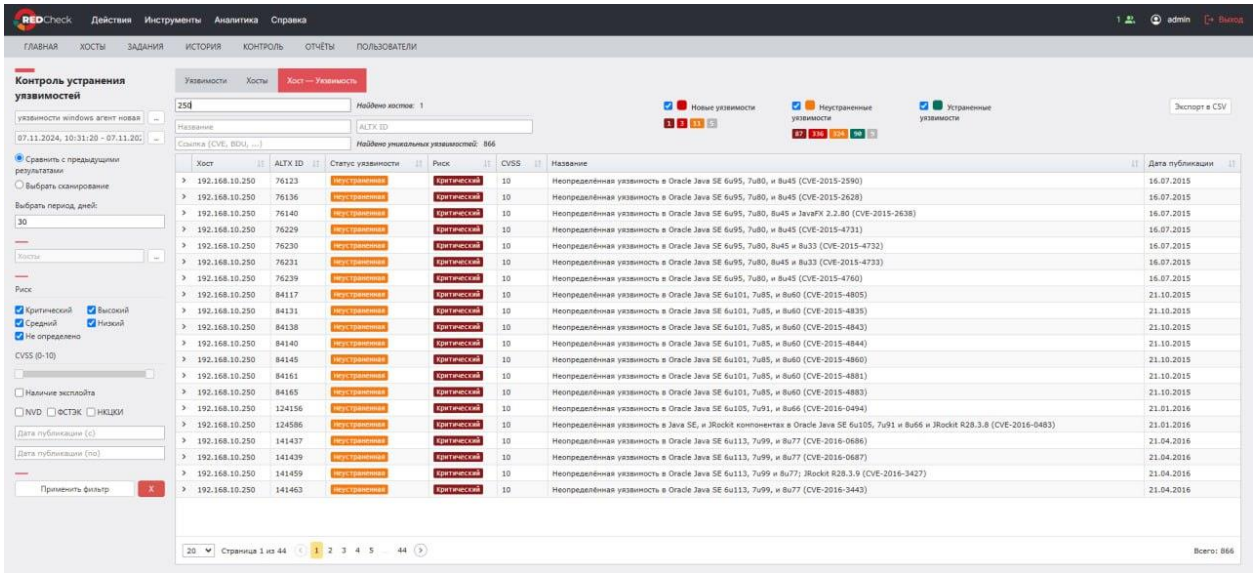


Информация об уязвимостях на хосте включает в себя:

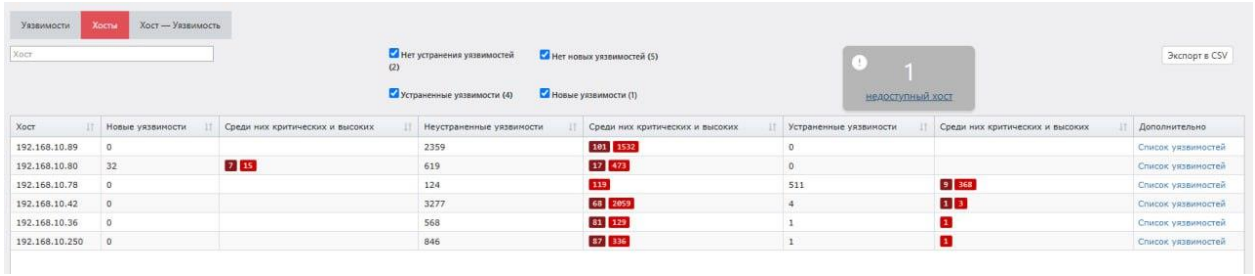
- Хост – IP-адрес или DNS-имя хоста;
- Новые уязвимости (среди них критических и высоких) – количество новых уязвимостей для хоста и сколько среди них с риском Критическая и Высокая;
- Неустраненные уязвимости (среди них критических и высоких) – количество неустраненных уязвимостей для хоста и сколько среди них с риском Критическая и Высокая;
- Устраненные уязвимости (среди них критических и высоких) – количество устраненных уязвимостей для хоста и сколько среди них с риском Критическая и Высокая;

Нажав **Список уязвимостей**, вы перейдете на вкладку **«Хост – Уязвимость»**, где в фильтре для результирующей таблицы уже будет указано имя выбранного

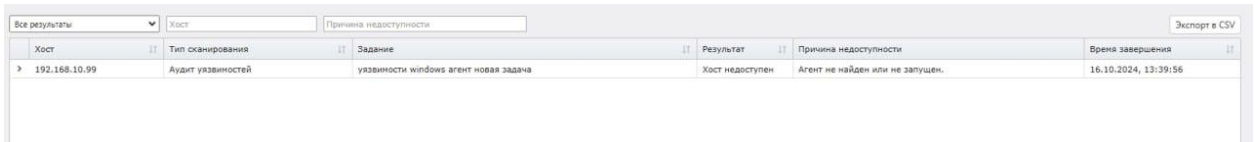
хоста. Под каждым чекбоксом фильтра по Статусу уязвимости будет отображаться количество уязвимостей с группировкой по риску.



Если в актуальном сканировании не найдены хосты, которые были в прошлых итерациях запуска, то появится баннер с указанием количества недоступных хостов.

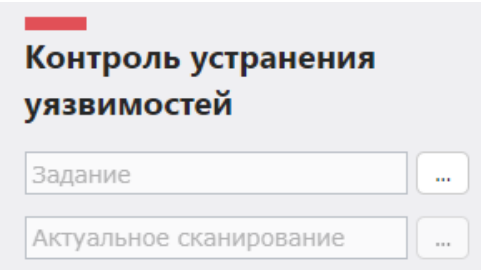


При нажатии на **Недоступный хост** будет открыта форма **«Недоступность хостов»** с перечнем хостов и причин их недоступности.



Общий фильтр

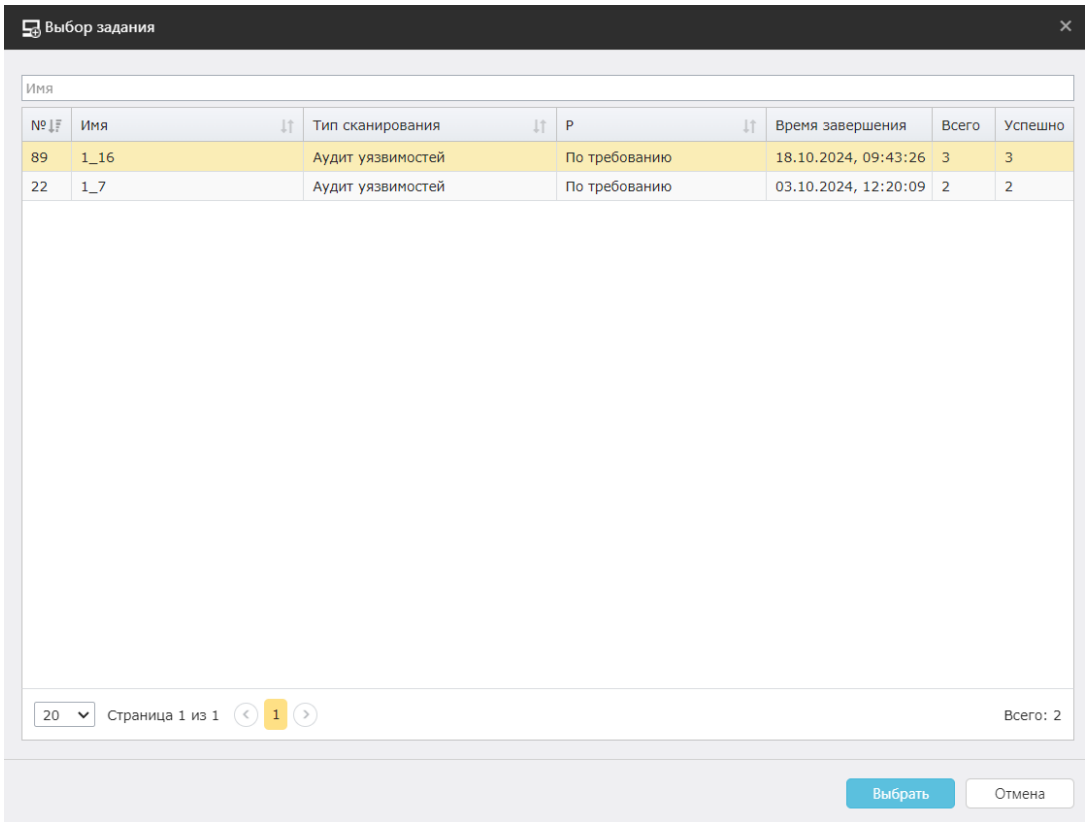
Общий фильтр располагается слева от результирующей таблицы.



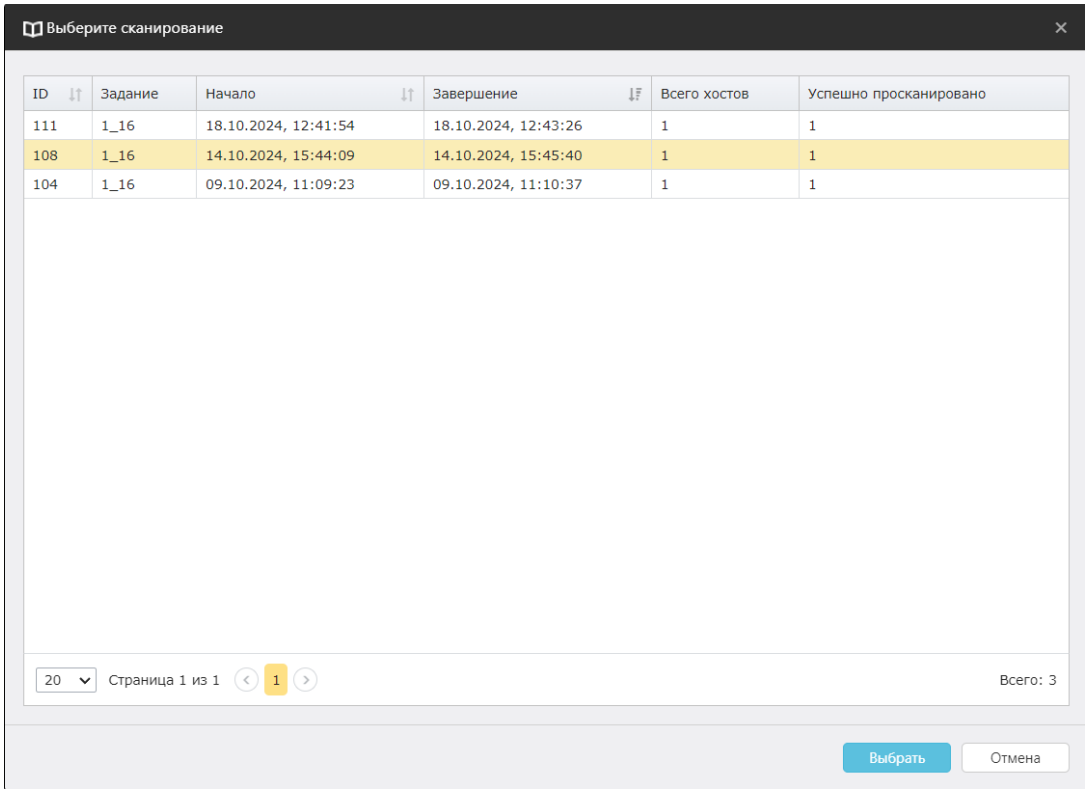
- Задание – необходимо выбрать задание типа Аудит уязвимостей.

  Нажмите на ..., после чего откроется окно выбора:

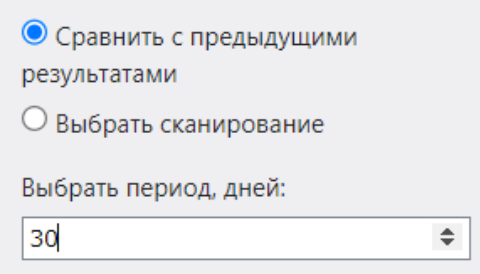
  - Всего – сколько было запусков задания;
  - Успешно – сколько из них выполнились успешно (хотя бы одно сканирование имеет статус **Завершено**);



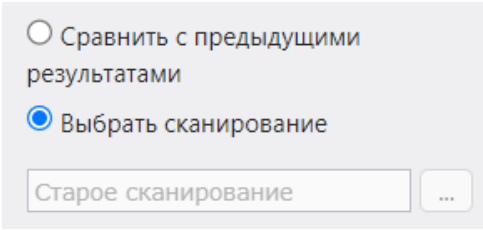
- Актуальное сканирование – необходимо выбрать итерацию запуска, с которой будут сравниваться предыдущие запуски. В такой итерации запуска должно быть хотя бы одно успешное сканирование;



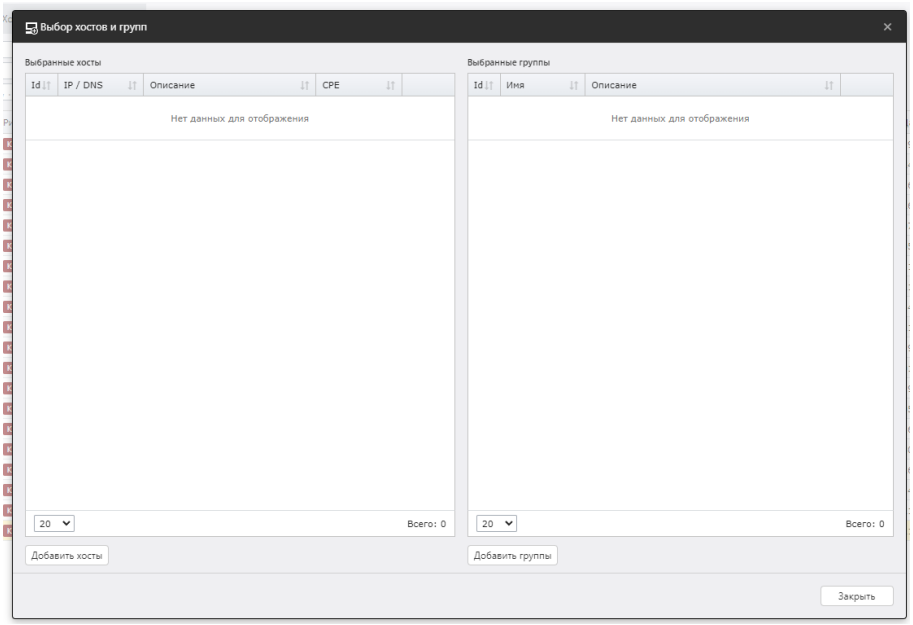
- Сравнивать с предыдущими результатами – сравнить с предыдущим успешным сканированием. Для каждого хоста предыдущее успешное сканирование подбирается индивидуально и может быть взято из разных итерацией запуска. Фильтр по времени позволяет ограничить период, за который подбирается предыдущее успешное сканирование;;

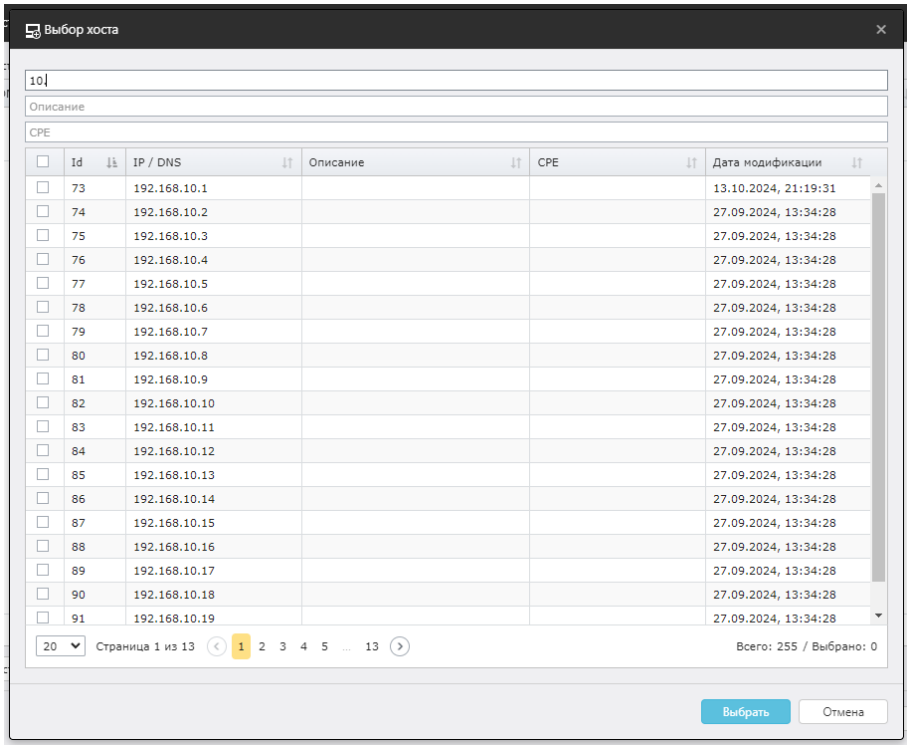


- Выбрать сканирование – сравнение выбранной выше итерации будет проходить с одной конкретной итерацией запуска для выбранного задания;

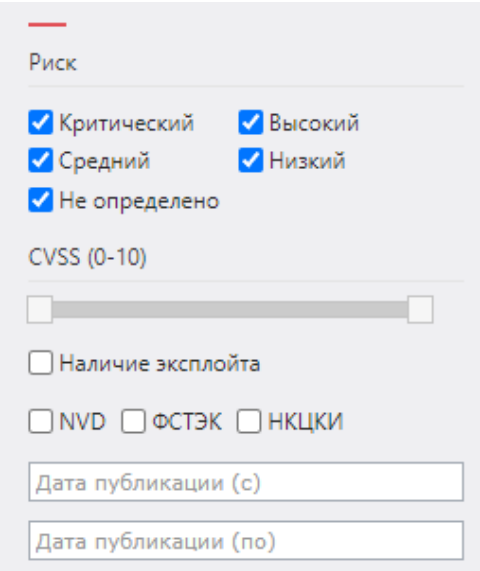


- Хосты – можно выбрать хосты, для которых будет проведен контроль устранения уязвимостей. Нажмите на ..., после чего откроется окно выбора групп и хостов:

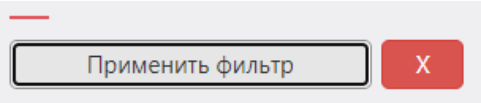




- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; Сведения об интегральной оценке по базовым метрикам CVSS;
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;
- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.



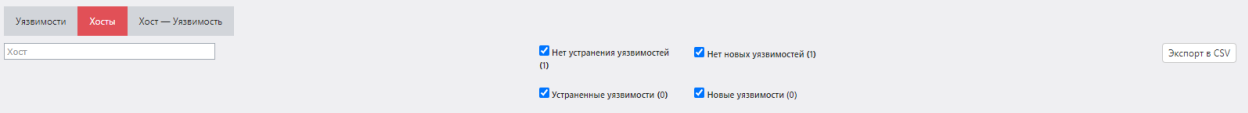
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Хост – IP-адрес или DNS-имя хоста. Можно указывать как полное значение, так и часть;
- Статус уязвимости – будет отображаться:
  - Нет устранения уязвимостей – хосты, у которых значение столбца **Устраненные уязвимости** равно 0;
  - Нет новых уязвимостей – хосты, у которых значение столбца **Новые уязвимости** равно 0;
  - Устраненные уязвимости – хосты, у которых значение столбца **Устраненные уязвимости** НЕ равно 0;
  - Новые уязвимости – хосты, у которых значение столбца **Новые уязвимости** НЕ равно 0;



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **VulnerabilityRemediationControl-Hosts-dd-mm-yyyy.csv**.

Структура CSV файла

Id хоста	ID хоста
Имя хоста	IP-адрес или DNS-имя хоста
Новые уязвимости	Количество новых уязвимостей
Новые критические уязвимости	Количество новых уязвимостей с критическим риском Сведения об интегральной оценке по базовым метрикам CVSS
Новые уязвимости с высокой критичностью	Количество новых уязвимостей с высоким риском
Неустраненные уязвимости	Количество неустраненных уязвимостей
Неустраненные критические уязвимости	Количество неустраненных уязвимостей с критическим риском
Неустраненные уязвимости с высоким уровнем критичности	Количество неустраненных уязвимостей с высоким риском
Устраненные уязвимости	Количество устраненных уязвимостей
Устранённые критичные уязвимости	Количество устраненных уязвимостей с критическим риском
Устранённые	Количество устраненных уязвимостей с высоким риском

уязвимости с высокой критичностью	

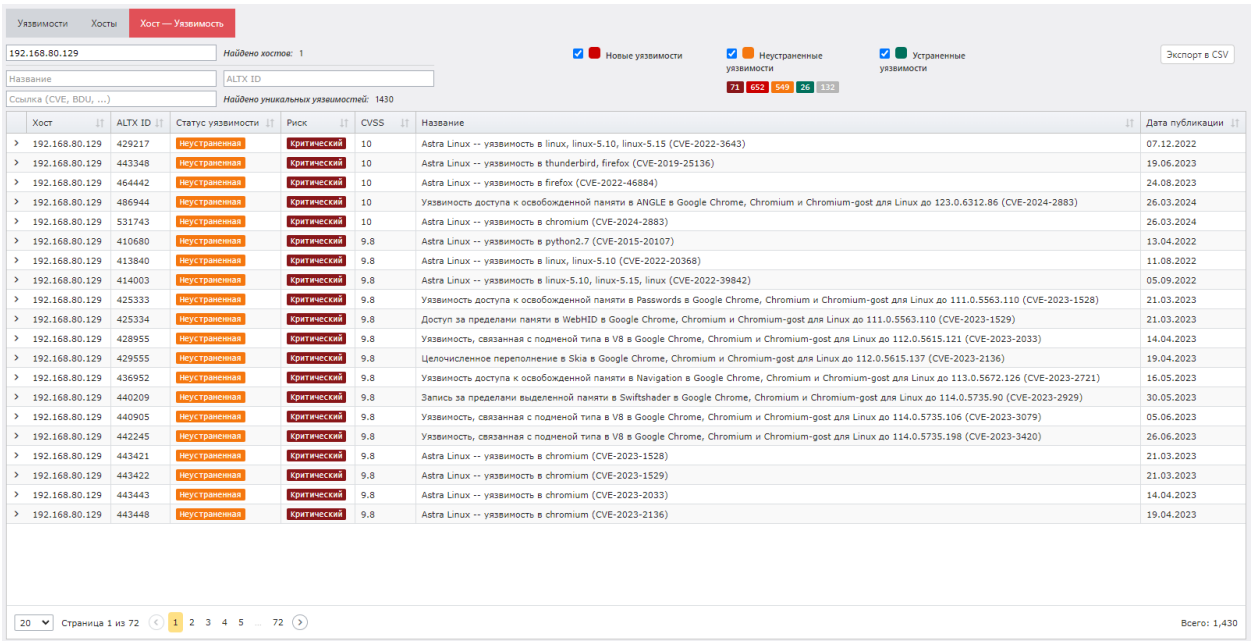
Пример:

Bash (оболочка Unix)

```
Id хоста,Имя хоста,Новые уязвимости,Новые критичные уязвимости,Новые
уязвимости с высокой критичностью,Неустраненные
уязвимости,Неустраненные критические уязвимости,Неустраненные
уязвимости с высоким уровнем критичности,Устраненные
уязвимости,Устранённые критичные уязвимости,Устранённые уязвимости с
высокой критичностью
67,192.168.80.129,0,0,0,1430,71,652,0,0,0
```

8.4.3 Вкладка Хост – Уязвимость

В данной вкладке отображается информация о наличии уязвимостей и их устранении с указанием к какому хосту они относятся, согласно выбранному заданию и итерации запуска в сравнении с предыдущими итерациями.

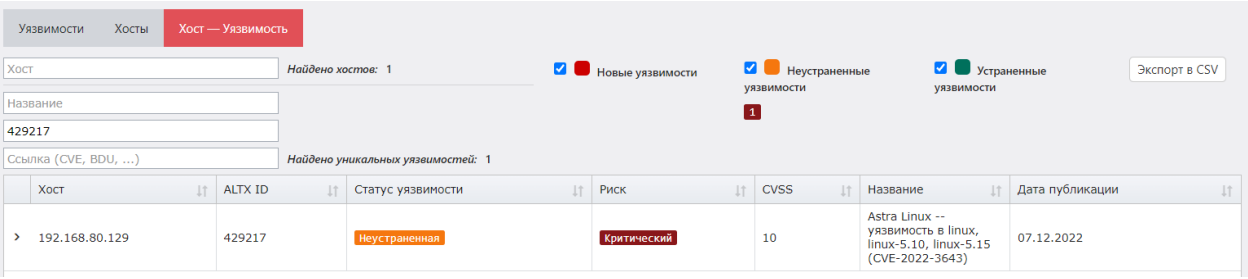


Хост	ALTX ID	Статус уязвимости	Риск	CVSS	Название	Дата публикации
192.168.80.129	429217	Неустраненная	Критический	10	Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)	07.12.2022
192.168.80.129	443348	Неустраненная	Критический	10	Astra Linux -- уязвимость в thunderbird, firefox (CVE-2019-25136)	19.06.2023
192.168.80.129	464442	Неустраненная	Критический	10	Astra Linux -- уязвимость в firefox (CVE-2022-46884)	24.08.2023
192.168.80.129	486944	Неустраненная	Критический	10	Уязвимость доступа к освобожденной памяти в ANGLE в Google Chrome, Chromium и Chromium-gost для Linux до 123.0.6312.86 (CVE-2024-2883)	26.03.2024
192.168.80.129	531743	Неустраненная	Критический	10	Astra Linux -- уязвимость в chromium (CVE-2024-2883)	26.03.2024
192.168.80.129	410680	Неустраненная	Критический	9.8	Astra Linux -- уязвимость в python2.7 (CVE-2015-20107)	13.04.2022
192.168.80.129	413840	Неустраненная	Критический	9.8	Astra Linux -- уязвимость в linux, linux-5.10 (CVE-2022-20368)	11.08.2022
192.168.80.129	414003	Неустраненная	Критический	9.8	Astra Linux -- уязвимость в linux-5.10, linux-5.15, linux (CVE-2022-39842)	05.09.2022
192.168.80.129	425333	Неустраненная	Критический	9.8	Уязвимость доступа к освобожденной памяти в Passwords в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1528)	21.03.2023
192.168.80.129	425334	Неустраненная	Критический	9.8	Доступ за пределами памяти в WebHID в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1529)	21.03.2023
192.168.80.129	428955	Неустраненная	Критический	9.8	Уязвимость, связанная с подменой типа в V8 в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.121 (CVE-2023-2033)	14.04.2023
192.168.80.129	429555	Неустраненная	Критический	9.8	Целочисленное переполнение в Skia в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.137 (CVE-2023-2136)	19.04.2023
192.168.80.129	436952	Неустраненная	Критический	9.8	Уязвимость доступа к освобожденной памяти в Navigation в Google Chrome, Chromium и Chromium-gost для Linux до 113.0.5672.126 (CVE-2023-2721)	16.05.2023
192.168.80.129	440209	Неустраненная	Критический	9.8	Запись за пределами выделенной памяти в Swiftshader в Google Chrome, Chromium и Chromium-gost для Linux до 114.0.5735.90 (CVE-2023-2929)	30.05.2023
192.168.80.129	440905	Неустраненная	Критический	9.8	Уязвимость, связанная с подменой типа в V8 в Google Chrome, Chromium и Chromium-gost для Linux до 114.0.5735.106 (CVE-2023-3079)	05.06.2023
192.168.80.129	442245	Неустраненная	Критический	9.8	Уязвимость, связанная с подменой типа в V8 в Google Chrome, Chromium и Chromium-gost для Linux до 114.0.5735.198 (CVE-2023-3420)	26.06.2023
192.168.80.129	443421	Неустраненная	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-1528)	21.03.2023
192.168.80.129	443422	Неустраненная	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-1529)	21.03.2023
192.168.80.129	443443	Неустраненная	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-2033)	14.04.2023
192.168.80.129	443448	Неустраненная	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-2136)	19.04.2023

Информация об уязвимости включает в себя:

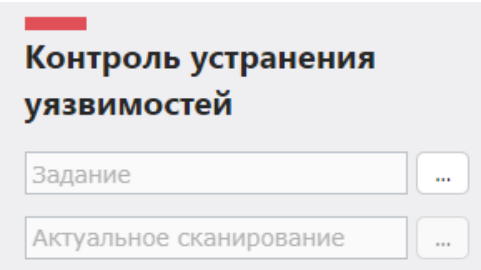
- Хост – IP-адрес или DNS-имя (ID хоста);
- Уникальный идентификатор ALTX ID;
- Ссылка на страницу уязвимости в OVALdb;
- Риск и CVSS – Сведения об интегральной оценке по базовым метрикам CVSS;
- Имя уязвимости, описание, дата публикации вендором;
- Ссылки на бюллетени по данной уязвимости;
- Детализация – какие пакеты или файлы уязвимы;

Нажав **Список хостов**, вы перейдете на вкладку **«Хост – Уязвимость»**, где в фильтре для результирующей таблицы уже будет указан ALTX ID выбранной уязвимости.



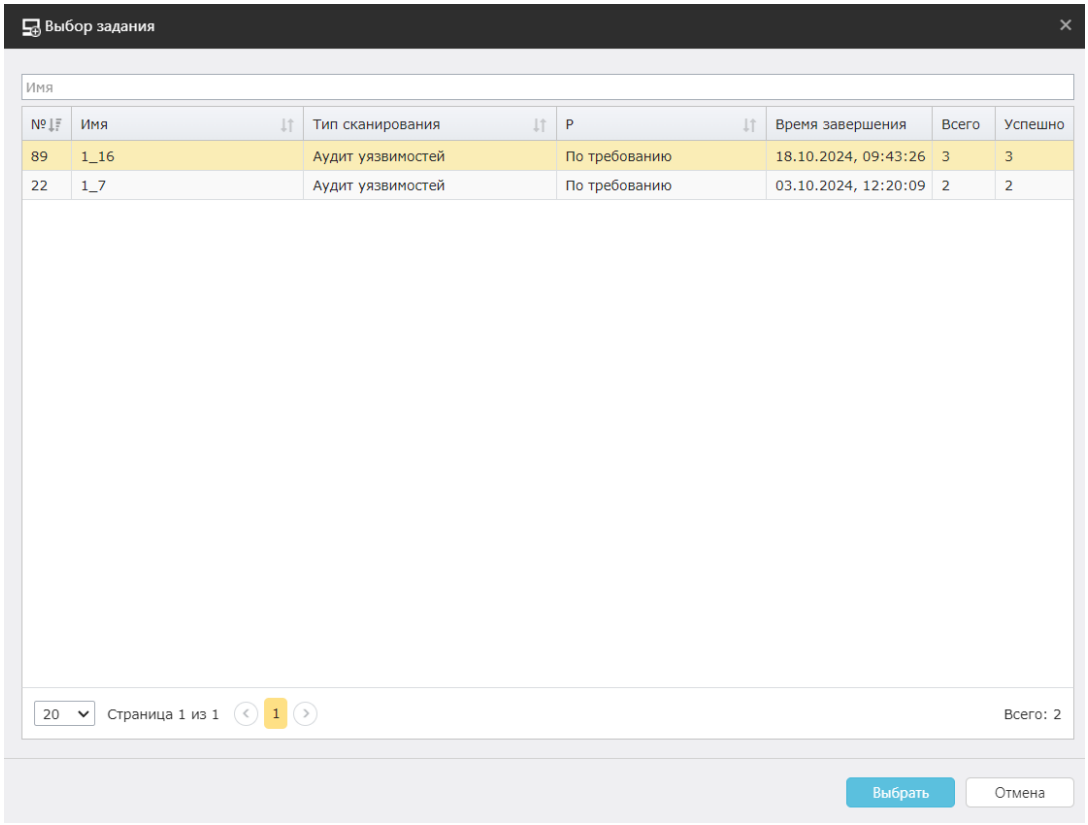
Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

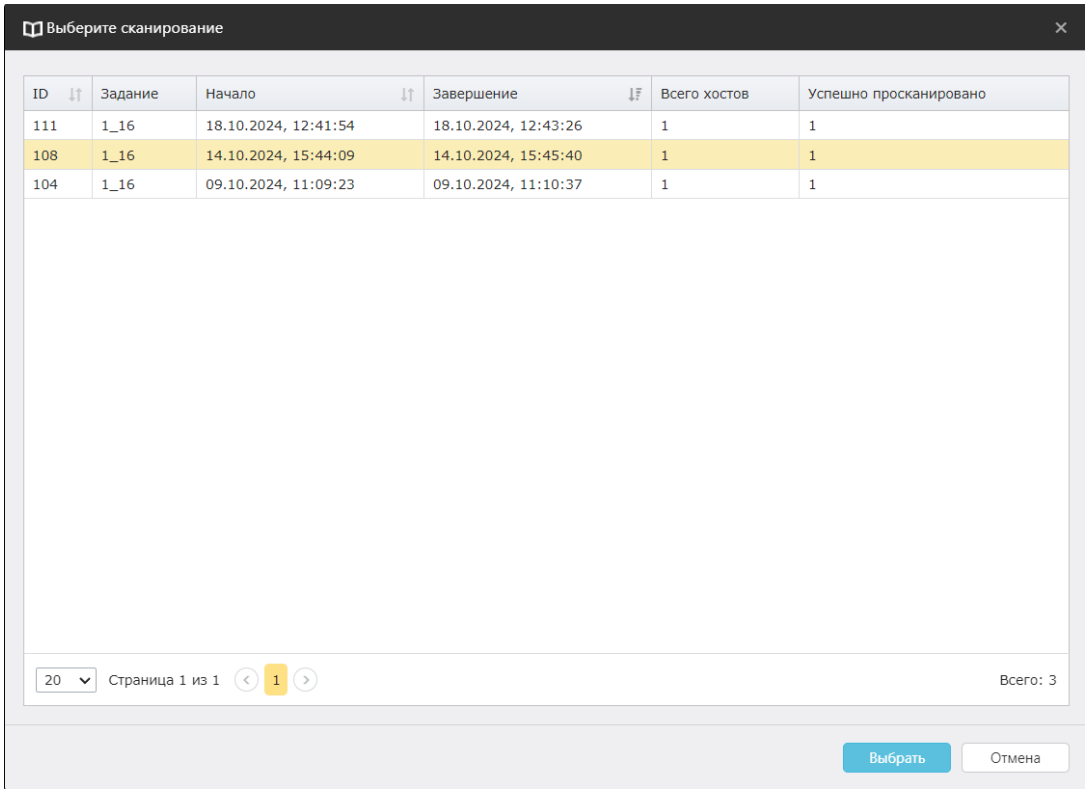


- Задание – необходимо выбрать задание типа Аудит уязвимостей.

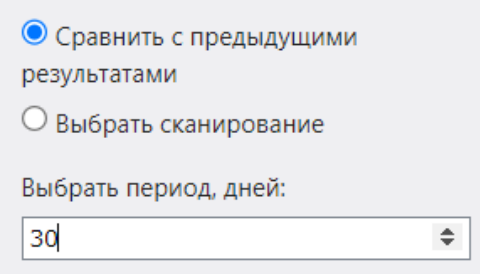
  Нажмите на ..., после чего откроется окно выбора:
  - Всего – сколько было запусков задания;
  - Успешно – сколько из них выполнились успешно (хотя бы одно сканирование имеет статус **Завершено**);



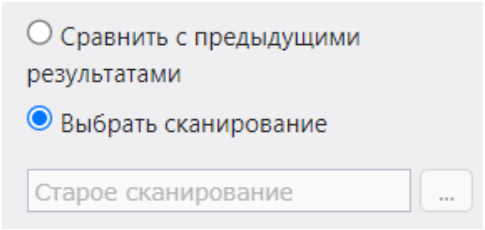
- Актуальное сканирование – необходимо выбрать итерацию запуска, с которой будут сравниваться предыдущие запуски. В такой итерации запуска должно быть хотя бы одно успешное сканирование;



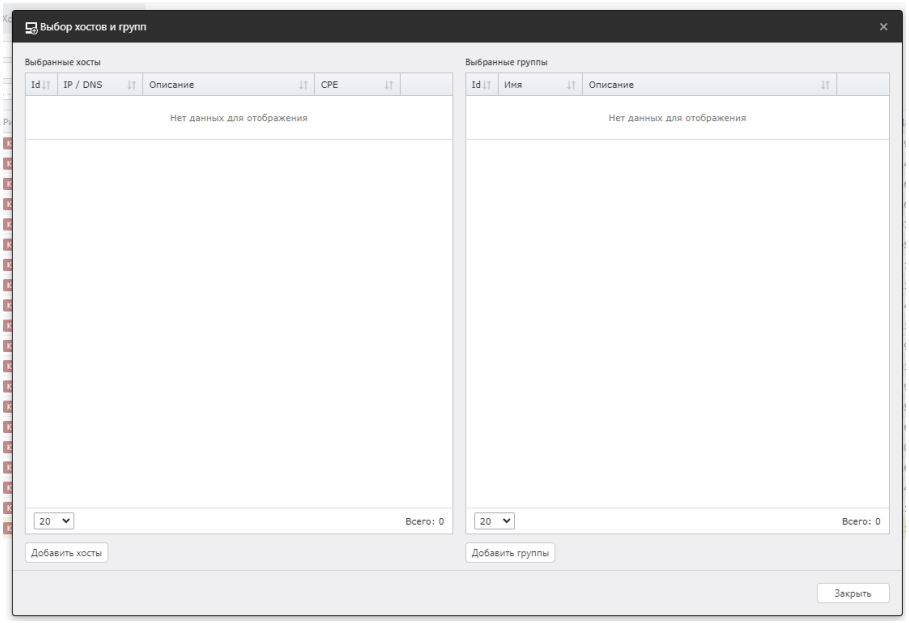
- Сравнивать с предыдущими результатами – сравнить с предыдущим успешным сканированием. Для каждого хоста предыдущее успешное сканирование подбирается индивидуально и может быть взято из разных итерацией запуска. Фильтр по времени позволяет ограничить период, за который подбирается предыдущее успешное сканирование;;

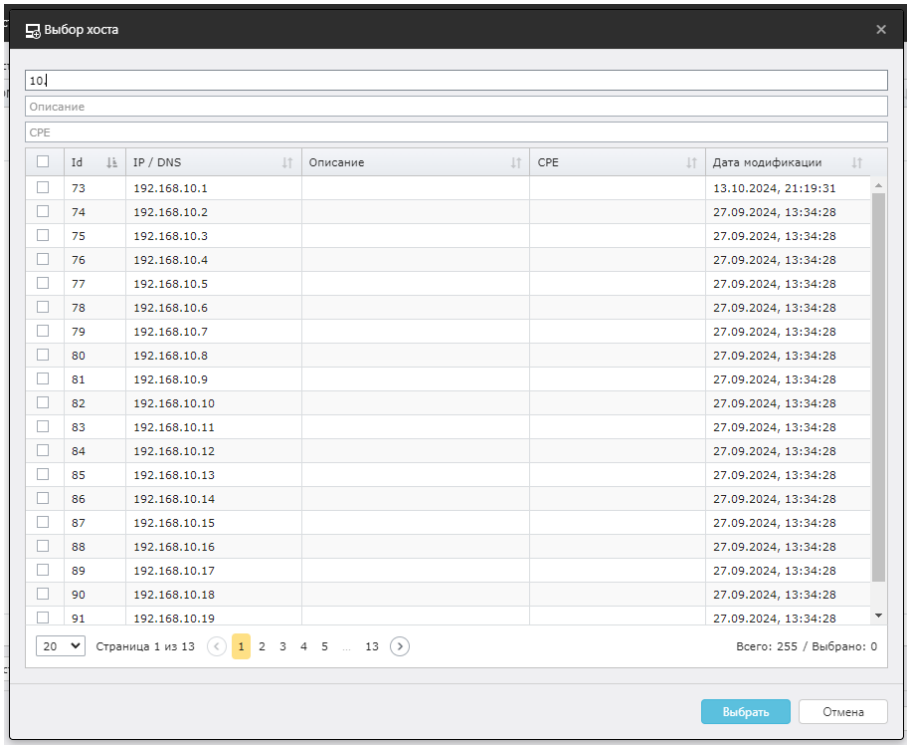


- Выбрать сканирование – сравнение выбранной выше итерации будет проходить с одной конкретной итерацией запуска для выбранного задания;

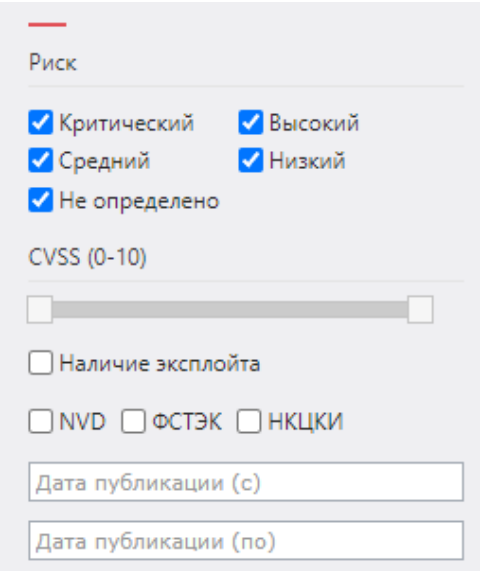


- Хосты – можно выбрать хосты, для которых будет проведен контроль устранения уязвимостей. Нажмите на ..., после чего откроется окно выбора групп и хостов:

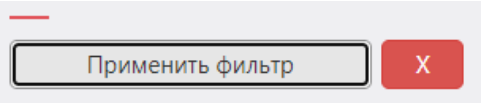




- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; Сведения об интегральной оценке по базовым метрикам CVSS;
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;
- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.



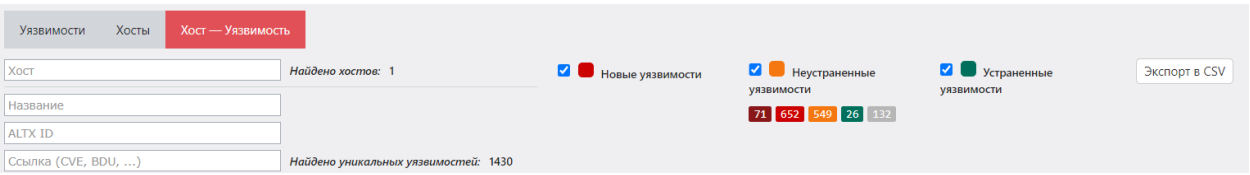
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Хост – IP-адрес или DNS-имя хоста. Можно указывать как полное значение, так и часть;
- Название – название уязвимости;
- ALTX ID – уникальный идентификатор уязвимости, состоящий из цифр;
- Ссылка – идентификатор бюллетеня по данной уязвимости;
- Статус уязвимости – в таблице будут отображаться уязвимости с отмеченными вариантами риска.
    - Новые уязвимости – уязвимости, появившиеся в актуальном сканировании (итерации запуска);
    - Неустраненные уязвимости – уязвимости, которые были найдены в предыдущих сканированиях и остались неустраненными в актуальном сканировании;
    - Устраненные уязвимости – уязвимости, которые были найдены в предыдущих сканированиях и устранены в актуальном сканировании;
- Найдено хостов – количество хостов;
- Найдено уникальных уязвимостей – количество уникальных уязвимостей, обнаруженных на всех найденных хостах;



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **VulnerabilityRemediationControl-HostVulnerability-dd-mm-yyyy.csv**.

Структура CSV файла

Id хоста	ID хоста
Имя хоста	IP-адрес или DNS-имя хоста
ALTX ID	Уникальный идентификатор уязвимости
OVAL определение	Название вендора или базы данных уязвимостей, откуда взято значение для оценки CVSS
Статус уязвимости	Принимает значения: Устраненная, Неустраненная, Новая
Риск	Принимает значения: Критический, Высокий, Средний, Низкий
Оценка CVSS	Значение указывается в двойных кавычках. Сведения об интегральной оценке по базовым метрикам CVSS
Источник CVSS	Название вендора или базы данных уязвимостей, откуда взято значение для оценки CVSS
Уязвимость	Имя уязвимости. Указывается в двойных кавычках
Описание	Описание уязвимости
Дата публикации	Дата публикации бюллетеня вендором

Детализация	Уязвимые пакеты или файлы. Если значений несколько, разделяется точкой с запятой

Пример:

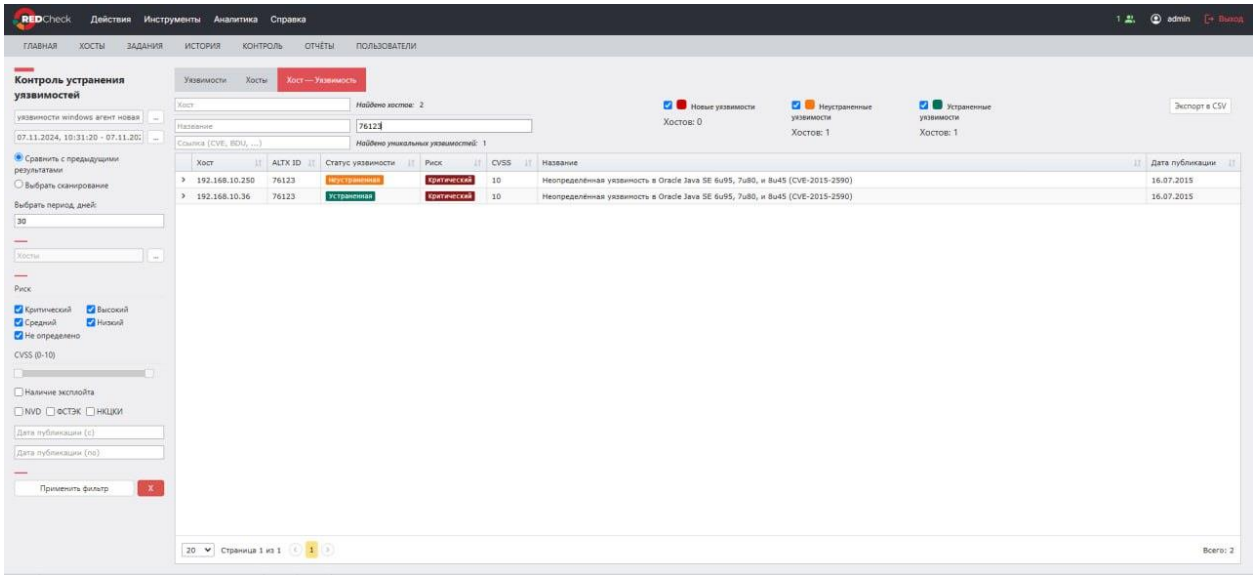
Bash (оболочка Unix)

```
Id хоста,Имя хоста,ALTX ID,OVAL определение,Статус
уязвимости,Риск,Оценка CVSS,Источник CVSS,Уязвимость,Описание,Дата
публикации,Детализация
67,192.168.80.129,404856,oval:ru.altx-
soft.nix:def:188035,Неустраненная,Средний,"6,5",BDU,"Astra Linux --
уязвимость в thunderbird, icu (CVE-2020-21913)","В продуктах
thunderbird, icu обнаружена уязвимость CVE-2020-
21913.",20.09.2021,thunderbird (1:102.9.1+build1-
0ubuntu1+ci202304061128+astra1);thunderbird-locale-ru
(1:102.9.1+build1-0ubuntu1+ci202304061128+astra1)
```

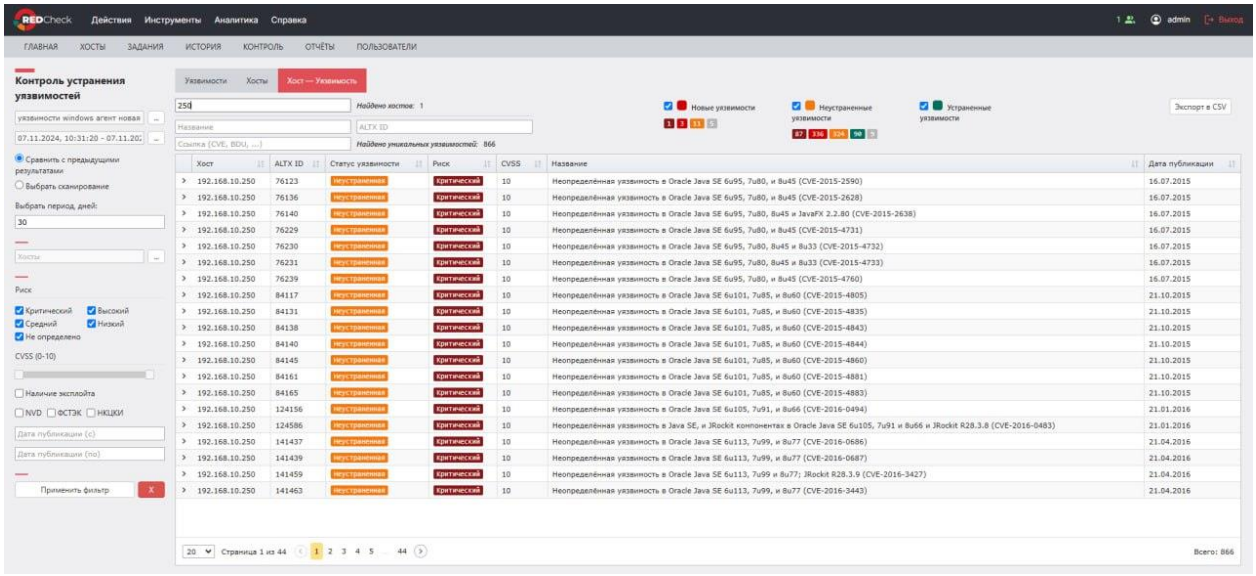
Дополнительная информация на форме

1 Случай. В фильтре для результирующей таблицы указан ALTX ID. В случае, если одна и та же уязвимость будет найдена в разных файлах / пакетах, то для каждого случая в таблице отобразится собственная строка с информацией.

Если анализируется одна уникальная уязвимость, то под чекбоксами фильтра «по Статусу уязвимости» будет указано количество хостов для каждого статуса.



2 Случай. В фильтре для результирующей таблицы указано имя выбранного хоста. Под каждым чекбоксом фильтра по Статусу уязвимости будет отображаться количество уязвимостей с группировкой по риску.



8.5 Анализ конфигураций

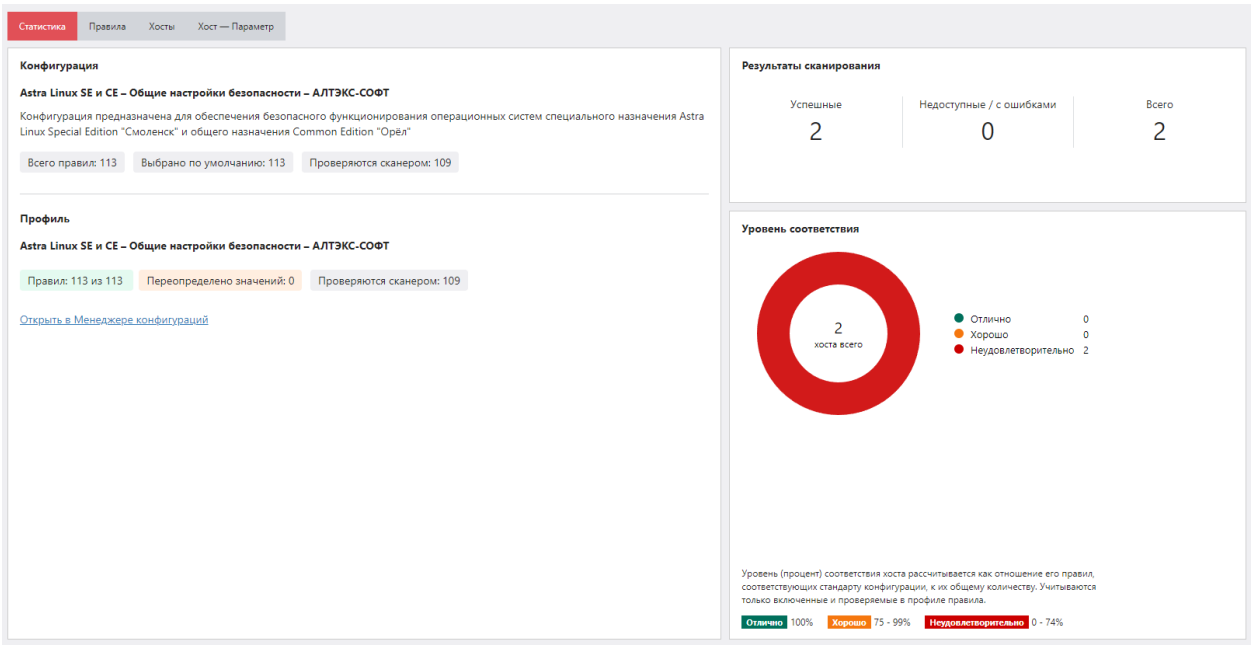
Данная форма аналитики позволяет оценить соответствие инфраструктуры правилам выбранной конфигурации.

Для перехода на форму нажмите **Аналитика** → **Анализ конфигураций**

Содержание

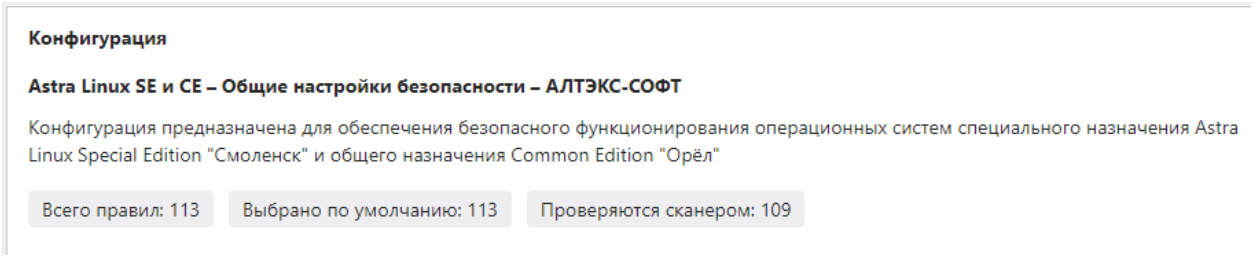
8.5.1 Вкладка Статистика

В данной вкладке отображается базовая информация о выбранной конфигурации, профиле, результатах сканирования и уровне соответствия хостов правилам конфигурации.

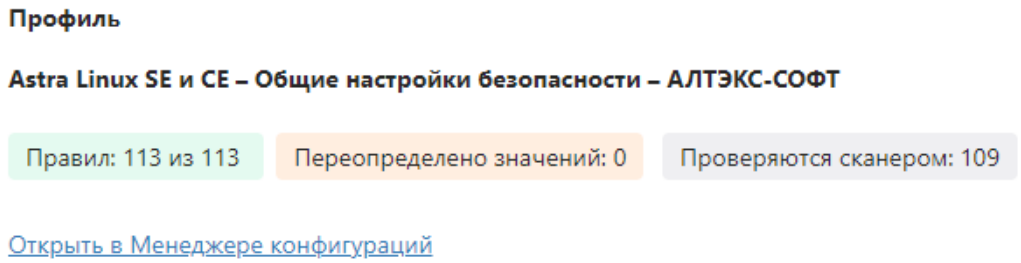


- Конфигурация – название и описание конфигурации, сколько всего правил в конфигурации, сколько правил включено для проверки, сколько правил проверяются сканером;

> Проверяются сканером – некоторые правила не могут быть проверены сканером. Это касается правил, например, связанных с процессами документирования. Фактически у сканера нет возможности узнать, документирует ли ваша команда какой-либо процесс, однако это является рекомендацией.

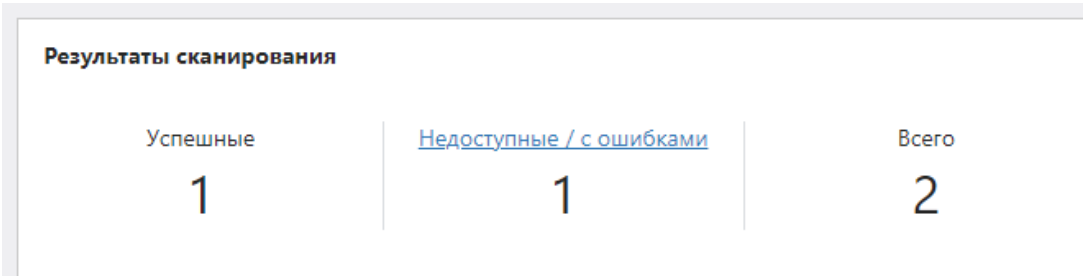


- Профиль – название профиля, количество включенных правил, количество переопределенных в правилах значений, количество проверяемых сканером правил;

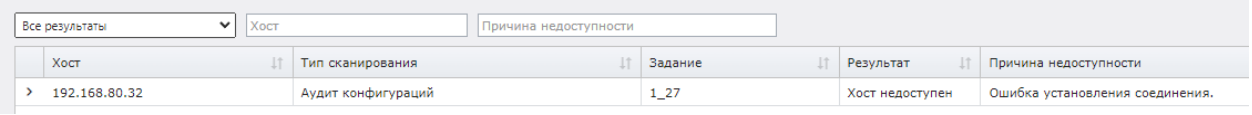


- Результаты сканирования – согласно общему фильтру отображается количество успешных сканирований, завершенных с ошибкой или недоступностью хоста, а также общее количество сканирований;

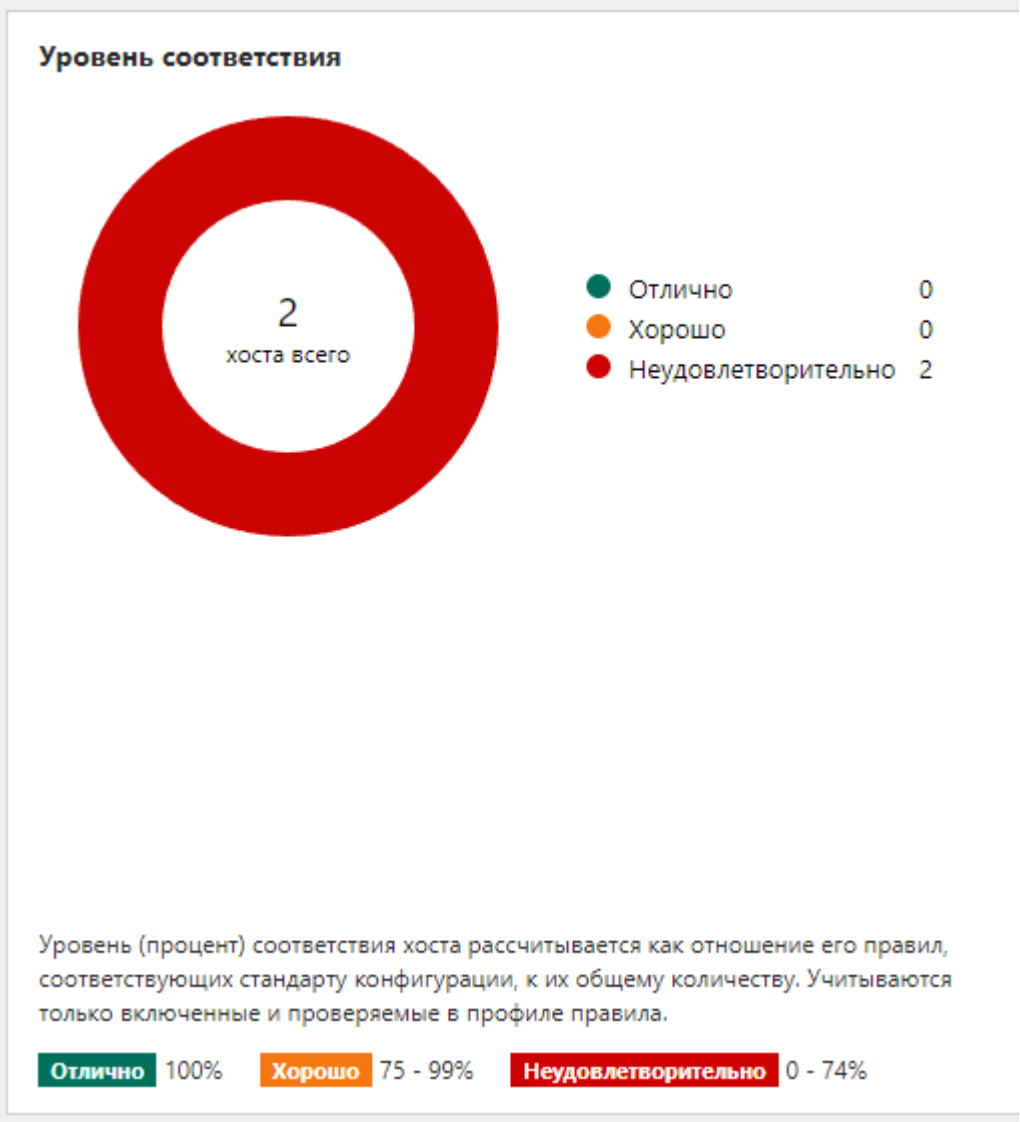
> Подсчет результатов сканирования со статусом **Хост недоступен** или **Ошибка** не будет произведен для сканирований, завершенных раньше обновления RedCheck до версии 2.8.0



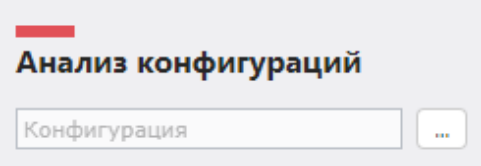
Нажав **Недоступные / с ошибками**, вы перейдете на форму **Недоступность хостов**, где в таблице будет информация по каждому недоступному хосту.



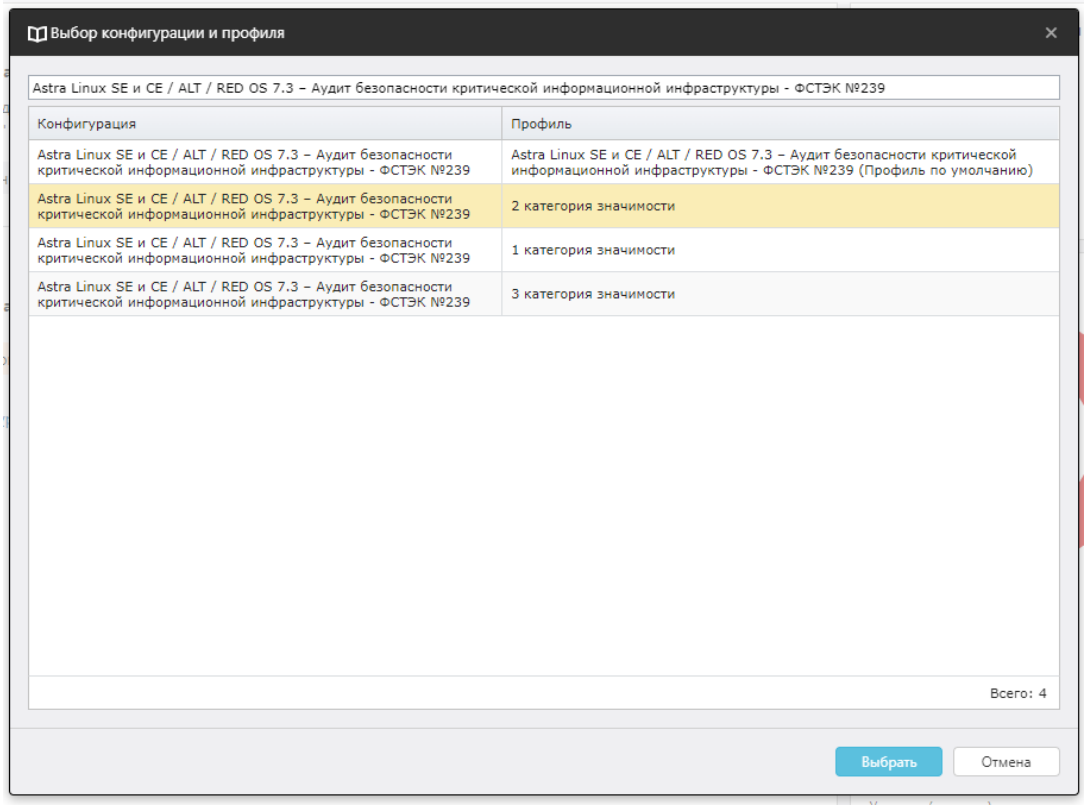
- Уровень соответствия – графическое изображение соответствия объектов инфраструктуры выбранной конфигурации;



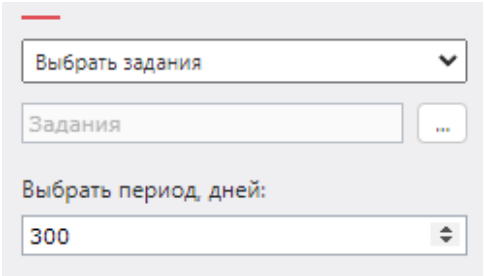
Общий фильтр



- Конфигурация – необходимо выбрать конфигурацию, соответствие которой будет определяться. Если у конфигурации есть несколько профилей, то в окне выбора будут отображаться несколько строк одной и той же конфигурации, но с разными профилями. Нажмите на ... и выберите нужную конфигурацию;

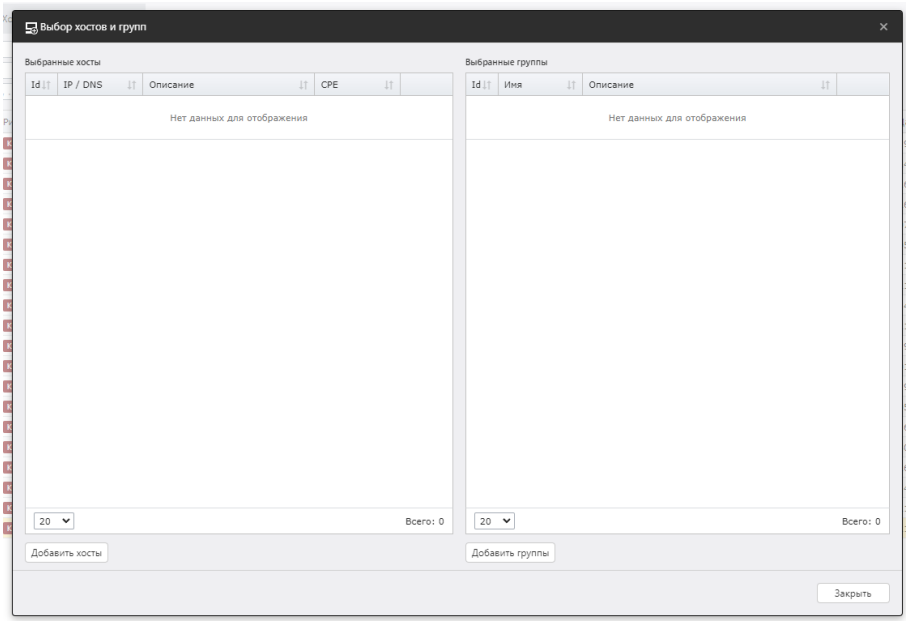


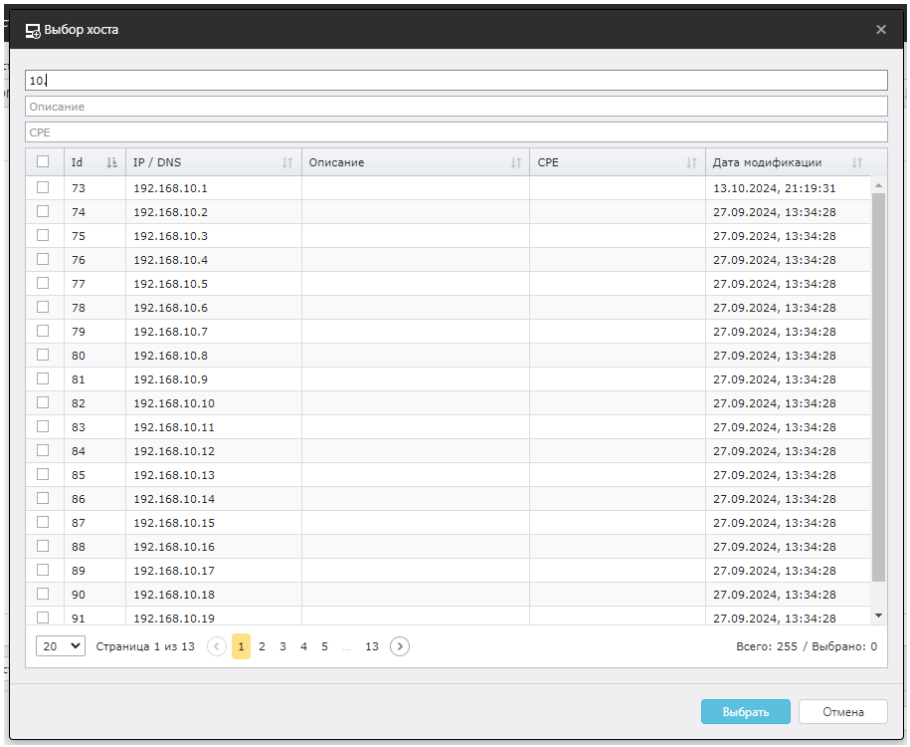
- Задания – можно выбрать задания, из результатов сканирования которых будет производиться анализ конфигураций. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:



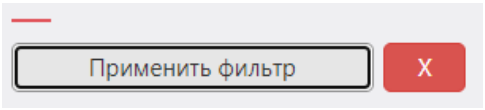
Нажмите на ..., после чего откроется окно выбора заданий;

- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для анализа конфигураций;
- Хосты – можно выбрать хосты, для которых будет проведен анализ конфигураций. Нажмите на ..., после чего откроется окно выбора групп и хостов:



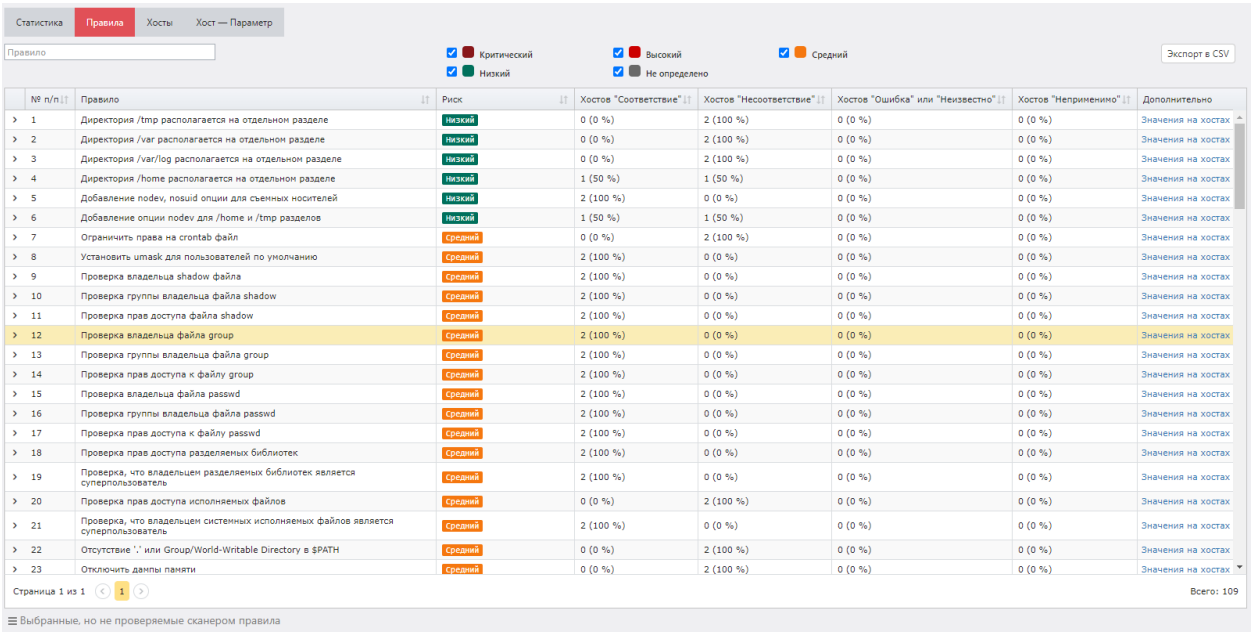


Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



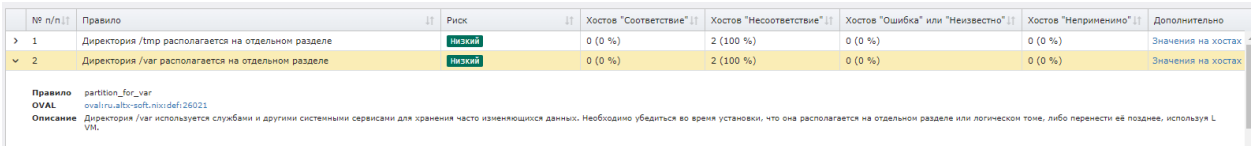
8.5.2 Вкладка Правила

В данной вкладке отображается информация по каждому проверяемому правилу конфигурации.



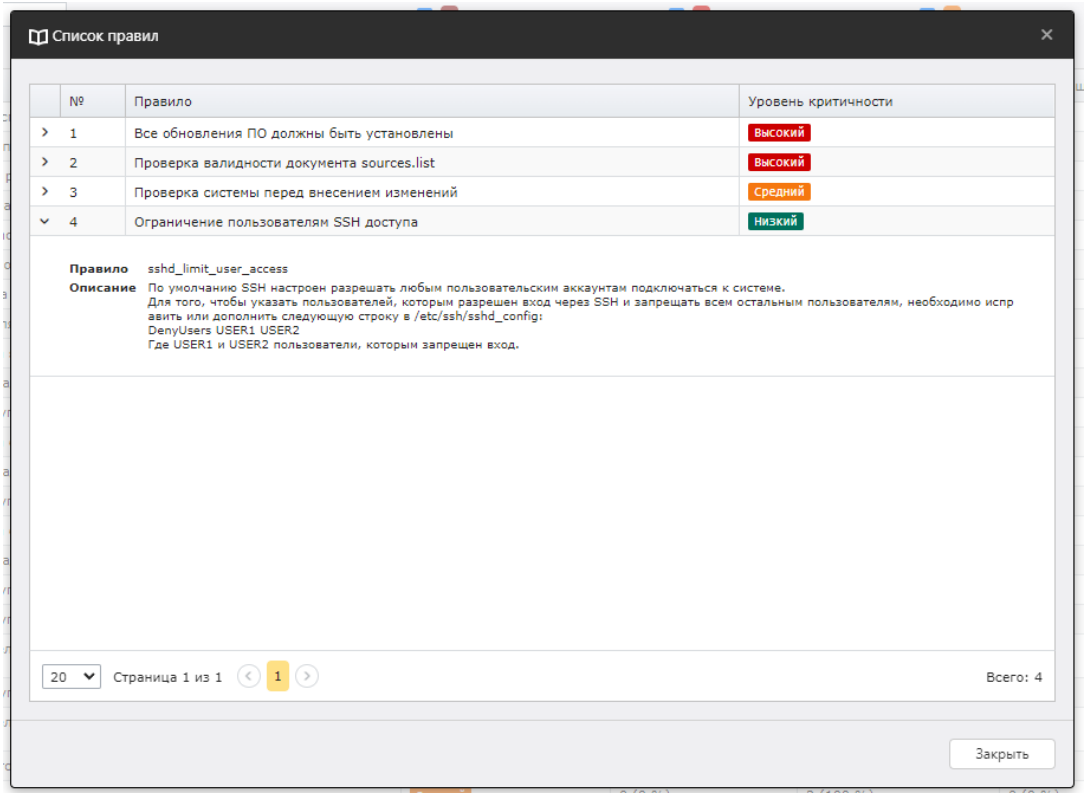
Информация о правиле включает в себя:

- Порядковый номер правила в конфигурации
- Правило – название и ID правила;
- OVAL – ссылка на страницу правила в OVALdb;
- Описание – описание правила;
- Уровень риска правила;
- Хостов "Соответствие" – количество хостов, которые соответствуют правилу;
- Хостов "Несоответствие" – количество хостов, которые не соответствуют правилу;
- Хостов "Ошибка" или "Неизвестно" – количество хостов, проверка правила на которых завершилась с результатом "Ошибка" или "Неизвестно";
- Хостов "Неприменимо" – количество хостов, для которых правило неприменимо;

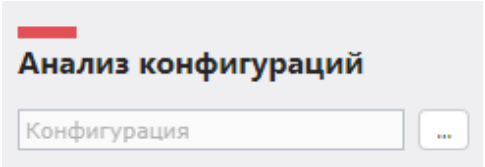


Нажав **Значения на хостах**, вы перейдете на вкладку **«Хост – Параметр»**, где уже будет выбрано соответствующее правило.

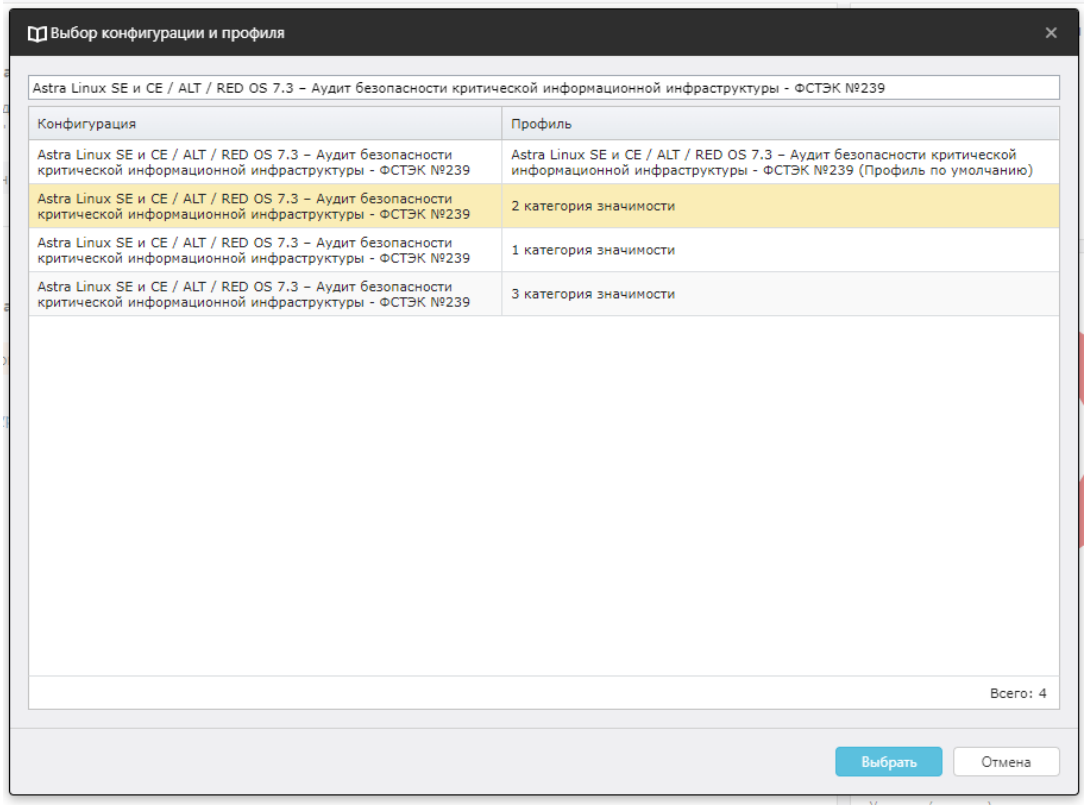
Под таблицей находится кликабельная ссылка **Выбранные, но не проверяемые сканером правила**. При нажатии открывается окно со списком правил, которые не проверяются сканером.



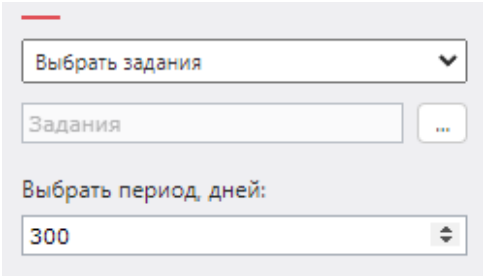
Общий фильтр



- Конфигурация – необходимо выбрать конфигурацию, соответствие которой будет определяться. Если у конфигурации есть несколько профилей, то в окне выбора будут отображаться несколько строк одной и той же конфигурации, но с разными профилями. Нажмите на ... и выберите нужную конфигурацию;

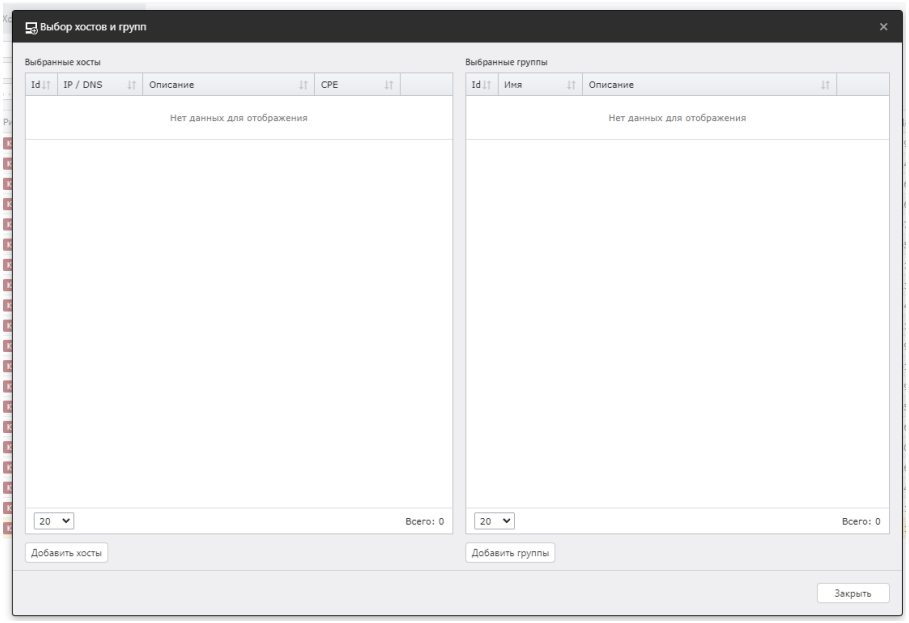


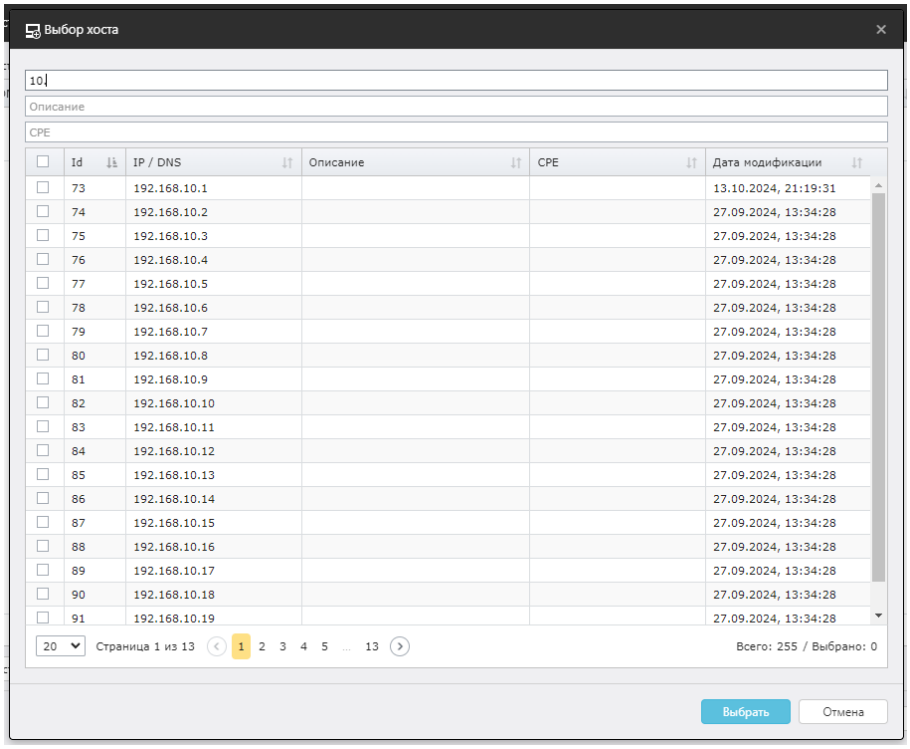
- Задания – можно выбрать задания, из результатов сканирования которых будет производиться анализ конфигураций. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:



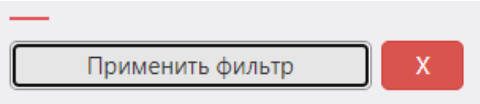
Нажмите на ..., после чего откроется окно выбора заданий;

- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для анализа конфигураций;
- Хосты – можно выбрать хосты, для которых будет проведен анализ конфигураций. Нажмите на ..., после чего откроется окно выбора групп и хостов:





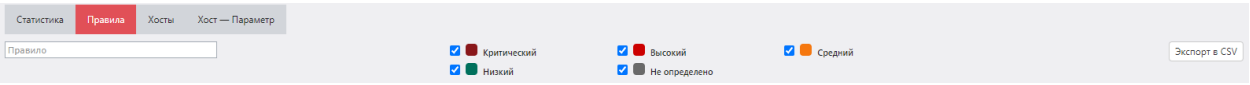
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Правило – название правила;
- Риск – в таблице будут отображаться правила с отмеченными вариантами риска.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **ComplianceAnalysis-RulesStatistics-dd-mm-yyyy.csv**.

Структура CSV файла

Номер правила	Порядковый номер правила в конфигурации
Правило	Название правила
Уровень критичности	Принимает значения: Критический, Высокий, Средний, Низкий
Количество хостов с результатом проверки правила Соответствие	Хостов "Соответствие"
Количество хостов с результатом проверки правила Несоответствие	Хостов "Несоответствие"
Количество хостов с результатом проверки правила Ошибка или Неизвестно	Хостов "Ошибка" или "Неизвестно"

Количество хостов с результатом проверки правила Неприменимо	Хостов "Неприменимо"
Id правила	ID правила, например partition_for_tmp
OVAL определение	Ссылка на OVAL-определение правила
Описание	Описание правила

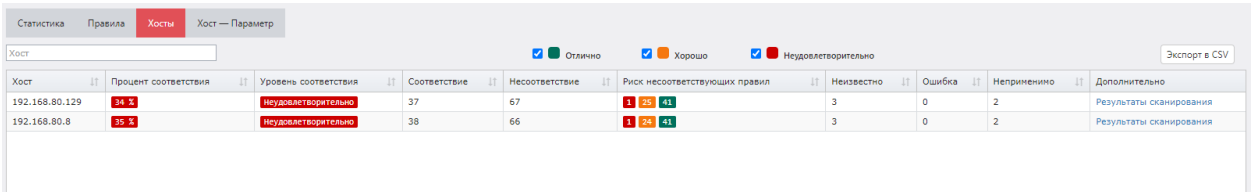
Пример:

Код

```
Номер правила,Правило,Уровень критичности,Количество хостов с
результатом проверки правила Соответствие,Количество хостов с
результатом проверки правила Несоответствие,Количество хостов с
результатом проверки правила Ошибка или Неизвестно,Количество хостов
с результатом проверки правила Неприменимо,Id правила,OVAL
определение,Описание
1,Директория /tmp располагается на отдельном
разделе,Низкий,0,2,0,0,partition_for_tmp,oval:ru.altx-
soft.nix:def:26020,"Директория /tmp доступна для всех на запись и
используется для хранения временных файлов. Необходимо убедиться во
время установки, что она располагается на отдельном разделе или
логическом томе, либо перенести её позднее, используя LVM."
```

8.5.3 Вкладка Хосты

В данной вкладке отображается информация о соответствии каждого хоста выбранной конфигурации.

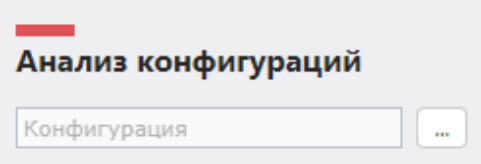


Информация о правиле включает в себя:

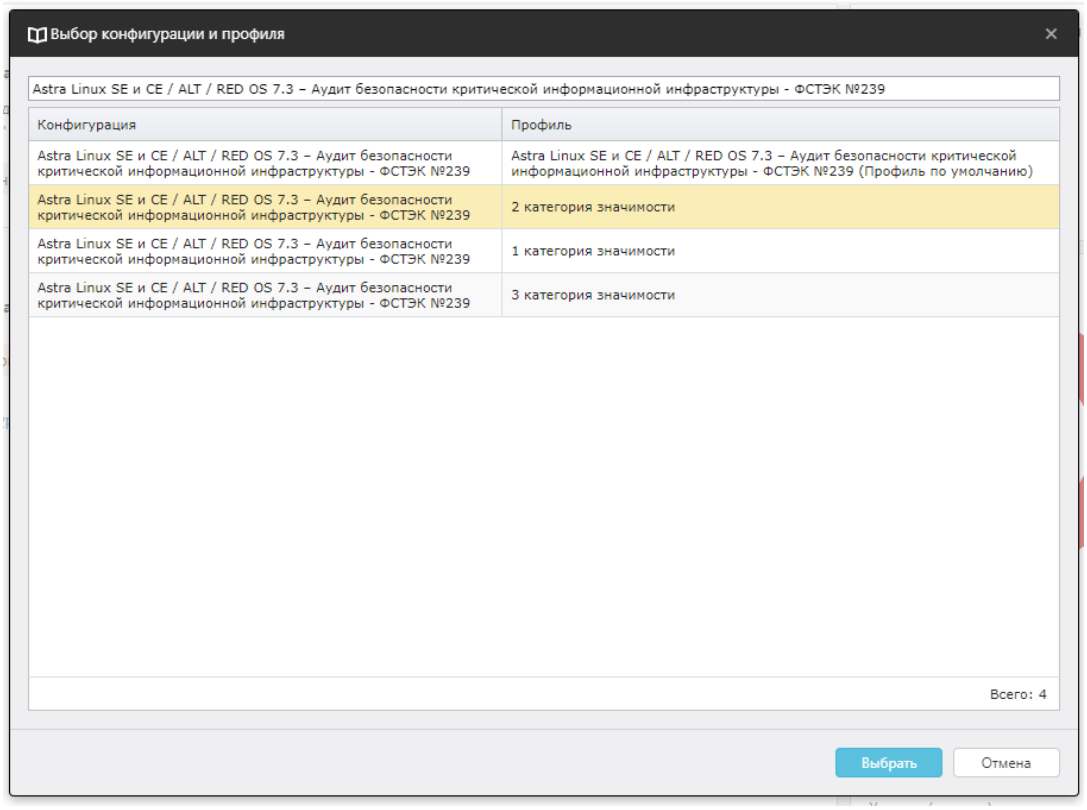
- Хост – IP-адрес или DNS-имя хоста;
- Процент соответствия – Уровень (процент) соответствия хоста рассчитывается как отношение его правил, соответствующих стандарту конфигурации, к их общему количеству. Учитываются только включенные и проверяемые в профиле правила.;
- Уровень соответствия – оценка соответствия:
  - 100% – Отлично;
  - 75-99% – Хорошо;
  - 0-74% – Неудовлетворительно;
- Соответствие – количество правил со статусом "Соответствие";
- Несоответствие – количество правил со статусом "Несоответствие";
- Риск несоответствующих правил – группировка несоответствующих правил по риску;
- Неизвестно – количество правил со статусом "Неизвестно";
- Ошибка – количество правил со статусом "Ошибка";
- Неприменимо – количество правил со статусом "Неприменимо";

Нажав **Результаты сканирования**, вы перейдете на страницу с актуальным результатом сканирования для данного хоста и выбранной конфигурации.

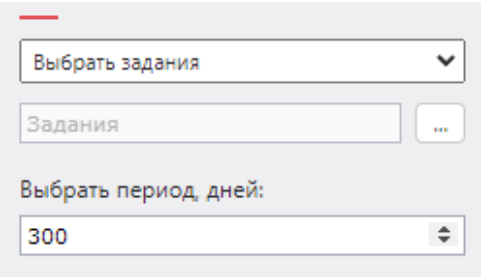
Общий фильтр



- Конфигурация – необходимо выбрать конфигурацию, соответствие которой будет определяться. Если у конфигурации есть несколько профилей, то в окне выбора будут отображаться несколько строк одной и той же конфигурации, но с разными профилями. Нажмите на ... и выберите нужную конфигурацию;

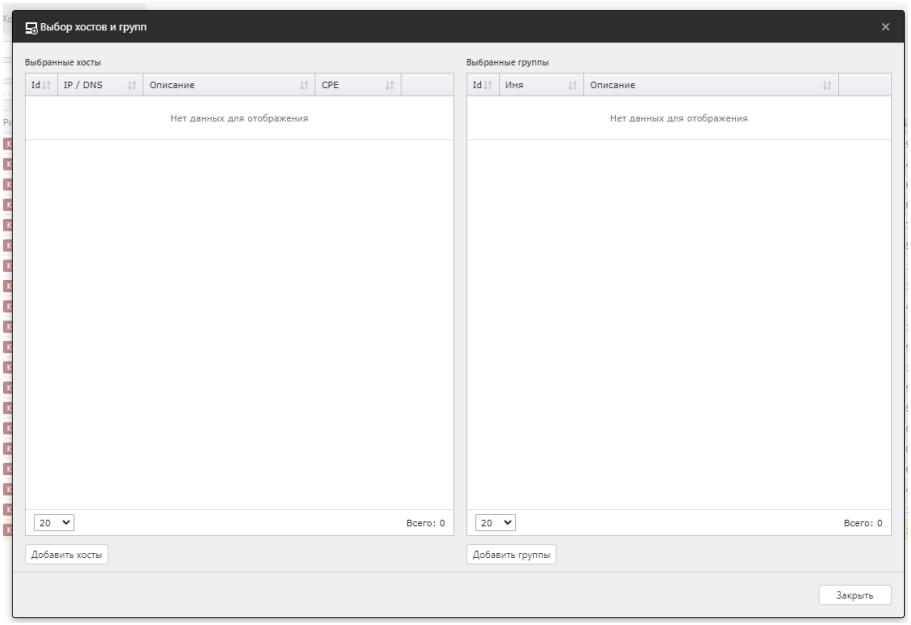


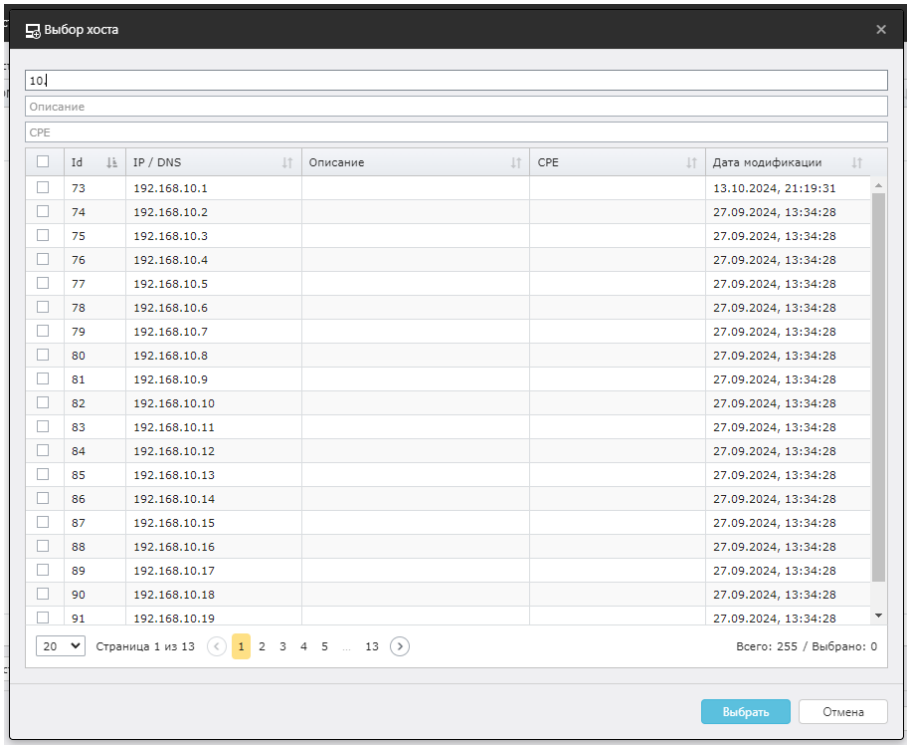
- Задания – можно выбрать задания, из результатов сканирования которых будет производиться анализ конфигураций. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:



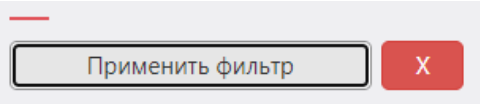
Нажмите на ... , после чего откроется окно выбора заданий;

- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для анализа конфигураций;
- Хосты – можно выбрать хосты, для которых будет проведен анализ конфигураций. Нажмите на ... , после чего откроется окно выбора групп и хостов:





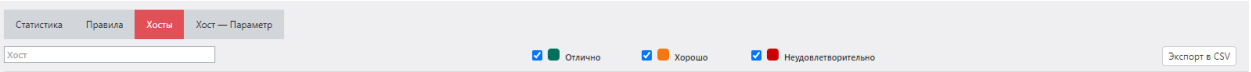
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Хост – IP-адрес или DNS-имя хоста;
- Уровень соответствия – в таблице будут отображаться хосты с отмеченными уровнями соответствия.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **ComplianceAnalysis-HostsStatistics-dd-mm-yyyy.csv**.

Структура CSV файла

Id хоста	ID хоста
Имя хоста	IP-адрес или DNS-имя хоста
Процент соответствия	Соответствие хоста выбранной конфигурации в процентном соотношении
Состояние конфигурации	Оценка соответствия: 100% – Отлично; 75-99% – Хорошо; 0-74% – Неудовлетворительно
Количество правил со значением Соответствие	Количество проверенных правил со статусом Соответствие
Количество правил со значением Несоответствие	Количество проверенных правил со статусом Несоответствие
Количество критичных правил со значением Несоответствие	Количество правил со статусом Несоответствие и риском Критический
Количество правил высокой критичности со значением Несоответствие	Количество правил со статусом Несоответствие и риском Высокий

Количество правил средней критичности со значением Несоответствие	Количество правил со статусом Несоответствие и риском Средний
Количество правил низкой критичности со значением Несоответствие	Количество правил со статусом Несоответствие и риском Низкий
Количество правил информационной критичности со значением Несоответствие	Количество правил со статусом Несоответствие и риском Информация
Количество правил без известной критичности со значением Несоответствие	Количество правил со статусом Несоответствие и риском Не определенно
Количество правил со значением Неизвестно	Количество правил со статусом Неизвестно
Количество правил со значением Ошибка	Количество правил со статусом Ошибка
Количество правил со значением Неприменимо	Количество правил со статусом Неприменимо

Пример:

Код

```
Id хоста,Имя хоста,Процент соответствия,Состояние
конфигурации,Количество правил со значением Соответствие,Количество
правил со значением Несоответствие,Количество критичных правил со
значением Несоответствие,Количество правил высокой критичности со
значением Несоответствие,Количество правил средней критичности со
значением Несоответствие,Количество правил низкой критичности со
значением Несоответствие,Количество правил информационной критичности
со значением Несоответствие,Количество правил без известной
критичности со значением Несоответствие,Количество правил со
```

```
значением Неизвестно,Количество правил со значением Ошибка,Количество
правил со значением Неприменимо
69,192.168.80.8,35,Неудовлетворительно,38,66,0,1,24,41,0,0,3,0,2
```

8.5.4 Вкладка Хост – Параметр

Статус проверки правила

Соответствие – значение параметра на хосте соответствует эталонному значению в конфигурации;

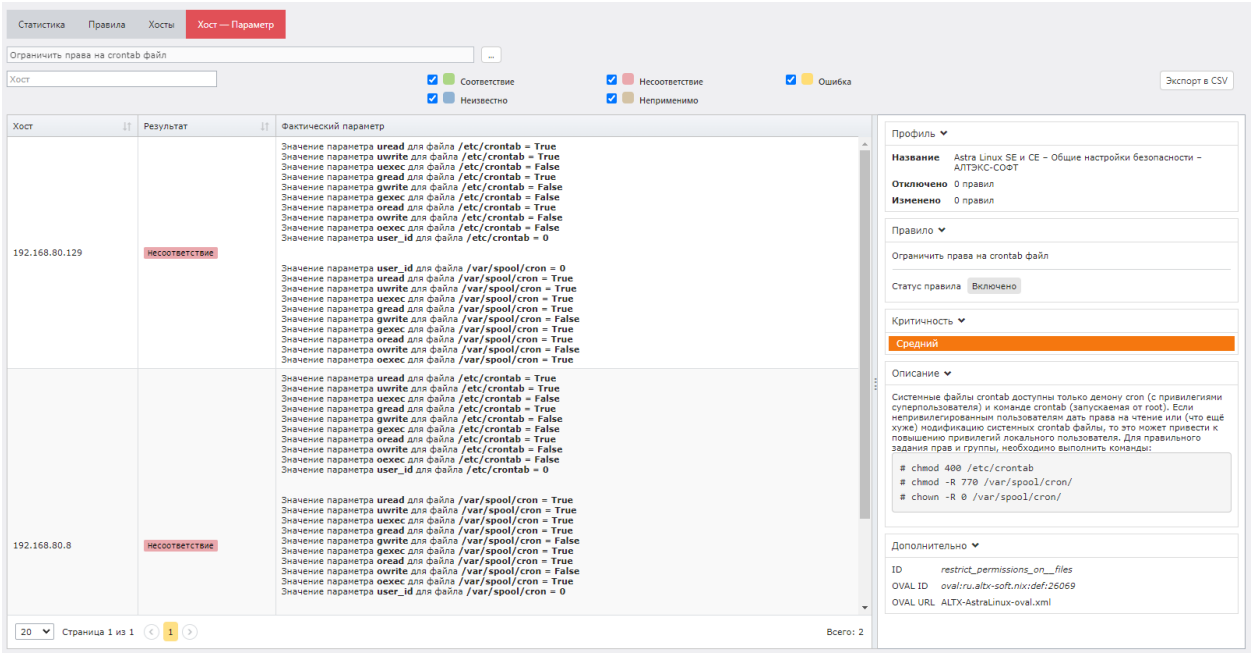
Несоответствие – значение параметра на хосте не соответствует эталонному значению в конфигурации;

Ошибка – критическая ошибка при выполнении проверки. При возникновении обратитесь в службу тех. поддержки;

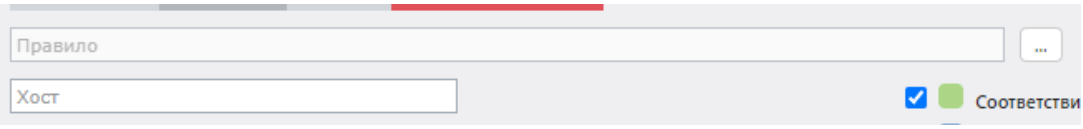
Неизвестно – ошибка при проверке правила. Убедитесь, что используемая для сканирования учетная запись обладает нужными правами, а примененные на хосте групповые политики позволяют проводить необходимые проверки;

Неприменимо – данное правило неприменимо для проверяемой платформы;

В данной вкладке отображается информация по выбранному проверяемому правилу конфигурации относительно хоста.



Сперва необходимо выбрать правило. Нажмите на ... и выберите нужное правило.

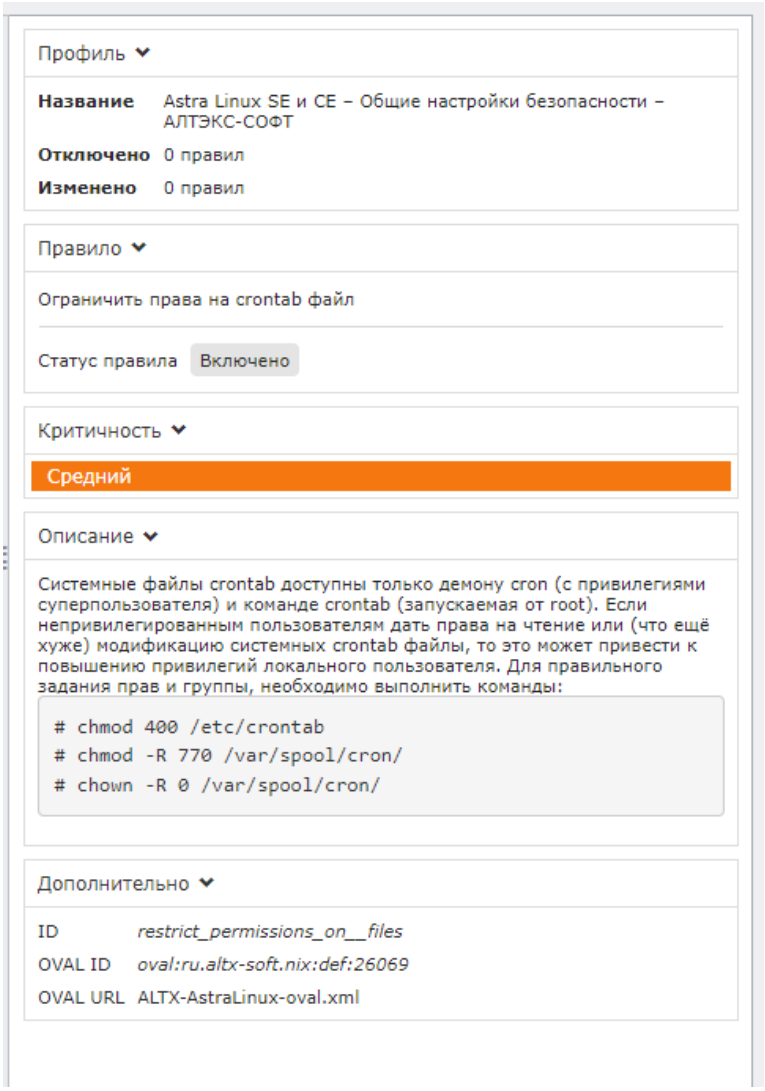


Информация о правиле включает в себя:

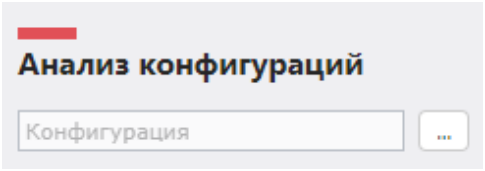
- Хост – IP-адрес или DNS-имя хоста;
- Результат – статус проверки правила;
- Фактический параметр – значения ключей реестра или подстрок конфигурационных файлов, проверяемых во время сканирования. Собирается только при включенной опции **Сохранять фактические значения xccdf** (4.3 Аудит конфигураций);

> Если ключа / подстроки нет в реестре / конфигурационном файле, или правило не подразумевает проверку ключа / подстроки, то фактическое значение будет пустым

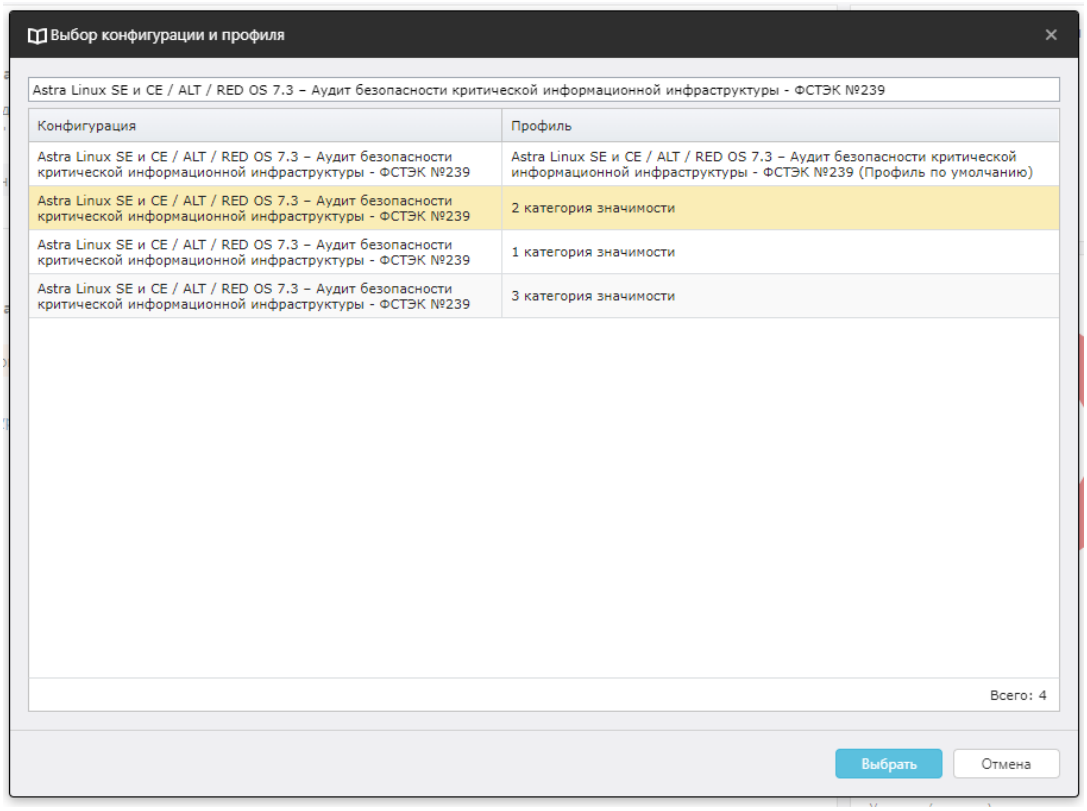
Справа отображается информация о профиле и правиле.



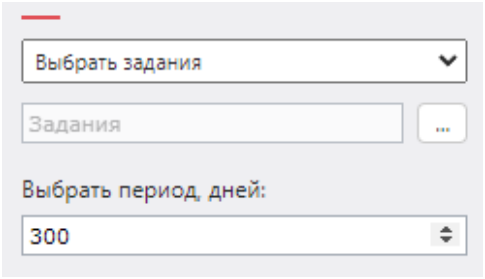
Общий фильтр



- Конфигурация – необходимо выбрать конфигурацию, соответствие которой будет определяться. Если у конфигурации есть несколько профилей, то в окне выбора будут отображаться несколько строк одной и той же конфигурации, но с разными профилями. Нажмите на ... и выберите нужную конфигурацию;



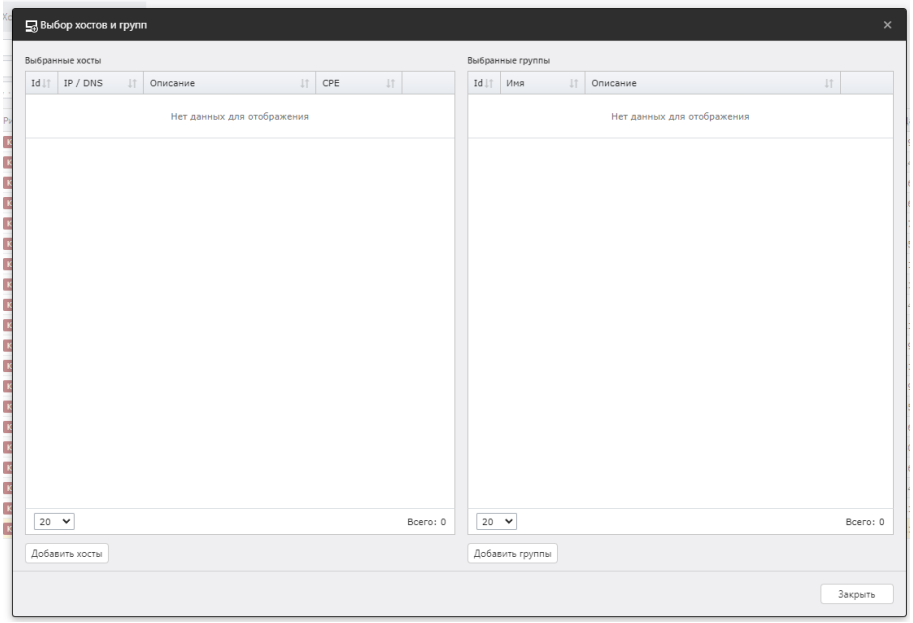
- Задания – можно выбрать задания, из результатов сканирования которых будет производиться анализ конфигураций. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

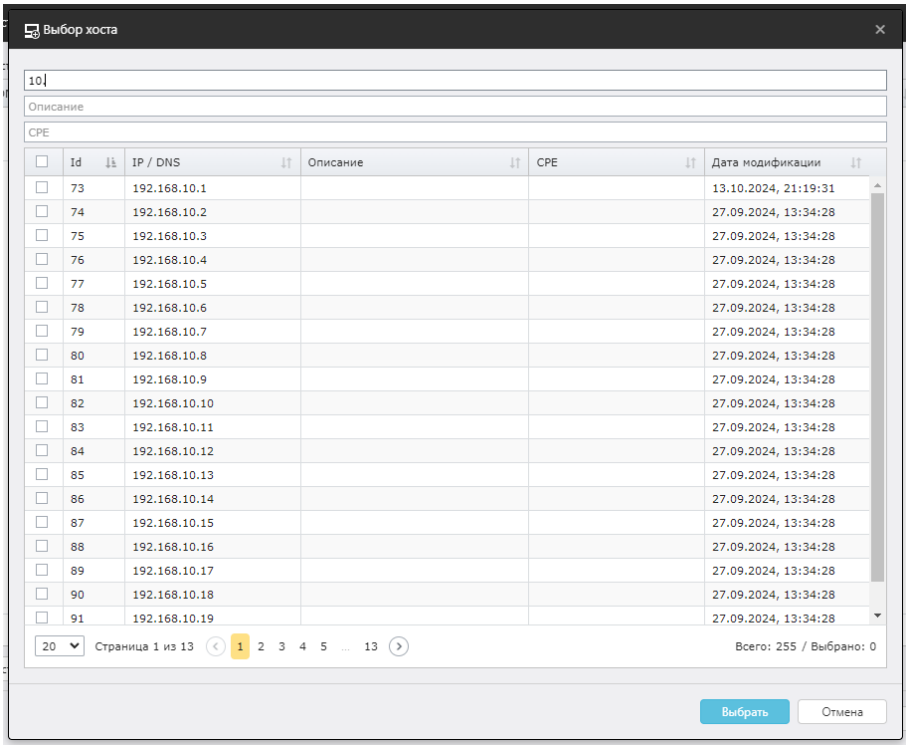


Нажмите на , после чего откроется окно выбора заданий;

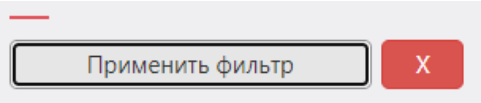
- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для анализа конфигураций;

- Хосты – можно выбрать хосты, для которых будет проведен анализ конфигураций. Нажмите на ..., после чего откроется окно выбора групп и хостов:





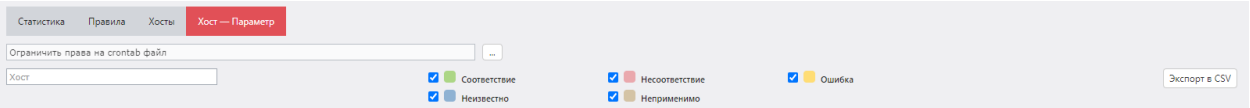
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Хост – IP-адрес или DNS-имя хоста;
- Статус проверки правила – в таблице будет отображаться информация только для тех хостов и правил, статусы проверки которых совпадают с отмеченными.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **ComplianceAnalysis-RuleResults-dd-mm-yyyy.csv**.

Структура CSV файла

Id хоста	ID хоста
Имя хоста	IP-адрес или DNS-имя хоста

Результаты сканирования	Статус проверки правила
Фактическое значение	Значение, обнаруженное на хосте во время проверки правила

Пример:

Код

```
Id хоста,Имя хоста,Результаты сканирования,Фактическое значение
69,192.168.80.8,Несоответствие,Значение параметра <b>uread</b> для
файла <b>/etc/crontab</b> = <b>True</b><br>Значение параметра
<b>uwrite</b> для файла <b>/etc/crontab</b> = <b>True</b><br>Значение
параметра <b>uexec</b> для файла <b>/etc/crontab</b> =
<b>False</b><br>Значение параметра <b>gread</b> для файла
<b>/etc/crontab</b> = <b>True</b><br>Значение параметра <b>gwrite</b>
для файла <b>/etc/crontab</b> = <b>False</b><br>Значение параметра
<b>gexec</b> для файла <b>/etc/crontab</b> = <b>False</b><br>Значение
параметра <b>oread</b> для файла <b>/etc/crontab</b> =
<b>True</b><br>Значение параметра <b>owrite</b> для файла
<b>/etc/crontab</b> = <b>False</b><br>Значение параметра <b>oexec</b>
для файла <b>/etc/crontab</b> = <b>False</b><br>Значение параметра
<b>user_id</b> для файла <b>/etc/crontab</b> =
<b>0</b><br><br><br>Значение параметра <b>uread</b> для файла
<b>/var/spool/cron</b> = <b>True</b><br>Значение параметра
<b>uwrite</b> для файла <b>/var/spool/cron</b> =
<b>True</b><br>Значение параметра <b>uexec</b> для файла
<b>/var/spool/cron</b> = <b>True</b><br>Значение параметра
<b>gread</b> для файла <b>/var/spool/cron</b> =
<b>True</b><br>Значение параметра <b>gwrite</b> для файла
<b>/var/spool/cron</b> = <b>False</b><br>Значение параметра
<b>gexec</b> для файла <b>/var/spool/cron</b> =
<b>True</b><br>Значение параметра <b>oread</b> для файла
<b>/var/spool/cron</b> = <b>True</b><br>Значение параметра
<b>owrite</b> для файла <b>/var/spool/cron</b> =
<b>False</b><br>Значение параметра <b>oexec</b> для файла
<b>/var/spool/cron</b> = <b>True</b><br>Значение параметра
<b>user_id</b> для файла <b>/var/spool/cron</b> =
<b>0</b><br><br><br>Значение параметра <b>uread</b> для файла
<b>/var/spool/cron/crontabs</b> = <b>True</b><br>Значение параметра
<b>uwrite</b> для файла <b>/var/spool/cron/crontabs</b> =
<b>True</b><br>Значение параметра <b>uexec</b> для файла
<b>/var/spool/cron/crontabs</b> = <b>True</b><br>Значение параметра
<b>gread</b> для файла <b>/var/spool/cron/crontabs</b> =
<b>False</b><br>Значение параметра <b>gwrite</b> для файла
<b>/var/spool/cron/crontabs</b> = <b>True</b><br>Значение параметра
<b>gexec</b> для файла <b>/var/spool/cron/crontabs</b> =
```

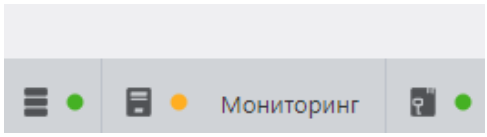
```
<b>True</b><br>Значение параметра <b>oread</b> для файла
<b>/var/spool/cron/crontabs</b> = <b>False</b><br>Значение параметра
<b>owrite</b> для файла <b>/var/spool/cron/crontabs</b> =
<b>False</b><br>Значение параметра <b>oexec</b> для файла
<b>/var/spool/cron/crontabs</b> = <b>False</b><br>Значение параметра
<b>user_id</b> для файла <b>/var/spool/cron/crontabs</b> =
<b>0</b><br>
```

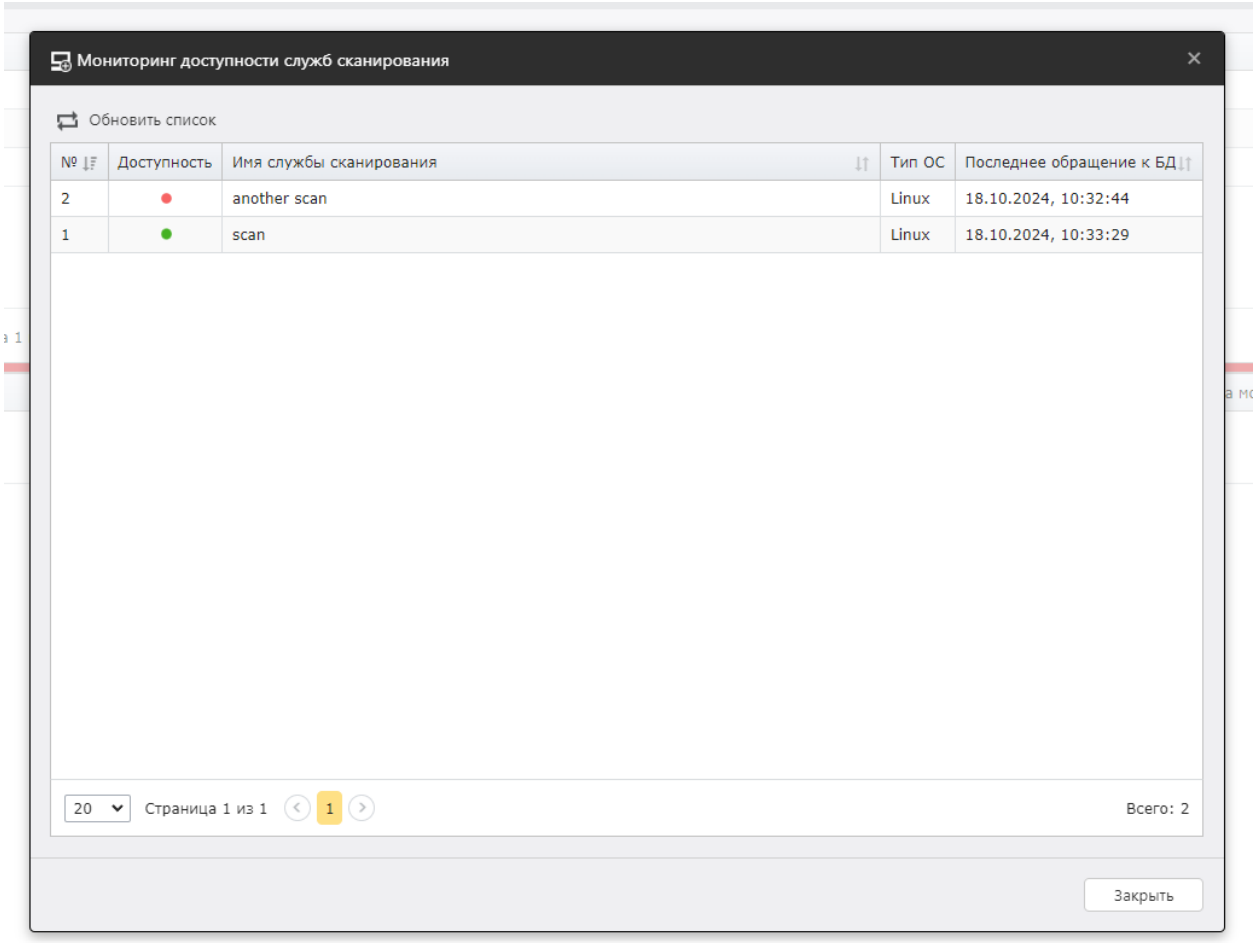
Дополнительные возможности

Содержание

Мониторинг служб сканирования

Если в БД установлено две и более служб сканирования, появляется возможность отслеживать состояние каждой из них. Для того, чтобы открыть окно мониторинга, нажмите в статус-баре **Мониторинг**:





Значение столбца **Последнее обращение к БД** в норме обновляется каждые 5 секунд. Если разница между обращением к БД и текущим временем (согласно часовому поясу хоста, на котором установлен компонент redcheck-client) не более 10 секунд, то служба сканирования будет считаться доступной.

Причин недоступности службы сканирования может быть несколько:

- Если значение последнего обращения к БД обновляется, но служба недоступна, возможно на хосте службы сканирования установлено неактуальное время;
- Если значение последнего обращения к БД не обновляется, возможно хост службы сканирования выключен или вне сетевой доступности;
- Если значение последнего обращения к БД не обновляется, возможно компонент redcheck-scan-service был удален с хоста.

Нажав **Обновить список**, данные в таблице обновятся.

Детальную информацию о службах сканирования можно посмотреть в **Справка → О программе**.