

RedCheck

СРЕДСТВО АНАЛИЗА
ЗАЩИЩЕННОСТИ



Руководство

пользователя

АЛМЮ.501410.RC02-01.РП

Версия документа 2.8.0.ru



Содержание

Перед началом работы	6
Рабочий процесс в RedCheck.....	8
Ролевая модель RedCheck	9
Сведения об интегральной оценке по базовым метрикам CVSS.....	11
1 Группы	12
1.1 Создание группы.....	14
1.2 Возможности группы	16
2 Хосты	18
2.1 Создание хостов вручную	22
2.2 Импорт из CSV-файла.....	24
2.3 Импорт из AD	27
2.4 Импорт из Host Discovery.....	30
2.5 Экспорт хостов в CSV	33
3 Учетные записи для сканирования	35
3.1 Менеджер учетных записей	37
3.2 Подбор учетных записей для сканирования	40
4 Задания для сканирования	43
4.1 Аудит уязвимостей	51
4.2 Аудит обновлений.....	56
4.3 Аудит конфигураций	61

4.4 Инвентаризация	66
4.5 Фиксация (контроль целостности)	70
4.6 Аудит уязвимостей АСУ ТП	75
4.7 Аудит СУБД	79
4.8 Проверка доступности	83
4.9 Обнаружение хостов	87
4.10 Аудит в режиме "Пентест"	91
Настройка расписания для задания	98
Повторный перезапуск недоступных хостов во время сканирования	101
5 Расширенные возможности для заданий сканирования	103
5.1 Профили аудитов	104
5.1.1 Менеджер профилей	108
5.2 Конфигурации	116
5.2.1 Импорт конфигураций	121
5.3 OVAL-определения	122
5.4 Отслеживание изменений результатов сканирования (Контроль)	125
5.5 Профили сканирования Altxmap	129
6 Результаты сканирований	130
6.1 Аудит уязвимостей	134
6.2 Аудит обновлений	137
6.3 Аудит конфигураций	140
6.4 Инвентаризация	147

6.5 Фиксация (контроль целостности)	150
6.6 Аудит уязвимостей АСУ ТП.....	151
6.7 Аудит СУБД.....	156
6.8 Проверка доступности	163
6.9 Обнаружение хостов.....	164
6.10 Аудит в режиме "Пентест"	165
6.11 Статистика выполненных заданий.....	168
7 Отчеты	172
7.1 Создание простого отчета.....	178
7.1.1 Настройки для разных типов задания.....	184
7.2 Создание дифференциального отчета	193
7.2.1 Настройки для разных типов задания.....	197
7.3 Шаблоны отчетов	202
7.3.1 Настройки для разных типов задания.....	208
7.4 Просмотр CSV отчетов	215
8 Аналитика.....	220
8.1 Актуальность сканирования	221
8.2 Недоступность хостов.....	226
8.3 Анализ уязвимостей	232
8.3.1 Вкладка Уязвимости	233
8.3.2 Вкладка Хосты.....	239
8.3.3 Вкладка Хост – Уязвимость	246
8.4 Контроль устранения уязвимостей.....	252
8.4.1 Вкладка Уязвимости	253

8.4.2 Вкладка Хосты.....	262
8.4.3 Вкладка Хост – Уязвимость	271
8.5 Анализ конфигураций.....	281
8.5.1 Вкладка Статистика.....	282
8.5.2 Вкладка Правила	288
8.5.3 Вкладка Хосты.....	295
8.5.4 Вкладка Хост – Параметр.....	302
Дополнительные возможности.....	310
Мониторинг служб сканирования	311

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

- [1 Группы](#)
- [2 Хосты](#)

- 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**.

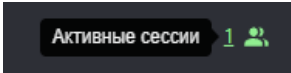
Ролевая модель RedCheck

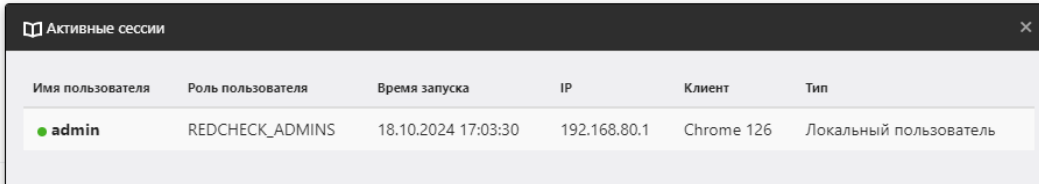
RedCheck для разграничения прав доступа использует ролевую модель. Роль пользователя в Системе определяется его принадлежностью к одной (или нескольким) из четырех групп RedCheck:

- **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).



Имя пользователя	Роль пользователя	Время запуска	IP	Клиент	Тип
admin	REDCHECK_ADMINS	18.10.2024 17:03:30	192.168.80.1	Chrome 126	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

Заккрыть

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
- 1.2 Возможности группы

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**;

Параметры группы хостов

Укажите требуемые параметры для новой или редактируемой группы хостов.

Имя

Описание

Выбранные хосты

ID	IP / DNS	Описание	CPE	
Нет данных для отображения				

Выбрано: 0

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

<input type="checkbox"/>	Id	IP / DNS	Описание	CPE	Дата модификации
<input type="checkbox"/>	1	Dns	Fqdn	NetBIOS	07.10.2022, 15:06:52
<input type="checkbox"/>	2	zyxel.altx-soft.ru			07.10.2022, 15:06:52
<input type="checkbox"/>	3	asn			07.10.2022, 15:06:52
<input type="checkbox"/>	4	YDV-RCWEBREST.test-domain.com		cpe:/o:microsoft:windows_server_2019	07.10.2022, 19:15:14
<input type="checkbox"/>	5	STORAGE.test-domain.com	storage		07.10.2022, 15:06:52
<input checked="" type="checkbox"/>	6	192.168.1.1			21.10.2022, 10:31:53
<input checked="" type="checkbox"/>	7	192.168.1.2			21.10.2022, 10:31:54
<input type="checkbox"/>	8	192.168.1.3			21.10.2022, 10:31:54
<input type="checkbox"/>	9	192.168.1.4			21.10.2022, 10:31:54
<input checked="" type="checkbox"/>	10	192.168.1.5			21.10.2022, 10:31:54
<input type="checkbox"/>	11	192.168.1.6			21.10.2022, 10:31:54
<input checked="" type="checkbox"/>	12	192.168.1.7			21.10.2022, 10:31:54
<input type="checkbox"/>	13	192.168.1.8			21.10.2022, 10:31:54
<input type="checkbox"/>	14	192.168.1.9			21.10.2022, 10:31:54
<input type="checkbox"/>	15	192.168.1.10			21.10.2022, 10:31:54
<input type="checkbox"/>	16	192.168.1.11			21.10.2022, 10:31:54

20 Page 1 of 1 (16 items) 1

Всего: 16 / Выбрано: 4

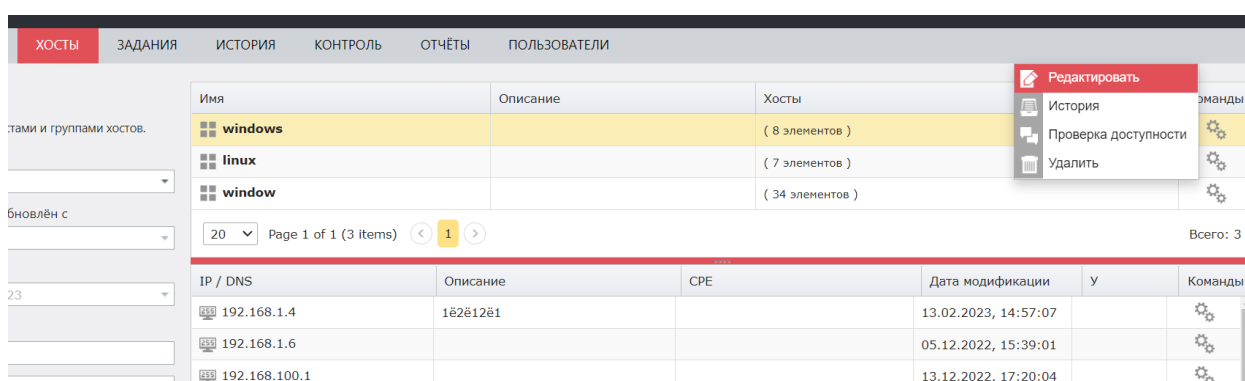
Выбрать Отмена

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;

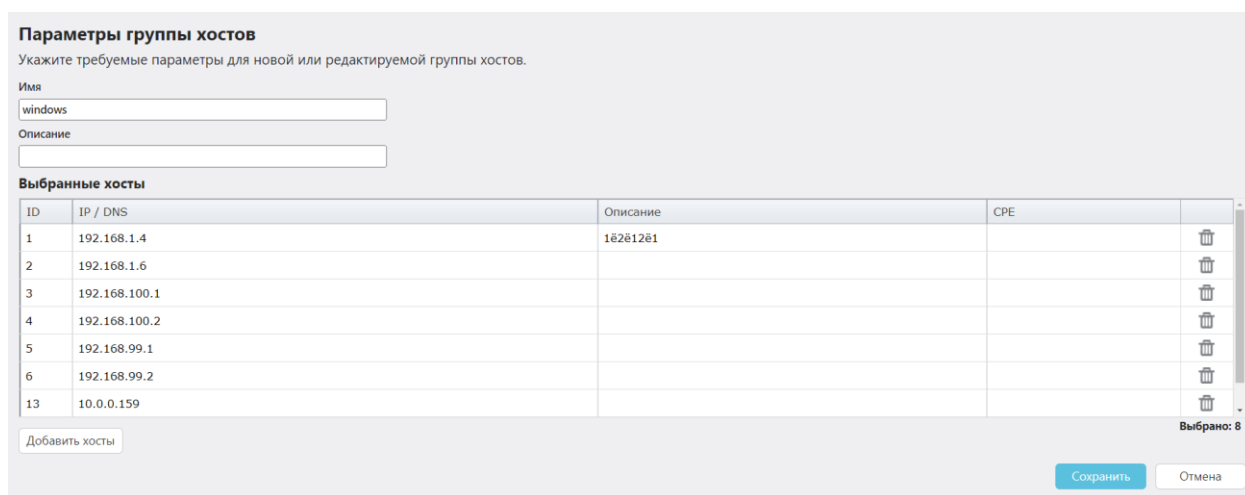
Шаг 2. Для редактирования группы нажмите  → **Редактировать**.



Имя	Описание	Хосты
windows		(8 элементов)
linux		(7 элементов)
window		(34 элементов)

IP / DNS	Описание	CPE	Дата модификации	У	Команды
192.168.1.4	1è2è12è1		13.02.2023, 14:57:07		
192.168.1.6			05.12.2022, 15:39:01		
192.168.100.1			13.12.2022, 17:20:04		

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



Параметры группы хостов
Укажите требуемые параметры для новой или редактируемой группы хостов.

Имя: windows
Описание:

Выбранные хосты

ID	IP / DNS	Описание	CPE	
1	192.168.1.4	1è2è12è1		
2	192.168.1.6			
3	192.168.100.1			
4	192.168.100.2			
5	192.168.99.1			
6	192.168.99.2			
13	10.0.0.159			

Добавить хосты

Сохранить Отмена

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

ГЛАВНАЯ ХОСТЫ ЗАДАНИЯ ИСТОРИЯ КОНТРОЛЬ ОТЧЁТЫ ПОЛЬЗОВАТЕЛИ						
Сканирования		№	Хост	Статус	Риск	К
Интервал	Все	194	10.0.0.168	Хост недоступен		
Начало		193	10.0.0.168	Хост недоступен		
Завершение	28 марта, 2023	192	10.0.0.182	Завершено	87 25 3	
Быстрый фильтр		191	10.0.0.182	Завершено	82 24 4	✓
Хост	...	190	10.0.0.182	Завершено	88 25 3	
window	...	189	10.0.0.182	Завершено	83 24 4	✓
Задание	...	188	10.0.0.182	Завершено	88 25 3	
Тип сканирования		187	10.0.0.182	Завершено	83 24 4	✗
Ссылки (CVE, проч.)		186	10.0.0.182	Завершено	87 25 3	
Статус		185	10.0.0.180	Хост недоступен		
Сканирования		184	10.0.0.182	Завершено	82 24 4	✓
<input checked="" type="radio"/> Все						
<input type="radio"/> Актуальные						
Применить фильтр						

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.

Хосты
Управление хостами и группами хостов.

Интервал
Все

Хост создан/обновлён с

По
28 марта, 2023

IP / DNS

Описание

CPE

UUID

Показать хосты, не состоящие в группах

Применить фильтр

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**;

Имя	Описание	Хосты
100-сеть		(28202 элементов)
80-сеть		(28178 элементов)
10-сеть асу тп		(28506 элементов)

IP / DNS	Описание	CPE	Дата модификации
192.168.100.12			17.09.2024, 11:40:04
192.168.100.14			17.09.2024, 11:40:04
192.168.100.16			17.09.2024, 11:40:04

- Редактировать
- История
- Проверка доступности
- Удалить

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

Параметры хоста

ID:

UUID:

Имя хоста:

Дата модификации:

Описание:

Группы
Необходимо выбрать как минимум одну группу

- 100-сеть
- 80-сеть
- 10-сеть асу тп

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

Просмотр результатов сканирования

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

[ГЛАВНАЯ](#)
[ХОСТЫ](#)
[ЗАДАНИЯ](#)
[ИСТОРИЯ](#)
[КОНТРОЛЬ](#)
[ОТЧЁТЫ](#)
[ПОЛЬЗОВАТЕЛИ](#)

Сканирования

Интервал:

Начало:

Завершение:

Быстрый фильтр:

sql-01

Группа:

Задание:

Тип сканирования:

Ссылки (CVE, проч.):

Статус:

Все
 Актуальные

Применить фильтр

№	Хост	Статус	Риск	К	Задание
917	sql-01	Завершено	1 391 774 30		уя-расписание
897	sql-01	Завершено	1 370 745 30		уя-расписание
884	sql-01	Завершено	4 376 736 30		уя-расписание
878	sql-01	Завершено	73 24 4		Аудит конфигурации WI SERVER
868	sql-01	Завершено	4 376 736 30		уя-расписание
860	sql-01	Завершено	1 363 724 30		vuln-win-269-646 - Duplicate - Duplicate
846	sql-01	Завершено	43 11 1		updates
840	sql-01	Завершено	1 363 724 30		уя-расписание
822	sql-01	Завершено	1 358 746 30		уя-расписание
807	sql-01	Завершено	50 490 444 85		уя-расписание

20 Page 1 of 1 (10 items)

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.

Создание хостов

Хосты
DNS-имена или IP-адреса, включая диапазоны и маски.
Например:
server2016, server-2016.domain, 192.168.1.1, 192.168.1.250-192.168.2.10, 192.168.1.1/25

Описание
Указывается по желанию

Группы
Необходимо выбрать как минимум одну группу

Используйте , или ; для перечисления значений

Не более 255 символов

100-сеть
 80-сеть
 10-сеть асу тп

Создать хосты Закрыть

При успешном создании хостов будет выведена дополнительная информация:

Создано новых хостов: **1**

Существующих хостов добавлено в новые группы: **1**

Существующим хостам обновлено описание: **1**

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

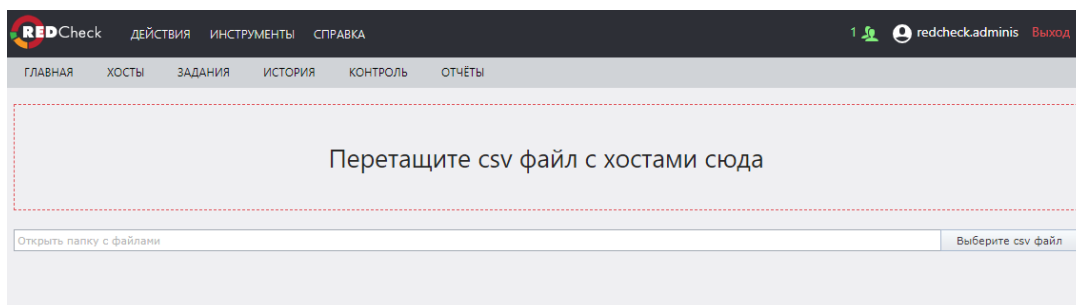
```
Group;Action  
*;Delete
```

Импортирование csv-файла

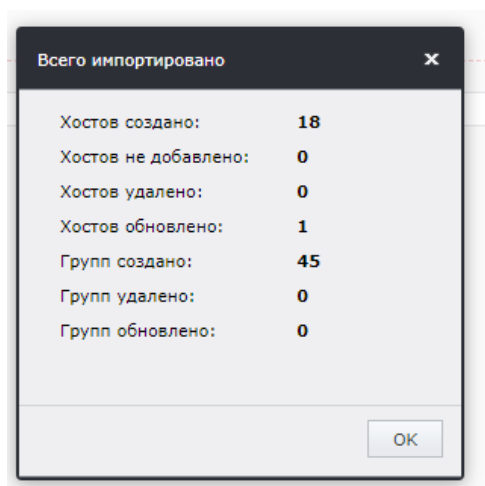
Для добавления хостов с помощью csv-файла выполните следующие шаги.

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.

Импорт хостов из Active Directory/LDAP

Укажите IP-адрес или DNS-имя контроллера домена, тип протокола, выберите учётную запись, укажите фильтр и получите хосты. Затем выберите необходимые хосты и добавьте их в общий список.

Тип протокола
ActiveDirectory

Адрес контроллера домена

Учетная запись

Группа

AD путь

Фильтр
(&(objectCategory=computer))

Импортировать
Хост

Искать только первые 1000 хостов

Искать хосты

Шаг 3. Отметьте необходимые хосты → Импортировать;

<input type="checkbox"/>	Хост	↓	Полное имя хоста	Операционная система
<input type="checkbox"/>	CL-01		CL-01.STAND.LAB	Windows 7 Корпоративная
<input type="checkbox"/>	DC-01		dc-01.STAND.LAB	Windows Server 2016 Standard
<input type="checkbox"/>	RC-01		rc-01.STAND.LAB	Windows Server 2019 Standard
<input type="checkbox"/>	SQL-01		sql-01.STAND.LAB	Windows Server 2016 Standard
<input type="checkbox"/>	WEB-01		web-01.STAND.LAB	Windows Server 2019 Standard

20 Page 1 of 1 (5 items) < 1 > Всего

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**

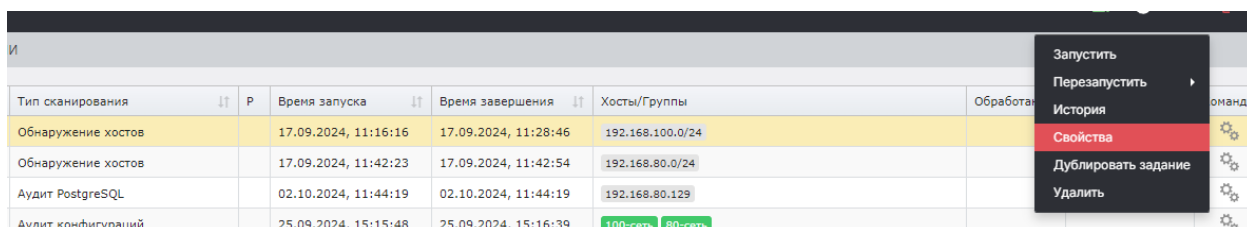
Существующих хостов добавлено в новые группы: **1**

2.4 Импорт из Host Discovery

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Шаг 1. Перейдите в свойства задания типа Обнаружение хостов, нажав  →

Свойства;

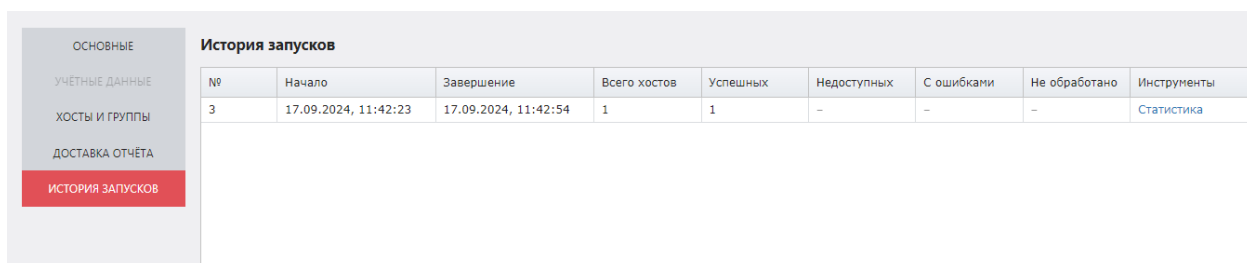


Тип сканирования	Время запуска	Время завершения	Хосты/Группы	Обработка
Обнаружение хостов	17.09.2024, 11:16:16	17.09.2024, 11:28:46	192.168.100.0/24	
Обнаружение хостов	17.09.2024, 11:42:23	17.09.2024, 11:42:54	192.168.80.0/24	
Аудит PostgreSQL	02.10.2024, 11:44:19	02.10.2024, 11:44:19	192.168.80.129	
Аудит конфигураций	25.09.2024, 15:15:48	25.09.2024, 15:16:39	100-сеть 80-сеть	

- Запустить
- Перезапустить
- История
- Свойства**
- Дублировать задание
- Удалить

Шаг 2. Перейдите во вкладку **История запусков** → нажмите **Статистика**

напротив нужного завершеного сканирования;



№	Начало	Завершение	Всего хостов	Успешных	Недоступных	С ошибками	Не обработано	Инструменты
3	17.09.2024, 11:42:23	17.09.2024, 11:42:54	1	1	-	-	-	Статистика

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

Статистика
Статистические данные по выбранному выполнению задания.

Задание: 80-я
Профиль: Обнаружение хостов
Запуск: 17.09.2024 11:42:23
Завершение: 17.09.2024 11:42:54
№ выполнений задания: 3
Экспорт в CSV

4 ВСЕГО ХОСТОВ ОБНАРУЖЕНО | 1 ИЗ НИХ НЕТ СООТВЕТСТВИЯ В СИСТЕМЕ

Соответствие в БД: Есть Нет
Операционная система: Windows Linux ОС не определена Другое

Поиск по IP хоста: _____ | Поиск по имени хоста, DNS, FQDN, NetBIOS: _____

Способ обнаружения	IP	DNS	FQDN	NetBIOS	Операционная система	Агент
ARP	192.168.80.129					Нет
ARP	192.168.80.254					Нет
ARP	192.168.80.1					Нет
LOCALHOST	192.168.80.8					Нет

20 | Страница 1 из 1 | 1 | Всего: 4

Добавить хосты в систему...

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**;

Добавить хосты

Поиск по IP хоста Поиск по имени хоста, DNS, FQDN, NetBIOS

Нет соответствия в БД Операционная система : Windows Linux ОС не определена Другое

Группа

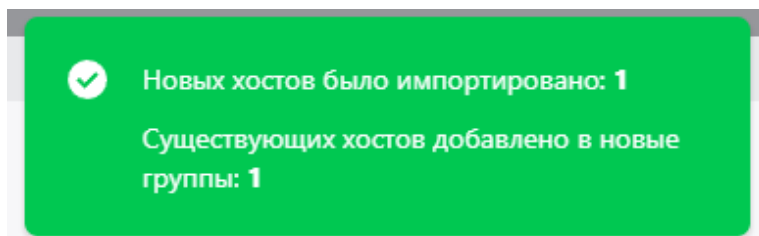
Добавить хосты по: IP DNS-имя FQDN NetBIOS-имя Любое из имен

<input checked="" type="checkbox"/>	IP	DNS-имя	FQDN	NetBIOS-имя	Операционная система
<input checked="" type="checkbox"/>	192.168.80.254				

20 Страница 1 из 1 < 1 > Всего: 1 Выбрано: 1

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

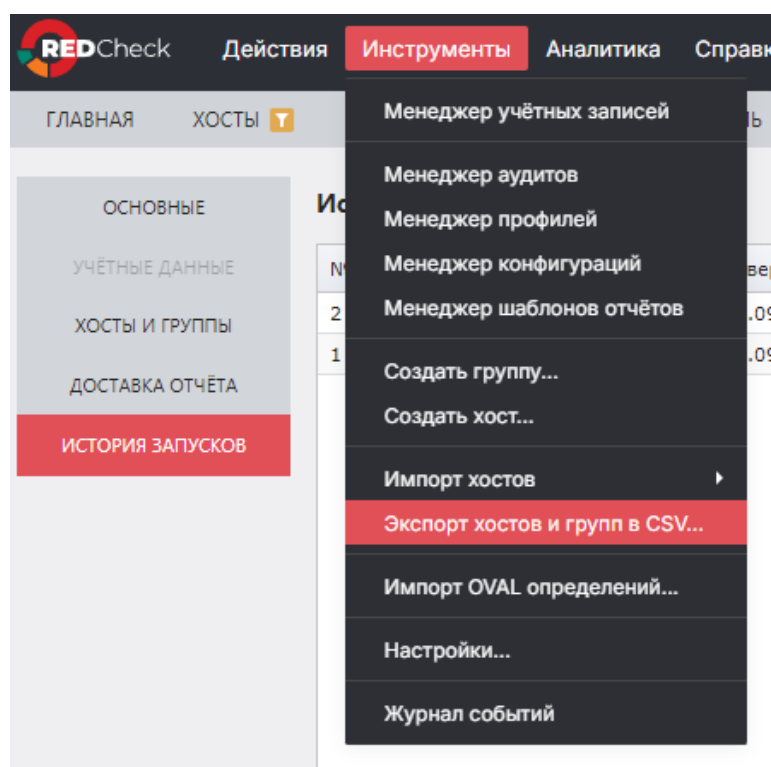
RedCheck позволяет экспортировать имеющуюся в базе данных инфраструктуру в CSV-файл. Получающийся файл можно [импортировать](#) в RedCheck.

Структура csv-файла

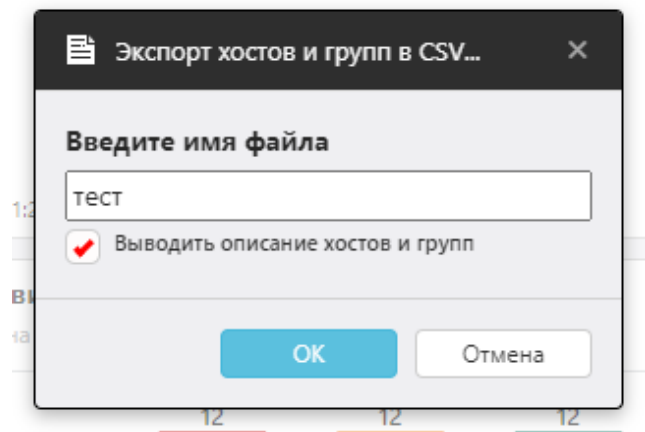
Group	GroupDesc	Host	HostDesc	CPE
Название группы	Описание группы	Имя/адрес хоста	Описание хоста	Конфигурация устройства

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 **ОК** 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;**

Менеджер учётных записей							
ID	Тип	Подтип	Имя профиля	Дата создания	Дата модификации	X	Команды
> 1	Windows		windows	29.11.2022, 16:03:01	23.01.2023, 10:04:59		⚙
> 2	Sql	MsSql	ms	05.12.2022, 13:47:10	05.12.2022, 13:47:10		⚙
> 3	Linux		linux	05.12.2022, 17:05:22	27.01.2023, 12:38:59	🖨	⚙
> 4	Cisco	Ios	cisco-ios	07.12.2022, 09:59:50	07.12.2022, 09:59:50		⚙
> 5	Cisco	Nxos	cisco-nxos	07.12.2022, 11:19:43	07.12.2022, 11:19:43		⚙
> 6	Huawei		huawei	07.12.2022, 11:54:18	07.12.2022, 11:54:18		⚙
> 7	VMware	ESXi	vm-esxi	07.12.2022, 11:55:15	07.12.2022, 11:55:15		⚙
> 8	VMware	vCenter	vm-vcenter	07.12.2022, 16:09:11	07.12.2022, 16:09:11		⚙
> 9	VMware	Nsx	vm-nsx	07.12.2022, 16:29:09	07.12.2022, 16:29:09		⚙
> 10	Solaris		solaris	07.12.2022, 17:23:47	07.12.2022, 17:23:47		⚙
> 11	FreeBsd		freebsd	07.12.2022, 17:24:54	07.12.2022, 17:24:54		⚙

20 Page 1 of 2 (25 items) 1 2 Всего: 25

Добавить учётные 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.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.


Имя профиля	<input type="text" value="some"/>
Тип учётной записи	<input type="text" value="Windows"/>
<hr/>	
Имя пользователя	<input type="text"/>
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
Домен	<input type="text"/>
WinRM порт	<input type="text" value="5985"/>
Порт RedCheck Agent	<input type="text" value="8732"/>
Порт RedCheck Update Agent	<input type="text" value="8733"/>

Указать WinRM порт

WinRM через HTTPS


Указать порт RedCheck Agent

Указать порт RedCheck Update Agent


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**;

Редактирование учётной записи ✕

Имя профиля:


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.

Хост недоступен

Причина: "Ошибка аутентификации."

Учётная запись: "test"

Причина: "Ошибка аутентификации."

Учётная запись: "test"

Причина: "Ошибка аутентификации."

Учётная запись: "admin"

Подробности в журнале событий службы сканирования.

Для получения детальной информации можно воспользоваться заданием "Проверка доступности".

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.

Параметры инвентаризации

Укажите профиль инвентаризации

Профиль Мультиплатформенный

[Выбрать все](#) [Сбросить все](#)

- Аппаратное обеспечение
- Программное обеспечение
- OVAL-Инвентаризация


4 Задания для сканирования

RedCheck предоставляет 10 различных типов задания:

- [4.1 Аудит уязвимостей](#)
- [4.2 Аудит обновлений](#)
- [4.3 Аудит конфигураций](#)
- [4.4 Инвентаризация](#)
- [4.5 Фиксация \(контроль целостности\)](#)
- [4.6 Аудит уязвимостей АСУ ТП](#)
- [4.7 Аудит СУБД](#)
- [4.8 Проверка доступности](#)
- [4.9 Обнаружение хостов](#)
- [4.10 Аудит в режиме "Пентест"](#)
- [Настройка расписания для задания](#)
- [Повторный перезапуск недоступных хостов во время сканирования](#)

Запуск задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

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

Запустить;

Для сортировки заданий воспользуйтесь фильтром:

Задания
Создание заданий сканирования и управление ими.

Период создания
Все

Создано с

Создано по
30 января, 2023

Задание

Хост

Тип сканирования


Тип запуска

Статус

Применить фильтр

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:

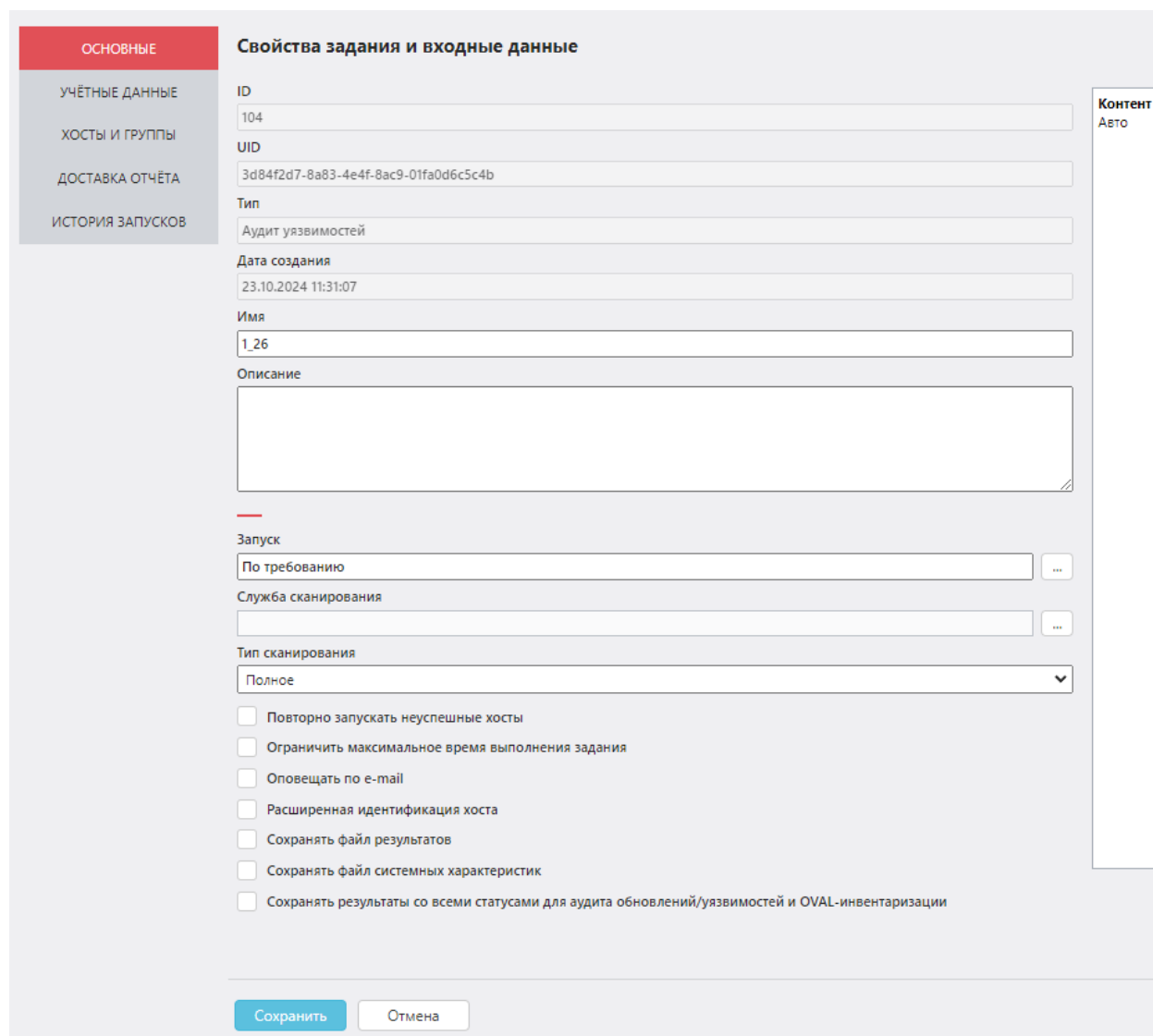
- Все – будет выполнено сканирование всех хостов, указанных в задании на момент перезапуска;
- Кроме успешных (последний запуск) – будет выполнено сканирование хостов, указанных в задании на момент перезапуска, которые при последнем выполнении задания завершились со статусом, отличным от **Завершено**;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



ОСНОВНЫЕ

УЧЁТНЫЕ ДАННЫЕ

ХОСТЫ И ГРУППЫ

ДОСТАВКА ОТЧЁТА

ИСТОРИЯ ЗАПУСКОВ

Свойства задания и входные данные

ID
104

UID
3d84f2d7-8a83-4e4f-8ac9-01fa0d6c5c4b

Тип
Аудит уязвимостей

Дата создания
23.10.2024 11:31:07

Имя
1_26

Описание

Запуск
По требованию

Служба сканирования

Тип сканирования
Полное

Повторно запускать неуспешные хосты

Ограничить максимальное время выполнения задания

Оповещать по e-mail

Расширенная идентификация хоста

Сохранять файл результатов

Сохранять файл системных характеристик

Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации


Сохранить Отмена

Контент
Авто

- 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;

ОСНОВНЫЕ
УЧЁТНЫЕ ДАННЫЕ
ХОСТЫ И ГРУППЫ
ДОСТАВКА ОТЧЁТА
ИСТОРИЯ ЗАПУСКОВ

Выбранные хосты

ID	IP / DNS	Описание	CPE	
8606	192.168.80.32			


Выбранные группы

ID	Имя
----	-----

Добавить хосты

Выбрано: 1

Добавить группы

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

Выбор хоста

IP-адрес

Описание

CPE

<input type="checkbox"/>	Id	IP / DNS	Описание	CPE	Дата модификации
<input type="checkbox"/>	1	192.168.1.4	1e2e12e1		13.02.2023, 14:57:07
<input type="checkbox"/>	2	192.168.1.6			05.12.2022, 15:39:01
<input type="checkbox"/>	3	192.168.100.1			13.12.2022, 17:20:04
<input type="checkbox"/>	4	192.168.100.2			13.12.2022, 17:20:12
<input type="checkbox"/>	5	192.168.99.1			13.12.2022, 17:23:54
<input type="checkbox"/>	6	192.168.99.2			13.12.2022, 17:23:59
<input type="checkbox"/>	7	192.168.99.3			13.12.2022, 17:40:35
<input type="checkbox"/>	8	192.168.99.4			13.12.2022, 17:40:41
<input type="checkbox"/>	9	192.168.99.5	some		15.12.2022, 14:53:03
<input type="checkbox"/>	10	192.168.99.6	some desc		15.12.2022, 14:53:12
<input type="checkbox"/>	11	192.168.99.7	some desc	cpe:windows8	15.12.2022, 14:55:53
<input type="checkbox"/>	12	192.168.99.8	some desc	cpe:windows10	15.12.2022, 14:56:00
<input type="checkbox"/>	13	10.0.0.159			23.01.2023, 10:03:32
<input type="checkbox"/>	14	10.0.0.150			24.01.2023, 12:22:39
<input type="checkbox"/>	15	zvs-pc.altx-soft.ru			24.01.2023, 12:34:55
<input type="checkbox"/>	17	ydv-pc.altx-soft.ru		cpe:/o:microsoft:windows_server_2022	03.02.2023, 16:53:10
<input type="checkbox"/>	18	10.0.0.136		cpe:/o:microsoft:windows	24.01.2023, 17:24:38

20 Page 1 of 3 (49 items) < 1 2 3 > Всего: 49 / Выбрано: 0

Выбрать Отмена

Нажмите **Сохранить** для внесения изменений.

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

Конфигурации

Фильтр по платформам... Фильтр по продуктам...

Поиск конфигураций

#	Имя
<input type="checkbox"/>	Ubuntu – Общие настройки безопасности – АЛТЭК-СОФТ
<input type="checkbox"/>	SUSE Linux Enterprise / openSUSE – Общие настройки безопасности – АЛТЭК-СОФТ
<input type="checkbox"/>	ROSA Linux – Общие настройки безопасности – АЛТЭК-СОФТ
<input type="checkbox"/>	RED OS – Общие настройки безопасности – АЛТЭК-СОФТ
<input type="checkbox"/>	Red Hat Enterprise Linux / CentOS / Oracle Linux / AlmaLinux – Общие настройки безопасности – АЛТЭК-СОФТ
<input type="checkbox"/>	Red Hat Enterprise Linux / CentOS / Oracle Linux – Оценка соответствия стандарту версии 3.2.1 - PCI DSS
<input type="checkbox"/>	PHP – Аудит безопасности – АЛТЭК-СОФТ
<input type="checkbox"/>	Photop OS – Общие настройки безопасности – АЛТЭК-СОФТ
<input type="checkbox"/>	ngnix – Аудит безопасности – АЛТЭК-СОФТ
<input type="checkbox"/>	Linux - Рекомендации по безопасной настройке - МД ФСТЭК России от 25.12.2022
<input type="checkbox"/>	Kubernetes – Общие настройки безопасности отдельного рабочего узла - CIS
<input type="checkbox"/>	Kubernetes – Общие настройки безопасности главного узла - CIS
<input type="checkbox"/>	Docker – Аудит безопасности платформы контейнеризации – CIS
<input type="checkbox"/>	Debian – Общие настройки безопасности – АЛТЭК-СОФТ
<input type="checkbox"/>	Debian – Общие настройки безопасности – АЛТЭК-СОФТ
<input type="checkbox"/>	Astra Linux SE и CE / ALT / RED OS 7.3 – Оценка соответствия стандарту - ГОСТ Р 57580.1-2017
<input type="checkbox"/>	Astra Linux SE и CE / ALT / RED OS 7.3 – Аудит безопасности критической информационной инфраструктуры - ФСТЭК №239
<input type="checkbox"/>	Astra Linux SE и CE / ALT / RED OS 7.3 – Аудит безопасности АСУ ТП - ФСТЭК №31
<input checked="" type="checkbox"/>	Astra Linux SE и CE – Общие настройки безопасности – АЛТЭК-СОФТ
<input checked="" type="checkbox"/>	Astra Linux SE 1.7 – Настройки по руководству Red Book - РусБИТех
<input type="checkbox"/>	Astra Linux SE 1.6 – Настройки по руководству Red Book - РусБИТех

Всего: 25 Выбрано: 2

- Astra Linux SE 1.7 – Настройки по руководству Red Book -
 - Профиль по умолчанию
- Astra Linux SE и CE – Общие настройки безопасности – АЛТЭК-СОФТ
 - Профиль по умолчанию
 - Astra Linux SE и CE – Общие настройки безопасности

Сканировать все профили
 Пропускать неприменимые конфигурации

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;

Доставка отчёта

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	Имя
Нет данных для отображения	

20

Добавить шаблон отчёта...

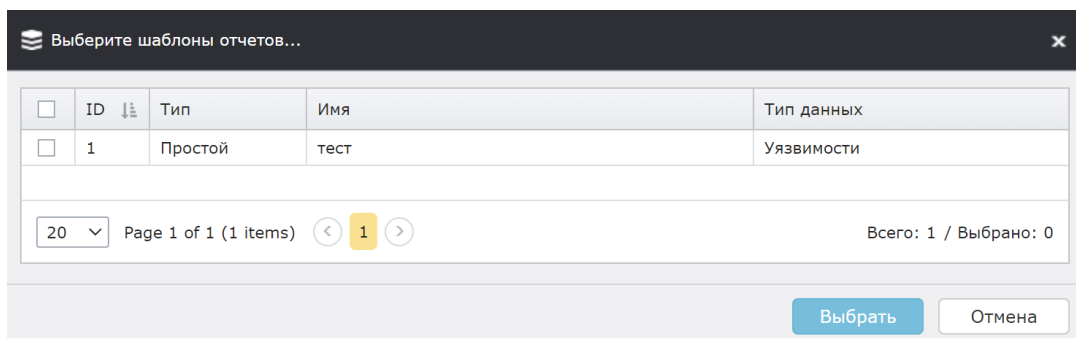
Адреса доставки для отчета

ID	Тип	Путь
Нет данных для отображения		

20

Добавить адрес 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.

The screenshot shows a sidebar with navigation options and a main table titled 'История запусков'. The table has columns for ID, Start, End, Total Hosts, Successful, Unavailable, With Errors, Not Processed, and Instruments.

№	Начало	Завершение	Всего хостов	Успешных	Недоступных	С ошибками	Не обработано	Инструменты
109	14.10.2024, 16:25:04	14.10.2024, 16:25:49	2	2	-	-	-	
103	09.10.2024, 11:08:13	09.10.2024, 11:08:22	1	1	-	-	-	

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;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя	<input type="text"/>
Описание	<input style="height: 40px;" type="text"/>
Тип сканирования	<input type="text" value="Аудит уязвимостей"/>
Служба сканирования	<input type="text" value="scan"/>
Запуск	<input type="text" value="По требованию"/>
Расширенный лог	<input checked="" type="checkbox"/> Запустить сразу после закрытия мастера <input type="checkbox"/> Повторно запускать неуспешные хосты <input type="checkbox"/> Ограничить максимальное время выполнения задания <input type="checkbox"/> Сохранять файл результатов <input type="checkbox"/> Сохранять файл системных характеристик <input type="checkbox"/> Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации
Дополнительно	<input type="checkbox"/> Оповещать по e-mail <input type="checkbox"/> Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

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

Настройки **Группы и хосты**

Группы и хосты
Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID	IP / DNS	Описание	CPE	
2	192.168.1.6			🗑️
4	192.168.100.2			🗑️
5	192.168.99.1			🗑️
7	192.168.99.3			🗑️

Добавить хосты Выбрано: 4

Выбранные группы

ID	Имя	Описание
Нет данных для отображения		

Добавить группы Выбрано: 0

Назад Вперед **Отмена**

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

Учётные данные задания
Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных	Команды
2	Ssh		90-сеть Переименовано	<input checked="" type="radio"/> Безагент	⚙️
3	Ssh		test	<input checked="" type="radio"/> Безагент	⚙️
8	Windows		winrm test	<input type="radio"/> С использованием агента <input type="radio"/> Безагент WMI <input checked="" type="radio"/> Безагент WinRM	⚙️

Добавить учётные данные... Всего: 3

Назад Вперед **Отмена**

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;

Настройки Группы и хосты Учётные данные **Профили сканирования**

Профили сканирования

Сканирование может осуществляться без профилей, либо с указанными ниже профилями из списка.

Профили	Тип сканирования
<input checked="" type="radio"/> Без профилей	<input type="radio"/> Быстрое
<input type="radio"/> Выбранные вручную	<input checked="" type="radio"/> Полное
<input type="checkbox"/> тест (Unix) Динамический профиль	<input type="radio"/> Полное с дополнительным сканированием JAR-файлов

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**;

Настройки Группы и hosts Учётные данные Профили сканирования **Отчёты**

Отчёты
Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчётов

Тип	ID	Имя	Тип данных	Команды
Нет данных для отображения				

20 ▼ Всего: 0

[Добавить шаблон отчёта...](#)

Адреса доставки для отчёта

ID	Тип	ID	Путь	Учётная запись	Формат	Команды
Нет данных для отображения						

20 ▼ Всего: 0

[Добавить адрес доставки...](#)

[Назад](#) [Вперёд](#) [Отмена](#)

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;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Служба сканирования

Запуск

Запустить сразу после закрытия мастера

Повторно запускать неуспешные хосты

Ограничить максимальное время выполнения задания

Расширенный лог

Сохранять файл результатов

Сохранять файл системных характеристик

Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации

Дополнительно

Оповещать по e-mail

Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

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

Настройки **Группы и хосты**

Группы и хосты

Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID	IP / DNS	Описание	CPE	
2	192.168.1.6			
4	192.168.100.2			
5	192.168.99.1			
7	192.168.99.3			

Выбрано: 4

Выбранные группы

ID	Имя	Описание	
Нет данных для отображения			

Выбрано: 0

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

Учётные данные задания
 Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных	Команды
2	Ssh		80-сеть Переименовано	<input checked="" type="radio"/> Безагент	
3	Ssh		test	<input checked="" type="radio"/> Безагент	
8	Windows		winnm test	<input type="radio"/> С использованием агента <input type="radio"/> Безагент WMI <input checked="" type="radio"/> Безагент WinRM	

Всего: 3

Добавить учётные данные...

Назад Вперед Отмена

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.

Настройки Группы и hosts Учётные данные **Профили сканирования**

Профили сканирования

Сканирование может осуществляться без профилей, либо с указанными ниже профилями из списка.

Профили **Тип сканирования**

Без профилей Полное

Выбранные вручную Быстрое

Не создано ни одного профиля

Для создания профилей воспользуйтесь менеджером аудитов

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**;

Настройки Группы и hosts Учётные данные Профили сканирования **Отчёт**

Отчёты

Вы можете формировать один или несколько отчетов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	ID	Имя	Тип данных	Команды
Нет данных для отображения				

20 Всего: 0

[Добавить шаблон отчёта...](#)

Адреса доставки для отчета

ID	Тип	ID	Путь	Учётная запись	Формат	Команды
Нет данных для отображения						

20 Всего: 0

[Добавить адрес доставки...](#)

Назад **Вперед** Отмена

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 стандартизированного 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;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Служба сканирования

Запуск

Запустить сразу после закрытия мастера

Повторно запускать неуспешные хосты

Ограничить максимальное время выполнения задания

Расширенный лог

Сохранять файл результатов

Сохранять файл системных характеристик

Сохранять фактические значения xccdf

Сохранять только ненастроенные фактические значения

Дополнительно

Оповещать по e-mail

Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

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

Настройки **Группы и хосты**

Группы и хосты

Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID	IP / DNS	Описание	CPE	
2	192.168.1.6			
4	192.168.100.2			
5	192.168.99.1			
7	192.168.99.3			

Выбрано: 4

Выбранные группы

ID	Имя	Описание	
Нет данных для отображения			

Выбрано: 0

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

Учётные данные задания
 Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных	Команды
2	Ssh		80-сеть Переименовано	<input checked="" type="radio"/> Безагент	
3	Ssh		test	<input checked="" type="radio"/> Безагент	
8	Windows		wingrm test	<input type="radio"/> С использованием агента <input type="radio"/> Безагент WMI <input checked="" type="radio"/> Безагент WinRM	

Всего: 3

Добавить учётные данные...

Назад Вперёд Отмена

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

[Подробнее про подбор учетных записей](#)

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

Настройки Группы и хосты Учётные данные **Конфигурации**

Выберите конфигурацию

Microsoft Windows 10

Выбрать все Сбросить все

Поиск конфигураций

#	Имя
<input type="checkbox"/>	Конфигурация Windows PrivateGuard для Windows 10
<input type="checkbox"/>	Windows 10 – Отключение передачи приватной информации – Microsoft
<input checked="" type="checkbox"/>	Windows 10 – Общие настройки безопасности – Microsoft
<input checked="" type="checkbox"/>	Windows – Оценка соответствия стандарту версии 3.2.1 - PCI DSS

Всего: 4 Выбрано: 2

Конфигурация

Название Windows – Оценка соответствия стандарту версии 3.2.1 - PCI DSS

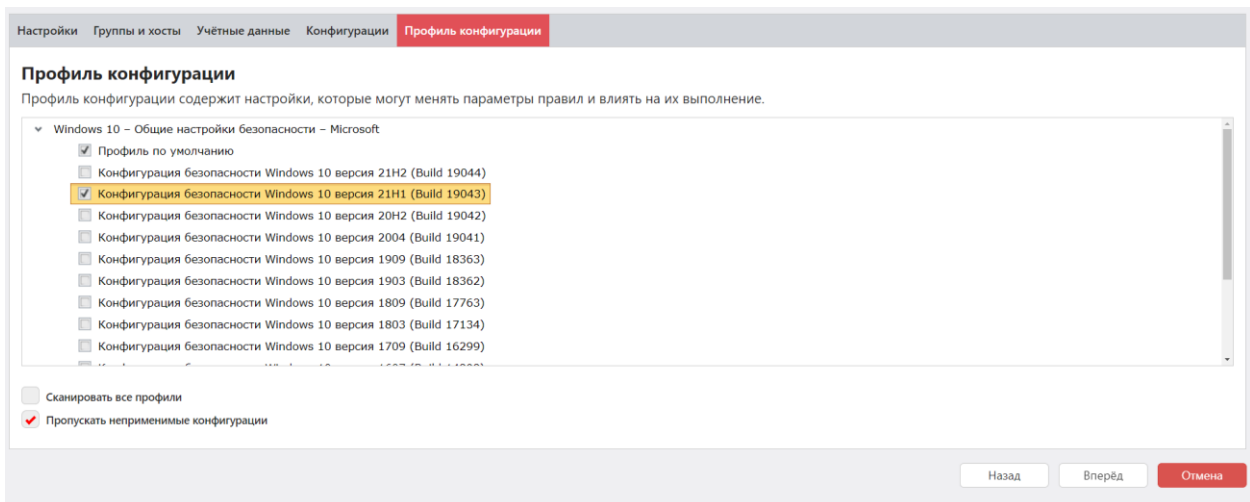
Версия 53

Файл Benchmarks\PCI DSS\ALT-X-PCI_DSS-xxcdf.xml

Платформа Microsoft Windows 10 (cpe:/o:microsoft:windows_10)
 Microsoft Windows 7 (cpe:/o:microsoft:windows_7)
 Microsoft Windows 8 (cpe:/o:microsoft:windows_8)
 Microsoft Windows 8.1 (cpe:/o:microsoft:windows_8:1)
 Microsoft Windows Server 2003 (cpe:/o:microsoft:windows_server_2003)
 Microsoft Windows Server 2008

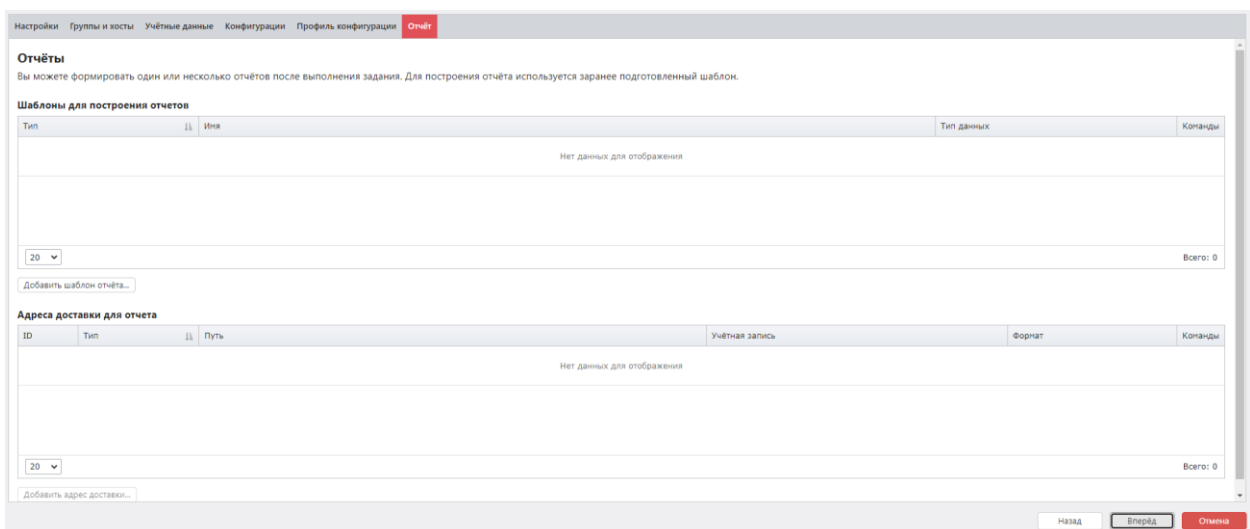
Назад Вперёд Отмена

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, пользователи 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;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя	<input type="text"/>
Описание	<div style="border: 1px solid #ccc; height: 40px;"></div>
Тип сканирования	<input type="text" value="Инвентаризация"/>
Служба сканирования	<input type="text" value="scan"/>
Запуск	<input type="text" value="По требованию"/>
	<input checked="" type="checkbox"/> Запустить сразу после закрытия мастера <input type="checkbox"/> Повторно запускать неуспешные хосты <input type="checkbox"/> Ограничить максимальное время выполнения задания
Расширенный лог	<input type="checkbox"/> Сохранять файл результатов
Дополнительно	<input type="checkbox"/> Оповещать по e-mail <input type="checkbox"/> Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

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

Настройки **Группы и хосты**

Группы и хосты

Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID	IP / DNS	Описание	CPE	
2	192.168.1.6			
4	192.168.100.2			
5	192.168.99.1			
7	192.168.99.3			

Выбрано: 4

[Добавить хосты](#)

Выбранные группы

ID	Имя	Описание	
Нет данных для отображения			

Выбрано: 0

[Добавить группы](#)

Назад Вперёд **Отмена**

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

Учётные данные задания

Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных	Команды
2	Ssh		80-сеть Переименовано	<input checked="" type="radio"/> Безагент	
3	Ssh		test	<input checked="" type="radio"/> Безагент	
8	Windows		winrm test	<input type="radio"/> С использованием агента <input type="radio"/> Безагент WMI <input checked="" type="radio"/> Безагент WinRM	

Всего: 3

[Добавить учётные данные...](#)

Назад Вперёд **Отмена**

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

[Подробнее про подбор учетных записей](#)

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

Настройки Группы и хосты Учётные данные **Параметры инвентаризации**

Параметры инвентаризации

Укажите профиль инвентаризации

Профиль windows

Выбрать все Сбросить все

- Аппаратное обеспечение**
 - Список CPU**
 - CPU**
 - Имя
 - Производитель
 - Описание
 - Максимальная частота
 - ID устройства
 - Материнская плата
 - BIOS
 - Слоты памяти
 - Сетевые адаптеры
 - Видеокарты
 - Физические диски
 - Оптические приводы
 - Логические диски
 - USB-устройства
- Программное обеспечение
- OVAL-Инвентаризация

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

Настройки Группы и хосты Учётные данные Параметры инвентаризации **Отчёт**

Отчёты

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчётов

Тип	Имя	Тип данных	Команды
Нет данных для отображения			

20 Всего: 0

[Добавить шаблон отчёта...](#)

Адреса доставки для отчёта

ID	Тип	Путь	Учётная запись	Формат	Команды
Нет данных для отображения					

20 Всего: 0

[Добавить адрес доставки...](#)

Назад **Вперед** Отмена

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;

Настройки

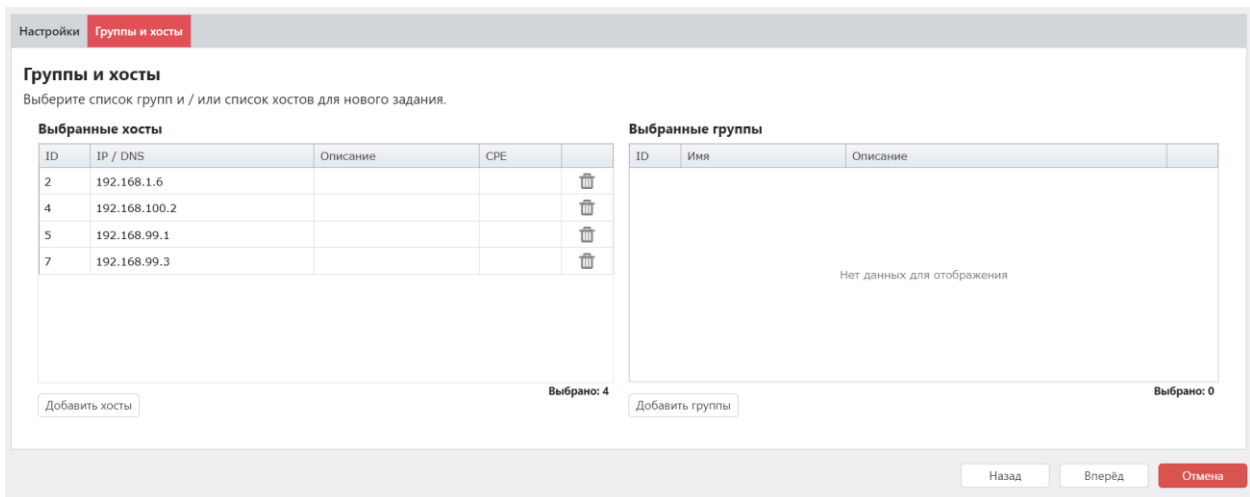
Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

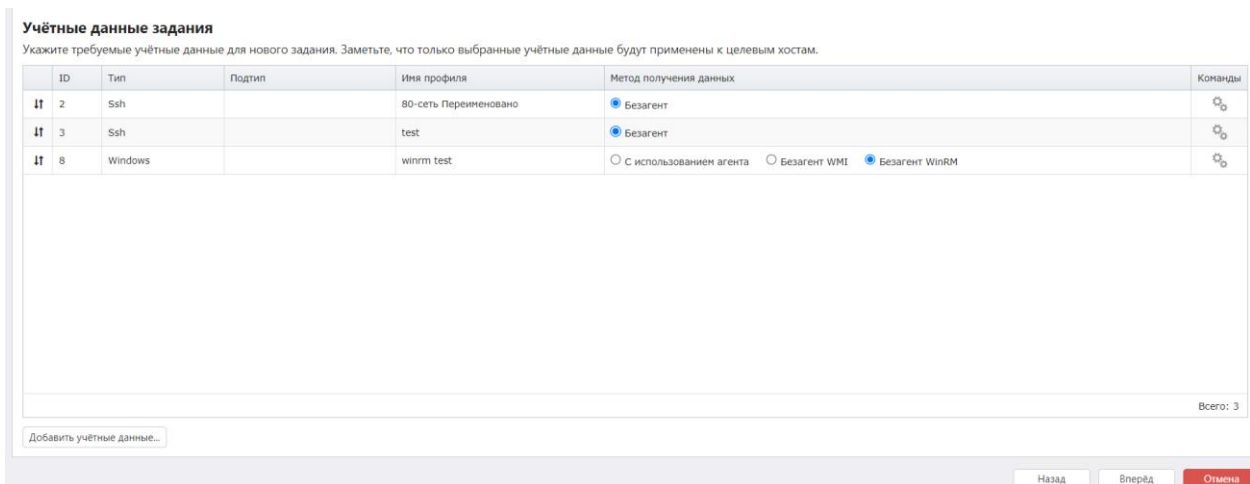
Имя	<input style="width: 90%;" type="text"/>
Описание	<div style="border: 1px solid #ccc; height: 40px; width: 90%;"></div>
Тип сканирования	<input style="width: 90%;" type="text" value="Фиксация"/>
Служба сканирования	<input style="width: 90%;" type="text" value="scan"/>
Запуск	<input style="width: 90%;" type="text" value="По требованию"/>
Дополнительно	<input checked="" type="checkbox"/> Запустить сразу после закрытия мастера <input type="checkbox"/> Повторно запускать неуспешные хосты <input type="checkbox"/> Ограничить максимальное время выполнения задания <input type="checkbox"/> Оповещать по e-mail <input type="checkbox"/> Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

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**;

Настройки Группы и хосты Учётные данные **Фиксация файловой системы**

Фиксация файловой системы

Укажите каталоги, которые должны быть зафиксированы и каталоги, которые должны быть исключены из процесса фиксации.

Каталог Имя файла или паттерна

Каталог	Имя файла	Вкл. подпапки	Исключить		
D:\Temp		<input type="checkbox"/>	<input checked="" type="checkbox"/>		
D:\Temp	*.gost	<input type="checkbox"/>	<input type="checkbox"/>		

Метод снятия КС

Всего: 2

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

Настройки Группы и хосты Учётные данные Фиксация файловой системы **Фиксация реестра**

Фиксация реестра

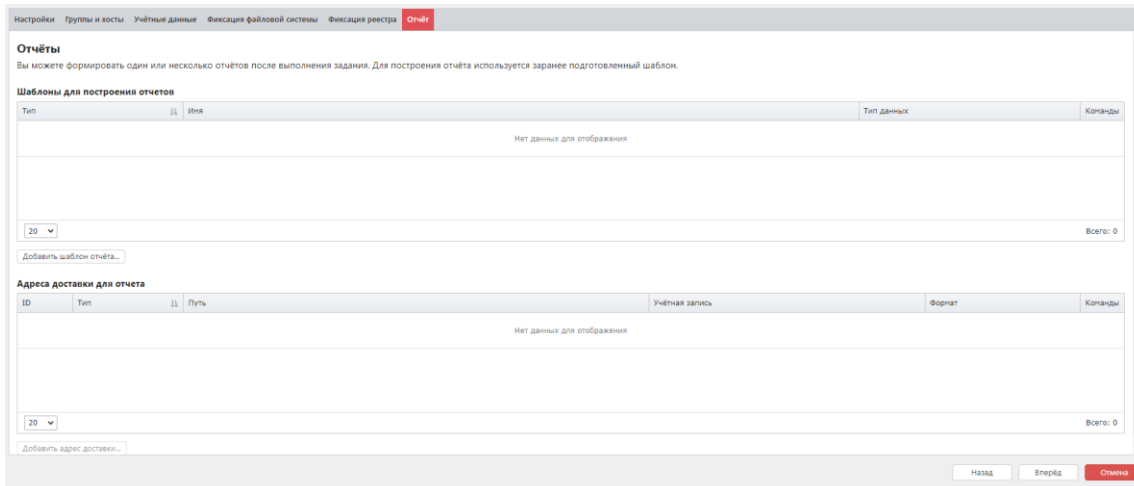
Укажите ключи реестра, которые должны быть зафиксированы и ключи реестра, которые должны быть исключены из процесса фиксации.

Ключи реестра

Ключ	Вкл. подключи	Исключить		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ASP.NET Core\Shared Framework	<input type="checkbox"/>	<input type="checkbox"/>		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ASP.NET\4.0.30319.0\AssemblyVersion	<input type="checkbox"/>	<input type="checkbox"/>		

Всего: 2

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;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые hosts.

Имя

Описание

Тип сканирования

Служба сканирования

Запуск

Запустить сразу после закрытия мастера

Ограничить максимальное время выполнения задания

Расширенный лог Сохранять файл результатов

Дополнительно

Оповещать по e-mail

Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

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

Настройки **Группы и hosts**

Группы и hosts

Выберите список групп и / или список hosts для нового задания.

Выбранные hosts

ID	IP / DNS	Описание	CPE	
2	192.168.1.6			
4	192.168.100.2			
5	192.168.99.1			
7	192.168.99.3			

Выбрано: 4

Выбранные группы

ID	Имя	Описание	
Нет данных для отображения			

Выбрано: 0

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

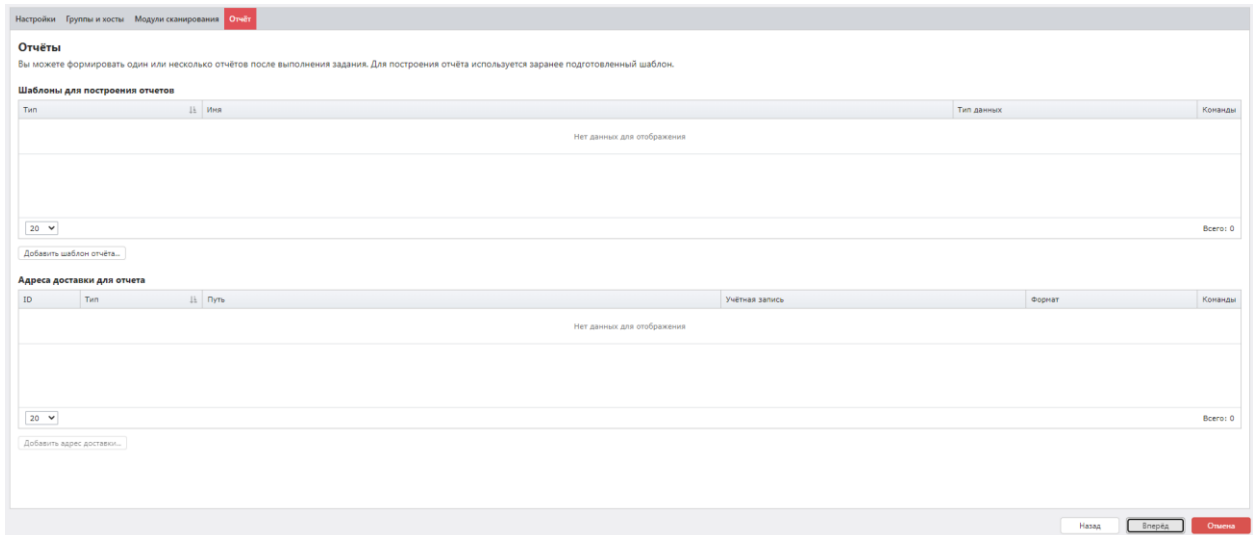
Модули сканирования

Укажите требуемые протоколы АСУ ТП/ПЛК

- Simatic ALM
- Simatic S7
- Sicam PAS IPC
- Citect SCADA
- Modbus TCP/UDP
- Profinet IO
- ArcestrA Logger
- BACnet/IP
- Ethernet/IP
- GenBroker (GENESIS32/64)
- Schneider Electric IGSS
- FINS
- ProConOS
- CoDeSysV2
- CoDeSysV3
- MZTA
- Segnetics
- IsaGraF

[Выбрать всё](#) [Сбросить всё](#)

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 хccdf – 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 хccdf**;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Служба сканирования

Запуск

Запустить сразу после закрытия мастера

Повторно запускать неуспешные хосты

Ограничить максимальное время выполнения задания

Расширенный лог

Сохранять файл результатов

Сохранять файл системных характеристик

Сохранять фактические значения xscdf

Сохранять только ненастроенные фактические значения

Дополнительно

Оповещать по e-mail

Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

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

Настройки **Группы и хосты**

Группы и хосты

Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID	IP / DNS	Описание	CPE	
2	192.168.1.6			
4	192.168.100.2			
5	192.168.99.1			
7	192.168.99.3			

Выбрано: 4

Выбранные группы

ID	Имя	Описание	
Нет данных для отображения			

Выбрано: 0

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

Учётные данные задания
 Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных	Команды
2	Ssh		80-сеть Переименовано	<input checked="" type="radio"/> Безагент	
3	Ssh		test	<input checked="" type="radio"/> Безагент	
8	Windows		wingrm test	<input type="radio"/> С использованием агента <input type="radio"/> Безагент WMI <input checked="" type="radio"/> Безагент WinRM	

Всего: 3

Добавить учётные данные...

Назад Вперед **Отмена**

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**;

Настройки Группы и хосты Учётные данные **Отчёт**

Отчёты
 Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчётов

Тип	ID	Имя	Тип данных	Команды
Нет данных для отображения				

20 Всего: 0

Добавить шаблон отчёта...

Адреса доставки для отчета

ID	Тип	ID	Путь	Учётная запись	Формат	Команды
Нет данных для отображения						

20 Всего: 0

Добавить адрес доставки...

Назад Вперед **Отмена**

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;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя	<input type="text"/>
Описание	<div style="border: 1px solid #ccc; height: 50px;"></div>
Тип сканирования	<input type="text" value="Проверка доступности"/>
Служба сканирования	<input type="text" value="scan"/>
Запуск	<input type="text" value="По требованию"/>
Дополнительно	<input checked="" type="checkbox"/> Запустить сразу после закрытия мастера <input type="checkbox"/> Повторно запускать неуспешные хосты <input type="checkbox"/> Ограничить максимальное время выполнения задания <input type="checkbox"/> Оповещать по e-mail

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

Настройки **Группы и хосты**

Группы и хосты

Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID	IP / DNS	Описание	CPE	
2	192.168.1.6			
4	192.168.100.2			
5	192.168.99.1			
7	192.168.99.3			

Выбрано: 4

[Добавить хосты](#)

Выбранные группы

ID	Имя	Описание	
Нет данных для отображения			

Выбрано: 0

[Добавить группы](#)

[Назад](#) [Вперёд](#) [Отмена](#)

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

Транспорт

Выберите, доступность какого транспорта требуется проверить. Для проверк

- Agent**
Компонент RedCheck Agent. Порт по умолчанию: TCP 8732.
- WMI**
Провайдер Windows Management Instrumentation (WMI).
- WinRM**
Провайдер Windows Remote Management (WinRM).
- SSH**
Доступ по протоколу SSH. Порт по умолчанию TCP 22.
- HTTP**
Доступ по протоколу HTTP.
- SQL**
Доступность баз данных SQL. Требуется учётная запись типа SQL.
- Update Agent**
Компонент RedCheck Update Agent. Порт по умолчанию: TCP 8733.

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

Учётные данные задания

Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных	Команды
5	Windows		wingrm		

Всего: 1

Добавить учётные данные...

Назад

Вперёд

Отмена

[Подробнее про подбор учетных записей](#)

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

Настройки Группы и хосты Транспорт Учётные данные **Отчёт**

Отчёты

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	ID	Имя	Тип данных	Команды
Нет данных для отображения				

20

Всего: 0

Добавить шаблон отчёта...

Адреса доставки для отчета

ID	Тип	ID	Путь	Учётная запись	Формат	Команды
Нет данных для отображения						

20

Всего: 0

Добавить адрес доставки...

Назад Вперёд Отмена

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;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Служба сканирования

Запуск

Запустить сразу после закрытия мастера

Ограничить максимальное время выполнения задания

Расширенный лог

Сохранять файл результатов

Уровень логирования [1-4]

Дополнительно

Оповещать по e-mail

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;

Настройки **Обнаружение хостов**

Диапазон хостов для сканирования

Вы можете использовать IP с диапазонами, DNS имена и их комбинации через пробел, например: 192.168.1.34 target1 192.168.0.1/24 10.6.15.2-46

TCP порты для определения доступности

Выберите профиль сканирования

Список портов

Методы определения доступности

ARP ICMP TCP_ACK TCP_SYN

Дополнительные параметры

Определять ОС

Расширенные настройки:

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

Расширенные настройки (экспертный режим)

Профиль временных настроек

Использовать интерфейс (eth[0-n])

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

Настройки Обнаружение хостов **Отчёт**

Отчёты

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	Имя	Тип данных	Команды
Нет данных для отображения			

20 Всего: 0

[Добавить шаблон отчёта...](#)

Адреса доставки для отчета

ID	Тип	Путь	Учётная запись	Формат	Команды
Нет данных для отображения					

20 Всего: 0

[Добавить адрес доставки...](#)

[Назад](#) [Вперёд](#) [Отмена](#)

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 Altxmar. Чем больше значение, тем детальнее будет лог;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя	<input type="text"/>
Описание	<div style="border: 1px solid #ccc; height: 40px;"></div>
Тип сканирования	Аудит в режиме "Пентест" ▾
Служба сканирования	<input type="text" value="scan"/>
Запуск	По требованию ▾
	<input checked="" type="checkbox"/> Запустить сразу после закрытия мастера <input type="checkbox"/> Ограничить максимальное время выполнения задания
Расширенный лог	<input type="checkbox"/> Сохранять файл результатов <input type="text" value="1"/> Уровень логирования [1-4]
Дополнительно	<input type="checkbox"/> Оповещать по e-mail <input type="checkbox"/> Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

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

Настройки **Группы и хосты**

Группы и хосты
Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID	IP / DNS	Описание	CPE	
2	192.168.1.6			
4	192.168.100.2			
5	192.168.99.1			
7	192.168.99.3			

Выбрано: 4

[Добавить хосты](#)

Выбранные группы

ID	Имя	Описание	
Нет данных для отображения			

Выбрано: 0

[Добавить группы](#)

[Назад](#)
[Вперёд](#)
[Отмена](#)

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 сканирования;
 - [Перечень портов для профиля TCP \[ТОП 50\]](#)
 - [Перечень портов для профиля TCP \[ТОП 1000\]](#)
 - [Перечень портов для профиля TCP-UDP \[ТОП 1000\]](#)

Настройки Группы и хосты **Типы сканирования**

Профили сканирования

По умолчанию

Типы сканирования

Выберите типы сканирования, которые требуется выполнить в задании.

Сканирование портов
 Подбор паролей
 Поиск уязвимостей

Настройки сканирования ALTXmar

Определять ОС и службы Расширенное определение служб
 WEB уязвимости

Показывать уязвимыми сертификаты, срок действия которых истекает в течение (дней)

Выберите профиль сканирования

Исключаемые TCP порты

Исключаемые UDP порты

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 Altxmar не тратил более получаса на один хост. В течение этого времени Altxmar 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 Altxmar 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 Altxmar 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).

Расширенные настройки (экспертный режим)

Профиль временных настроек	Активный
Таймаут для хоста (h,m,s)	1h
Использовать интерфейс (eth[0-n])	
Максимальное количество веб страниц (по умолчанию: 20, без ограничений: -1)	20
Максимальная глубина поиска веб страниц (по умолчанию: 3, без ограничений: -1)	3
Максимальное количество запросов для группы хостов	900
Максимальное время ожидания ответа на запрос (мс)	1250
Максимальное количество повторных передач запроса	6

Использовать TCP SYN сканирование для ускорения определения открытых портов

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

Настройки Группы и хосты Типы сканирования **Настройки подбора паролей**

Настройки подбора паролей

Укажите тип подбора, порт и имя экземпляра

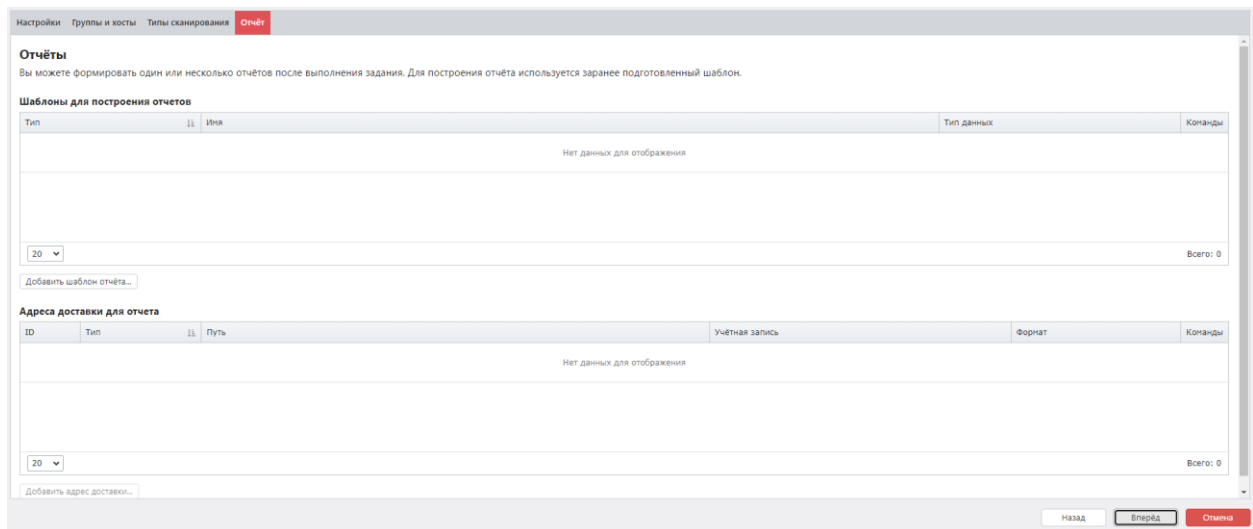
Тип	<input type="text" value="Подбор паролей к MS SQL Server"/>
Имя экземпляра	<input type="text"/>
	<input type="checkbox"/> Сканировать все экземпляры
Порт	<input type="text" value="1433"/>
Таймаут подбора (h,m,s). 0 - без ограничений	<input type="text" value="3h"/>
Использовать интерфейс (eth[0-n])	<input type="text"/>
Профиль временных настроек	<input type="text" value="Активный"/>

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

Компонент ALTXMAP

	<input type="checkbox"/> Использовать встроенные словари
Путь к словарю логинов	<input type="text" value="/var/opt/altxmap/nselib/data/usernames.lst"/>
Путь к словарю паролей	<input type="text" value="/var/opt/altxmap/nselib/data/passwords.lst"/>

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.

Расписание задания

Укажите расписание для нового планового задания.

Когда следует запускать задание

Ежечасно

Время запуска

01/31/2023 11:09 AM

Истекает

01/31/2023 12:24 PM

Повторять каждые 1 (часы)

Приостанавливать задания

Время

Длительность

06:30 PM 03:00 PM

- Понедельник
- Вторник
- Среда
- Четверг
- Пятница
- Суббота
- Воскресенье

Пример использования

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

Расписание

Тип: Еженедельно

Время первого запуска: 06.04.2023 12:00:00

Время истечения: 06.05.2023 12:00:00

Повтор: Повторять каждые 1 (недели)

Расписание задания

Укажите расписание для нового планового задания.

Тип запуска

По расписанию

Когда следует запускать задание

Еженедельно

Время запуска

06.04.2023 12:00

Истекает

06.05.2023 12:00

Повторять каждые 1 (недели)

Настройка в момент создания

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

Тип запуска

По расписанию

Запустить сразу после закрытия мастера

Оповещать по e-mail

Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые
Просмотр параметров доступен на странице результатов сканирования.

Настройка при редактировании задания

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

Запуск

По требованию

Служба сканирования

a2e2f25a-ad8d-4c8a-b021-71382a8e2af7

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.

Повторно запускать неуспешные хосты

Интервал повторного запуска

Количество попыток

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

количество попыток

Ограничить максимальное время выполнения задания

Максимальное время, ч. (6 д. 23 ч.)

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](#)
- [5.2 Конфигурации](#)
- [5.3 OVAL-определения](#)
- [5.4 Отслеживание изменений результатов сканирования \(Контроль\)](#)
- [5.5 Профили сканирования Altxmap](#)

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 интересных нас уязвимостей.

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

REDCheck ДЕЙСТВИЯ ИНСТРУМЕНТЫ СПРАВКА

ГЛАВНАЯ ХОСТЫ ЗАДАНИЯ ИСТОРИЯ КОНТРОЛЬ ОТЧЁТЫ ПОЛЬЗОВАТЕЛИ

OVAL-профили

Просмотр и редактирование OVAL-профилей.

Семейство
Windows

Класс
Уязвимость

Статические профили
 Динамические профили

Создать статический профиль...
Создать динамический профиль...

ID	Имя	Описание	Тип
1	profile		Статический профиль
2	dynamic-profile		Динамический профиль
3	high		Динамический профиль
4	test		Статический профиль

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

Новый профиль

Статический профиль, содержит вручную сформированный набор аудитов.

Имя
Тестовый профиль

Описание

Семейство
Windows

Класс
Уязвимость

Добавить аудиты...

Сохранить Отмена

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

Аудиты

Семейство: Windows | Класс: Уязвимость | Название: | Ссылки: |

CVSS [0 - 10] | База данных: CVE ФСТЭК НКЦКИ | Риск: Недоступно Низкий Высокий Критический | Информация Средний

ALTIX ID	Риск	Ссылки	Название
<input type="checkbox"/>	Критический		Уязвимость внедрения команд в Node.js пакете im-metadata во всех версиях (CVE-2019-10788)
<input type="checkbox"/>	Критический		Уязвимость в iTunes до 12.10.5, iCloud до 10.9.3, iCloud до 7.18 (CVE-2020-3910)
<input type="checkbox"/>	Критический		Уязвимость в X-Plane до 11.41 (CVE-2019-19606)
<input type="checkbox"/>	Критический		Уязвимость в IBM Tivoli Storage FlashCopy Manager for VMware 3.1 до версии 3.1.1.3, 3.2 до версии 3.2.0.6, и 4.1 до версии 4.1.4 (CVE-2015-7425)
<input type="checkbox"/>	Критический		Уязвимость в Citrix NetScaler ADC и NetScaler Gateway 11.x до 11.0 Build 64.34, 10.5 до 10.5 Build 59.13, и 10.5.e до Build 59.1305.e (CVE-2016-2071)
<input checked="" type="checkbox"/>	Критический		Уязвимость в Git до 2.7.4 (CVE-2016-2324)
<input type="checkbox"/>	Критический		Уязвимость в Pidgin-OTR до 4.0.2 (CVE-2015-8833)
<input type="checkbox"/>	Критический		Уязвимость в Ruby gem rubyzip до 1.2.1 (CVE-2017-5946)
<input type="checkbox"/>	Критический		Уязвимость в Artifex Ghostscript 9.50 и 9.52 (CVE-2020-15900)
<input type="checkbox"/>	Критический		Уязвимость в HMS Industrial Networks eCatcher до 6.5.5 (CVE-2020-14498)
<input type="checkbox"/>	Критический		Уязвимость в Yaws по 2.0.7 (CVE-2020-24379)
<input type="checkbox"/>	Критический		Уязвимость в HPE Data Protector до 7.03_108, 8.x до 8.15, и 9.x до 9.06 (CVE-2016-2008)
<input type="checkbox"/>	Критический		Уязвимость в Veritas NetBackup 7.x по 7.5.0.7, 7.6.0.x по 7.6.0.4, 7.6.1.x по 7.6.1.2, и 7.7.x до 7.7.2 (CVE-2015-6552)
<input type="checkbox"/>	Критический		Уязвимость в Apple iTunes до 12.4.2 и в iCloud для Windows до 5.2.1 (CVE-2016-4609)
<input type="checkbox"/>	Критический		Уязвимость в Apple iTunes до 12.4.2 и в iCloud для Windows до 5.2.1 (CVE-2016-4610)
<input checked="" type="checkbox"/>	Критический		Уязвимость в PHP до 5.5.38, 5.6.x до 5.6.24, и 7.x до 7.0.9 (CVE-2016-6295)
<input type="checkbox"/>	Критический		Уязвимость в PHP до 5.6.7 (CVE-2015-4601)
<input type="checkbox"/>	Критический		Переполнение стека в PHP до 5.5.32, 5.6.x до 5.6.18, и 7.x до 7.0.3 (CVE-2016-2554)

20 Page 3 of 128 (2559 items) | Всего: 2,559 | Выбрано: 4

Выбрать аудиты | Отмена

Сохраним созданный профиль, нажав соответствующую кнопку.

Новый профиль

Статический профиль, содержит вручную сформированный набор аудитов.

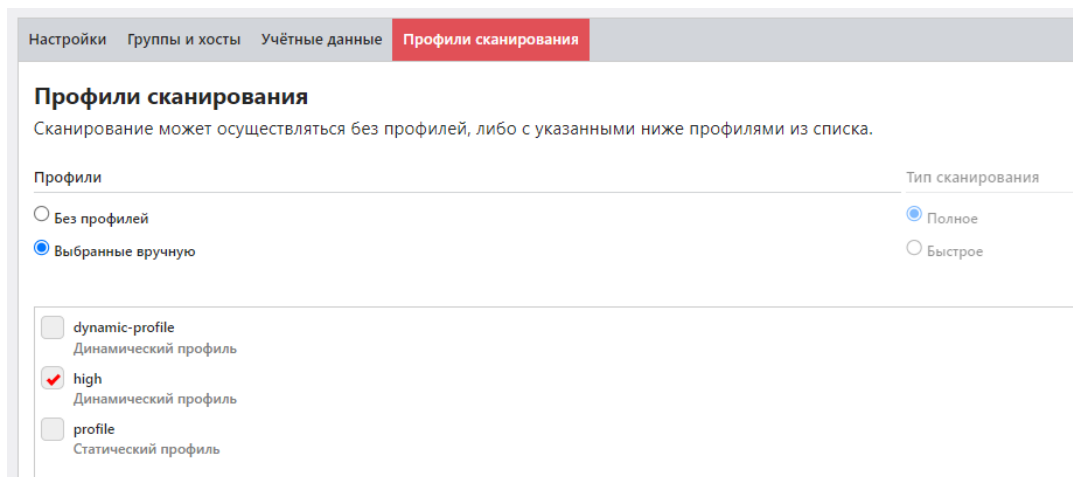
Имя:

Описание:

Семейство: Windows | Класс: Уязвимость

ALTIX ID	Риск	Ссылки	Название
> 319355	Критический		Уязвимость внедрения SQL в pip пакете django до 3.0.3 и до 2.2.10 и до 1.11.28 (CVE-2020-7471)
> 319563	Критический		Уязвимость удаленного выполнения кода в Node.js пакете pdf-image во всех версиях (CVE-2020-8132)
> 139196	Критический		Уязвимость в Git до 2.7.4 (CVE-2016-2324)
> 150860	Критический		Уязвимость в PHP до 5.5.38, 5.6.x до 5.6.24, и 7.x до 7.0.9 (CVE-2016-6295)

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



Настройки Группы и хосты Учётные данные **Профили сканирования**

Профили сканирования

Сканирование может осуществляться без профилей, либо с указанными ниже профилями из списка.

Профили Тип сканирования

Без профилей Полное

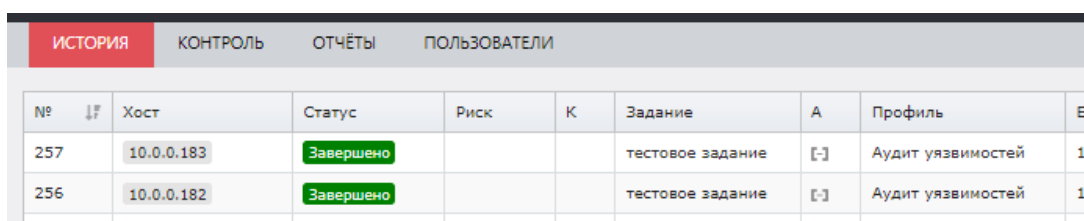
Выбранные вручную Быстрое

dynamic-profile
Динамический профиль

high
Динамический профиль

profile
Статический профиль

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



№	IP	Хост	Статус	Риск	К	Задание	А	Профиль	Е
257		10.0.0.183	Завершено			тестовое задание	[1]	Аудит уязвимостей	1
256		10.0.0.182	Завершено			тестовое задание	[1]	Аудит уязвимостей	1

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**;

ID	Имя	Описание
----	-----	----------

Статический профиль

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

Новый профиль
Статический профиль, содержит ручную сформированный набор аудитов.

Имя

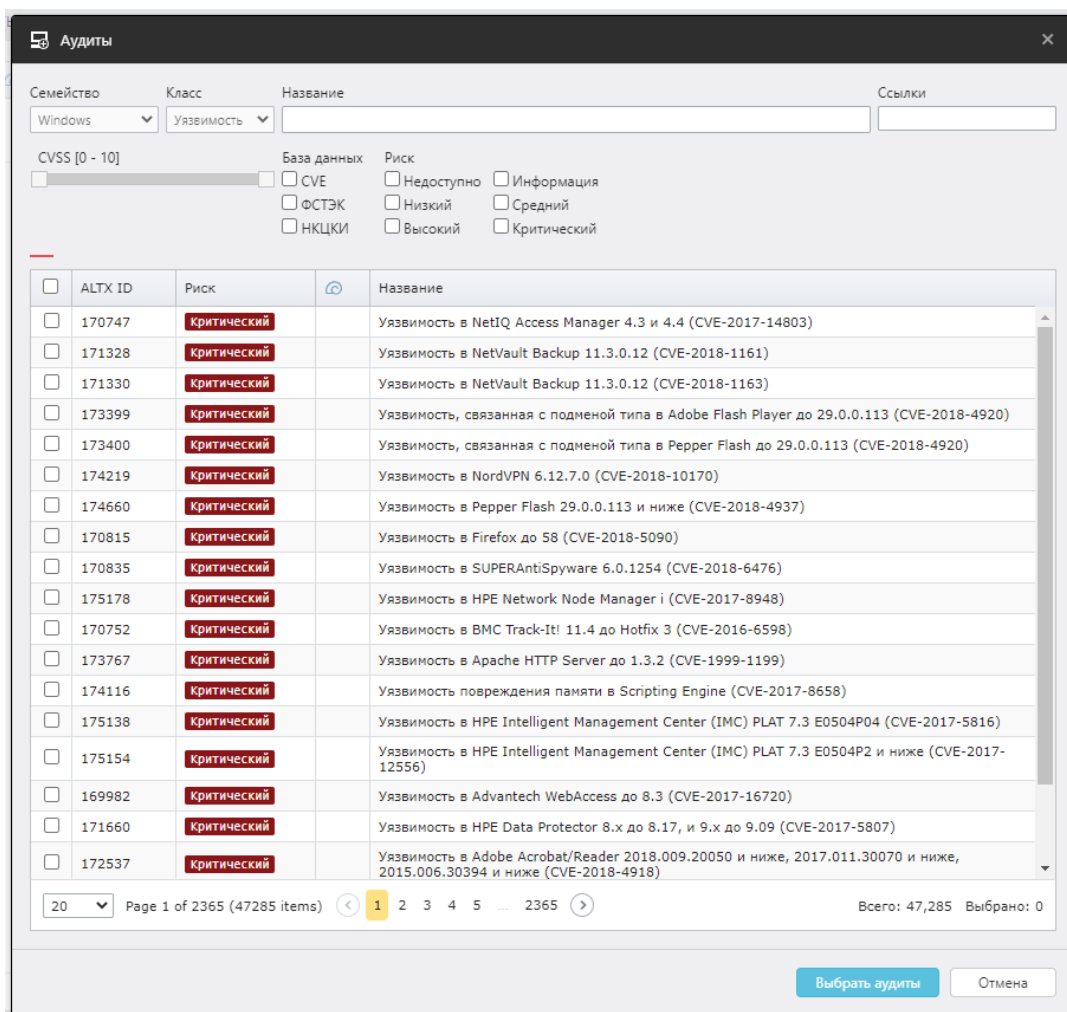
Описание

Семейство
Windows

Класс
Уязвимость

ALTX ID	Риск
---------	------

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

Класс

Фильтр по названию

Фильтр по описанию

CVE ФСТЭК НКЦКИ

Дата публикации (начало)

Не учитывать

Начиная с

Начиная с дней назад

Дата публикации (конец)

Не учитывать

Заканчивая

Заканчивая дней назад

Риск

Недоступно Информация
 Низкий Средний
 Высокий Критический

CVSS [0 - 10]

Наличие эксплоита

CVSS3 векторы атаки

Сетевой Смежная сеть
 Локальный Физический

CVSS3 параметры

Высокая сложность атаки
 Значит. влияние на целостность
 Значит. влияние на доступность
 Низкий уровень привилегий
 Влияние на друг. компон. системы
 Взаимодействие с пользователем

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**;

Редактирование профиля

Статический профиль содержит вручную сформированный набор аудитов.

Имя

Описание


Семейство

Класс

ALTX ID	Риск	🔗	Название
> 169224	Критический		Уязвимость в Adobe ColdFusion 2016 Update 4 и ниже, ColdFusion 11 update 12 и ниже (CVE-2017-11283)
> 170747	Критический		Уязвимость в NetIQ Access Manager 4.3 и 4.4 (CVE-2017-14803)
> 171328	Критический		Уязвимость в NetVault Backup 11.3.0.12 (CVE-2018-1161)
> 171330	Критический		Уязвимость в NetVault Backup 11.3.0.12 (CVE-2018-1163)
> 174219	Критический		Уязвимость в NordVPN 6.12.7.0 (CVE-2018-10170)
> 170835	Критический		Уязвимость в SUPERAntiSpyware 6.0.1254 (CVE-2018-6476)
> 170752	Критический		Уязвимость в BMC Track-It! 11.4 до Hotfix 3 (CVE-2016-6598)
> 173767	Критический		Уязвимость в Apache HTTP Server до 1.3.2 (CVE-1999-1199)
> 175138	Критический		Уязвимость в HPE Intelligent Management Center (IMC) PLAT 7.3 E0504P04 (CVE-2017-5816)
> 175154	Критический		Уязвимость в HPE Intelligent Management Center (IMC) PLAT 7.3 E0504P2 и ниже (CVE-2017-12556)
> 169982	Критический		Уязвимость в Advantech WebAccess до 8.3 (CVE-2017-16720)
> 171660	Критический		Уязвимость в HPE Data Protector 8.x до 8.17, и 9.x до 9.09 (CVE-2017-5807)
> 169253	Высокий		Уязвимость чтения за пределами выделенной памяти в Adobe Acrobat Reader 2017.012.20098 и ниже, 2017.011.30066 и ниже, 2015.006.30355 и ниже, и 11.0.22 и ниже (CVE-2017-16376)
> 169255	Высокий		Уязвимость обхода безопасности в Adobe Acrobat Reader 2017.012.20098 и ниже, 2017.011.30066 и ниже, 2015.006.30355 и ниже, и 11.0.22 и ниже (CVE-2017-16380)
> 169256	Высокий		Уязвимость чтения за пределами выделенной памяти в Adobe Acrobat Reader 2017.012.20098 и ниже, 2017.011.30066 и ниже, 2015.006.30355 и ниже, и 11.0.22 и ниже (CVE-2017-16403)
> 169342	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome до 63.0.3239.84 (CVE-2017-15412)
> 169343	Высокий		Уязвимость в Google Chrome до 63.0.3239.84 (CVE-2017-15413)
> 169455	Высокий		Уязвимость в Adobe Acrobat и Reader: 2017.012.20098 и ниже, 2017.011.30066 и ниже, 2015.006.30355 и ниже, и 11.0.22 и ниже (CVE-2017-16376)

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  ;

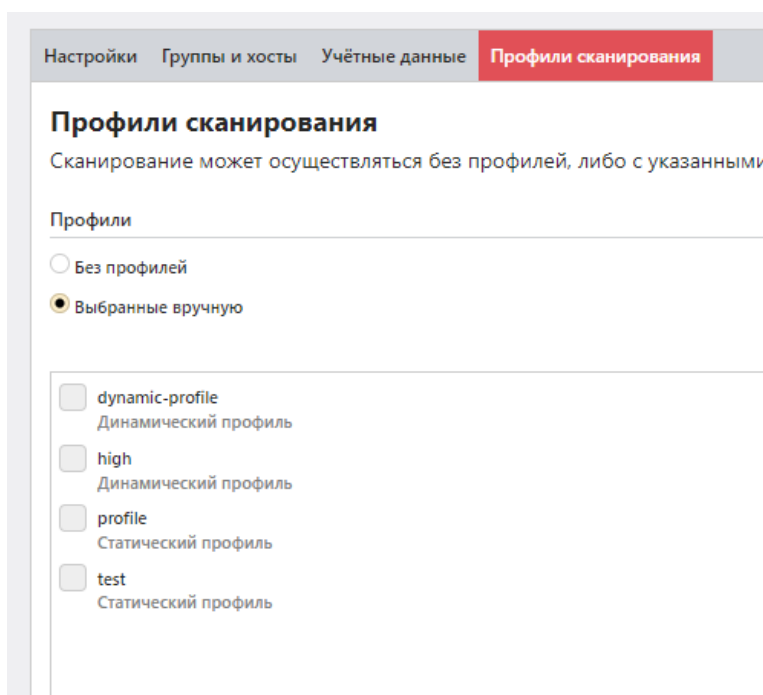
	ALTX ID	Риск	🔗	Название	Дата публикации	🗑️
>	169982	Критический		Уязвимость в Adva	05.01.2018, 08:29:00	🗑️
>	171660	Критический		Уязвимость в HPE	15.02.2018, 22:29:00	🗑️
>	170752	Критический		Уязвимость в BMC	30.01.2018, 20:29:00	🗑️
>	175138	Критический		Уязвимость в HPE	15.02.2018, 22:29:00	🗑️
>	175154	Критический		Уязвимость в HPE	15.02.2018, 22:29:00	🗑️
>	170835	Критический		Уязвимость в SUPE	31.01.2018, 19:29:00	🗑️

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**;

Включаемые статические профили аудитов ▾

ID	Название	Семейство	
4	test	windows	

Выбрано: 1

[Добавить профиль аудитов](#)

Исключаемые статические профили аудитов >

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

Выбор профиля аудитов

Название

<input type="checkbox"/>	ID	Название	Семейство
<input type="checkbox"/>	1	profile	Windows
<input type="checkbox"/>	4	test	Windows

20 Page 1 of 1 (2 items) 1 Всего: 2 / Выбрано: 0

[Выбрать](#) [Отмена](#)

5.2 Конфигурации

RedCheck предоставляет возможность изменять конфигурации, имеющиеся в базе данных, для проведения Аудита конфигураций согласно собственным 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».

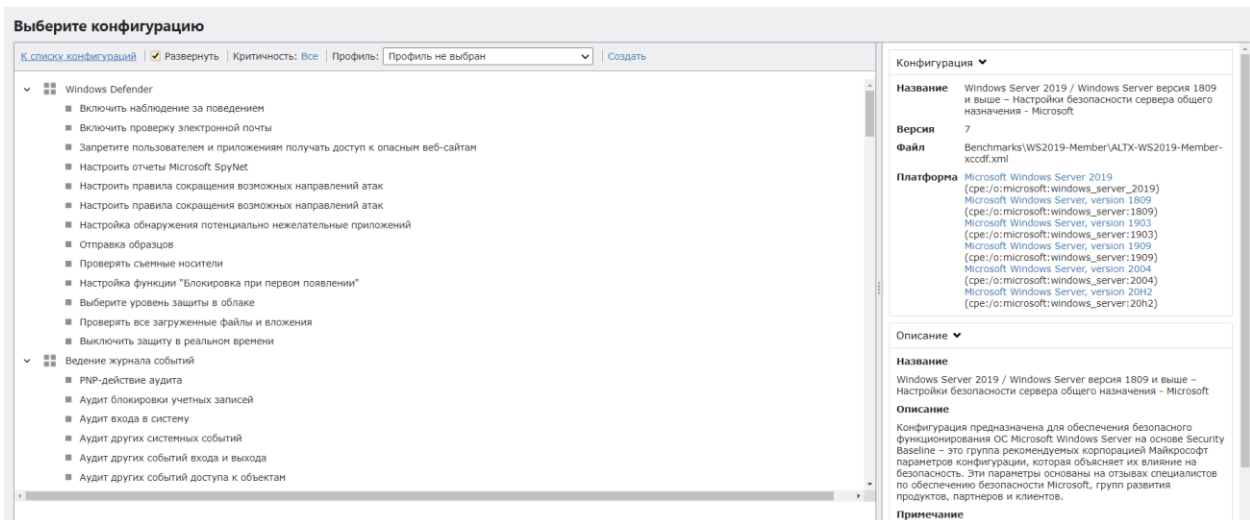
Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

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

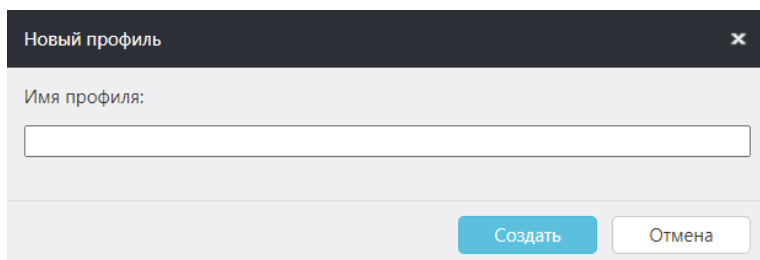
Имя		
Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения - Microsoft		
Windows Server 2019 / Windows Server версия 1809 и выше – Настройки для роли контроллера домена - Microsoft		
Windows – Оценка соответствия стандарту версии 3.2.1 - PCI DSS		

Для редактирования конфигурации для сервера общего назначения

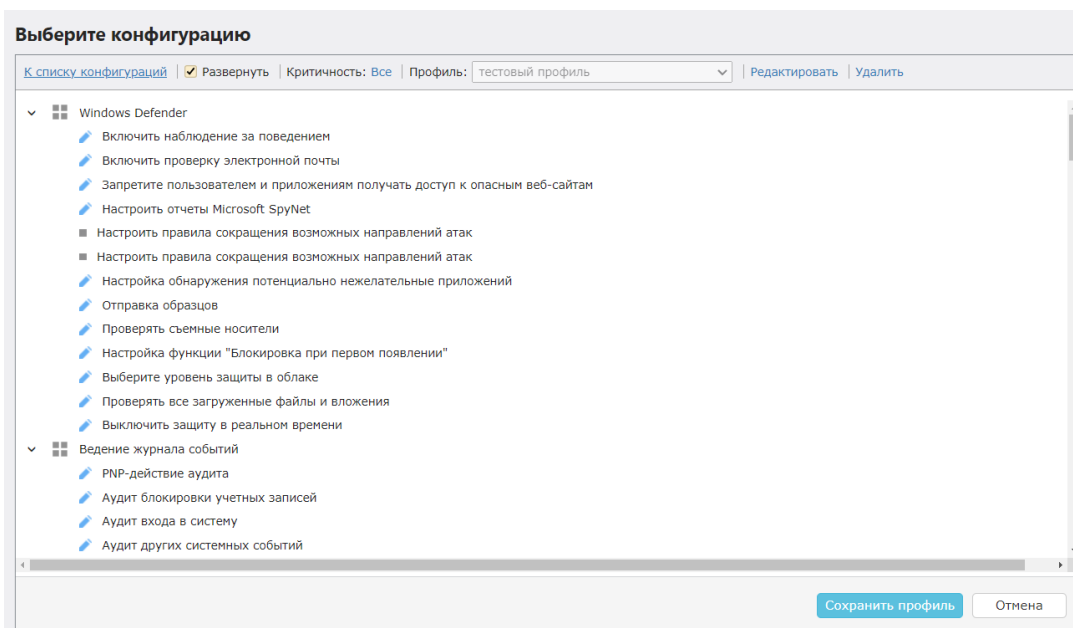
нажмем



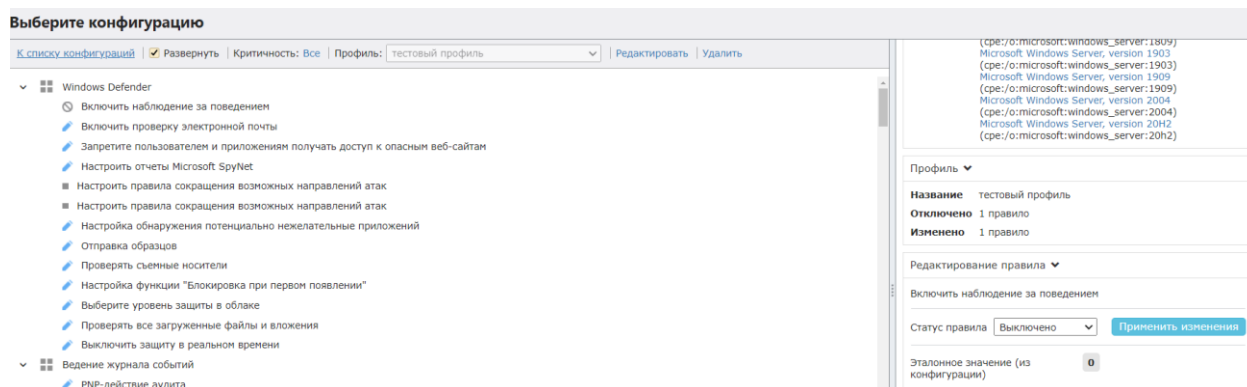
Создадим собственный профиль для изменения правил в конфигурации. Для этого нажмем **Создать** → введем имя для профиля → **Создать**.



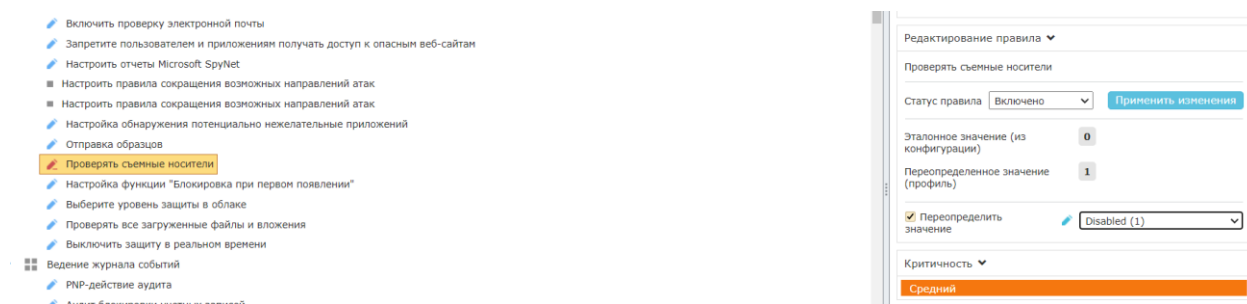
После создания профиля можно изменять нужные нам правила.



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

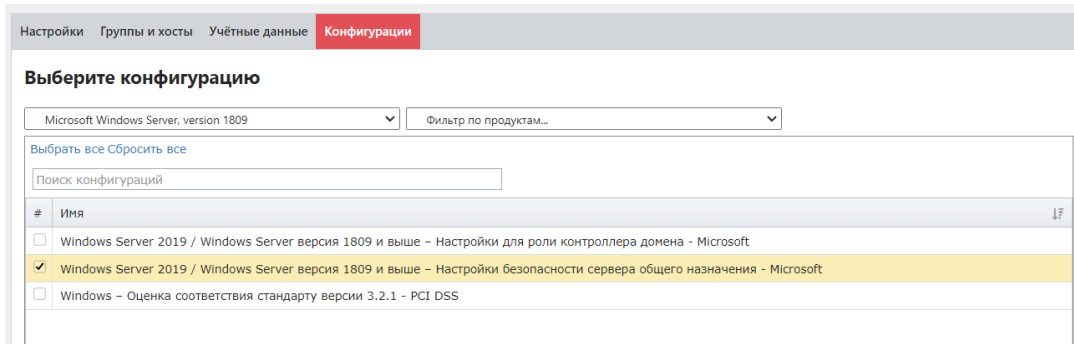


Изменим эталонное значение для правила **Проверять съемные носители**. Отметим **Переопределить эталонное значение** и изменим в списке значение с **Enabled (0)** на **Disabled (1)** → **Применить изменения**. Возле правила изменится иконка, уведомляющая, что эталонное значение правила было переопределено.

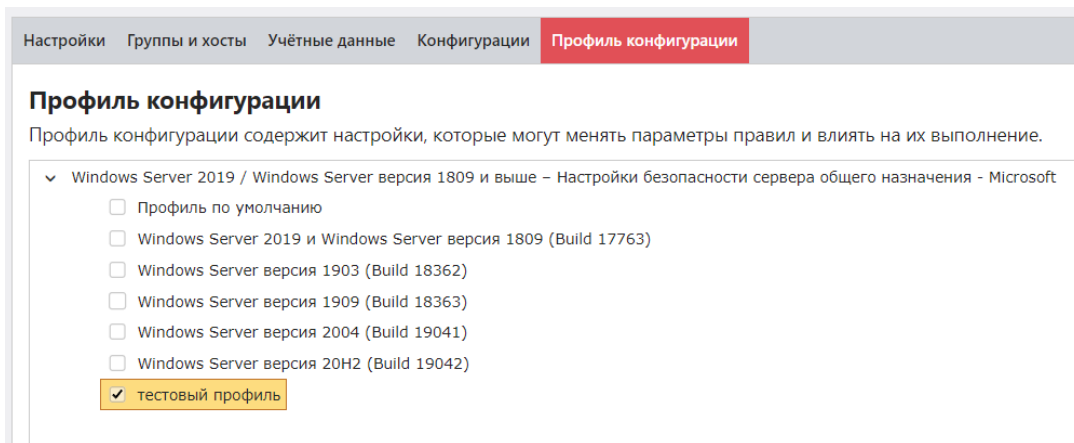


Сохраним созданный нами профиль, нажав **Сохранить профиль**.

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.**

№	Хост	Статус	Риск	К	Задание
258	10.0.0.182	Завершено	86 25 4		тестовое задание конфигурация

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

The screenshot shows the RedCheck interface with the following details:

- Top Bar:** Tabs for 'Результат', 'OVAL-Конфигурация', 'OVAL-Инвентаризация', and 'Расширенные параметры'. The 'Результат' tab is active.
- Main Content Area:**
 - Buttons: 'Развернуть', 'Критичность: Все', 'Результаты: Все'.
 - Windows Defender:**
 - * Включить наблюдение за поведением
 - Включить проверку электронной почты
 - Запретите пользователям и приложениям получать доступ к опасным веб-сайтам
 - Настроить отчеты Microsoft SpyNet
 - Настроить правила сокращения возможных направлений атак
 - Настроить правила сокращения возможных направлений атак
 - Настройка обнаружения потенциально нежелательные приложений
 - Отправка образцов
 - * Проверять съемные носители (highlighted)
 - Настройка функции "Блокировка при первом появлении"
 - Выберите уровень защиты в облаке
 - Проверять все загруженные файлы и вложения
 - Выключить защиту в реальном времени
 - Ведение журнала событий:**
 - RNR-действие аудита
 - Аудит блокировки учетных записей
 - Аудит входа в систему
 - Аудит других системных событий
 - Аудит других событий входа и выхода

The right-hand pane shows the rule configuration for 'Проверять съемные носители':

- Файл:** Benchmarks\WS2019-Member\ALTx-WS2019-Member-xccdf.xml
- Платформа:** Microsoft Windows Server 2019 (cpe:/o:microsoft:windows_server_2019), Microsoft Windows Server, version 1809 (cpe:/o:microsoft:windows_server:1809), Microsoft Windows Server, version 1903 (cpe:/o:microsoft:windows_server:1903), Microsoft Windows Server, version 1909 (cpe:/o:microsoft:windows_server:1909), Microsoft Windows Server, version 2004 (cpe:/o:microsoft:windows_server:2004), Microsoft Windows Server, version 20H2 (cpe:/o:microsoft:windows_server:20h2)
- Легенда:** Несоответствие (highlighted in red)
- Правило:** Проверять съемные носители
- Статус правила:** Включено
- Эталонное значение (из конфигурации):** 0
- Переопределенное значение (профиль):** 1

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

Выберите конфигурацию

Фильтр по платформам... Фильтр по продуктам...

Поиск конфигураций

Имя	Версия	Файл	Платформа
ALT - Общие настройки безопасности - АЛТЭК-СОФТ	6	Benchmarks\ALT\ALT-X-ALT-xccdf.xml	ALT 10.x (cpe:/o:alt:alt_10) ALT 8 SP (cpe:/o:alt:alt_8_sp) ALT 9.x (cpe:/o:alt:alt_9)
Apache HTTP Server - Аудит безопасности - АЛТЭК-СОФТ			
Apache Tomcat - Аудит безопасности - АЛТЭК-СОФТ			
Astra Linux SE 1.6 - Настройки по руководству Red Book - РусБИТех			
Astra Linux SE 1.7 - Настройки по руководству Red Book - РусБИТех			
Astra Linux SE и CE - Общие настройки безопасности - АЛТЭК-СОФТ			
Check Point Firewall - Общие настройки безопасности межсетевого экрана - АЛТЭК-СОФТ			
Cisco IOS - Оценка уровня безопасности Level-1 (минимальный) Router - CIS			
Cisco IOS - Оценка уровня безопасности Level-1 (минимальный) Switch - CIS			
Cisco IOS - Оценка уровня безопасности Level-2 (расширенный) Router - CIS			
Cisco IOS - Оценка уровня безопасности Level-2 (расширенный) Switch - CIS			
Cisco NX-OS - Общие настройки безопасности - Cisco			
Dallas Lock 8.0 - Оценка соответствия классу 1Г - РД АС			
Debian - Общие настройки безопасности - АЛТЭК-СОФТ			
Docker - Аудит безопасности платформы контейнеризации - CIS			
FortiGate - Общие настройки безопасности межсетевого экрана - CIS			
Huawei VRP - Общие настройки безопасности - АЛТЭК-СОФТ			
IBM DB2 - Общие настройки безопасности СУБД - CIS			
IIS и .NET - Аудит безопасности - АЛТЭК-СОФТ			
Kubernetes - Общие настройки безопасности главного узла - CIS			
Kubernetes - Общие настройки безопасности отдельного рабочего узла - CIS			
Microsoft Office 2013 - Настройки уровня пользователя - Microsoft			

Всего: 116

Импортировать конфигурацию...

Конфигурация

Название ALT - Общие настройки безопасности - АЛТЭК-СОФТ

Версия 6

Файл Benchmarks\ALT\ALT-X-ALT-xccdf.xml

Платформа ALT 10.x (cpe:/o:alt:alt_10)
ALT 8 SP (cpe:/o:alt:alt_8_sp)
ALT 9.x (cpe:/o:alt:alt_9)

Описание

Название ALT - Общие настройки безопасности - АЛТЭК-СОФТ

Описание Конфигурация предназначена для обеспечения безопасного функционирования ОС ALT

Примечание Не рекомендуется применять настройки данной конфигурации без предварительного тестирования и проверки в непродуктивной среде. В случае возникновения вопросов Вы можете обратиться в службу технической поддержки компании АЛТЭК-СОФТ: support@altx-soft.ru

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.

Аудиты	ALTX ID	Риск	Ссылки
Просмотр аудитов.	> 169106	Средний	EXPLOIT-DB,CVE
Класс	> 169224	Высокий	CVE
Уязвимость	> 169226	Средний	CVE
Семейство	> 169238	Средний	Oracle,CVE
Windows	> 169253	Высокий	CVE,Adobe
Название	> 169255	Высокий	CVE,Adobe
Описание	> 169256	Высокий	CVE,Adobe
Ссылки	> 169283	Средний	FS TEC,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	FS TEC,Securityfocus,CVE
	> 168545	Высокий	FS TEC,CVE,Oracle
	> 169675	Средний	CVE,Foxitsoftware
	> 169706	Средний	FS TEC,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.alth-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

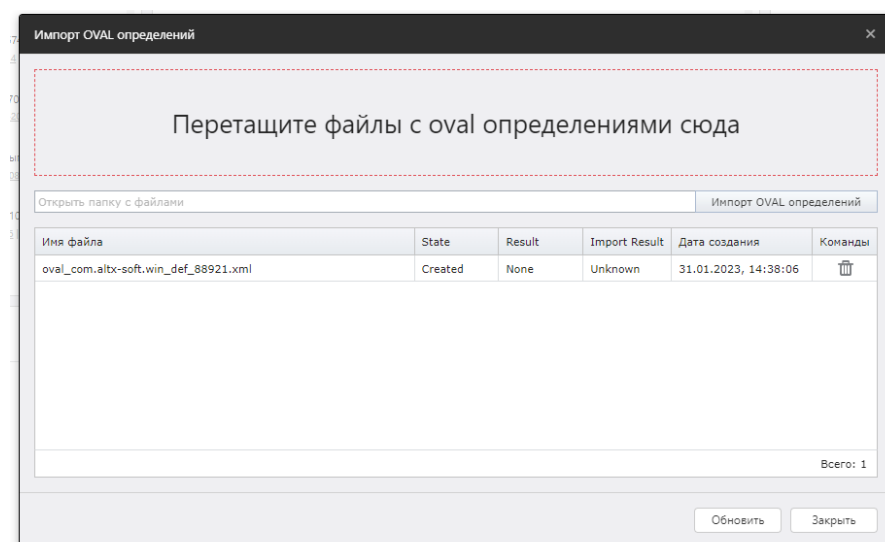
Необходимая роль: RedCheck_Admins / RedCheck_Adminis

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**.

Имя файла	State	Result	Import Result	Дата создания	Команды
oval_com.altx-soft.win_def_88921.xml	Finished	Success	Success	31.01.2023, 14:38:06	

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

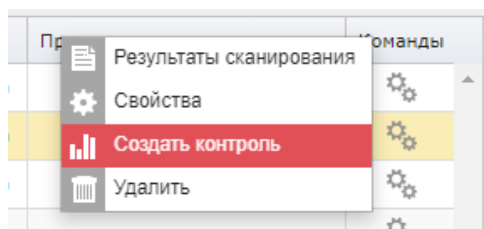
Необходимая роль: любая

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

У нас есть результат сканирования хоста заданием Аудит конфигураций.

№	Хост	Статус	Риск	К	Примечание	Команды
258	10.0.0.182	Завершено	86 25 4		Benchmarks\WS2019-Member\ALTX-WS2019-Member-xccdf.xml f40d217c-af77-4055-b8d8-32d4d6d1daac	
252	10.0.0.182	Завершено	83 24 4		Benchmarks\WS2019-Member\ALTX-WS2019-Member-xccdf.xml WS2019_WS1809	

Нажмем → **Создать контроль;**



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

252	10.0.0.182	Завершено	83 24 4		test-conf_2
-----	------------	-----------	---------	--	-------------

Исправим несоответствие некоторых правил конфигурации на хосте.

Результат | OVAL-Конфигурация | OVAL-Инвентаризация | Расширенные параметры

Развернуть | Критичность: Все | Результаты: Все

- Windows Defender
 - Включить наблюдение за поведением
 - Включить проверку электронной почты
 - Запретите пользователям и приложениям получать доступ к опасным веб-сайтам
 - Настроить отчеты Microsoft SpyNet
 - * Настроить правила сокращения возможных направлений атак
 - Настроить правила сокращения возможных направлений атак
 - Настройка обнаружения потенциально нежелательных приложений
 - Отправка образцов
 - Проверять съемные носители
 - * Настройка функции "Блокировка при первом появлении"
 - * Выберите уровень защиты в облаке
 - * Проверять все загруженные файлы и вложения
 - * Выключить защиту в реальном времени


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

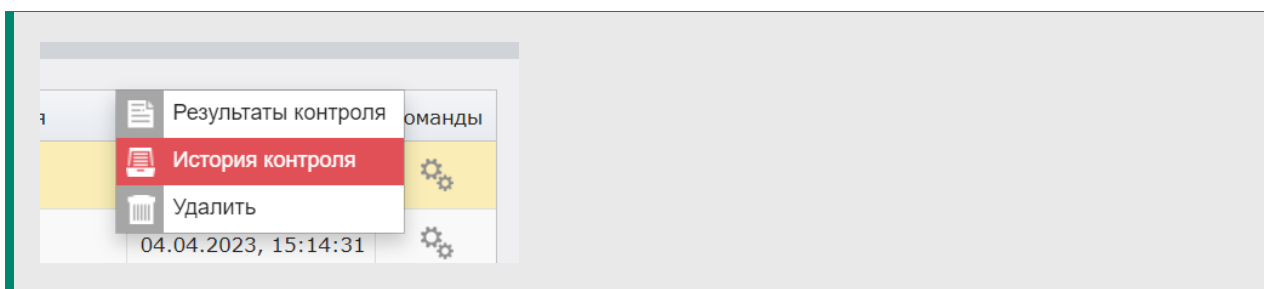
№	Хост	Статус	Риск	К	Задание
259	10.0.0.182	Завершено	79 22 4	⊗	test-conf_2

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

ИСТОРИЯ | КОНТРОЛЬ | ОТЧЁТЫ | ПОЛЬЗОВАТЕЛИ

№	Хост	Статус	Задание	№ сканирования	Команды
23	10.0.0.182	Несоответствие	test-conf_2	252	⚙️

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 > Всего: 6

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.

№	ИД	Хост	Статус	Риск	К	Задание	А	Профиль	Е	Начало	Завершение	Время	Примечание	Команда
259		10.0.0.182	Закончено	2 2 1		test-conf_2	Е	Аудит конфигураций	171	06.04.2023, 16:29:58	06.04.2023, 16:30:03	00:00:05	Benchmarks\WS2019-Member\ALT-X-WS2019-Member-vcconf.xml WS2019_WS1809	
258		10.0.0.182	Закончено	4 2 2 1		тестовое задание конфигурация	Е	Аудит конфигураций	170	06.04.2023, 12:18:29	06.04.2023, 12:18:34	00:00:04	Benchmarks\WS2019-Member\ALT-X-WS2019-Member-vcconf.xml 1468217c-a777-4055-8848-3284661d8ec	
257		10.0.0.183	Закончено			тестовое задание	Е	Аудит уязвимостей	169	06.04.2023, 10:18:37	06.04.2023, 10:19:08	00:00:30		
256		10.0.0.182	Закончено			тестовое задание	Е	Аудит уязвимостей	169	06.04.2023, 10:18:37	06.04.2023, 10:19:01	00:00:24		
255		10.0.0.182	Ошибка			test_1	Е	Аудит конфигураций	168	05.04.2023, 12:28:25	05.04.2023, 12:28:25	00:00:00	Benchmarks\ALT-X-Win8\ALT-X-Win8-vcconf.xml	
254		10.0.0.182	Ошибка			test-fix	Е	Фиксация	160	05.04.2023, 10:59:27	05.04.2023, 10:59:30	00:00:02		
253		10.0.0.183	Ошибка			test-fix	Е	Фиксация	160	05.04.2023, 10:59:27	05.04.2023, 10:59:28	00:00:01		
252		10.0.0.182	Закончено	2 2 1 1		test-conf_2	Е	Аудит конфигураций	158	05.04.2023, 10:45:52	05.04.2023, 10:45:58	00:00:05	Benchmarks\WS2019-Member\ALT-X-WS2019-Member-vcconf.xml WS2019_WS1809	
251		10.0.0.183	Закончено	3 2 2 2 1 1		test-vulns	Е	Аудит уязвимостей	154	05.04.2023, 10:20:49	05.04.2023, 10:29:17	00:08:27		
250		10.0.0.183	Закончено			test-invent	Е	Инвентаризация	155	05.04.2023, 10:24:52	05.04.2023, 10:28:24	00:03:31		
249		10.0.0.182	Закончено	3		test-upd	Е	Аудит обновлений	153	05.04.2023, 10:19:08	05.04.2023, 10:22:31	00:03:22		
248		10.0.0.182	Закончено	2 2 1 1 1		test-upd	Е	Аудит обновлений	152	05.04.2023, 10:12:56	05.04.2023, 10:16:16	00:03:19		
247		10.0.0.183	В процессе			test-upd	Е	Аудит обновлений	152	05.04.2023, 10:12:56	05.04.2023, 10:12:58	00:00:02		
246		10.0.0.182	Закончено	3 2 2 2 2 1 1		test-vulns	Е	Аудит уязвимостей	151	05.04.2023, 09:51:46	05.04.2023, 10:00:14	00:08:27		
245		10.0.0.173	Закончено	1 1		astra-postgre	Е	Аудит PostgreSQL	150	04.04.2023, 16:56:47	04.04.2023, 16:58:20	00:01:33		
244		10.0.0.182	Закончено	2 2 1 1		microsoft-conf	Е	Аудит конфигураций	149	04.04.2023, 15:14:28	04.04.2023, 15:14:30	00:00:01	Benchmarks\WS2019-Domain\ALT-X-WS2019-Domain-vcconf.xml WS2019_WS1809	
243		10.0.0.182	Закончено	4 2 2 1		microsoft-conf	Е	Аудит конфигураций	149	04.04.2023, 15:14:25	04.04.2023, 15:14:28	00:00:02	Benchmarks\WS2019-Member\ALT-X-WS2019-Member-vcconf.xml WS2019_WS1809	

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.
- Применение – 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**.

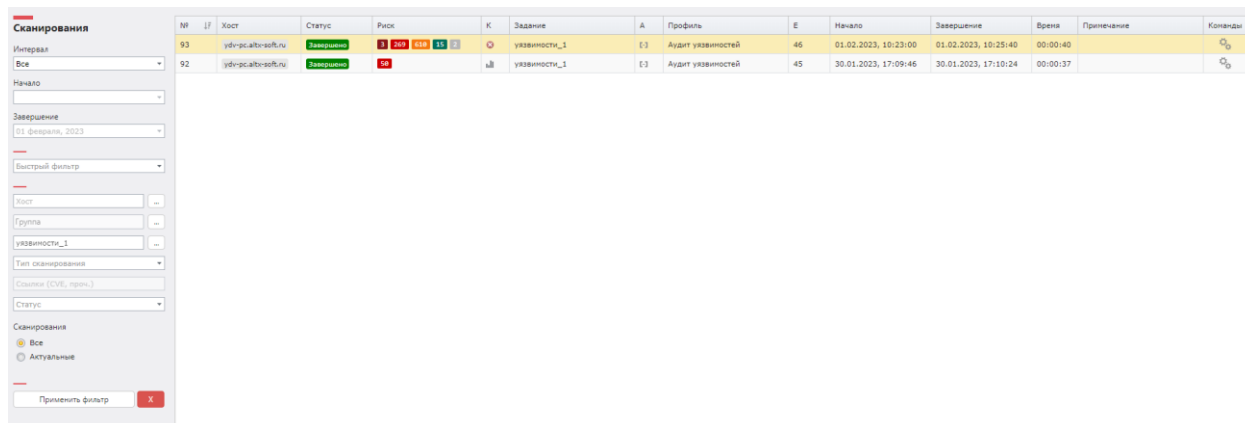
Каждый тип задания предоставляет отличную от других информацию о выполненном сканировании.

- [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**;



№	ИД	Хост	Статус	Риск	К	Задание	А	Профиль	Е	Начало	Завершение	Время	Примечание	Команды
93		ub-rcsai7cyeib.ru	Завершено	1 204 159 15		уязвимости_1	E3	Аудит уязвимостей	45	01.02.2023, 10:23:00	01.02.2023, 10:25:40	00:00:40		
92		ub-rcsai7cyeib.ru	Завершено	1 204 159 15		уязвимости_1	E3	Аудит уязвимостей	45	30.01.2023, 17:09:46	30.01.2023, 17:10:24	00:00:37		

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

Аудит в режиме "Пентест"

№ сканирования
144

Хост
10.0.0.150

Задача
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 отчет](#)

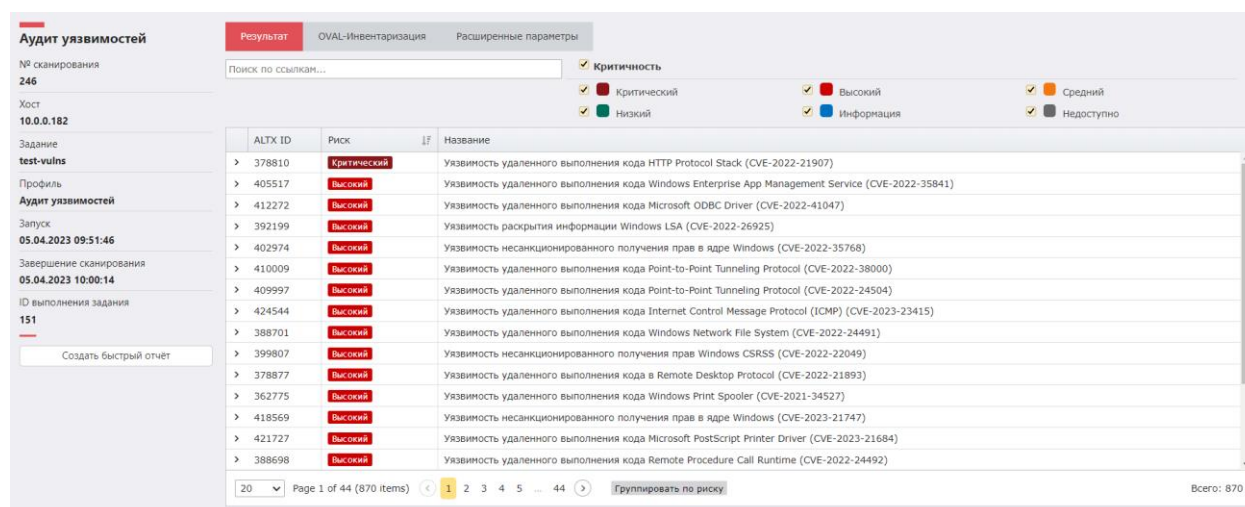
Поиск уязвимостей		Инвентаризация	Информация о хосте	Расширенные параметры	
CVE	Порт	Риск	Точность	Описание	
> ALTXID-416982	8080	Высокий	Высокая	Веб сервер подвержен семейству атак Anti DNS pinning (DNS rebinding), т.к. отвечает на HTTP-запросы с произвольным значением заголовка Host.	
> CVE-2010-0097	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 вызывать 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 удаленно, вызвать отказ в обслуживании (вызовение имя-сервиса "service failure", зашифрование ответа, denial-of-service, отказ в обслуживании).	

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.



Аудит уязвимостей

№ сканирования: 246

Хост: 10.0.0.182

Задание: test-vulns

Профиль: Аудит уязвимостей

Запуск: 05.04.2023 09:51:46

Завершение сканирования: 05.04.2023 10:00:14

ID выполнения задания: 151

Создать быстрый отчет

Результат OVAL-Инвентаризация Расширенные параметры

Поиск по ссылке...

Критичность

Критический Высокий Средний

Низкий Информация Недоступно

ALTIX ID	Риск	Название
> 378810	Критический	Уязвимость удаленного выполнения кода HTTP Protocol Stack (CVE-2022-21907)
> 405517	Высокий	Уязвимость удаленного выполнения кода Windows Enterprise App Management Service (CVE-2022-35841)
> 412272	Высокий	Уязвимость удаленного выполнения кода Microsoft ODBC Driver (CVE-2022-41047)
> 392199	Высокий	Уязвимость раскрытия информации Windows LSA (CVE-2022-26925)
> 402974	Высокий	Уязвимость несанкционированного получения прав в ядре Windows (CVE-2022-35768)
> 410009	Высокий	Уязвимость удаленного выполнения кода Point-to-Point Tunneling Protocol (CVE-2022-38000)
> 409997	Высокий	Уязвимость удаленного выполнения кода Point-to-Point Tunneling Protocol (CVE-2022-24504)
> 424544	Высокий	Уязвимость удаленного выполнения кода Internet Control Message Protocol (ICMP) (CVE-2023-23415)
> 388701	Высокий	Уязвимость удаленного выполнения кода Windows Network File System (CVE-2022-24491)
> 399807	Высокий	Уязвимость несанкционированного получения прав Windows CSRSS (CVE-2022-22049)
> 378877	Высокий	Уязвимость удаленного выполнения кода в Remote Desktop Protocol (CVE-2022-21893)
> 362775	Высокий	Уязвимость удаленного выполнения кода Windows Print Spooler (CVE-2021-34527)
> 418569	Высокий	Уязвимость несанкционированного получения прав в ядре Windows (CVE-2023-21747)
> 421727	Высокий	Уязвимость удаленного выполнения кода Microsoft PostScript Printer Driver (CVE-2023-21684)
> 388698	Высокий	Уязвимость удаленного выполнения кода Remote Procedure Call Runtime (CVE-2022-24492)

Page 1 of 44 (870 items) 1 2 3 4 5 ... 44 Группировать по риску Всего: 870

OVAL-определение состоит из:

- ALTIX 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;

▼ 378810 **Критический** Уязвимость удаленного выполнения кода HTTP Protocol Stack (CVE-2022-21907)

ALTX ID 378810
Риск **Критический**
OVAL oval:ru.altx-soft.win:def:81162 (Версия 7)
Название Уязвимость удаленного выполнения кода HTTP Protocol Stack (CVE-2022-21907)
Описание Уязвимость удаленного выполнения кода HTTP Protocol Stack.
Ссылки

NKCKI	VULN-20220112.22	■■■■■■■■■■ (AV:N/AC:L/Au:N/C:C/I:C/A:C) (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) NVD-CWE-noinfo
FSTEC	BDU:2022-00163	
Microsoft	CVE-2022-21907	
CVE	CVE-2022-21907	■■■■■■■■■■ (AV:N/AC:L/Au:N/C:C/I:C/A:C) (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) NVD-CWE-noinfo

Детализация C:\Windows\System32\drivers\http.sys (10.0.17763.1935) |
 Показать собранные OVAL-элементы

OVAL-Инвентаризация

Вкладка отображает список с OVAL-определениями класса Информация.

Информация – OVAL-определение для инвентаря (ПО).

ALTX ID	Риск	Название	Ссылки
> 346924	Информация	Microsoft Windows Server is installed	cpe:/o:microsoft:windows_server
> 260707	Информация	Microsoft Windows Server 2019 is installed	cpe:/o:microsoft:windows_server_2019
> 175014	Информация	Microsoft .NET Core Runtime is installed	cpe:/a:microsoft:.net_core_runtime
> 281967	Информация	Google Chrome is installed (admin install for all users)	cpe:/a:google:chrome:admin_install_for_all_users
> 84876	Информация	Microsoft Edge is installed	cpe:/a:microsoft:edge
> 346844	Информация	Microsoft Internet Explorer 11 is installed	cpe:/a:microsoft:ie:11
> 346468	Информация	Microsoft XML Core Services 6 is installed	cpe:/a:microsoft:xml_core_services:6
> 346817	Информация	PostgreSQL is installed	cpe:/a:postgresql:postgresql
> 346848	Информация	Google Chrome is installed	cpe:/a:google:chrome
> 346792	Информация	Microsoft Windows is installed	cpe:/o:microsoft:windows
> 346548	Информация	Microsoft Windows Defender is installed	cpe:/a:microsoft:windows_defender
> 282726	Информация	Microsoft .NET Framework 4.8 is installed	cpe:/a:microsoft:.net_framework:4.8
> 175058	Информация	Microsoft ASP.NET Core is installed	cpe:/a:microsoft:asp.net_core
> 346471	Информация	Microsoft XML Core Services 3 is installed	cpe:/a:microsoft:xml_core_services:3
> 248902	Информация	Microsoft .NET Core is installed	cpe:/a:microsoft:.net_core
> 317982	Информация	Microsoft SQL Server 2019 is installed	cpe:/a:microsoft:sql_server:2019
> 307056	Информация	Microsoft SQL Server Management Studio is installed	cpe:/a:microsoft:sql_server_management_studio

Page 1 of 2 (24 items) 1 2

Всего: 24

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.

346924	Информация	Microsoft Windows Server is installed
ALTX ID	346924	
Риск	Информация	
OVAL	oval:ru.altx-soft.win:def:74377 (Версия 27)	
Название	Microsoft Windows Server is installed	
Описание	The operating system installed on the system is Microsoft Windows Server.	
Ссылки	CPE	cpe:/o:microsoft:windows_server

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.

The screenshot shows the 'Аудит обновлений' (Update Audit) interface. The main content is a table with the following columns: ALTX ID, Риск (Risk), and Название (Name). The table lists 15 updates, all with a 'Критический' (Critical) risk level. The updates are for various Windows Server and Windows 10 versions, including cumulative updates and .NET Framework updates. The interface also includes a search bar, a filter for 'Критичность' (Criticality) with options for 'Критический', 'Высокий', 'Средний', 'Низкий', and 'Информация', and a 'Создать быстрый отчет' (Create quick report) button.

ALTX ID	Риск	Название
399850	Критический	Накопительный пакет для Windows Server 2019 и Windows 10 версии 1809 для систем на базе 64-разрядных (x64) процессоров (KB5015811)
371775	Критический	Накопительный пакет для Windows Server 2019 и Windows 10 версии 1809 для систем на базе 64-разрядных (x64) процессоров (KB5007206)
410079	Критический	Накопительный пакет для Windows Server 2019 и Windows 10 версии 1809 для систем на базе 64-разрядных (x64) процессоров (KB5018419)
403077	Критический	Накопительный пакет для Windows 10 версии 1809 и Windows Server 2019 для систем на базе 64-разрядных (x64) процессоров (KB5016623)
392314	Критический	Накопительный пакет для Windows 10 версии 1809 и Windows Server 2019 для систем на базе 64-разрядных (x64) процессоров (KB5013941)
330431	Критический	2020-07 Накопительный пакет для .NET Framework 3.5 и 4.8 для Windows Server 2019, Windows 10 для систем на базе 64-разрядных (x64) процессоров (KB4565632)
379015	Критический	Накопительный пакет для Windows Server 2019 и Windows 10 версии 1809 для систем на базе 64-разрядных (x64) процессоров (KB5009557)
405549	Критический	Накопительный пакет для Windows Server 2019 и Windows 10 версии 1809 для систем на базе 64-разрядных (x64) процессоров (KB5017315)
388930	Критический	Накопительный пакет для Windows Server 2019 и Windows 10 версии 1809 для систем на базе 64-разрядных (x64) процессоров (KB5012647)
368079	Критический	2021-09 Накопительный пакет для Windows Server 2019 и Windows 10 версии 1809 для 64-битных ОС (KB5005568)
397966	Критический	Накопительный пакет для Windows Server 2019 и Windows 10 версии 1809 для систем на базе 64-разрядных (x64) процессоров (KB5014692)
375587	Критический	Накопительный пакет для Windows Server 2019 и Windows 10 версии 1809 для систем на базе 64-разрядных (x64) процессоров (KB5008218)
334559	Критический	Накопительный пакет для .NET Framework 3.5 и 4.8 для Windows Server 2019, Windows 10 для систем на базе 64-разрядных (x64) процессоров (KB4569750)
367283	Критический	2021-08 Обновление служебного стека для Windows 10 версии 1809 и Windows Server 2019 для систем на базе 64-разрядных (x64) процессоров (KB5005112)
362791	Критический	Накопительный пакет для Windows 10 версии 1809 и Windows Server 2019 для систем на базе 64-разрядных (x64) процессоров (KB5004947)

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;

330431 **Критический** 2020-07 Накопительный пакет для .NET Framework 3.5 и 4.8 для Windows Server 2019, Windows 10 для систем на базе 64-разрядных (x64) процессоров (KB4565632)

ALTX ID 330431
Риск **Критический**
OVAL oval:ru.altx-soft.win:def:70334 (Версия 1)
Название 2020-07 Накопительный пакет для .NET Framework 3.5 и 4.8 для Windows Server 2019, Windows 10 для систем на базе 64-разрядных (x64) процессоров (KB4565632)
Описание В программном продукте Microsoft обнаружена проблема безопасности, которая может повлиять на вашу систему.
Ссылки
 VENDOR windows10.0-kb4565632-x64-ndp48_dbab0773d0b336c20b095d9144120d487992066c.msu
 MSWSUSID acead73c-d39e-44a9-9adc-fb033898ee1b
 MSWSUSID 45df7d20-5fd9-4aa0-8c1f-4010e30f3662
 Microsoft CVE-2020-1147
 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
 NVD-CWE-Other
 Microsoft KB4565632
Продукты Microsoft .NET Framework 3.5
 Microsoft .NET Framework 4.8
Детализация
 Показать собранные OVAL-элементы

OVAL-Инвентаризация

Вкладка отображает список с OVAL-определениями класса Информация.

Информация – OVAL-определение для инвентаря (ПО).

ALTX ID	Риск	Название	Ссылки
> 346924	Информация	Microsoft Windows Server is installed	cpe:/o:microsoft:windows_server
> 260707	Информация	Microsoft Windows Server 2019 is installed	cpe:/o:microsoft:windows_server_2019
> 175014	Информация	Microsoft .NET Core Runtime is installed	cpe:/a:microsoft:.net_core_runtime
> 281967	Информация	Google Chrome is installed (admin install for all users)	cpe:/a:google:chrome:admin_install_for_all_users
> 84876	Информация	Microsoft Edge is installed	cpe:/a:microsoft:edge
> 346844	Информация	Microsoft Internet Explorer 11 is installed	cpe:/a:microsoft:ie:11
> 346468	Информация	Microsoft XML Core Services 6 is installed	cpe:/a:microsoft:xml_core_services:6
> 346817	Информация	PostgreSQL is installed	cpe:/a:postgresql:postgresql
> 346848	Информация	Google Chrome is installed	cpe:/a:google:chrome
> 346792	Информация	Microsoft Windows is installed	cpe:/o:microsoft:windows
> 346548	Информация	Microsoft Windows Defender is installed	cpe:/a:microsoft:windows_defender
> 282726	Информация	Microsoft .NET Framework 4.8 is installed	cpe:/a:microsoft:.net_framework:4.8
> 175058	Информация	Microsoft ASP.NET Core is installed	cpe:/a:microsoft:asp_net_core
> 346471	Информация	Microsoft XML Core Services 3 is installed	cpe:/a:microsoft:xml_core_services:3
> 248902	Информация	Microsoft .NET Core is installed	cpe:/a:microsoft:.net_core
> 317982	Информация	Microsoft SQL Server 2019 is installed	cpe:/a:microsoft:sql_server:2019
> 307056	Информация	Microsoft SQL Server Management Studio is installed	cpe:/a:microsoft:sql_server_management_studio

Page 1 of 2 (24 items) 1 2

Всего: 24

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.

346924	Информация	Microsoft Windows Server is installed
ALTX ID	346924	
Риск	Информация	
OVAL	oval:ru.altx-soft.win:def:74377 (Версия 27)	
Название	Microsoft Windows Server is installed	
Описание	The operating system installed on the system is Microsoft Windows Server.	
Ссылки	CPE cpe:/o:microsoft:windows_server	

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.

Конфигурация ▾		
Название	Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения - Microsoft	
Версия	7	
Файл	Benchmarks\WS2019-Member\ALTX-WS2019-Member-xccdf.xml	
Платформа	<ul style="list-style-type: none"> ■ Microsoft Windows Server 2019 (cpe:/o:microsoft:windows_server_2019) ■ Microsoft Windows Server, version 1809 (cpe:/o:microsoft:windows_server:1809) ■ Microsoft Windows Server, version 1903 (cpe:/o:microsoft:windows_server:1903) ■ Microsoft Windows Server, version 1909 (cpe:/o:microsoft:windows_server:1909) ■ Microsoft Windows Server, version 2004 (cpe:/o:microsoft:windows_server:2004) ■ Microsoft Windows Server, version 20H2 (cpe:/o:microsoft:windows_server:20h2) 	
Легенда ▾		
Несоответствие		
0 Соответствие	11 Несоответствие	0 Ошибка
0 Не проверено	2 Не выбрано	0 Неизвестно
0 Информация	0 Исправлено	0 Неприменимо
Критичность ▾		
10 Высокий	0 Информация	0 Низкий
3 Средний	0 Недоступно	
Дополнительно ▾		
ID	Windows_Defender	

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.

Легенда ▼	
Несоответствие	
Правило ▼	
Включить проверку электронной почты	
Статус правила	Включено
Эталонное значение (из конфигурации)	0
Критичность ▼	
Средний	
Ссылки ▼	
Тип	GPO
Источник	Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Защитник Windows (Endpoint Protection)\Проверка
Описание ▼	
<i>Эталонное значение:</i> Включено	
<p>Этот параметр политики позволяет настроить проверку электронной почты. Когда проверка электронной почты включена, модуль защиты анализирует почтовый ящик и файлы почты (тексты сообщений и вложения) в соответствии с их форматом. На данный момент поддерживаются несколько форматов электронной почты, например pst (Outlook), dbx, mbx, mime (Outlook Express), binhex (Mac).</p> <p>Если вы включаете этот параметр политики, проверка электронной почты включена.</p> <p>Если вы отключаете или не настраиваете этот параметр политики, проверка электронной почты отключена.</p>	
Дополнительно ▼	
ID	<i>Turn_on_e-mail_scanning</i>
OVAL ID	<i>oval:ru.altx-soft.win:def:28384</i>
OVAL URL	<i>ALTX-WS2019-Member-oval.xml</i>

OVAL-Конфигурация

Вкладка содержит детализацию проверок правил конфигурации.

Результат	OVAL-Конфигурация	OVAL-Инвентаризация	Расширенные параметры
Поиск по ссылкам...			
ALTX ID	Название		
> 295427	PNP-действие аудита		
> 65433	Автоматически выполнить вход последнего текущего пользователя после иницизированной системой перезагрузки		
> 46721	Аудит входа в систему		
> 46782	Блокировка страниц в памяти - Никто		
> 295443	Включение защиты от перезаписи обработчика структурных исключений (SEHOP)		
> 46842	Выполнение задач по обслуживанию томов - Администраторы		
> 46856	Доступ к диспетчеру учетных данных от имени доверенного вызывающего - Никто		
> 46860	Доступ к сети: разрешить трансляцию анонимного SID в имя		
> 46868	Загрузка и выгрузка драйверов устройств - Администраторы		
> 46884	Изменение параметров среды изготовителя - Администраторы		
> 46909	Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам		
> 46917	Контроль учетных записей: Все администраторы работают в режиме одобрения администратором		
> 46918	Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав		
> 46922	Контроль учетных записей: повышать права для UIAccess-приложений только при установке в безопасных местах		
> 46924	Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в место размещения пользователя		
> 46933	Максимальный срок действия пароля		
> 295429	Отключение протокола Windows SMB 1.0		
> 295428	Отключение протокола Windows SMB 1.0		
> 46981	Отладка программ - Администраторы		
> 46987	Пароль должен отвечать требованиям сложности		

OVAL-определение состоит из:

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

▼ 295427	PNP-действие аудита
ALTX ID	295427
OVAL	oval:ru:altx-soft.win:def:29893 (Версия 1)
Название	PNP-действие аудита
Описание	Этот параметр политики позволяет выполнять аудит, когда самонастраивающееся устройство обнаруживает внешнее устройство.
Детализация	
	Показать собранные OVAL-элементы

OVAL-Инвентаризация

Вкладка отображает список с OVAL-определениями класса Информация.

Информация – OVAL-определение для инвентаря (ПО).

Результат	OVAL-Конфигурация	OVAL-Инвентаризация	Расширенные параметры
Поиск по ссылкам...			
ALTX ID	Риск	Имя	Ссылки
> 346999	Информация	Microsoft Windows 10 is installed	cpe:/o:micro
> 268558	Информация	Microsoft Windows 10 Version 1809 is installed	cpe:/o:micro
▼ 295663	Информация	Microsoft Windows Desktop is installed	cpe:/o:micro
ALTX ID	295663		
Риск	Информация		
OVAL	oval:ru.altx-soft.win:def:37930 (Версия 3)		
Название	Microsoft Windows Desktop is installed		
Описание	The operating system installed on the system is Microsoft Windows Desktop.		
Ссылки	CPE	cpe:/o:microsoft:windows_desktop	
> 84876	Информация	Microsoft Edge is installed	cpe:/a:micro
> 346844	Информация	Microsoft Internet Explorer 11 is installed	cpe:/a:micro

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.

▼ 346924	Информация	Microsoft Windows Server is installed
ALTX ID	346924	
Риск	Информация	
OVAL	oval:ru.altx-soft.win:def:74377 (Версия 27)	
Название	Microsoft Windows Server is installed	
Описание	The operating system installed on the system is Microsoft Windows Server.	
Ссылки	CPE	cpe:/o:microsoft:windows_server

Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

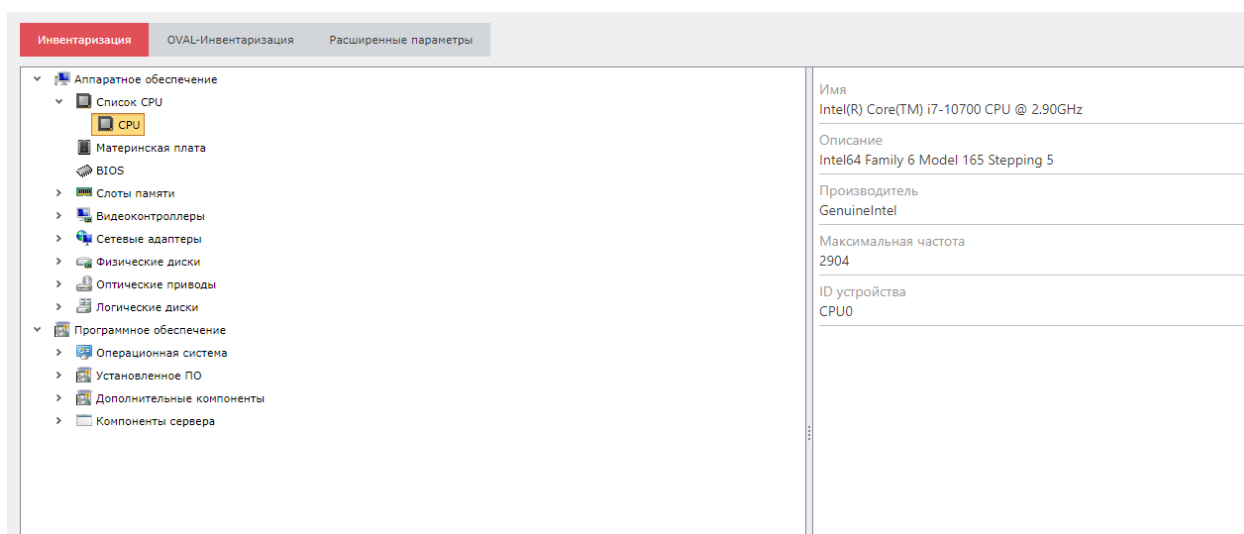
Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

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).

Инвентаризация		OVAL-Инвентаризация		Расширенные параметры	
Поиск по ссылкам...					
ALTX ID	Риск	Название	Ссылки		
> 69564	Информация	Microsoft Windows (x64) is installed	cpe:/o:microsoft:windows:x64		
> 43320	Информация	RedCheck Agent is installed on Windows	cpe:/a:altex-soft:redcheckagent		
> 347098	Информация	Microsoft IIS is installed	cpe:/a:microsoft:iis		
> 369333	Информация	Microsoft Office 2021 is installed	cpe:/a:microsoft:office:2021		
> 72689	Информация	Microsoft .NET Framework is installed	cpe:/a:microsoft:.net_framework		
> 72690	Информация	Microsoft .NET Framework 2.0 or later is installed	cpe:/a:microsoft:.net_framework:2.0_or_later		
> 72691	Информация	Microsoft .NET Framework 4.0 or later is installed	cpe:/a:microsoft:.net_framework:4.0_or_later		
> 84206	Информация	Software Restriction Policies (SRP) is supported	cpe:/a:microsoft:software_restriction_policies		
> 295663	Информация	Microsoft Windows Desktop is installed	cpe:/o:microsoft:windows_desktop		
> 68463	Информация	DHCP Client service is installed	cpe:/a:microsoft:dhcp_client		
> 76099	Информация	Microsoft Message Queuing is installed	cpe:/a:microsoft:message_queueing		
> 314166	Информация	Microsoft Edge (Chromium-based) is installed	cpe:/a:microsoft:edge:chromium-based		
> 139186	Информация	Git is installed	cpe:/a:git_project:git		
> 154810	Информация	Yandex Browser is installed	cpe:/a:yandex:browser		
> 155089	Информация	Docker is installed	cpe:/a:docker:docker		
> 155269	Информация	NVIDIA GeForce Experience is installed	cpe:/a:nvidia:geforce_experience		
> 155270	Информация	NVIDIA Graphics Driver is installed	cpe:/a:nvidia:graphics_driver		

Page 1 of 4 (67 items) 1 2 3 4 Всего: 67

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.

346924	Информация	Microsoft Windows Server is installed
ALTX ID	346924	
Риск	Информация	
OVAL	oval:ru.altx-soft.win:def:74377 (Версия 27)	
Название	Microsoft Windows Server is installed	
Описание	The operating system installed on the system is Microsoft Windows Server.	
Ссылки	CPE	cpe:/o:microsoft:windows_server

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.

Файловая система		Реестр
Путь к файлу	Контрольная сумма	
> D:\Temp\some\packedges.txt	9131096C	
> D:\Temp\some\server.py	FB00170B	

Каждая запись содержит следующую информацию о файле:

- Путь к файлу;
- Контрольная сумма.

Путь к файлу	Контрольная сумма
▼ D:\Temp\some\packedges.txt	9131096C

Путь к файлу D:\Temp\some\packedges.txt
Контрольная сумма 9131096CB5910A88240477BAF0EA3899

Реестр

Вкладка отображает зафиксированные ключи и параметры реестра.

Файловая система		Реестр
Ключ	Параметр	Значение
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ASP.NET Core\Shared Framework	InstallDir	C:\Program Files\dotnet\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX		1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	MinFeatureLevel	49408
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	MaxFeatureLevel	49408
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	D3D12MinFeatureLevel	49408
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	D3D12MaxFeatureLevel	49408
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	MaxDedicatedVideoMemory	134217728
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	LastSeen	133198781070805030
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	InstalledVersion	00-00-00-09-00-00-00-00
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	Version	4.09.00.0904
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	LastUpdaterStartTimestamp	UTC.2022-09-21.13:39:04
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	LastUpdaterStartHresult	0

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.

ALTX ID	Риск	ИЗ	Название
> 308542	Высокий		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2016-8565)
> 308543	Высокий		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2018-11455)
> 308536	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2011-4530)
> 308537	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2011-4531)
> 308538	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2011-4532)
> 308540	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2016-8563)
> 308541	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2016-8564)
> 308544	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2018-11456)
> 281419	Средний		Уязвимость средств разработки Siemens Simatic STEP7 и пакета программ Simatic PCS7 (CVE-2012-3015)
> 281496	Средний		Уязвимость программного обеспечения Siemens SIMATIC STEP 7 (CVE-2015-1594)
> 308539	Низкий		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2012-4691)

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.

281418	Высокий	Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2011-4529)
ALT X ID	281418	
Риск	Высокий	
OVAL	oval:ru.altx-soft.scada:def:1 (Версия 5)	
Название	Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2011-4529)	
Описание	Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) связана с некорректной проверкой входных данных при Siemens ALM до версии 5.1 sp1 upd1 включительно	
Исправление	Обновление ПО Siemens ALM до версии 5.1 sp1 upd2.	
Ссылки	CVE CVE-2011-4529 (AV:N/AC:L/Au:N/C:P/I:P/A:P) CWE-119	
Продукты	Siemens ALM	
Показать собранные OVAL-элементы		

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.

Результат						
Инвентаризация						
Расширенные параметры						
Порт	Протокол	Риск	SCADA CPE	Модуль	Дополнительно	
4410	tcp	Высокий	cpe:2.3:a:siemens:automation_license_manager:5.1:::...	Simatic ALM		
Риск Высокий Продукты cpe:2.3:a:siemens:automation_license_manager:5.1:::... Порт 4410 (tcp) Модуль Simatic ALM						
4410	tcp	Информация	cpe:2.3:a:siemens:simatic_step_7:5.5:::...	Simatic ALM		

Page 1 of 1 (2 items) 1 Всего: 2

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

Simatic ALM ▼ Инфо 4410 тср - сервис Simatic Automation License Management, версия 5.1. Установленное ПО (лицензии): STEP 7, версия 5.5 STEP 7 Professional Edition 2010, версия 5.5 ПО Siemens ALM 5.1 Simatic STEP 7 5.5
Simatic S7 ▼
Sicam PAS IPC ▼
Citect SCADA ▼
Modbus TCP/UDP ▼
Profinet IO ▼
ArchestrA Logger ▼
BACnet/IP ▼
Ethernet/IP ▼
GenBroker (GENESIS32/64) ▼
Schneider Electric IGSS ▼
FINS ▼
ProConOS ▼

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.

The screenshot shows the OVAL configuration tool interface. At the top, there are tabs for 'Результат', 'OVAL-Конфигурация', 'OVAL-Инвентаризация', and 'Расширенные параметры'. Below the tabs, there are filters for 'Развернуть', 'Критичность: Все', and 'Результаты: Все'. The main area is divided into two panes. The left pane shows a tree view of rules grouped into categories: 'Настройки подключения', 'Привилегии', 'Шаблоны баз данных', and 'Настройки безопасности'. Each rule is accompanied by a small colored icon (green for compliance, red for non-compliance, blue for inapplicable, and grey for not checked). The right pane shows the configuration details for a selected rule, including its name, version, file path, product, and a detailed description.

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.

Конфигурация ▼		
Название	PostgreSQL - Общие настройки безопасности СУБД - CIS	
Версия	19	
Файл	Benchmarks\PostgreSQL\ALTX-PostgreSQL-xccdf.xml	
Продукт	 PostgreSQL (cpe:/a:postgresql:postgresql:-)	
Легенда ▼		
 Несоответствие		
 Соответствие	 Несоответствие	 Ошибка
 Не проверено	 Не выбрано	 Неизвестно
 Информация	 Исправлено	 Неприменимо
Критичность ▼		
 Высокий	 Информация	 Низкий
 Средний	 Недоступно	
Дополнительно ▼		
ID	<i>connection_settings</i>	

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.

Конфигурация ▾	
Название	PostgreSQL - Общие настройки безопасности СУБД - CIS
Версия	19
Файл	Benchmarks\PostgreSQL\ALTX-PostgreSQL-xccdf.xml
Продукт	 PostgreSQL (cpe:/a:postgresql:postgresql:-)
Легенда ▾	
Соответствие	
Критичность ▾	
Высокий	
Описание ▾	
Рекомендуемое действие: Значение не равно '*'	
<p>Параметр <code>listen_addresses</code> задаёт адреса TCP/IP, по которым сервер будет принимать подключения клиентских приложений. Это значение принимает форму списка, разделённого запятыми, из имён и/или числовых IP-адресов компьютеров. Особый элемент, <code>*</code>, обозначает все имеющиеся IP-интерфейсы. Запись <code>0.0.0.0</code> позволяет задействовать все адреса IPv4, а <code>::</code> — все адреса IPv6. Если список пуст, сервер не будет привязываться ни к какому IP-интерфейсу, а значит, подключиться к нему можно будет только через доменные сокеты Unix. По умолчанию этот параметр содержит <code>localhost</code>, что допускает подключение к серверу по TCP/IP только через локальный интерфейс «замыкания». Параметр <code>listen_address</code> не должен равняться <code>*</code>, так как это сделает СУБД PostgreSQL доступной для всех IP адресов.</p>	
Дополнительно ▾	
ID	<code>listen_addresses</code>
OVAL ID	<code>oval:ru.altx-soft.ind:def:201</code>
OVAL URL	<code>ALTX-PostgreSQL-Server-oval.xml</code>

ОVAL-Конфигурация

Вкладка содержит детализацию проверок правил конфигурации.

Результат	OVAL-Конфигурация	OVAL-Инвентаризация	Расширенные параметры
Поиск по ссылкам...			
ALTIX ID	Название		
> 159580	Строгое управление привилегией CREATEROLE		
> 159579	Строгое управление привилегией CREATEDB		
> 159605	Роли с привилегиями WITH GRANT OPTION должны строго контролироваться		
> 159607	Параметр wal_level как минимум archive		
> 159574	Параметр unix_socket_group настроен		
> 159578	Параметр superuser_reserved_connections настроен		
> 159610	Параметр password_encryption		
> 159577	Параметр max_connections настроен		
> 159593	Параметр log_truncate_on_rotation настроен		
> 159596	Параметр log_statement как минимум DDL		
> 159590	Параметр log_rotation_size настроен		
> 159600	Параметр log_rotation_age настроен		
> 159599	Параметр log_min_messages как минимум WARNING		
> 159598	Параметр log_min_error_statement как минимум ERROR		
> 159602	Параметр log_hostname = off		
> 159591	Параметр log_file_mode = 600		
> 159601	Параметр log_error_verbosity как минимум DEFAULT		
> 159573	Параметр listen_addresses не содержит *		
> 159597	Параметр client_min_messages как минимум NOTICE		
> 159576	Параметр bonjour = off		

OVAL-определение состоит из:

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

▼ 159580	Строгое управление привилегией CREATEROLE
ALTIX ID	159580
OVAL	oval:ru.altix-soft.ind:def:206 (Версия 2)
Название	Строгое управление привилегией CREATEROLE
Описание	Привилегия CREATEROLE должна быть только у суперпользователей. Роль с привилегией CRE/
Продукты	PostgreSQL PostgreSQL
Детализация	
	Показать собранные OVAL-элементы

OVAL-Инвентаризация

Вкладка отображает список с OVAL-определениями класса Информация.

Информация – OVAL-определение для инвентаря (ПО).

Результат		ОVAL-Конфигурация	ОVAL-Инвентаризация	Расширенные параметры
Поиск по ссылкам...				
ALTX ID	Риск	IF	Название	Ссылки
> 159570	Информация		PostgreSQL is installed	cpe:/a:postgresql:postgresql:-
> 159571	Информация		PostgreSQL is installed on Linux	cpe:/a:postgresql:postgresql_on_linux

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.

159570	Информация	PostgreSQL is installed
ALTX ID	159570	
Риск	Информация	
OVAL	oval:ru.altx-soft.ind:def:199 (Версия 2)	
Название	PostgreSQL is installed	
Описание	PostgreSQL is installed.	
Ссылки	CPE cpe:/a:postgresql:postgresql:-	
Продукты	PostgreSQL PostgreSQL	

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.

Результат				
Транспорт	Доступность	Учётная запись	Сообщение	Версия агента
Wmi	Доступен	windows		
Тип пинга WMI				
Учётная запись windows (Windows)				

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

Page 1 of 3 (44 items) 1 2 3 20 Всего: 44

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.

Аудит в режиме "Пентест"		Поиск уязвимостей	Инвентаризация	Информация о хосте	Расширенные параметры		
№ сканирования	Хост	CVE	Порт	IF	Риск	Точность	Описание
149	10.0.0.150	> ALTIXID-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.
		> ALTIXID-404180	8080		Высокий	Средняя	Обнаружена DDoS уязвимость (Slowloris) веб-серверов, атака осуществляется на основании большого количества открытых соединений путем непрерывной отправки незавершенных HTTP-запросов
		> 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 добавлять 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 запросом 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- R7-P4 позволяет удаленным злоумышленникам вызвать отказ в обслуживании (с именем daemon Name) 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 вызвать 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 удаленно, вызвать отказ в обслуживании (появление окна с ошибкой "Assertion failure", завершение работы демона) при помощи специально сформированного пакета в rndc-

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.

▼	ALTIXID-416982	8080	Высокий	Высокая	Веб сервер подвержен семейству атак Anti DNS pinning (DNS rebinding), т.к. значением заголовка Host.
Описание	Веб сервер подвержен семейству атак Anti DNS pinning (DNS rebinding), т.к. отвечает на HTTP-запросы с произвольным значением заголовка Host.				
Риск	Высокий				
CVE	ALTIXID-416982				
Продукты	cpe:/a::zyxel_zywall_usg210_http_config:				
Порт	8080 (tcp)				
Точность	Высокая				
Детализация	domain rebinding iatptfyn.com (http-dns-rebinding)				

Инвентаризация

Вкладка отображает список служб, которые работают на открытых портах.

Поиск уязвимостей							
Инвентаризация							
Информация о хосте							
Расширенные параметры							
	Порт	↓	Протокол	Риск	Продукт	Служба	Дополн
>	21		tcp	Высокий		ftp	
>	53		tcp	Высокий	cpe:/a:isc:bind:9.6-ESV-R11	domain	
>	8080		tcp	Высокий	cpe:/a::zyxel_zywall_usg210_http_config:	http	

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;

▼	53	tcp	Высокий	cpe:/a:isc:bind:9.6-ESV-R11
Риск	Высокий			
Продукты	cpe:/a:isc:bind:9.6-ESV-R11			
Порт	53 tcp			
Метод определения	Probed			
Служба	domain			
Дополнительно				

Количество информации может изменяться в зависимости от службы.

Информация о хосте

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

Поиск уязвимостей	Инвентаризация	Информация о хосте	Расширенные параметры
Общая информация		DNS-имя Домен NetBIOS-имя Домен NetBIOS ipv4Address	ydv-pc.altx-soft.ru altx-soft.ru YDV-PC ALTX-SOFT
OS Windows build 10.0.20348		Имя сре	Windows build 10.0.20348 сре:/o:microsoft:windows

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

6.11 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	4		2		Соответствие в БД: <input type="checkbox"/> Есть <input type="checkbox"/> Нет				
	ВСЕГО ХОСТОВ ОБНАРУЖЕНО	ИЗ НИХ НЕТ СООТВЕТСТВИЯ В СИСТЕМЕ	Операционная система: <input type="checkbox"/> Windows <input type="checkbox"/> Linux <input type="checkbox"/> ОС не определена <input type="checkbox"/> Другое						
Статистические данные по выбранному выполнению задания.		Поиск по IP хоста						Поиск по имени хоста, DNS, FQDN, NetBIOS	
Задание	Профиль	Способ обнаружения	IP	DNS	FQDN	NetBIOS	Операционная система	Агент	
80-я	Обнаружение хостов	ARP	192.168.80.129					Нет	
Запуск		ARP	192.168.80.254					Нет	
17.09.2024 11:42:23		ARP	192.168.80.1					Нет	
Завершение		LOCALHOST	192.168.80.8					Нет	
17.09.2024 11:42:54									
№ выполнения задания									
3									
Экспорт в CSV									

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.

Статистика
Статистические данные по выбранному выполнению задания.

Задание: проверка доступности Linux
Профиль: Проверка доступности
Запуск: 13.02.2023 14:52:54
Завершение: 13.02.2023 14:53:16
№ выполнения задания: 93
Экспорт в CSV

1 ДСТУПНО | 1 НЕДОСТУПНО

✓ Доступен | ✓ Недоступен

Все хосты | Все учетные записи | Все версии агентов | Поиск

Хост	Транспорт	Доступность	Учетная запись	Сообщение	Версия агента
> 10.0.0.173	Ssh	Доступен	linux		
> 192.168.1.4	Ssh	Недоступен	linux	Ошибка установления соединения.	

Экспорт в CSV

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

Статистика
Статистические данные по выбранному выполнению задания.

Задание: проверка доступности_2
Профиль: Проверка доступности
Запуск: 30.01.2023 11:30:49
Завершение: 30.01.2023 11:30:50
№ выполнения задания: 44
Экспорт в CSV

0 ДСТУПНО | 1 НЕДОСТУПНО

Хост	Транспорт
> 10.0.0.173	Winrm

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
<pre>Ip,Reason,Dns,Fqdn,NetBIOS,Os,OpenPorts,IsAgent,IdExistingHost 192.168.80.129,ARP,,,,,False,67 192.168.80.8,LOCALHOST,,,,,False,69</pre>

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](#).

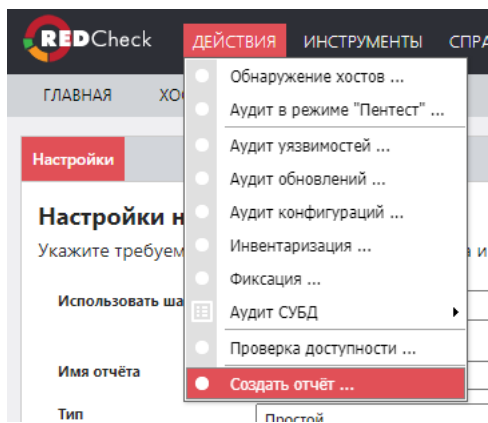
Типы отчетов

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.

Настройки

Настройки нового отчёта

Укажите требуемые параметры для нового отчёта и заполните описание, если нужно.

Использовать шаблон	Нет
Имя отчёта	отчет обновление
Тип	Простой
Отчёт	Обновления
Выбор данных	По заданию
Описание	

Выберем задание → **Вперед**;

Настройки **Задания**

Задания

№ п/п	Имя	Время запуска	Время завершения	Длительность	Всего	Успешно
96	test-upd	05.04.2023, 10:19:08	05.04.2023, 10:22:31	00:00:22	2	2
65	my-comp-update	03.02.2023, 16:53:05	03.02.2023, 16:54:23	00:00:17	2	2

20 Page 1 of 1 (2 items) 1 2 Всего: 2

Назад Вперед

Выберем результат сканирования → **Вперед;**

Настройки **Задания** **Результаты сканирования**

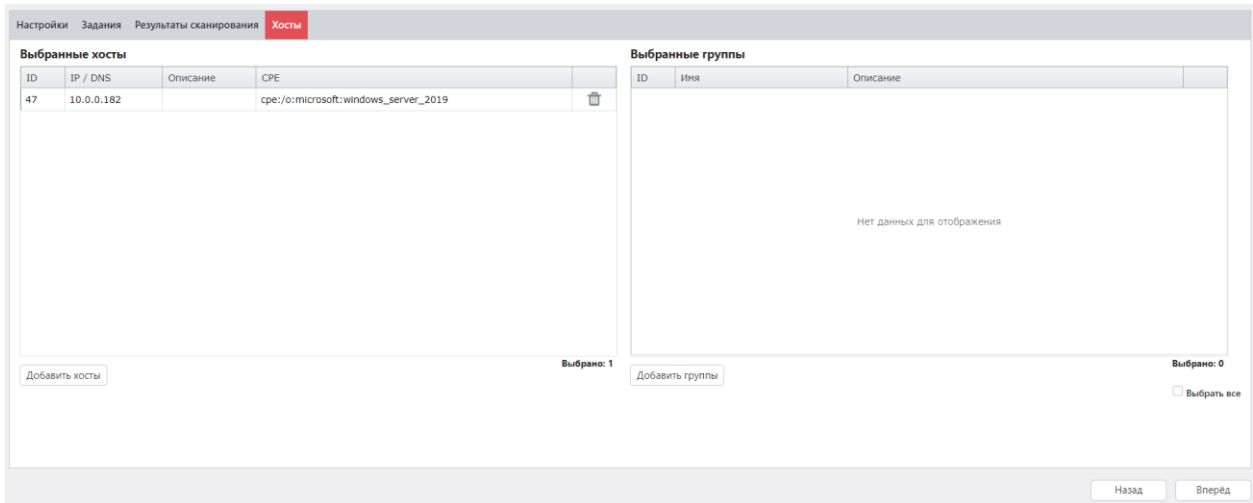
Результаты сканирования

№ п/п	Задание	Начало	Завершение	Всего	Успешно
153	test-upd	05.04.2023, 10:19:08	05.04.2023, 10:22:31	1	1
152	test-upd	05.04.2023, 10:12:56	05.04.2023, 10:16:16	2	1

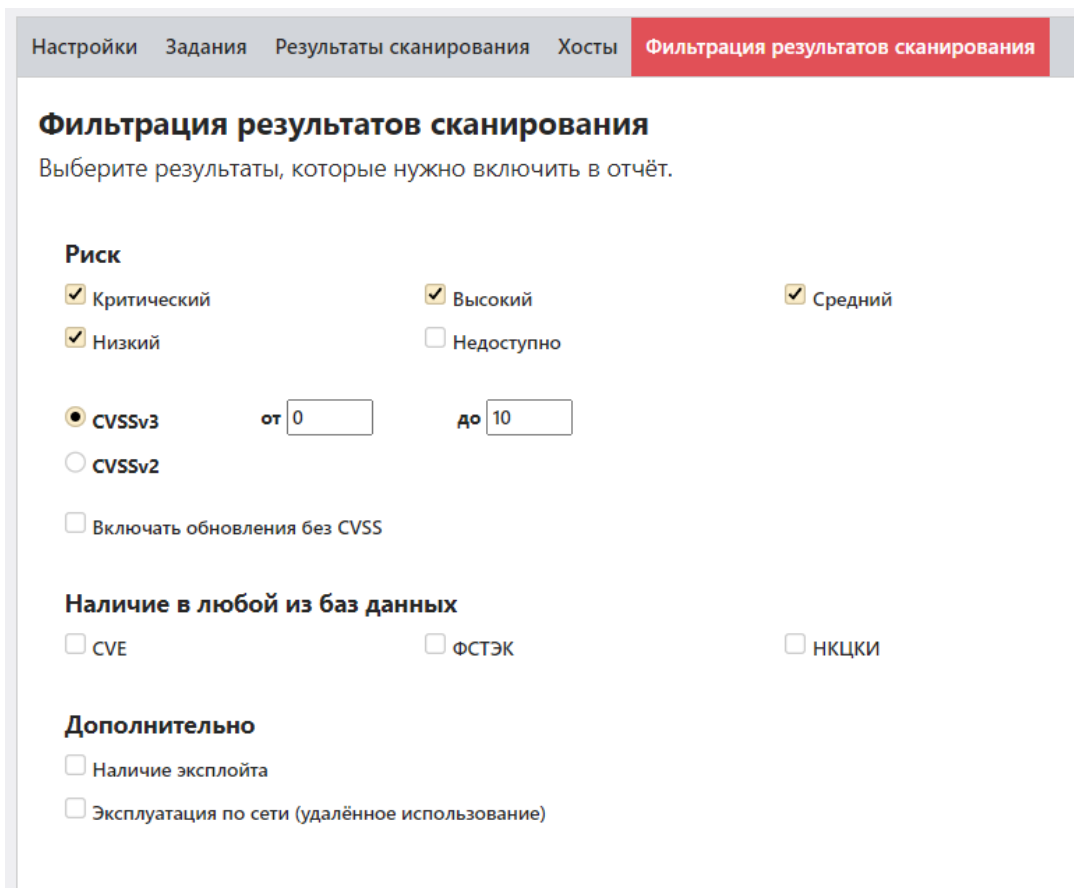
20 Page 1 of 1 (2 items) 1 2 Всего: 2

Назад 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**;

Настройки Задания Результаты сканирования Хосты Фильтрация результатов сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Диаграмма распределения обновлений по уровням риска
- Таблица распределения обновлений по хостам
- Таблица распределения обновлений по продуктам
- Результаты сканирования
- Описание хостов
- Список обновлений

Выберите, как следует сгруппировать найденные обновления

- По хостам
- По продуктам
- По уровням риска

Назад Создать

Дождемся окончания процесса создания отчета.

Создание отчёта ✕

Создание отчёта ...

Операция может занять довольно длительное время.

отчёт создан

Заккрыть

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

ГЛАВНАЯ ХОСТЫ ЗАДАНИЯ ИСТОРИЯ КОНТРОЛЬ **ОТЧЁТЫ** ПОЛЬЗОВАТЕЛИ

Отчёты

Интервал
Сегодня

Начиная с

Заканчивая

Имя и описание

Тип отчёта

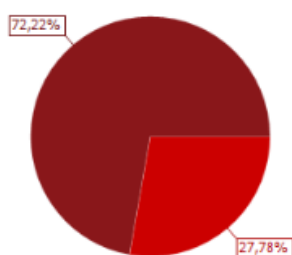
Тип данных

Применить фильтр

№	Тип	Имя	Тип данных	Создан	Статус	Описание	Команды
55	Простой	отчет обновление	Обновления	10.04.2023, 16:00:25	html pdf mht csv xml		⚙️

Отчет имеет следующий вид.

№ отчёта	4s161f62-cb43-4df7-804c-96adcba22ac6
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

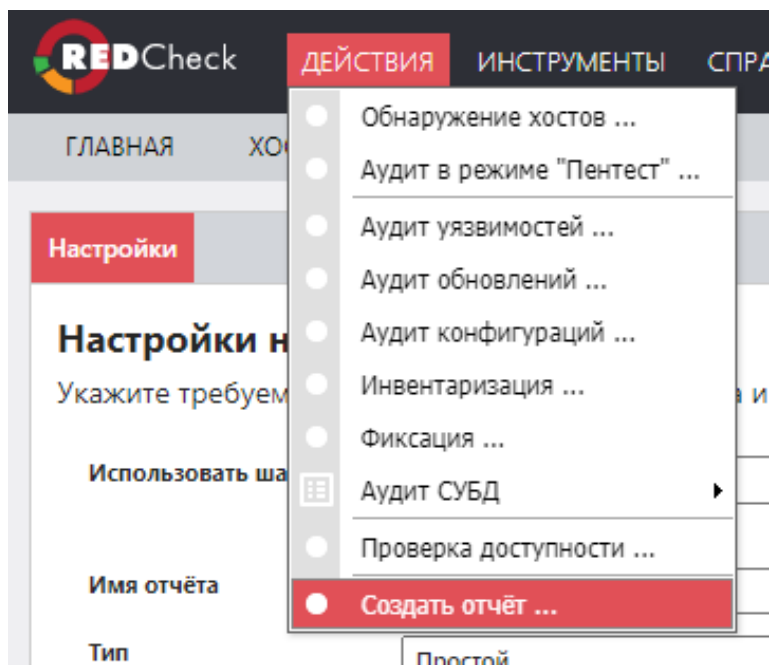
Более подробное описание создания отчета находится в разделе [7.1 Создание простого отчета](#).

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**;

Настройки

Настройки нового отчёта

Укажите требуемые параметры для нового отчёта и заполните описание, если нужно.

Использовать шаблон: Нет

Имя отчёта:

Тип: Простой

Отчёт: Конфигурации

Выбор данных: По заданию

Описание:

Вперёд

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

Конфигурации

- Инвентаризация
- Обновления
- Уязвимости
- Фиксация
- Аудит MS SQL Server
- Аудит БД Oracle
- Аудит БД MySQL
- Установка обновлений
- Аудит PostgreSQL
- Индекс соответствия комплайнс-политике (конфигурации)
- Индекс соответствия комплайнс-политике (конфигурации) для MS SQL Server
- Индекс соответствия комплайнс-политике (конфигурации) для БД Oracle
- Индекс соответствия комплайнс-политике (конфигурации) для БД MySQL
- Индекс соответствия комплайнс-политике (конфигурации) для PostgreSQL
- Аудит IBM Db2
- Аналитика индекса соответствия комплайнс-политике (конфигурации)
- Аудит SAP HANA
- Аудит в режиме "Пентест"
- Проверка доступности
- Обнаружение хостов

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:**

№ ID	Имя	Время запуска	Время завершения	Длительность	Всего	Успешно
78	уязвимости_1	01.02.2023, 10:21:59	01.02.2023, 10:26:03	00:00:03	2	2
69	уязвимости	27.01.2023, 10:37:32	27.01.2023, 10:41:23	00:00:50	1	1

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

→ **Вперед:**

№	Задание	Начало	Завершение	Всего	Успешно
27	уязвимости	27.01.2023, 10:37:32	27.01.2023, 10:41:23	1	1

Page 1 of 1 (1 items) 1 Всего: 1

Назад Вперед

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

Выбранные хосты				Выбранные группы		
ID	IP / DNS	Описание	CPE	ID	Имя	Описание
17	ydv-pc.altx-soft.ru		cpe:/o:microsoft:windows_server_2022	Нет данных для отображения		

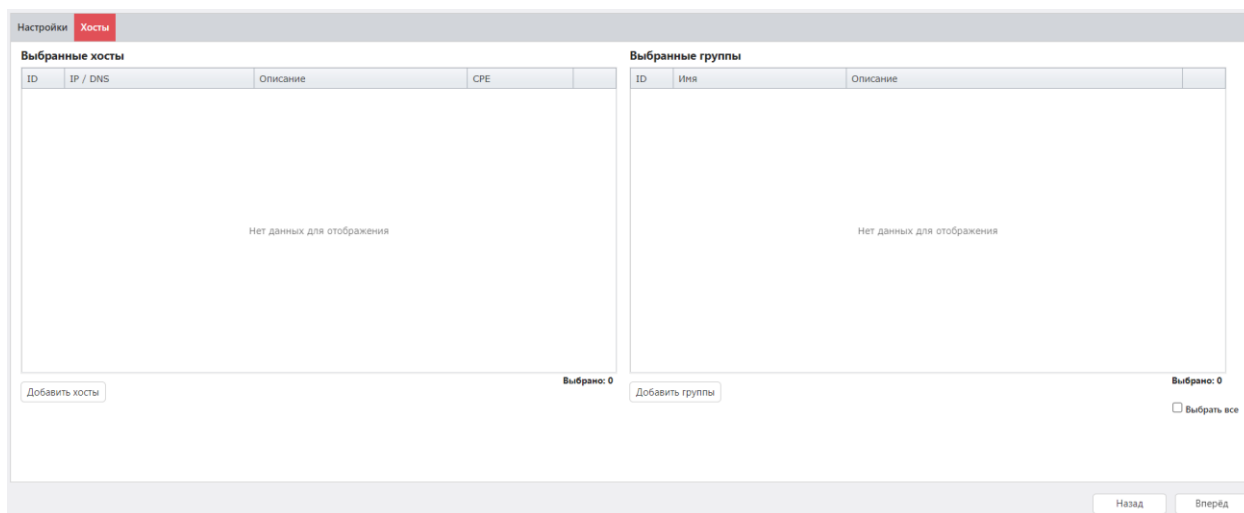
Добавить хосты Выбрано: 1 Добавить группы Выбрано: 0 Выбрать все

Назад Вперед

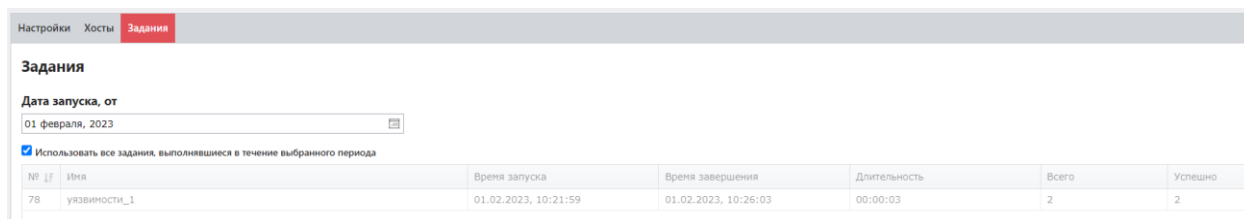
Шаг 6. Укажите дополнительные настройки для отчета ([7.1.1 Настройки для разных типов заданий](#))

Выбор данных: По хостам

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



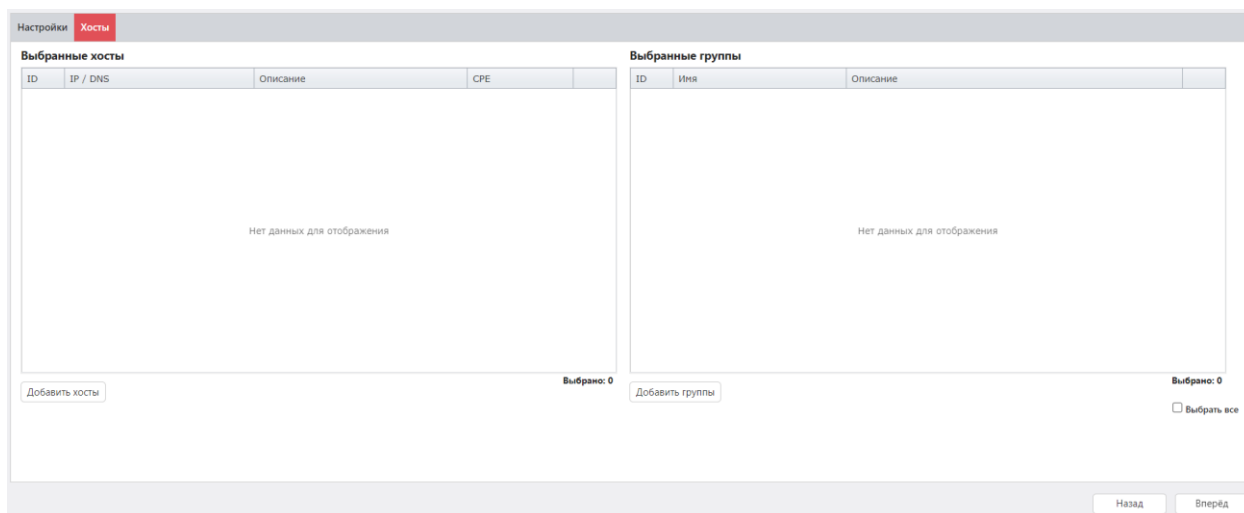
Шаг 4. Выберите задания, которые хотите видеть в отчете, или воспользуйтесь фильтром по дате запуска → **Вперед:**



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:**

№	Задание	Начало
93	уязвимости_1	01.02.2023, 10:23:00
92	уязвимости_1	30.01.2023, 17:09:46
28	уязвимости	27.01.2023, 10:37:32

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](#)
- [Инвентаризация](#)
- [Уязвимости](#)
- [Обновления](#)
- [Фиксация](#)
- [Аудит СУБД](#)
- [Индекс соответствия комплайнс-политике \(конфигурации\)](#)
- [Аналитика индекса соответствия комплайнс-политике \(конфигурации\)](#)
- [Аудит в режиме «Пентест»](#)
- [Проверка доступности](#)
- [Обнаружение хостов](#)

Конфигурации

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

Настройки Задания Результаты сканирования Хосты **Выполненные конфигурации**

Выбор конфигураций

Выберите конфигурации, которые необходимо включить в отчёт.

- ▼ Astra Linux SE и CE – Общие настройки безопасности – АЛТЭКС-СОФТ
 - Профиль по умолчанию
- ▼ Конфигурация аудита безопасности Remote Access Checklist
 - Профиль по умолчанию

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

Настройки Задания Результаты сканирования Хосты Выполненные конфигурации **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Сводная таблица результатов сканирования
- Результаты сканирования
- Описание хостов
- Фактические значения параметров
- Описание параметров

Фильтрация результатов

Укажите, какие правила следует включать в отчёт.

Результаты выполнения правил

<input checked="" type="checkbox"/> Соответствие	<input checked="" type="checkbox"/> Несоответствие	<input checked="" type="checkbox"/> Ошибка
<input checked="" type="checkbox"/> Неизвестно	<input checked="" type="checkbox"/> Неприменимо	<input checked="" type="checkbox"/> Не проверено
<input checked="" type="checkbox"/> Не выбрано	<input checked="" type="checkbox"/> Информация	<input checked="" type="checkbox"/> Исправлено

Критичность правил

<input checked="" type="checkbox"/> Недоступно	<input checked="" type="checkbox"/> Информация	<input checked="" type="checkbox"/> Низкий
<input checked="" type="checkbox"/> Средний	<input checked="" type="checkbox"/> Высокий	

Дополнительно

- Отображать пустые группы в отчёте

Инвентаризация

Укажите настройки содержимого отчета → **Создать**:

Настройки Задания Результаты сканирования Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Профиль
- Результаты сканирования
- Описание хостов

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;

Настройки Задания Результаты сканирования Хосты **Фильтрация результатов сканирования**

Фильтрация результатов сканирования

Выберите результаты, которые нужно включить в отчёт.

Риск

Критический Высокий Средний

Низкий Недоступно

CVSSv3 от до

CVSSv2

Включать уязвимости без CVSS

Наличие в любой из баз данных

CVE ФСТЭК НКЦКИ

Дополнительно

Наличие эксплойта

Эксплуатация по сети (удалённое использование)

К отчету можно применить профиль сканирования ([5.1 Профили сканирования](#)).

Укажите, что будет содержаться в отчете и варианты группировки уязвимостей

→ **Создать:**

Настройки Задания Результаты сканирования Хосты Фильтрация результатов сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

Заголовок отчёта

Диаграмма распределения уязвимостей по уровням риска

Таблица распределения уязвимостей по хостам

Таблица распределения уязвимостей по продуктам

Результаты сканирования

Описание хостов

Список уязвимостей

Выберите, как следует группировать найденные уязвимости

По хостам

По продуктам

По уровням риска

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

Настройки Задания Результаты сканирования Хосты **Фильтрация результатов сканирования**

Фильтрация результатов сканирования

Выберите результаты, которые нужно включить в отчёт.

Риск

Критический Высокий Средний

Низкий Недоступно

CVSSv3 от до

CVSSv2

Включать уязвимости без CVSS

Наличие в любой из баз данных

CVE ФСТЭК НКЦКИ

Дополнительно

Наличие эксплойта

Эксплуатация по сети (удалённое использование)

К отчету можно применить профиль сканирования ([5.1 Профили сканирования](#)).

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

Настройки Задания Результаты сканирования Хосты Фильтрация результатов сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Диаграмма распределения обновлений по уровням риска
- Таблица распределения обновлений по хостам
- Таблица распределения обновлений по продуктам
- Результаты сканирования
- Описание хостов
- Список обновлений

Выберите, как следует сгруппировать найденные обновления

- По хостам
- По продуктам
- По уровням риска

Фиксация

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

Настройки Задания Результаты сканирования Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Настройки задания
- Результаты сканирования
- Описание хостов

Аудит СУБД

Выберите профиль конфигурации, проверку с которым хотите увидеть в отчете

→ **Вперед:**

Настройки Задания Результаты сканирования Хосты **Выполненные конфигурации**

Выбор конфигураций

Выберите конфигурации, которые необходимо включить в отчёт.

- Microsoft SQL Server - Общие настройки безопасности - АЛТЭКС-СОФТ
 - Профиль по умолчанию

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

Настройки Задания Результаты сканирования Хосты Выполненные конфигурации **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Сводная таблица результатов сканирования
- Результаты сканирования
- Описание хостов
- Фактические значения параметров
- Описание параметров

Фильтрация результатов

Укажите, какие правила следует включать в отчёт.

Результаты выполнения правил

<input checked="" type="checkbox"/> Соответствие	<input checked="" type="checkbox"/> Несоответствие	<input checked="" type="checkbox"/> Ошибка
<input checked="" type="checkbox"/> Неизвестно	<input checked="" type="checkbox"/> Неприменимо	<input checked="" type="checkbox"/> Не проверено
<input checked="" type="checkbox"/> Не выбрано	<input checked="" type="checkbox"/> Информация	<input checked="" type="checkbox"/> Исправлено

Критичность правил

<input checked="" type="checkbox"/> Недоступно	<input checked="" type="checkbox"/> Информация	<input checked="" type="checkbox"/> Низкий
<input checked="" type="checkbox"/> Средний	<input checked="" type="checkbox"/> Высокий	

Дополнительно

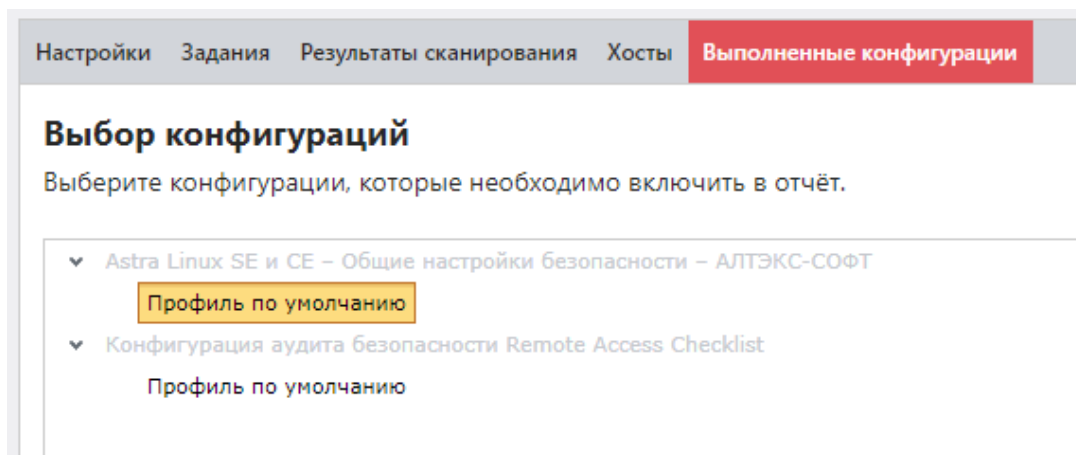
- Отображать пустые группы в отчёте

Индекс соответствия комплайнс-политике (конфигурации)

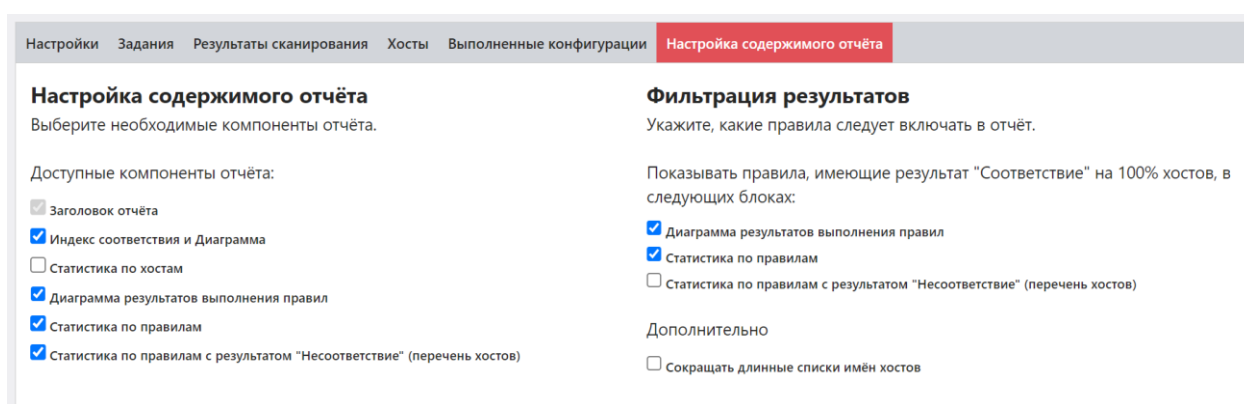
Отчет показывает, насколько хосты соответствуют выбранной конфигурации, детально информируя о каждом правиле.

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

Настройки Задания **Результаты сканирования**

Результаты сканирования

Дата запуска, от
02 января, 2023

Дата завершения, до
02 февраля, 2023

Использовать все результаты за выбранный период

№	ИД	Задание	Начало	Завершение
31		Конфигурация Linux	27.01.2023, 14:57:35	27.01.2023, 14:58:36

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

Настройки Задания Результаты сканирования **Выполненные конфигурации**

Выбор конфигураций

Выберите конфигурации, которые необходимо включить в отчёт.

ВНИМАНИЕ: в отчёт будут включены только результаты сканирований по конфигурации/профилю, выбранному на данном шаге.

- ▼ Astra Linux SE и CE – Общие настройки безопасности – АЛТЭК-СОФТ
 - Профиль по умолчанию**
- ▼ Конфигурация аудита безопасности Remote Access Checklist
 - Профиль по умолчанию

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

Настройки Задания Результаты сканирования Выполненные конфигурации **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Таблица индекса соответствия комплайнс-политике
- График индекса соответствия комплайнс-политике
- График количества хостов на 100% соответствующих комплайнс-политике

Аудит в режиме «Пентест»

Укажите, что будет содержаться в отчете → **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

Проверка доступности

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

Настройки Задания Результаты сканирования Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Результаты сканирования

Фильтрация результатов

Укажите, какие правила следует включать в отчёт.

Успешно Не успешно

Сортировка результатов

По хостам

По результату - сначала недоступные

По результату - сначала доступные

Обнаружение хостов

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

Настройки Задания Результаты сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

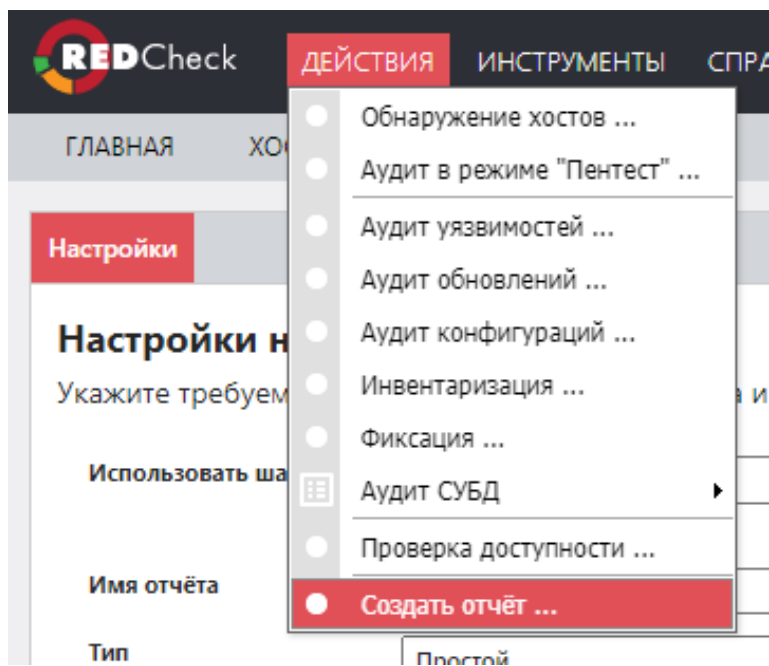
- Заголовок отчёта
- Результаты сканирования

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**;

Настройки нового отчёта

Укажите требуемые параметры для нового отчёта и заполните описание, если нужно.

Использовать шаблон	Нет
Имя отчёта	<input type="text"/>
Тип	Дифференциальный
Отчёт	Конфигурации
Выбор данных	По заданию
Описание	<input type="text"/>

Вперёд

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

- Конфигурации
- Инвентаризация
- Обновления
- Уязвимости
- Фиксация
- Аудит MS SQL Server
- Аудит БД Oracle
- Аудит БД MySQL
- Аудит PostgreSQL
- Аудит IBM Db2
- Аудит SAP HANA
- Аудит в режиме "Пентест"

Шаг 3. Выберите задание → **Вперед:**

Настройки **Задания**

Задания

№	Имя	Время запуска	Время завершения	Длительность	Всего	Успешно
78	уязвимости_1	01.02.2023, 10:21:59	01.02.2023, 10:26:03	00:00:03	2	2

20 Page 1 of 1 (1 items) < 1 > Всего: 1

Назад Вперед

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

Настройки **Задания** **Результаты сканирования**

Результаты сканирования

Сканирование 1 (Исходное)

№	Задание	Начало	Завершение	Всего	Успешно
46	уязвимости_1	01.02.2023, 10:21:59	01.02.2023, 10:26:03	1	1
45	уязвимости_1	30.01.2023, 17:08:50	30.01.2023, 17:10:24	1	1

20 Page 1 of 1 (2 items) < 1 > Всего: 2

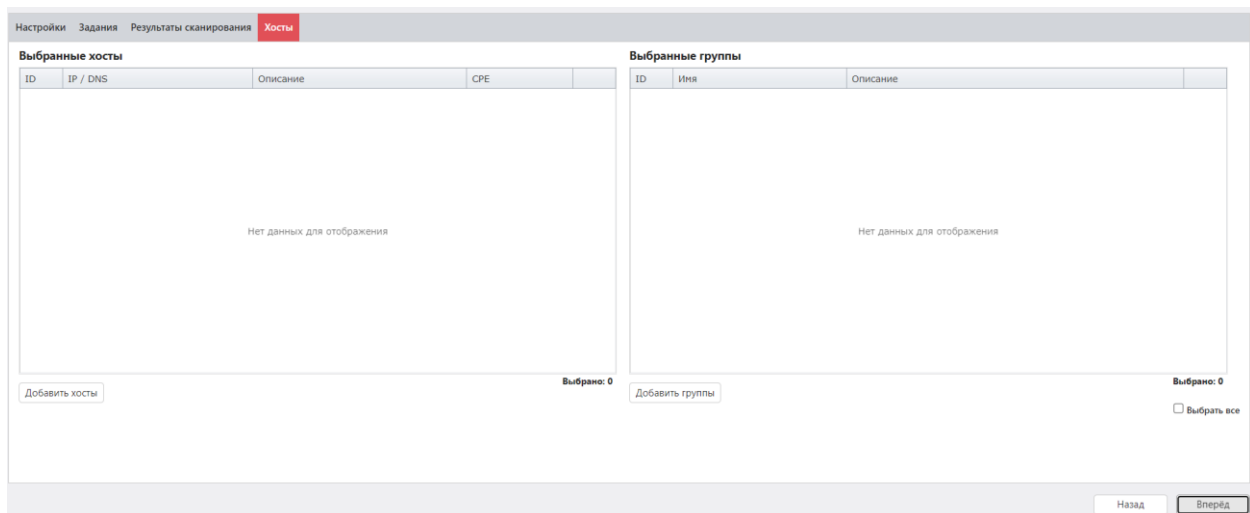
Сканирование 2 (Текущее)

№	Задание	Начало	Завершение	Всего	Успешно
46	уязвимости_1	01.02.2023, 10:21:59	01.02.2023, 10:26:03	1	1

20 Page 1 of 1 (1 items) < 1 > Всего: 1

Назад 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](#)
- [Инвентаризация](#)
- [Обновления](#)
- [Уязвимости](#)
- [Фиксация](#)
- [Аудит СУБД](#)
- [Аудит в режиме «Пентест»](#)

Конфигурации

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

Настройки Задания Результаты сканирования Хосты **Выполненные конфигурации**

Выбор конфигураций

Выберите конфигурации, которые необходимо включить в отчёт.

- ▼ Astra Linux SE и CE – Общие настройки безопасности – АЛТЭК-СОФТ
 - Профиль по умолчанию
- ▼ Конфигурация аудита безопасности Remote Access Checklist
 - Профиль по умолчанию

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

Настройки Задания Результаты сканирования Хосты Выполненные конфигурации **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Результаты сканирования
- Описание хостов
- Фактические значения параметров
- Описание параметров

Инвентаризация

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
- Профиль
- Результаты сканирования
- Описание хостов

Обновления

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
- Результаты сканирования
- Описание хостов
- Список обновлений

Уязвимости

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
- Результаты сканирования
- Описание хостов
- Список уязвимостей

Фиксация

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
- Настройки задания
- Результаты сканирования
- Описание хостов

Аудит СУБД

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

Настройки Задания Результаты сканирования Хосты Выполненные конфигурации **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Результаты сканирования
- Описание хостов
- Фактические значения параметров
- Описание параметров

Аудит в режиме «Пентест»

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

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Выберите степень точности отображения уязвимостей

Точность

Доступные компоненты отчёта:

- Заголовок отчёта
- Сканирование портов
- Подбор паролей
- Поиск уязвимостей
- Информация о хосте на основе данных Nmap
- Описание хостов
- Список уязвимостей

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;

Шаблоны отчётов								
№	Тип	Имя	Тип данных	Дата создания	Дата модификации	Имя отчёта	Описание	Команды
1	Простой	тест	Уязвимости	02.12.2022, 14:23:59		какое-то имя		
2	Простой	уязвимости	Аудит в режиме "Пентест"	03.02.2023, 14:36:29		уязвимости		

20 Page 1 of 1 (2 items) < 1 > Всего: 2

Добавить шаблон отчёта ...

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;

Настройки

Настройки нового шаблона отчётов

Укажите требуемые параметры для нового отчёта и заполните описание, если нужно.

Название шаблона	<input type="text" value="уязвимости по профилю"/>
Имя отчёта	<input type="text" value="уязвимость по профилю"/>
Тип	<input type="text" value="Простой"/>
Отчёт	<input type="text" value="Уязвимости"/>
Выбор хостов	<input type="radio"/> Выбранные хосты и/или группы <input checked="" type="radio"/> Все хосты, попавшие в выбранные сканирования
Выбор заданий и сканирований	<input type="radio"/> Только результаты из текущего выполнения <input type="radio"/> Текущее задание (то, в котором используется шаблон) <input checked="" type="radio"/> Список выбранных заданий + текущее задание Для выбранных заданий включать сканирования, начиная с <input type="text" value="30"/> дней до времени построения отчета
Описание	<input type="text"/>

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

Настройки **Задания**

Задания

Использовать все задания, выполнявшиеся в течение выбранного периода

№ ↑ ↓	Имя	↑ ↓	Время запуска	Время завершения	Длительность	Всего	Успешно
106	тестовое задание		06.04.2023, 10:18:35	06.04.2023, 10:19:08	00:00:32	1	1
95	test-vulns		05.04.2023, 10:19:49	05.04.2023, 10:29:17	00:00:28	2	2
83	уязвимости_3		03.02.2023, 17:45:22	03.02.2023, 17:47:36	00:00:13	1	1
78	уязвимости_1		01.02.2023, 13:21:59	01.02.2023, 13:26:03	00:00:03	2	2
69	уязвимости		27.01.2023, 13:37:32	27.01.2023, 13:41:23	00:00:50	1	1

Всего: 5 / Выбрано: 2

Назад Вперёд

Укажем следующие параметры для фильтрации результатов сканирования.

Настройки **Задания** **Фильтрация результатов сканирования**

Фильтрация результатов сканирования

Выберите результаты, которые нужно включить в отчёт.

Риск

Критический Высокий Средний
 Низкий Недоступно

CVSSv3 от до
 CVSSv2

Включать уязвимости без CVSS

Наличие в любой из баз данных

CVE ФСТЭК НКЦКИ

Дополнительно

Наличие эксплойта
 Эксплуатация по сети (удалённое использование)

Укажем профиль аудитов для исключения некоторых уязвимостей из отчета.

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

Исключаемые статические профили аудитов ▾

ID	Название	Семейство
Нет данных для отображения		

Выбрано: 0

Добавить профиль аудитов

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

Выбор профиля аудитов

Название

<input type="checkbox"/>	ID	Название	Семейство
<input type="checkbox"/>	1	profile	Windows
<input type="checkbox"/>	4	test	Windows
<input type="checkbox"/>	5	Тестовый профиль	Windows

20 Page 1 of 1 (3 items) 1 Всего: 3 / Выбрано: 0

Выбрать Отмена

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

Настройки Задания Фильтрация результатов сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта
Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Диаграмма распределения уязвимостей по уровням риска
- Таблица распределения уязвимостей по хостам
- Таблица распределения уязвимостей по продуктам
- Результаты сканирования
- Описание хостов
- Список уязвимостей

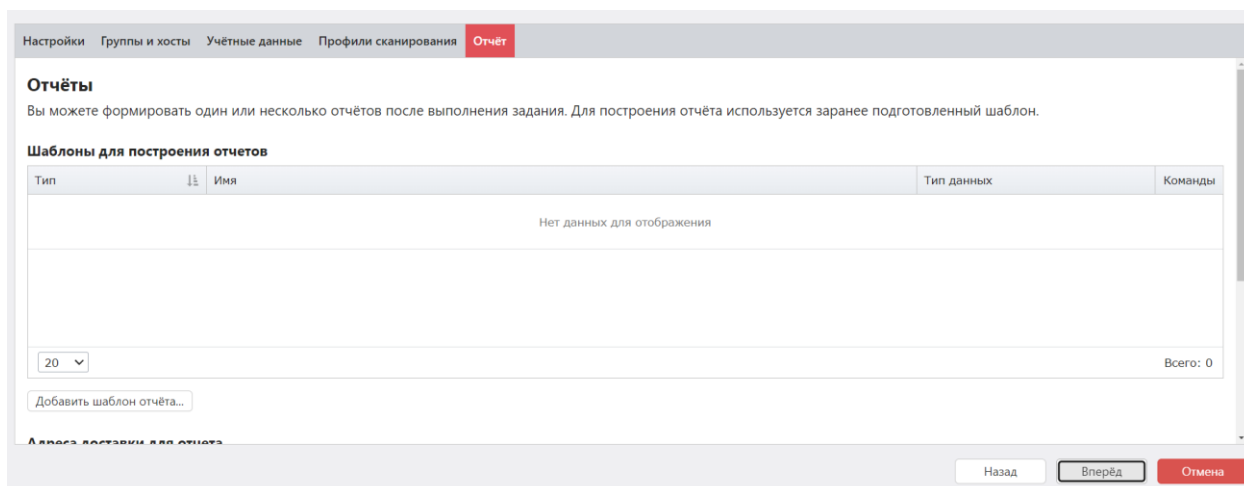
Выберите, как следует сгруппировать найденные уязвимости

- По хостам
- По продуктам
- По уровням риска

Назад Создать шаблон

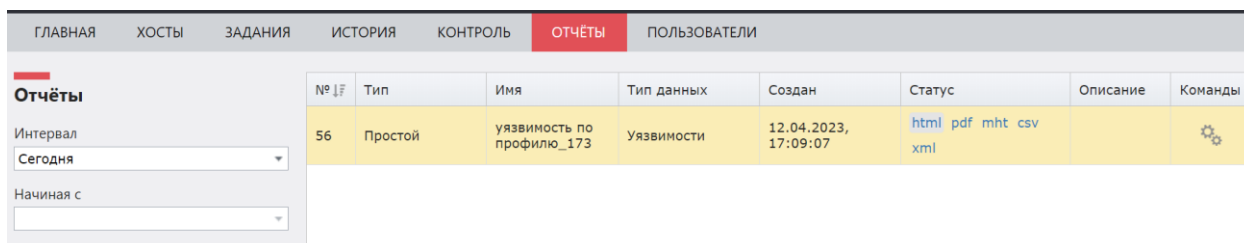
Настройки шаблона отличаются друг от друга в зависимости от выбранного типа задания ([7.3.1 Настройки для разных типов задания](#)).

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



После завершения сканирования посмотрим созданный по шаблону отчет.

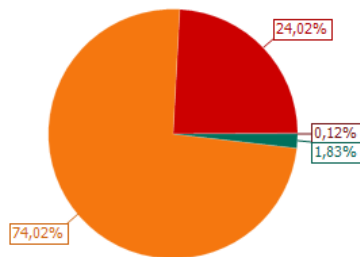
Перейдем в **Отчеты** и скачаем в формате html отчет.



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

№ 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](#)
- [Инвентаризация](#)
- [Обновления](#)
- [Уязвимости](#)
- [Фиксация](#)
- [Аудит СУБД](#)
- [Аудит в режиме «Пентест»](#)
- [Проверка доступности](#)
- [Обнаружение хостов](#)

Конфигурации

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

Настройки Хосты **Конфигурации**

Выберите конфигурацию

Фильтр по платформам... Фильтр по продуктам...

Выбрать все Сбросить все

Поиск конфигураций

#	Имя
<input checked="" type="checkbox"/>	Расширенная конфигурация безопасности Windows 8
<input checked="" type="checkbox"/>	КриптоПро CSP - Настройки согласно руководству администратора безопасности - КриптоПро
<input checked="" type="checkbox"/>	Конфигурация рядового сервера "Корпоративный клиент Windows Server 2008"
<input checked="" type="checkbox"/>	Конфигурация рядового сервера "Корпоративный клиент Windows Server 2008 R2"
<input type="checkbox"/>	Конфигурация рядового сервера "Безопасная среда Windows Server 2008"
<input type="checkbox"/>	Конфигурация рядового сервера "Безопасная среда Windows Server 2008 R2"
<input type="checkbox"/>	Конфигурация по безопасной настройке ОС Microsoft Windows 7 Optima для IT-профессионалов
<input type="checkbox"/>	Конфигурация контроллера домена "Корпоративный клиент Windows Server 2008 R2"
<input type="checkbox"/>	Конфигурация контроллера домена "Безопасная среда Windows Server 2008"
<input type="checkbox"/>	Конфигурация контроллера домена "Безопасная среда Windows Server 2008 R2"
<input type="checkbox"/>	Конфигурация контроллера домена "Безопасная среда Microsoft Windows Server 2003"

Всего: 113 Выбрано: 4

Конфигурация

Название: Конфигурация рядового сервера "Корпоративный клиент Windows Server 2008 R2"

Версия: 43

Файл: Benchmark\WS2008R2_EC_Member_Server\ALTX-WS2008-EC-Member-xccdf.xml

Платформа: Microsoft Windows Server 2008 R2 (cpu:/o:microsoft:windows_server_2008:r2)

Описание

Название: Конфигурация рядового сервера "Корпоративный клиент Windows Server 2008 R2"

Описание: Конфигурация предназначена для обеспечения безопасного функционирования ОС Microsoft Windows Server 2008 R2

Примечание: Не рекомендуется применять настройки данной конфигурации без первичного тестирования и проверки в не критичной среде. В случае возникновения вопросов Вы можете обратиться в службу технической поддержки компании АЛТЭК-СОФТ: support@altx-

Назад Вперед

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

Настройки Хосты Конфигурации **Профиль конфигурации** Настройка содержимого отчёта

Профиль конфигурации

Профиль конфигурации содержит настройки, которые могут менять параметры правил и влиять на их выполнение.

- ▼ Конфигурация рядового сервера "Корпоративный клиент Windows Server 2008"
 - Профиль по умолчанию
 - Конфигурация рядового сервера "Корпоративный клиент Windows Server 2008"
- ▼ Конфигурация рядового сервера "Корпоративный клиент Windows Server 2008 R2"
 - Профиль по умолчанию
 - Конфигурация рядового сервера "Корпоративный клиент Windows Server 2008 R2"
- ▼ КриптоПро CSP – Настройки согласно руководству администратора безопасности – КриптоПро
 - Профиль по умолчанию
 - КриптоПро CSP – Настройки согласно руководству администратора безопасности – КриптоПро
- ▼ Расширенная конфигурация безопасности Windows 8
 - Профиль по умолчанию
 - Расширенная конфигурация безопасности Windows 8

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

Настройки Хосты Конфигурации Профиль конфигурации **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Сводная таблица результатов сканирования
- Результаты сканирования
- Описание хостов
- Фактические значения параметров
- Описание параметров

Фильтрация результатов

Укажите, какие правила следует включать в отчёт.

Результаты выполнения правил

<input checked="" type="checkbox"/> Соответствие	<input checked="" type="checkbox"/> Несоответствие	<input checked="" type="checkbox"/> Ошибка
<input checked="" type="checkbox"/> Неизвестно	<input checked="" type="checkbox"/> Неприменимо	<input checked="" type="checkbox"/> Не проверено
<input checked="" type="checkbox"/> Не выбрано	<input checked="" type="checkbox"/> Информация	<input checked="" type="checkbox"/> Исправлено

Критичность правил

<input checked="" type="checkbox"/> Недоступно	<input checked="" type="checkbox"/> Информация	<input checked="" type="checkbox"/> Низкий
<input checked="" type="checkbox"/> Средний	<input checked="" type="checkbox"/> Высокий	

Дополнительно

- Отображать пустые группы в отчёте

Назад [Создать шаблон](#)

Инвентаризация

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

Настройки Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Профиль
- Результаты сканирования
- Описание хостов

Обновления

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

Настройки Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Результаты сканирования

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;

Настройки Хосты Фильтрация результатов сканирования

Фильтрация результатов сканирования

Выберите результаты, которые нужно включить в отчет.

Риск

Критический Высокий Средний

Низкий Недоступно

CVSSv3 от до

CVSSv2

Включать уязвимости без CVSS

Наличие в любой из баз данных

CVE ФСТЭК НКЦКИ

Дополнительно

Наличие эксплойта

Эксплуатация по сети (удалённое использование)

К отчету можно применить профиль сканирования ([5.1 Профили сканирования](#)).

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

Настройки Хосты Фильтрация результатов сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Диаграмма распределения уязвимостей по уровням риска
- Таблица распределения уязвимостей по хостам
- Таблица распределения уязвимостей по продуктам
- Результаты сканирования
- Описание хостов
- Список уязвимостей

Выберите, как следует сгруппировать найденные уязвимости

- По хостам
- По продуктам
- По уровням риска

Фиксация

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

Настройки Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Профиль
- Результаты сканирования
- Описание хостов

Аудит СУБД

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

Настройки Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Сводная таблица результатов сканирования
- Результаты сканирования
- Описание хостов
- Фактические значения параметров
- Описание параметров

Фильтрация результатов

Укажите, какие правила следует включать в отчёт.

Результаты выполнения правил

<input checked="" type="checkbox"/> Соответствие	<input checked="" type="checkbox"/> Несоответствие	<input checked="" type="checkbox"/> Ошибка
<input checked="" type="checkbox"/> Неизвестно	<input checked="" type="checkbox"/> Неприменимо	<input checked="" type="checkbox"/> Не проверено
<input checked="" type="checkbox"/> Не выбрано	<input checked="" type="checkbox"/> Информация	<input checked="" type="checkbox"/> Исправлено

Критичность правил

<input checked="" type="checkbox"/> Недоступно	<input checked="" type="checkbox"/> Информация	<input checked="" type="checkbox"/> Низкий
<input checked="" type="checkbox"/> Средний	<input checked="" type="checkbox"/> Высокий	

Дополнительно

- Отображать пустые группы в отчёте

Аудит в режиме «Пентест»

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

Настройки 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

Проверка доступности

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

Настройки Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Результаты сканирования

Фильтрация результатов

Укажите, какие правила следует включать в отчёт.

<input checked="" type="checkbox"/> Успешно	<input checked="" type="checkbox"/> Не успешно
---	--

Сортировка результатов

По хостам

По результату - сначала недоступные

По результату - сначала доступные

Обнаружение хостов

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

Настройки Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- Заголовок отчёта
- Результаты сканирования

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

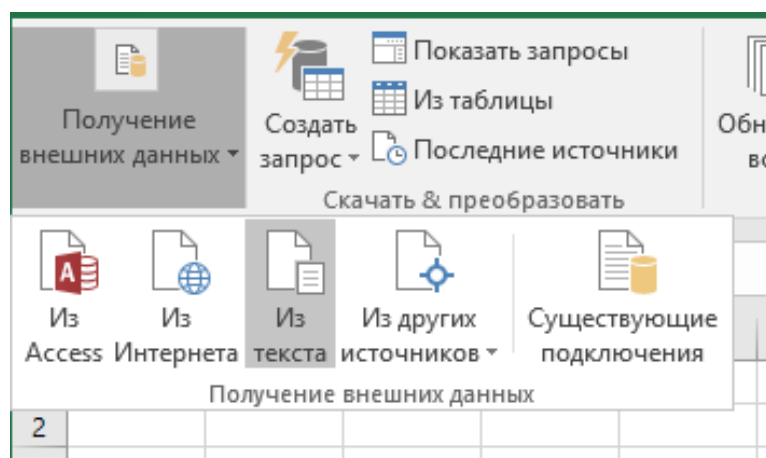
В примере используется Excel 2016. Для других версий шаги идентичны.

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;

Мастер текстов (импорт) - шаг 1 из 3

Данные восприняты как список значений с разделителями.
Если это верно, нажмите кнопку "Далее >", в противном случае укажите формат данных.

Формат исходных данных

Укажите формат данных:

с разделителями — значения полей отделяются знаками-разделителями

фиксированной ширины — поля имеют заданную ширину

Начать импорт со строки: 1 Формат файла: 65001 : Юникод (UTF-8)

Мои данные содержат заголовки

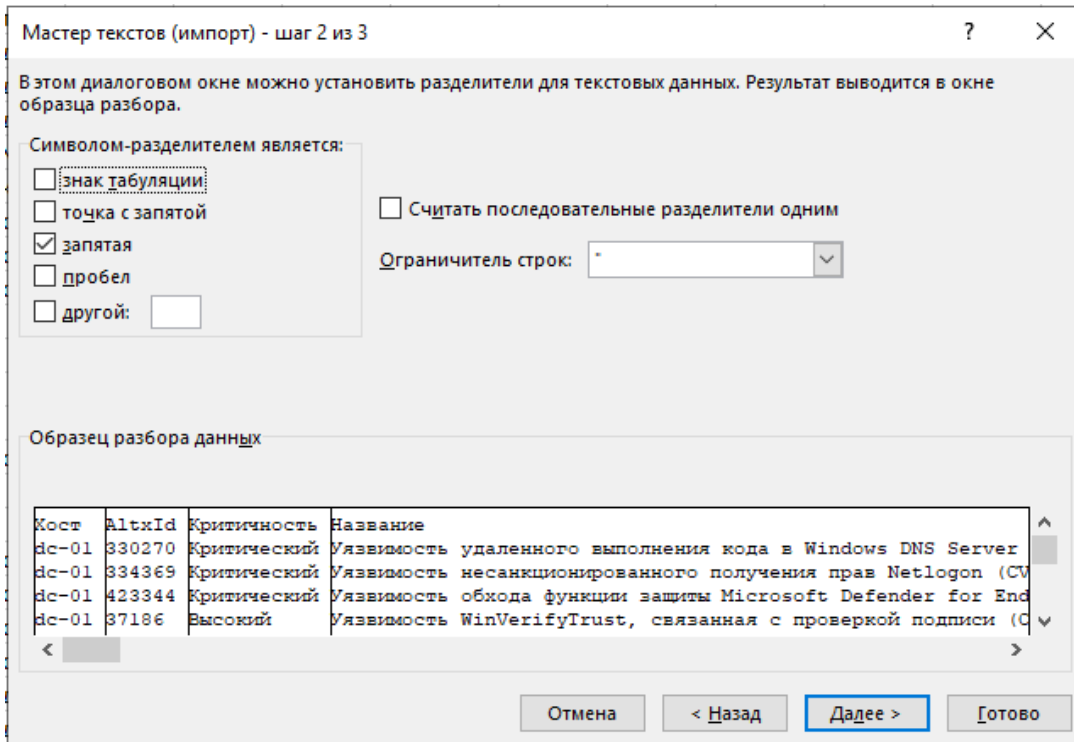
Предварительный просмотр файла C:\Users\Administrator\Downloads\Отчет-уязвимостями.csv.

1	Кост, AltxId, Критичность, Название, Описание, Продукты, Детализация, Cvss2, Cvss2 Вектор,
2	dc-01, 330270, Критический, Уязвимость удаленного выполнения кода в Windows DNS Serve
3	dc-01, 334369, Критический, Уязвимость несанкционированного получения прав Netlogon (
4	dc-01, 423344, Критический, Уязвимость обхода функции защиты Microsoft Defender for E
5	dc-01, 37186, Высокий, "Уязвимость WinVerifyTrust, связанная с проверкой подписи (CVE

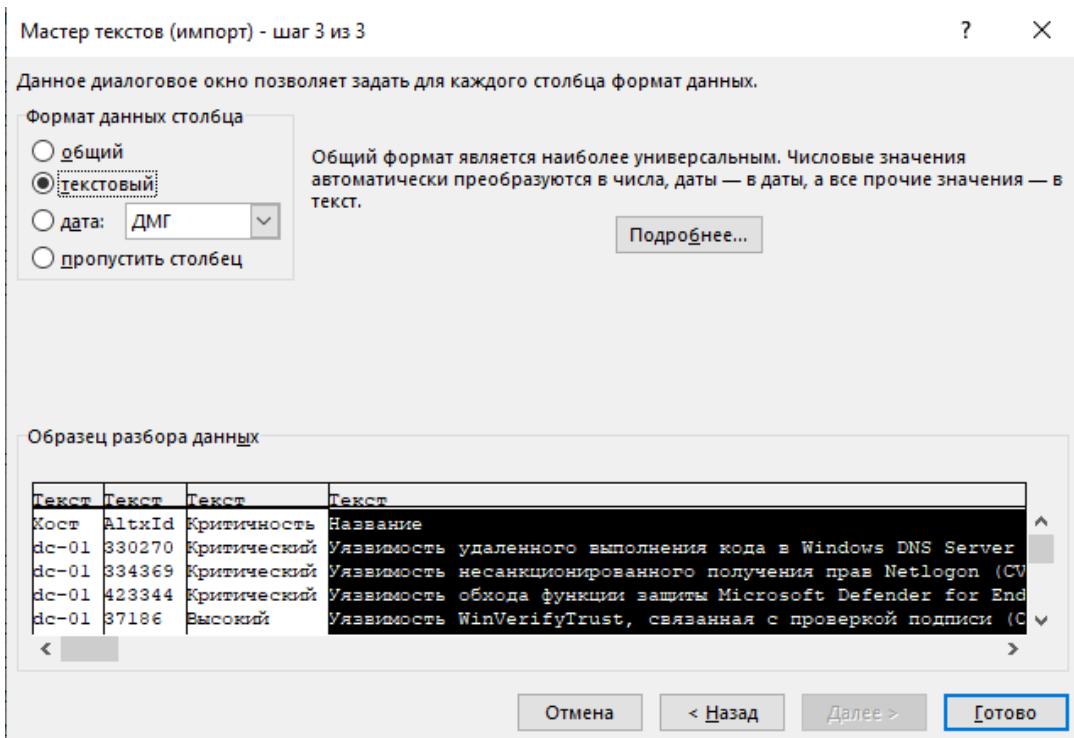
< >

Отмена < Назад **Далее >** Готово

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



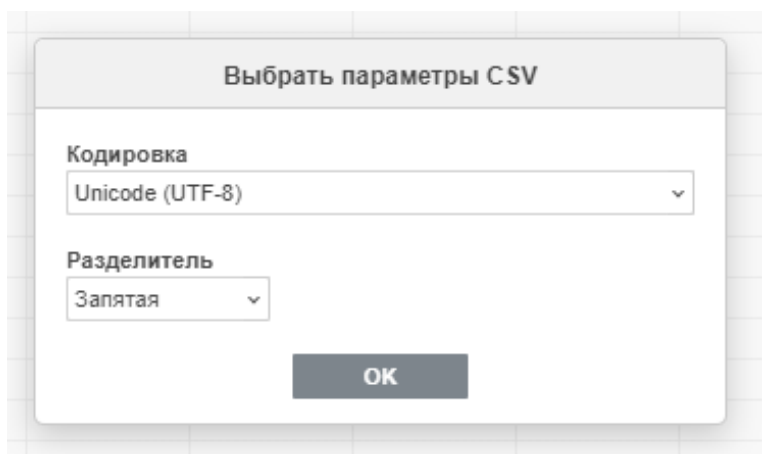
Шаг 3. Для каждого столбца укажите **текстовый** формат данных → **Готово**;



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:

	C
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](#)
- [8.2 Недоступность хостов](#)
- [8.3 Анализ уязвимостей](#)
- [8.4 Контроль устранения уязвимостей](#)
- [8.5 Анализ конфигураций](#)

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**

Хост	Проблема	Наличие в группе
192.168.100.14	Нет задания	Да
192.168.100.16	Нет задания	Да
192.168.100.26	Нет задания	Да
192.168.100.46	Нет задания	Да
192.168.100.67	Нет задания	Да
192.168.100.81	Нет задания	Да
192.168.100.94	Нет задания	Да
192.168.100.95	Нет задания	Да
192.168.100.96	Нет задания	Да
192.168.100.98	Нет задания	Да
192.168.100.99	Нет задания	Да
192.168.100.105	Нет задания	Да
192.168.100.120	Нет задания	Да
192.168.100.130	Нет задания	Да
192.168.100.131	Нет задания	Да
192.168.100.132	Нет задания	Да
192.168.100.133	Нет задания	Да
192.168.100.144	Нет задания	Да
192.168.100.150	Нет задания	Да
192.168.100.155	Нет задания	Да

Поддерживается 4 типа сканирования:

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

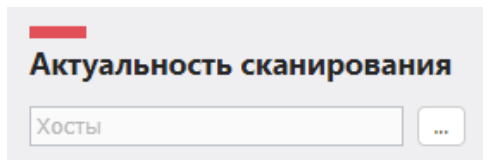
Информация об актуальности сканирования включает в себя:


- 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;

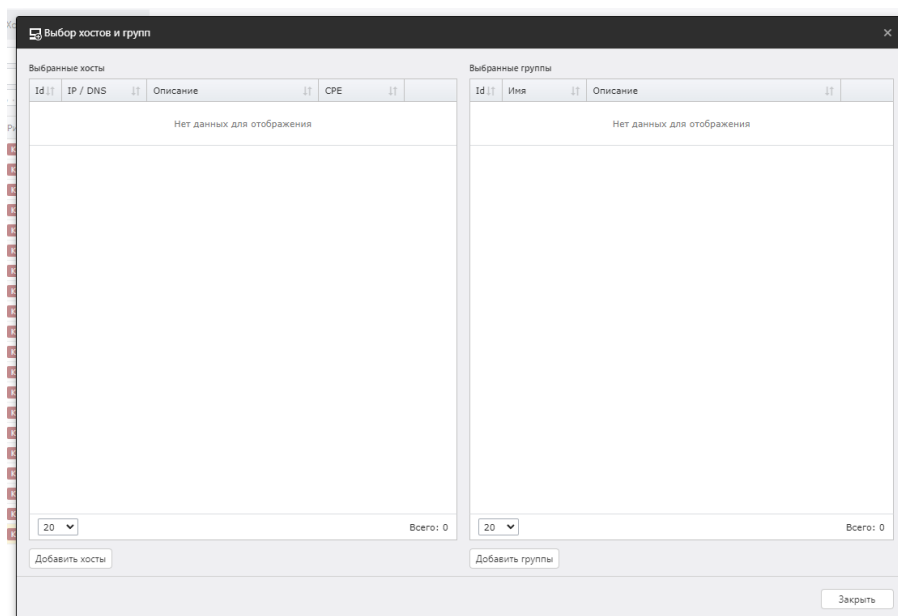
- Наличие в группе – находится ли хост в какой-либо группе.

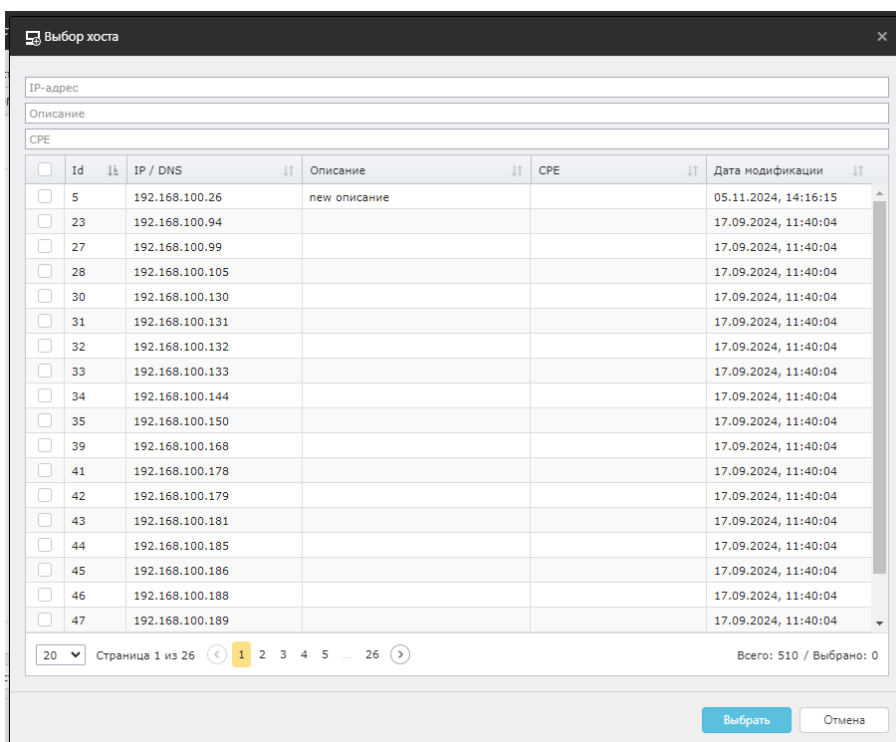
Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

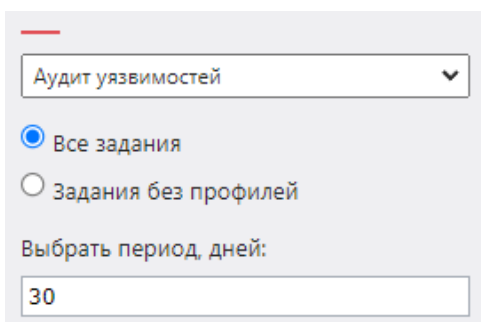


- Хосты – можно выбрать хосты, уязвимости для которых будут отображаться. Нажмите на , после чего откроется окно выбора групп и хостов:

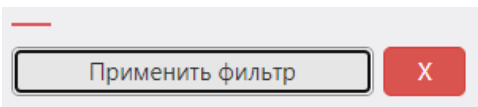




- Тип сканирования – для какого типа сканирования проверять результаты сканирования хостов;
 - Для аудита уязвимостей / обновлений – учитывать или нет задания с профилями сканирования ([5.1 Профили аудитов](#));
- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований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



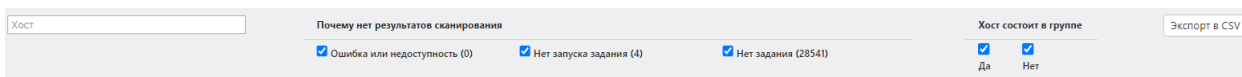
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



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**

Хост	Тип сканирования	Задание	Результат	Причина недоступности	Время завершения
192.168.80.129	Аудит конфигураций	1_15	Ошибка	Платформа в конфигурации "Benchmarks\AstraLinux-RedBook\ALT-X-AstraLinux-RedBook-xccdf.xml" не совпадает на хосте "192.168.80.129".	09.10.2024, 07:32:16
192.168.100.12	Аудит PostgreSQL	1_10	Хост недоступен	Хост недоступен. Причина: "Connection refused [::ffff:192.168.100.12]:5432". Подробности в журнале событий службы сканирования. Для получения детальной информации можно воспользоваться заданием "Проверка доступности".	04.10.2024, 11:06:06
192.168.80.129	Аудит конфигураций	test_14	Ошибка	Платформа в конфигурации "Benchmarks\Debian\ALT-X-Debian-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 10:51:39
192.168.80.129	Аудит конфигураций	test123123	Ошибка	Платформа в конфигурации "Benchmarks\Debian\ALT-X-Debian-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 10:08:26
192.168.80.129	Аудит PostgreSQL	test_6	Ошибка	No applicable scanners for any tunnel found.	04.10.2024, 08:56:01
192.168.80.129	Аудит PostgreSQL	test_5	Ошибка	No applicable scanners for any tunnel found.	04.10.2024, 08:51:55
192.168.80.129	Аудит PostgreSQL	test_4	Ошибка	No applicable scanners for any tunnel found.	04.10.2024, 08:50:45
192.168.80.129	Аудит конфигураций	тест конфигураций	Ошибка	Платформа в конфигурации "Benchmarks\Debian\ALT-X-debian7-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 07:36:40
192.168.80.129	Аудит конфигураций	тест конфигураций	Ошибка	Платформа в конфигурации "Benchmarks\Debian\ALT-X-debian7-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 07:36:36
192.168.80.129	Аудит конфигураций	тест конфигураций	Ошибка	Платформа в конфигурации "Benchmarks\Debian\ALT-X-Debian-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 07:34:11
192.168.80.129	Аудит конфигураций	тест конфигураций	Ошибка	Платформа в конфигурации "Benchmarks\Debian\ALT-X-Debian-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 07:34:08
192.168.80.129	Аудит конфигураций	тест конфигураций	Ошибка	Платформа в конфигурации "Benchmarks\Debian\ALT-X-Debian7-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 07:34:08
192.168.80.129	Аудит конфигураций	тест конфигураций	Ошибка	Платформа в конфигурации "Benchmarks\Debian\ALT-X-Debian7-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 07:34:08
192.168.80.129	Аудит конфигураций	тест конфигураций	Ошибка	Платформа в конфигурации "Benchmarks\Debian\ALT-X-Debian7-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 07:34:07
192.168.80.129	Аудит конфигураций	тест конфигураций	Ошибка	Платформа в конфигурации "Benchmarks\Ubuntu\ALT-X-ubuntu-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 07:34:07
192.168.80.129	Аудит конфигураций	тест конфигураций	Ошибка	Платформа в конфигурации "Benchmarks\Ubuntu\ALT-X-ubuntu-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 07:34:06
192.168.80.129	Аудит конфигураций	тест конфигураций	Ошибка	Платформа в конфигурации "Benchmarks\Debian\ALT-X-Debian-xccdf.xml" не совпадает на хосте "192.168.80.129".	04.10.2024, 07:34:06
192.168.80.129	Инвентаризация	1_1	Хост недоступен	Ошибка аутентификации.	02.10.2024, 08:34:40

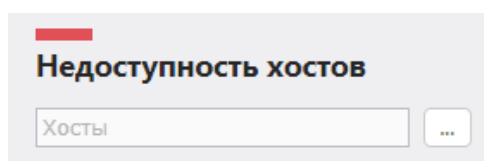
Информация о недоступности хоста включает в себя:


- 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;

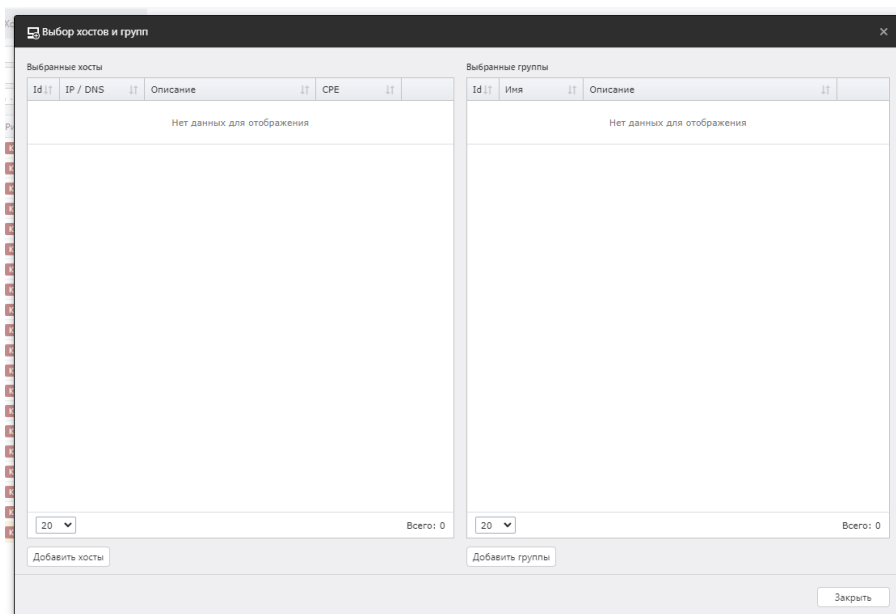
Хост	Тип сканирования	Задание	Результат	Причина
192.168.80.25	Аудит уязвимостей	2008 r2 vulns	Ошибка	.NET
Сканирование		1861		
Хост		192.168.80.25 (Id = 8545)		
Тип сканирования		Аудит уязвимостей		
Задание		2008 r2 vulns		
Результаты сканирования		Ошибка		
Завершение сканирования		09.10.2024, 12:55:39		
Причина неуспешного результата		.NET 4.0 or later is not installed on "192.168.80.25".		

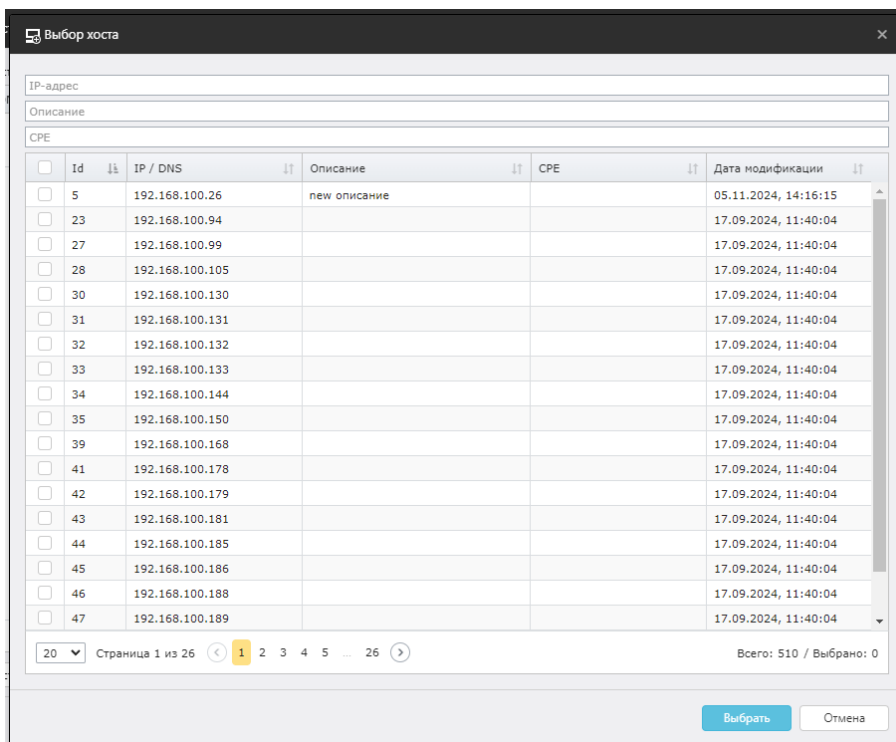
Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

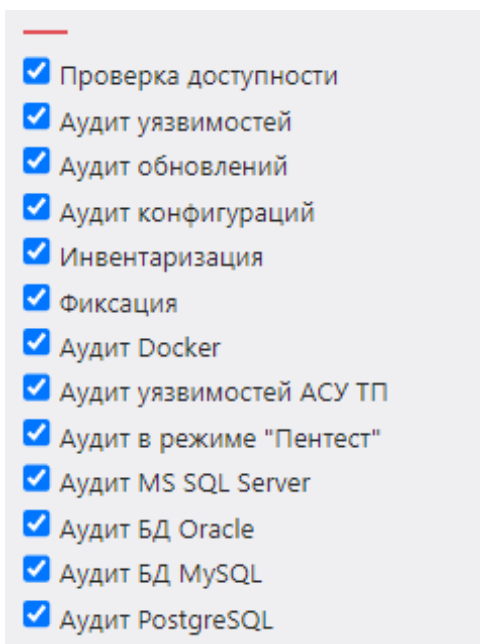


- Хосты – можно выбрать хосты, которые будут отображаться. Нажмите на , после чего откроется окно выбора групп и хостов:



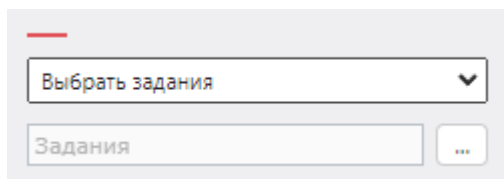


- Типы сканирований, по которым будет производиться поиск причины недоступности хостов;



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

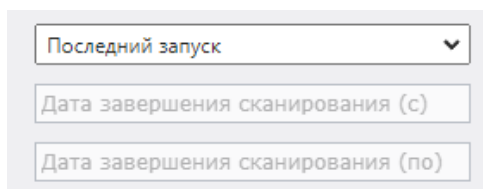
Выбрать задания. Если указать **Выбрать задания**, появится дополнительное поле:



The screenshot shows a light gray panel with a red minus sign in the top left corner. It contains a dropdown menu with the text 'Выбрать задания' and a downward arrow. Below it is a text input field with the text 'Задания' and a three-dot menu icon to its right.

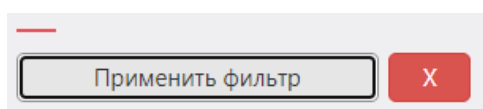
Нажмите на , после чего откроется окно выбора заданий;

- 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.



The screenshot shows a light gray panel with a red minus sign in the top left corner. It contains a dropdown menu with the text 'Последний запуск' and a downward arrow. Below it are two text input fields: 'Дата завершения сканирования (с)' and 'Дата завершения сканирования (по)'. The second field is currently empty.

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



The screenshot shows a light gray panel with a red minus sign in the top left corner. It contains a button with the text 'Применить фильтр' and a red button with a white 'X' icon.

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): " <code><exception name=""TypeException"" > <prop name=""Message"" > </prop> </exception></code> "

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](#)
- [8.3.2 Вкладка Хосты](#)
- [8.3.3 Вкладка Хост – Уязвимость](#)

8.3.1 Вкладка Уязвимости

В данной вкладке отображается информация об уязвимостях, обнаруженных во время сканирования 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 поданной 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 поданной 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 поданной 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 WebMID 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;

ALTX ID	Риск	CVSS	Название	Дата публикации	Количество хостов	Дополнительно
405114	Критический	10	Astra Linux -- уязвимость в chromium (CVE-2022-0289)	12.02.2022	1	Список хостов

ALTX ID	405114														
OVAL	oval:ru.altx-soft.nix:def:188293														
Риск	Критический														
Оценка CVSS	10,0 (BDU)														
Название	Astra Linux -- уязвимость в chromium (CVE-2022-0289)														
Описание	В продукте chromium обнаружена уязвимость CVE-2022-0289.														
Дата публикации	12.02.2022														
Ссылки	<table border="1"> <tr> <td>NKCKI</td> <td>VULN-20220124.25</td> </tr> <tr> <td>FSTEC</td> <td>BDU:2022-00867</td> </tr> <tr> <td>VENDOR</td> <td>20220829SE16</td> </tr> <tr> <td>packetstormsecurity</td> <td>Chrome-safe_browsing-ThreatDetails-OnReceivedThreatDOMDetails-Use-After-Free</td> </tr> <tr> <td>NKCKI</td> <td>VULN-20220124.26</td> </tr> <tr> <td>VENDOR</td> <td>2022-0819SE17</td> </tr> <tr> <td>CVE</td> <td>CVE-2022-0289</td> </tr> </table>	NKCKI	VULN-20220124.25	FSTEC	BDU:2022-00867	VENDOR	20220829SE16	packetstormsecurity	Chrome-safe_browsing-ThreatDetails-OnReceivedThreatDOMDetails-Use-After-Free	NKCKI	VULN-20220124.26	VENDOR	2022-0819SE17	CVE	CVE-2022-0289
NKCKI	VULN-20220124.25														
FSTEC	BDU:2022-00867														
VENDOR	20220829SE16														
packetstormsecurity	Chrome-safe_browsing-ThreatDetails-OnReceivedThreatDOMDetails-Use-After-Free														
NKCKI	VULN-20220124.26														
VENDOR	2022-0819SE17														
CVE	CVE-2022-0289														

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

Уязвимости Хосты **Хост - Уязвимость**

Хост: Найдено хостов: Критический (1) Высокий (0) Средний (0)

Низкий (0) Не определено (0)

Название:

516497

Ссылка (CVE, BDU, ...):

Найдено уникальных уязвимостей: 1

Хост	ALTX ID	Риск	CVSS	Название	Дата публикации
192.168.80.32	516497	Критический	9.9	RED OS -- уязвимость в ghostscript (CVE-2021-3781)	16.02.2022

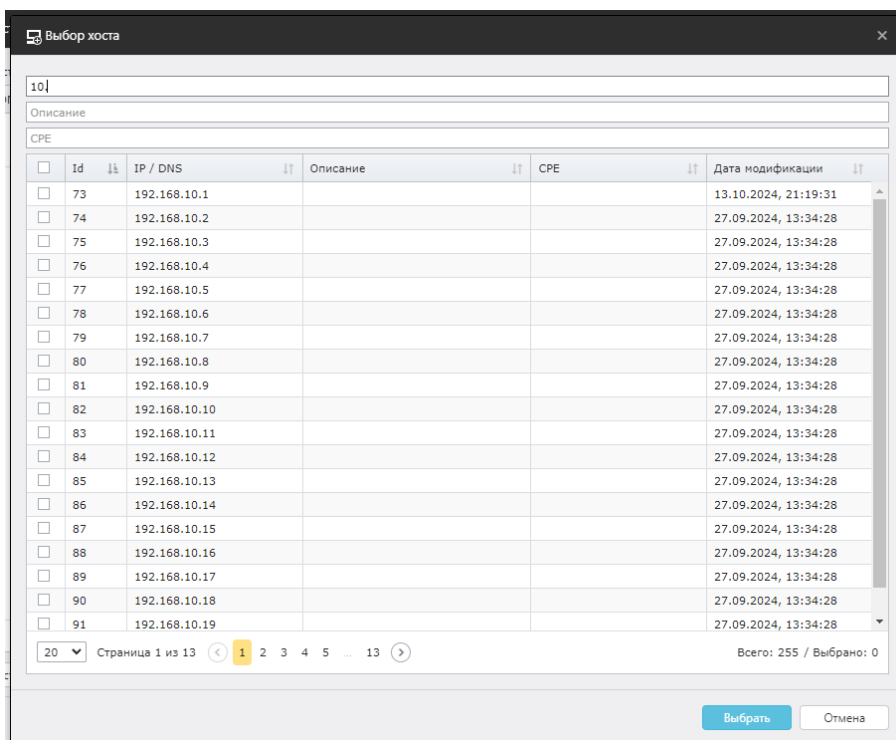
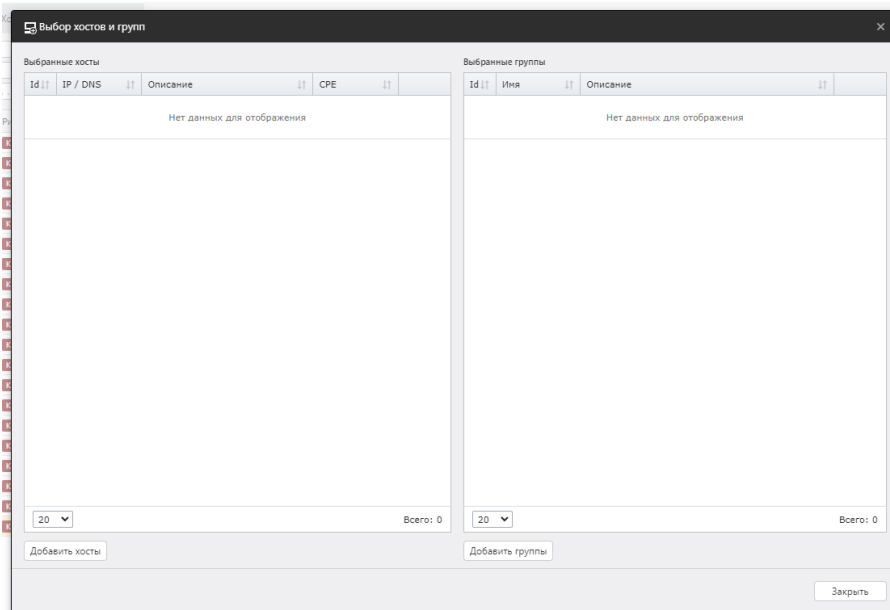
Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

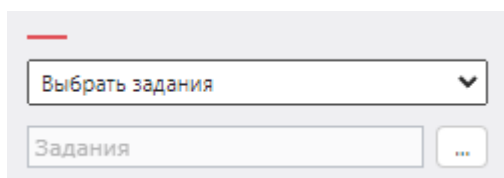
Анализ уязвимостей

Хосты

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

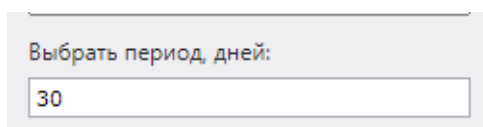


- **Задания** – можно выбрать задания, из результатов сканирования которых будет производиться поиск уязвимостей. Учитываются результаты сканирования со статусом **Завершено**. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится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

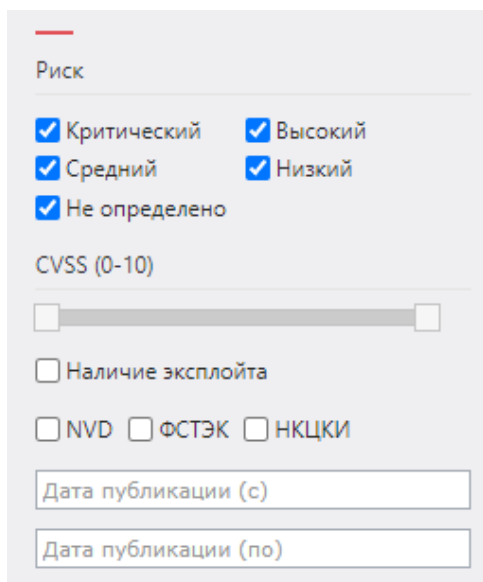


Нажмите на , после чего откроется окно выбора заданий;

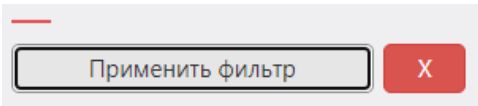
- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для поиска уязвимостей;



- 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.



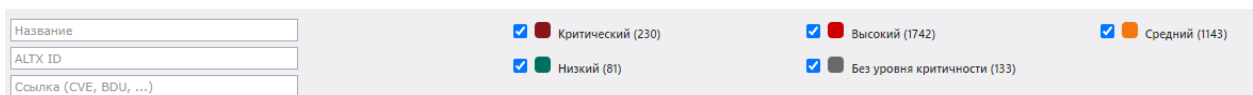
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



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
<p>ALTX ID, Количество хостов, Хосты, OVAL определение, Уровень критичности, Оценка CVSS, Источник CVSS, Уязвимость, Описание, Дата публикации</p> <p>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</p>

8.3.2 Вкладка Хосты

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

Хост	Всего уязвимостей	Уровни риска	Дополнительно
192.168.80.129	1430	71 652 559 26 132	Список уязвимостей

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;

Хост	Всего уязвимостей	Уровни риска	Дополнительно
192.168.80.32	729	23 261 418 17 18	Список уязвимостей
Id хоста 8606			
Имя хоста 192.168.80.32			
ID сканирования 1871			
Дата сканирования 23.10.2024 08:33:51			

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

Уязвимости Хосты **Хост - Уязвимость**

192.168.80.8

Найдено хостов: 1

Название

ALTX ID

Ссылка (CVE, BDU, ...)

Найдено уникальных уязвимостей: 3312

Критический (228) Высокий (1731) Средний (1139) Экспорт в CSV

Низкий (81) Не определено (133)

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

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.

Хосты без данных о проведённых сканированиях

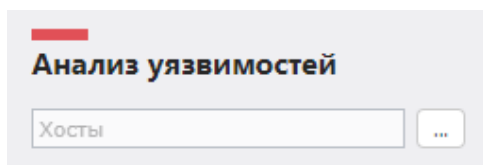
Id хоста	Хост
221	192.168.10.149
222	192.168.10.150
223	192.168.10.151
224	192.168.10.152
225	192.168.10.153
226	192.168.10.154
227	192.168.10.155
228	192.168.10.156
229	192.168.10.157
230	192.168.10.158
231	192.168.10.159
232	192.168.10.160
233	192.168.10.161
234	192.168.10.162
235	192.168.10.163
236	192.168.10.164
237	192.168.10.165
238	192.168.10.166
239	192.168.10.167


50 Страница 5 из 10 Всего: 497

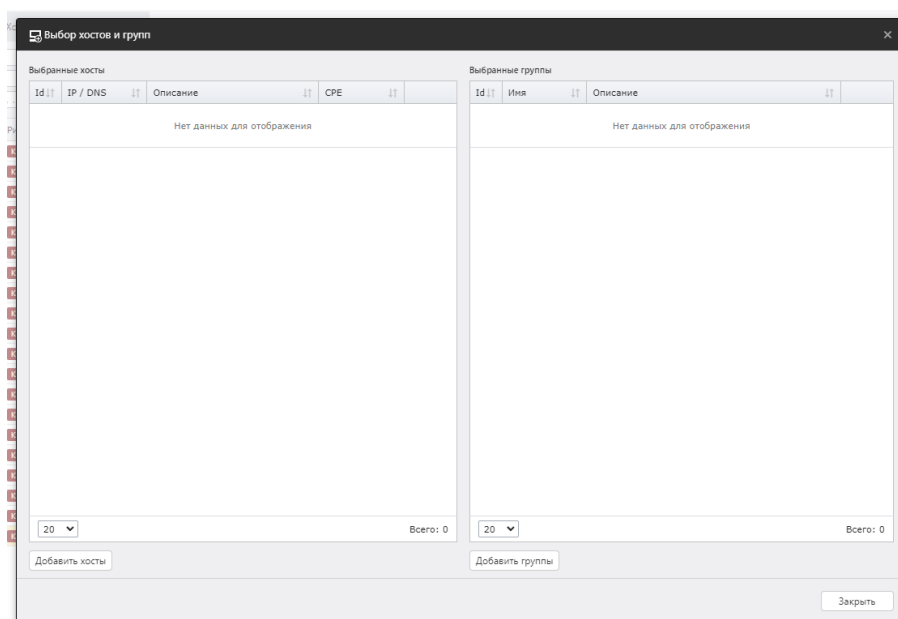
Закрыть

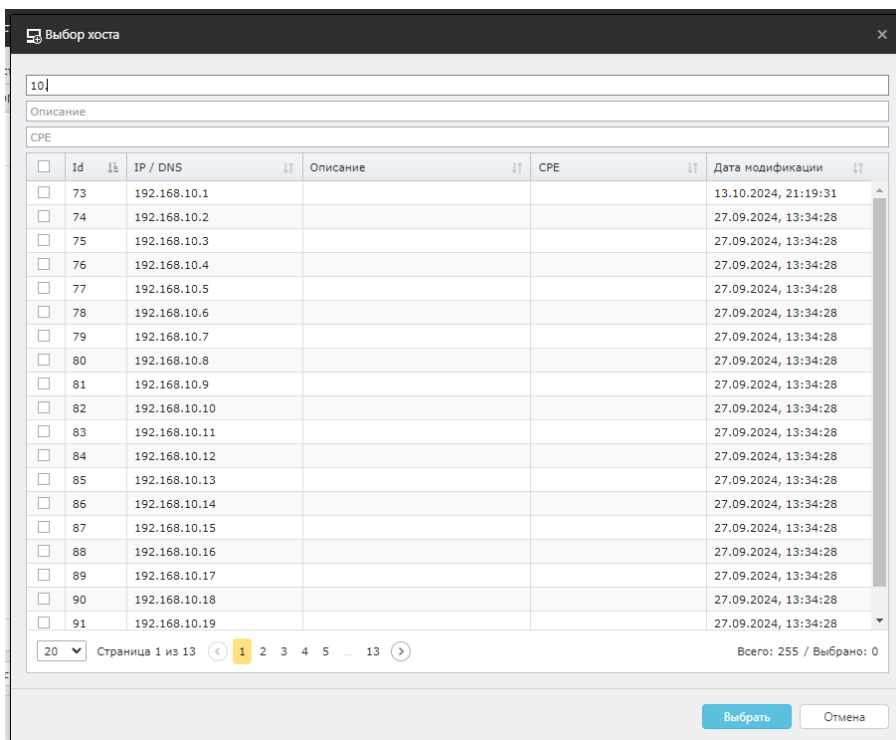
Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

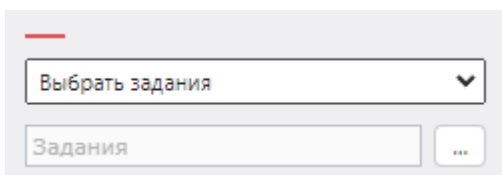


- Хосты – можно выбрать хосты, уязвимости для которых будут отображаться. Нажмите на , после чего откроется окно выбора групп и хостов;





- **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.

Хост	Всего уязвимостей	Среди них критических и высоких	Дополнительно
> 192.168.80.8	3312	228 1731	Список уязвимостей
> 192.168.80.129	1430	71 692	Список уязвимостей
> 192.168.80.32	729	23 261	Список уязвимостей

Нет данных для отображения

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-yyuu.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
<p>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</p> <p>67,192.168.80.129,123,,1430,71,652,549,26,132,1862,14.10.2024 12:45:37</p>

8.3.3 Вкладка Хост – Уязвимость

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

Хост	ALTIX ID	Риск	CVSS	Название	Дата публикации
192.168.80.8	375267	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	383924	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:

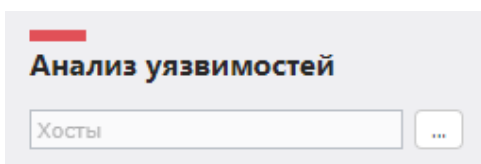
- ID последнего сканирования со статусом Завершено, в котором была обнаружена данная уязвимость;
- IP-адрес или DNS имя хоста и ID хоста, на котором обнаружена уязвимость;
- Уникальный идентификатор ALTIX ID;
- Ссылка на страницу уязвимости в OVALdb;
- Риск и CVSS – Сведения об интегральной оценке по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

Хост	ALTX ID	Риск	CVSS	Название	Дата публикации
192.168.80.129	429217	Критический	10	Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)	07.12.2022

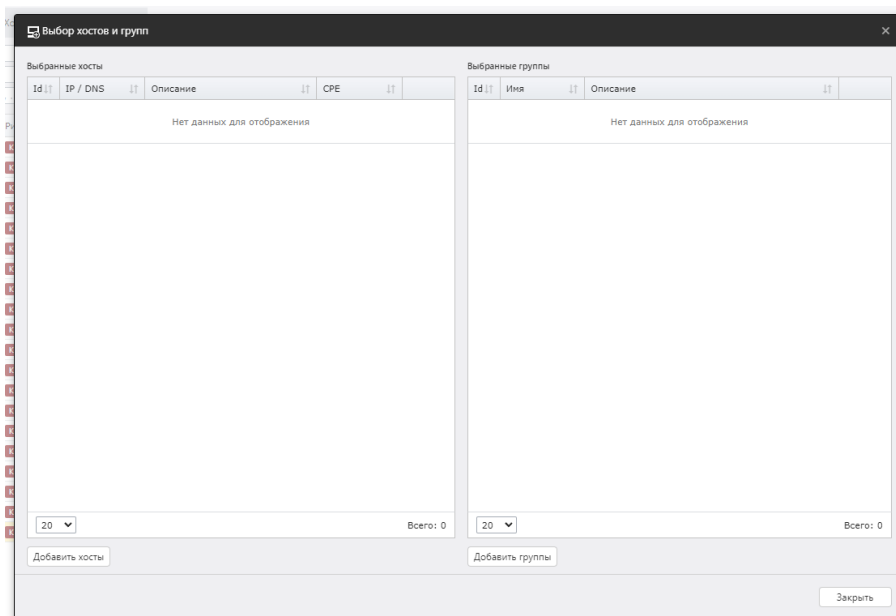
ID сканирования	1862										
Хост	192.168.80.129 (Id = 67)										
ALTX ID	429217										
OVAL	oval:ru.altx-soft.nlx:def:207605										
Риск	Критический										
Оценка CVSS	10 (BDU)										
Название	Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)										
Описание	В продуктах linux, linux-5.10, linux-5.15 обнаружена уязвимость CVE-2022-3643.										
Дата публикации	07.12.2022										
Ссылки	<table border="1"> <tr> <td>CVE</td> <td>CVE-2022-3643</td> </tr> <tr> <td>VENDOR</td> <td>2023-0303SE17MD</td> </tr> <tr> <td>VENDOR</td> <td>2.12.46</td> </tr> <tr> <td>FSTEC</td> <td>BDU:2023-00265</td> </tr> <tr> <td>VENDOR</td> <td>2023-1023SE17</td> </tr> </table>	CVE	CVE-2022-3643	VENDOR	2023-0303SE17MD	VENDOR	2.12.46	FSTEC	BDU:2023-00265	VENDOR	2023-1023SE17
CVE	CVE-2022-3643										
VENDOR	2023-0303SE17MD										
VENDOR	2.12.46										
FSTEC	BDU:2023-00265										
VENDOR	2023-1023SE17										
Детализация	<table border="1"> <tr> <td>linux-image-5.4-generic (0:5.4.0-54astra7+c157)</td> </tr> <tr> <td>linux-image-5.4.0-110-generic (0:5.4.0-110.astra35+c194)</td> </tr> <tr> <td>linux-image-5.4.0-54-generic (0:5.4.0-54.astra31+c149)</td> </tr> </table>	linux-image-5.4-generic (0:5.4.0-54astra7+c157)	linux-image-5.4.0-110-generic (0:5.4.0-110.astra35+c194)	linux-image-5.4.0-54-generic (0:5.4.0-54.astra31+c149)							
linux-image-5.4-generic (0:5.4.0-54astra7+c157)											
linux-image-5.4.0-110-generic (0:5.4.0-110.astra35+c194)											
linux-image-5.4.0-54-generic (0:5.4.0-54.astra31+c149)											

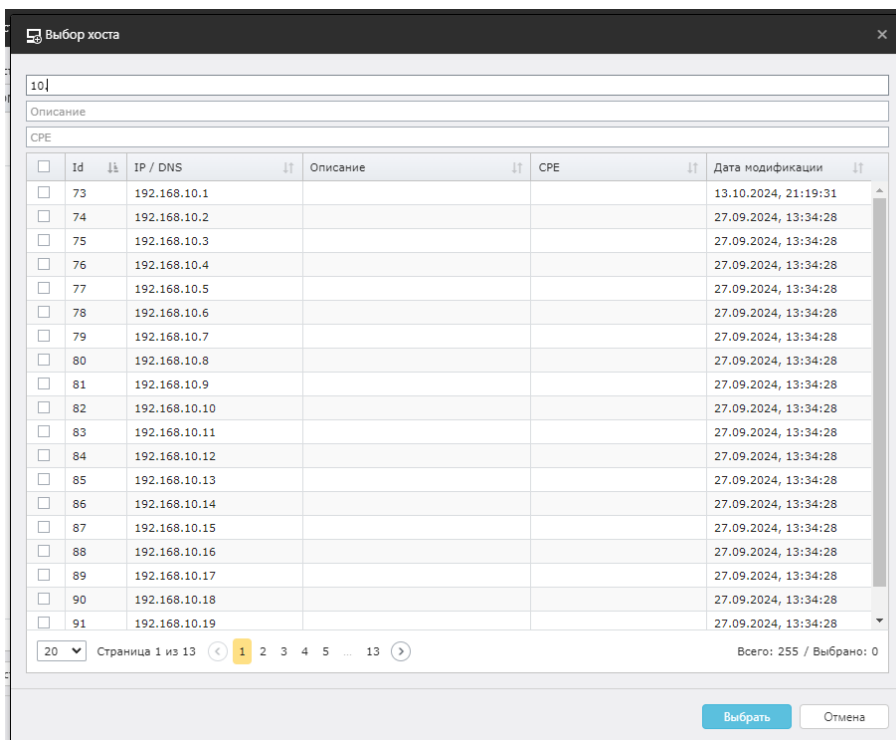
Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

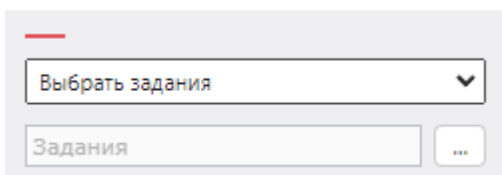


- Хосты – можно выбрать хосты, уязвимости для которых будут отображаться. Нажмите на ..., после чего откроется окно выбора групп и хостов;





- **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.

The screenshot shows a search interface with the following elements:

- Navigation tabs: Уязвимости, Хосты, **Хост - Уязвимость** (selected).
- Search input: 192.168.80.8. Below it: Найдено хостов: 1.
- Filters:
 - Название
 - ALTX ID
 - Ссылка (CVE, BDU, ...)
- Statistics:
 - Высокий (1731) [checked]
 - Средний (1139) [checked]
 - Низкий (81) [checked]
 - Не определено (133) [checked]
- Summary: Найдено уникальных уязвимостей: 3084

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](#)
- [8.4.2 Вкладка Хосты](#)
- [8.4.3 Вкладка Хост – Уязвимость](#)

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.

ALTX ID	Риск	CVSS	Название	Дата публикации	Новая для хостов	Неустраненная для хостов	Устраненная для хостов	Дополнительно
> 429217	Критический	10	Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)	07.12.2022	0	1	0	Список хостов
> 443348	Критический	10	Astra Linux -- уязвимость в thunderbird, firefox (CVE-2019-25136)	19.06.2023	0	1	0	Список хостов
> 464442	Критический	10	Astra Linux -- уязвимость в firefox (CVE-2022-46884)	24.08.2023	0	1	0	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	0	1	0	Список хостов
> 531743	Критический	10	Astra Linux -- уязвимость в chromium (CVE-2024-2883)	26.03.2024	0	1	0	Список хостов
> 410680	Критический	9.8	Astra Linux -- уязвимость в python2.7 (CVE-2015-20107)	13.04.2022	0	1	0	Список хостов
> 413840	Критический	9.8	Astra Linux -- уязвимость в linux, linux-5.10 (CVE-2022-20368)	11.08.2022	0	1	0	Список хостов
> 414003	Критический	9.8	Astra Linux -- уязвимость в linux-5.10, linux-5.15, linux (CVE-2022-39842)	05.09.2022	0	1	0	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	0	1	0	Список хостов
> 425334	Критический	9.8	Доступ за пределами памяти в WebPnD в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1529)	21.03.2023	0	1	0	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	0	1	0	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	0	1	0	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	0	1	0	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	0	1	0	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	0	1	0	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	0	1	0	Список хостов
> 443421	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-1528)	21.03.2023	0	1	0	Список хостов
> 443422	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-1529)	21.03.2023	0	1	0	Список хостов
> 443443	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-2033)	14.04.2023	0	1	0	Список хостов
> 443448	Критический	9.8	Astra Linux -- уязвимость в chromium (CVE-2023-2136)	19.04.2023	0	1	0	Список хостов

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;

ALTX ID	Риск	CVSS	Название	Дата публикации	Новая для хостов	Неустраненная для хостов	Устраненная для хостов	Дополнительно
429217	Критический	10	Astra Linux -- уязвимость в llinux, llinux-5.10, llinux-5.15 (CVE-2022-3643)	07.12.2022	0	1	0	Список хостов

ALTX ID	429217										
OVAL											
Риск	Критический										
Оценка CVSS	10,0 (BDU)										
Название	Astra Linux -- уязвимость в llinux, llinux-5.10, llinux-5.15 (CVE-2022-3643)										
Описание	В продуктах llinux, llinux-5.10, llinux-5.15 обнаружена уязвимость CVE-2022-3643.										
Дата публикации	07.12.2022										
Ссылки	<table border="0"> <tr> <td>VENDOR</td> <td>2023-1023SE17</td> </tr> <tr> <td>VENDOR</td> <td>2.12.46</td> </tr> <tr> <td>FSTEC</td> <td>BDU:2023-00265</td> </tr> <tr> <td>CVE</td> <td>CVE-2022-3643</td> </tr> <tr> <td>VENDOR</td> <td>2023-0303SE17MD</td> </tr> </table>	VENDOR	2023-1023SE17	VENDOR	2.12.46	FSTEC	BDU:2023-00265	CVE	CVE-2022-3643	VENDOR	2023-0303SE17MD
VENDOR	2023-1023SE17										
VENDOR	2.12.46										
FSTEC	BDU:2023-00265										
CVE	CVE-2022-3643										
VENDOR	2023-0303SE17MD										

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.

The screenshot shows the REDCheck interface with the following details:

- Navigation:** Главная, Хосты, Задачи, История, Контроль, Отчеты, Пользователи.
- Control Panel:**
 - Уязвимости: Хосты, Хост - Уязвимость (Активно)
 - Найдено хостов: 2
 - Название: 76123
 - Ссылка (CVE, BDU): Найдено уникальных уязвимостей: 1
 - Статусы: Новые уязвимости (Хостов: 0), Неустраненные уязвимости (Хостов: 1), Устраненные уязвимости (Хостов: 1)
 - Экспорт в CSV
- Table:**

Хост	ALTX ID	Статус уязвимости	Риск	CVSS	Название	Дата публикации
192.168.10.250	76123	Неустраненная	Критический	10	Неопределенная уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-2590)	16.07.2015
192.168.10.36	76123	Устраненная	Критический	10	Неопределенная уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-2590)	16.07.2015
- Filters (Left):**
 - Сравнить с предыдущими результатами
 - Выбор сканирования
 - Выбор периода, дней: 30
 - Хосты
 - Риск: Критический, Высокий, Средний, Низкий, Не определено
 - CVSS (0-10): [Slider]
 - Наличие эксплойта
 - NVD, ФСТЭК, НКДКИ
 - Дата публикации (с), Дата публикации (по)
 - Применить фильтр
- Page Info:** 20, Страница 1 из 1, Всего: 2

Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

Контроль устранения уязвимостей

Задание

Актуальное сканирование

- 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**);

Выбор задания

Имя

№	Имя	Тип сканирования	P	Время завершения	Всего	Успешно
89	1_16	Аудит уязвимостей	По требованию	18.10.2024, 09:43:26	3	3
22	1_7	Аудит уязвимостей	По требованию	03.10.2024, 12:20:09	2	2

20 Страница 1 из 1 1 Всего: 2

Выбрать Отмена

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

ID	Задание	Начало	Завершение	Всего хостов	Успешно просканировано
111	1_16	18.10.2024, 12:41:54	18.10.2024, 12:43:26	1	1
108	1_16	14.10.2024, 15:44:09	14.10.2024, 15:45:40	1	1
104	1_16	09.10.2024, 11:09:23	09.10.2024, 11:10:37	1	1

20 | Страница 1 из 1 | 1 | Всего: 3

Выбрать | Отмена

- 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;

Сравнить с предыдущими результатами

Выбрать сканирование

Выбрать период, дней:

30

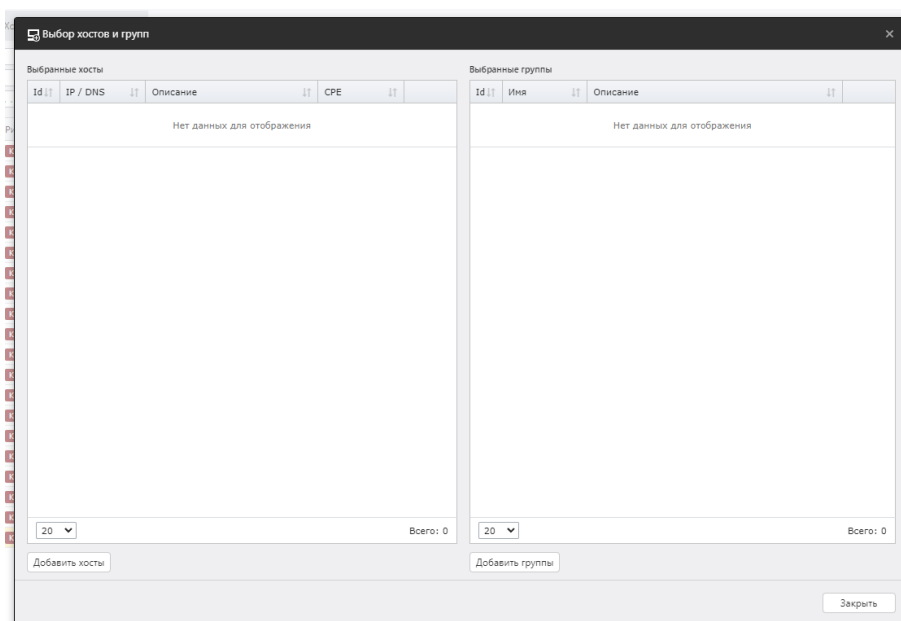
- Выбрать сканирование – сравнение выбранной выше итерации будет проходить с одной конкретной итерацией запуска для выбранного задания;

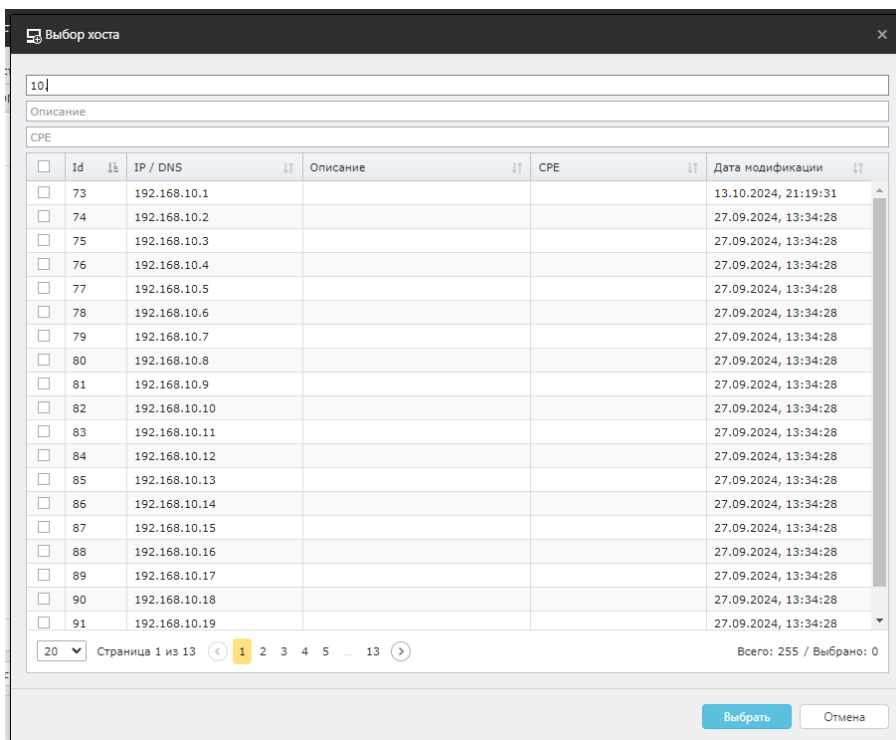
Сравнить с предыдущими результатами

Выбрать сканирование

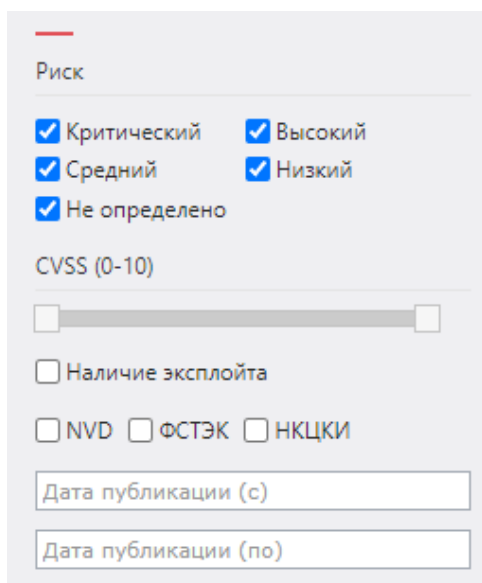
Старое сканирование

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

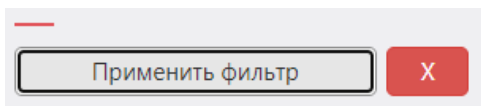




- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; [Сведения об интегральной оценке по базовым метрикам CVSS](#);
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;
- Дата публикации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



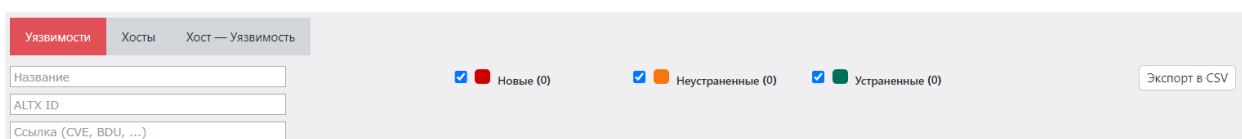
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



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);
 - Неустранимые – уязвимости, которые были найдены в предыдущих сканированиях и остались неустранимыми 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)
Неустранимая для хостов	Количество хостов, для которых данная уязвимость была найдены в предыдущих сканированиях и осталась неустранимой 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.

Хост	Новые уязвимости	Среди них критических и высоких	Неустраненные уязвимости	Среди них критических и высоких	Устраненные уязвимости	Среди них критических и высоких	Дополнительно
192.168.80.129	0		1430	71	652	0	Список уязвимостей

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.

The screenshot shows the 'Уязвимости' (Vulnerabilities) section for a specific host. The table contains the following data:

Хост	ALT ID	Статус уязвимости	Риск	CVSS	Название	Дата публикации
192.168.10.250	76123	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-2590)	16.07.2015
192.168.10.250	76136	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-2628)	16.07.2015
192.168.10.250	76140	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 + JavaFX 2.2.80 (CVE-2015-2638)	16.07.2015
192.168.10.250	76229	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-4731)	16.07.2015
192.168.10.250	76230	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 + 8u33 (CVE-2015-4732)	16.07.2015
192.168.10.250	76231	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 + 8u33 (CVE-2015-4733)	16.07.2015
192.168.10.250	76239	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-4760)	16.07.2015
192.168.10.250	84117	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4805)	21.10.2015
192.168.10.250	84131	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4835)	21.10.2015
192.168.10.250	84138	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4843)	21.10.2015
192.168.10.250	84140	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4844)	21.10.2015
192.168.10.250	84145	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4860)	21.10.2015
192.168.10.250	84161	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4881)	21.10.2015
192.168.10.250	84165	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4883)	21.10.2015
192.168.10.250	124156	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u105, 7u91, и 8u66 (CVE-2016-0494)	21.01.2016
192.168.10.250	124586	Устранена	Критический	10	Неопределённая уязвимость в Java SE, и JRockit компонентах в Oracle Java SE 6u105, 7u91 и 8u66 и JRockit R28.3.8 (CVE-2016-0493)	21.01.2016
192.168.10.250	141437	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u113, 7u99, и 8u77 (CVE-2016-0686)	21.04.2016
192.168.10.250	141439	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u113, 7u99, и 8u77 (CVE-2016-0687)	21.04.2016
192.168.10.250	141459	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u113, 7u99, и 8u77; JRockit R28.3.9 (CVE-2016-3427)	21.04.2016
192.168.10.250	141463	Устранена	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u113, 7u99, и 8u77 (CVE-2016-3443)	21.04.2016

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

The summary table shows the following data:

Хост	Новые уязвимости	Среди них критических и высоких	Неустранённые уязвимости	Среди них критических и высоких	Устранённые уязвимости	Среди них критических и высоких	Дополнительно
192.168.10.89	0		2359	801 352	0		Список уязвимостей
192.168.10.80	32	7 15	619	27 47	0		Список уязвимостей
192.168.10.78	0		124	310	511	9 368	Список уязвимостей
192.168.10.42	0		3277	68 209	4	1 1	Список уязвимостей
192.168.10.36	0		568	81 129	1	2	Список уязвимостей
192.168.10.250	0		846	87 136	1	1	Список уязвимостей

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

The table shows the following data:

Хост	Тип сканирования	Задача	Результат	Причина недоступности	Время завершения
192.168.10.99	Аудит уязвимостей	уязвимости windows агент новая задача	Хост недоступен	Агент не найден или не запущен.	16.10.2024, 13:39:56

Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

Контроль устранения уязвимостей

Задание

Актуальное сканирование

- 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**);

Выбор задания

Имя

№	Имя	Тип сканирования	Р	Время завершения	Всего	Успешно
89	1_16	Аудит уязвимостей	По требованию	18.10.2024, 09:43:26	3	3
22	1_7	Аудит уязвимостей	По требованию	03.10.2024, 12:20:09	2	2

20 Страница 1 из 1 1 Всего: 2

Выбрать Отмена

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

ID	Задание	Начало	Завершение	Всего хостов	Успешно просканировано
111	1_16	18.10.2024, 12:41:54	18.10.2024, 12:43:26	1	1
108	1_16	14.10.2024, 15:44:09	14.10.2024, 15:45:40	1	1
104	1_16	09.10.2024, 11:09:23	09.10.2024, 11:10:37	1	1

20 | Страница 1 из 1 | 1 | Всего: 3

Выбрать | Отмена

- 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;;

Сравнить с предыдущими результатами

Выбрать сканирование

Выбрать период, дней:

30

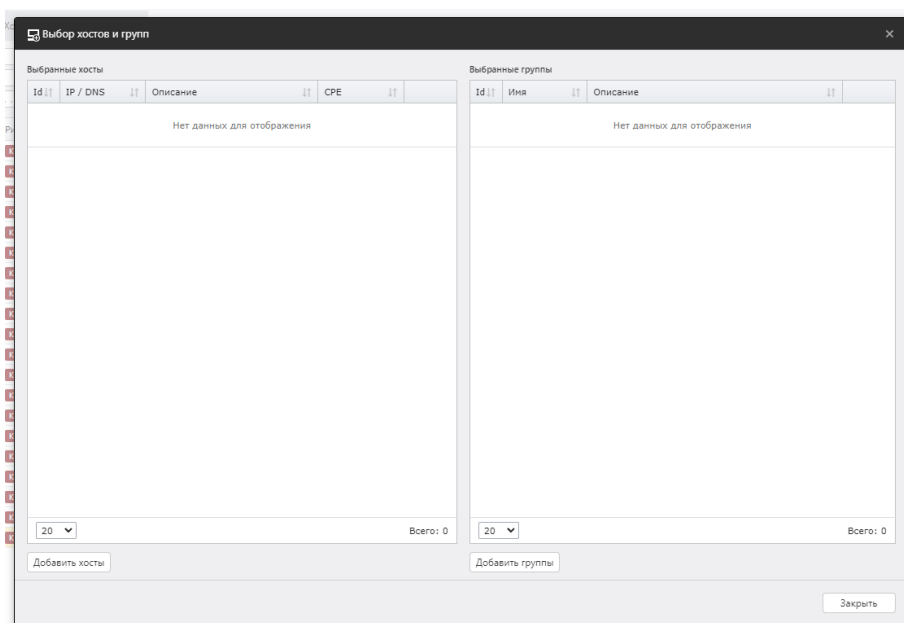
- Выбрать сканирование – сравнение выбранной выше итерации будет проходить с одной конкретной итерацией запуска для выбранного задания;

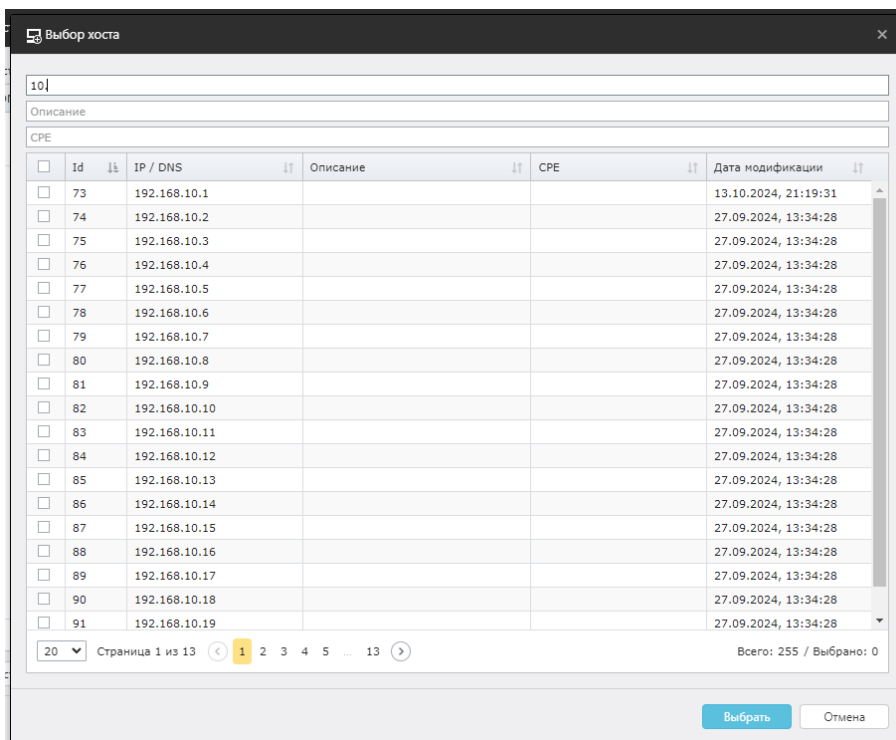
Сравнить с предыдущими результатами

Выбрать сканирование

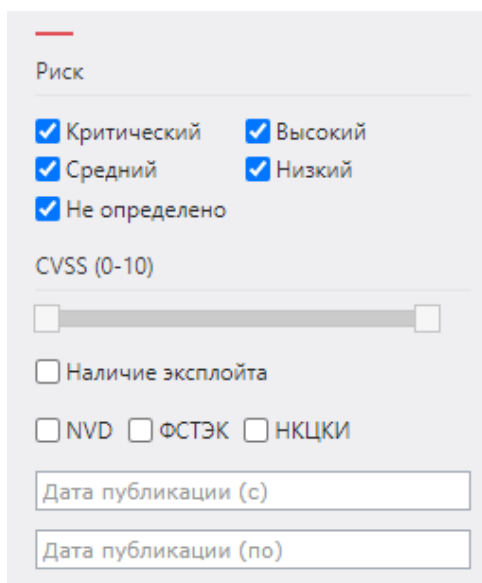
Старое сканирование

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

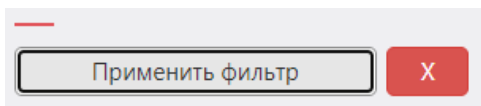




- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; [Сведения об интегральной оценке по базовым метрикам CVSS](#);
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;
- Дата публикации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



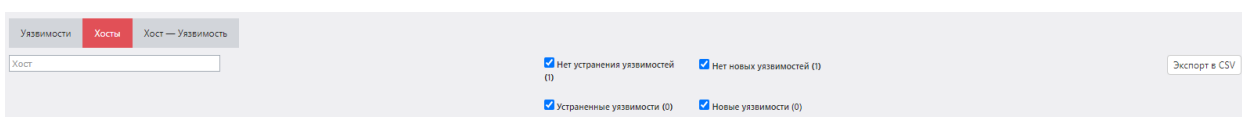
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



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
Неустранимые уязвимости	Количество неустранимых уязвимостей
Неустранимые критические уязвимости	Количество неустранимых уязвимостей с критическим риском
Неустранимые уязвимости с высоким уровнем критичности	Количество неустранимых уязвимостей с высоким риском
Устраненные уязвимости	Количество устраненных уязвимостей
Устранённые критические 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,Неустранимые  
уязвимости,Неустранимые критические уязвимости,Неустранимые  
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 подной тип 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 подной тип 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 подной тип 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;

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

Хост	192.168.80.129 (Id = 67)
ALTX ID	429217
OVAL	oval:ru.altx-soft.nix:def:207605
Риск	Критический
Оценка CVSS	10,0 (BDU)
Название	Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)
Описание	В продуктах linux, linux-5.10, linux-5.15 обнаружена уязвимость CVE-2022-3643.
Дата публикации	07.12.2022
Ссылки	VENDOR 2023-10235E17 VENDOR 2.12.46 FSTEC BDU:2023-00265 CVE CVE-2022-3643 VENDOR 2023-03035E17MD
Детализация	linux-image-5.4-generic (0:5.4.0-54astra7+c57) linux-image-5.4.0-54-generic (0:5.4.0-54.astra31+c49) linux-image-5.4.0-110-generic (0:5.4.0-110.astra35+c194)

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

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

Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

Контроль устранения уязвимостей

Задание ...

Актуальное сканирование ...

- 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**);

Выбор задания

Имя

№	Имя	Тип сканирования	P	Время завершения	Всего	Успешно
89	1_16	Аудит уязвимостей	По требованию	18.10.2024, 09:43:26	3	3
22	1_7	Аудит уязвимостей	По требованию	03.10.2024, 12:20:09	2	2

20 Страница 1 из 1 1 Всего: 2

Выбрать Отмена

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

ID	Задание	Начало	Завершение	Всего хостов	Успешно просканировано
111	1_16	18.10.2024, 12:41:54	18.10.2024, 12:43:26	1	1
108	1_16	14.10.2024, 15:44:09	14.10.2024, 15:45:40	1	1
104	1_16	09.10.2024, 11:09:23	09.10.2024, 11:10:37	1	1

20 | Страница 1 из 1 | 1 | Всего: 3

Выбрать | Отмена

- 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;;

Сравнить с предыдущими результатами

Выбрать сканирование

Выбрать период, дней:

30

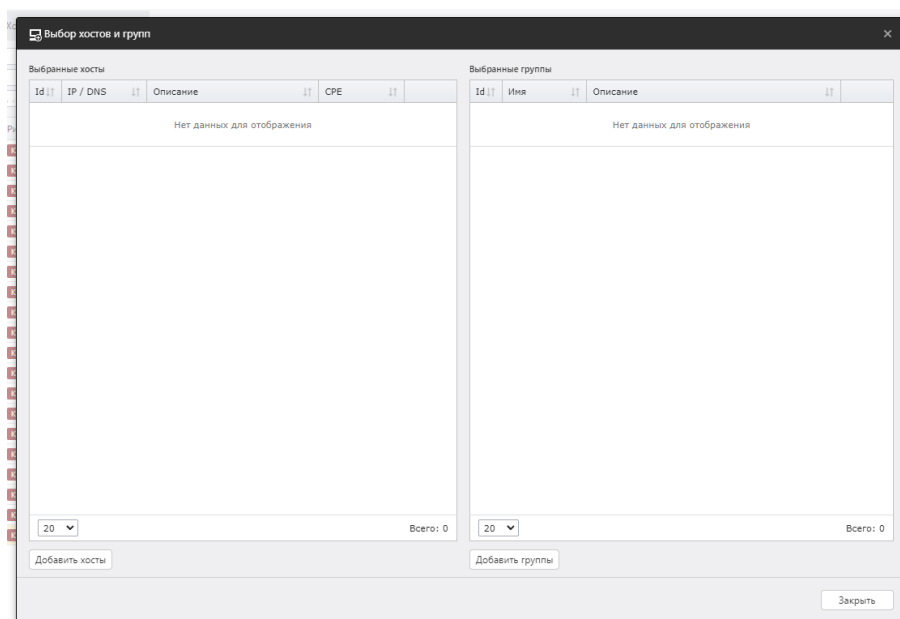
- Выбрать сканирование – сравнение выбранной выше итерации будет проходить с одной конкретной итерацией запуска для выбранного задания;

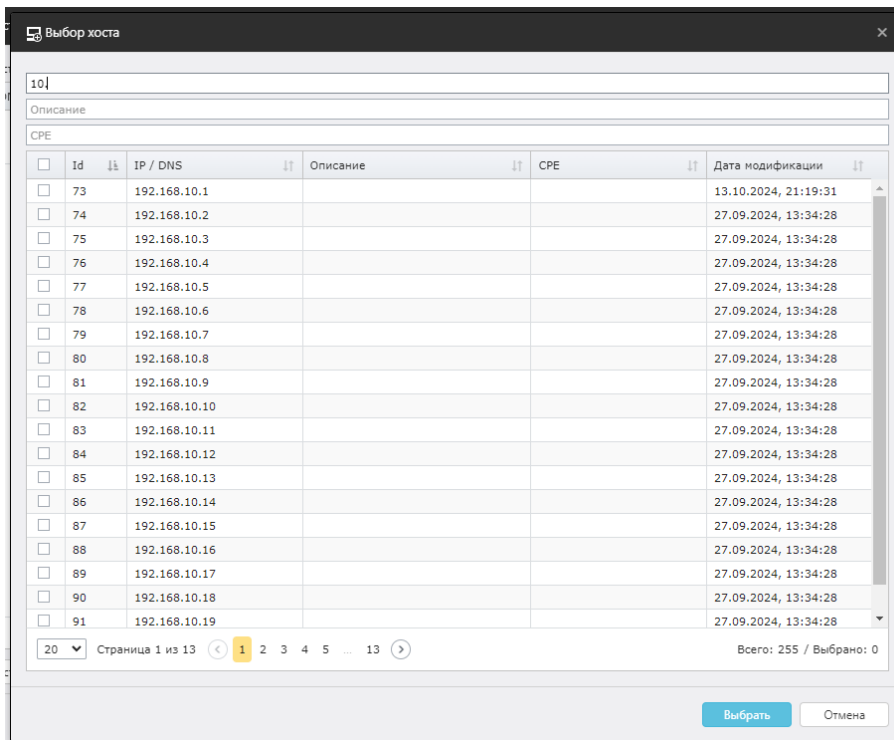
Сравнить с предыдущими результатами

Выбрать сканирование

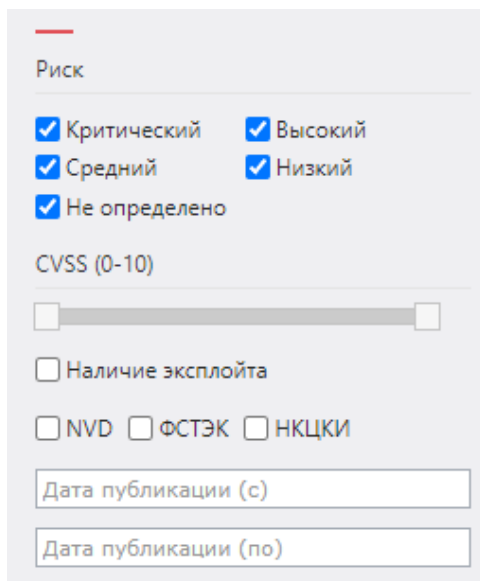
Старое сканирование

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

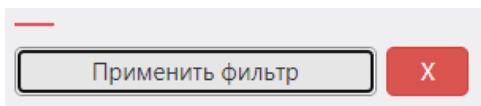




- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; [Сведения об интегральной оценке по базовым метрикам CVSS](#);
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;
- Дата публикации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



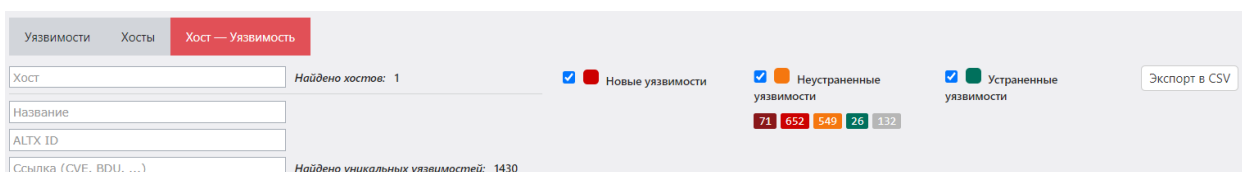
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



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

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,Неустранимая,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+astral);thunderbird-locale-ru
(1:102.9.1+build1-0ubuntu1+ci202304061128+astral)
```

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.

Контроль устранения уязвимостей

уязвимости windows agent новая
07.11.2024, 10:31:20 - 07.11.2024

Сравнить с предыдущими результатами
Выбор сканирование
Выбор период дней: 30

Хосты: [76123]

Риск:
 Критический Высокий
 Средний Низкий
 Не определено

CVSS (0-10): [10]

Наличие эксплойта
 NVD ФСТЭК НКЦКИ

Дата публикации (с):
Дата публикации (по):

Применить фильтр

Хост	ALTJ ID	Статус уязвимости	Риск	CVSS	Название	Дата публикации
192.168.10.250	76123	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-2590)	16.07.2015
192.168.10.36	76123	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-2590)	16.07.2015

Страница 1 из 1

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.

Контроль устранения уязвимостей

уязвимости windows agent новая
07.11.2024, 10:31:20 - 07.11.2024

Сравнить с предыдущими результатами
Выбор сканирование
Выбор период дней: 30

Хосты: [254]

Риск:
 Критический Высокий
 Средний Низкий
 Не определено

CVSS (0-10): [10]

Наличие эксплойта
 NVD ФСТЭК НКЦКИ

Дата публикации (с):
Дата публикации (по):

Применить фильтр

Хост	ALTJ ID	Статус уязвимости	Риск	CVSS	Название	Дата публикации
192.168.10.250	76123	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-2590)	16.07.2015
192.168.10.250	76136	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-2628)	16.07.2015
192.168.10.250	76140	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, 8u45 и JavaFX 2.2.80 (CVE-2015-2638)	16.07.2015
192.168.10.250	76229	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-4731)	16.07.2015
192.168.10.250	76230	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, 8u45 и 8u33 (CVE-2015-4732)	16.07.2015
192.168.10.250	76231	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, 8u45 и 8u33 (CVE-2015-4733)	16.07.2015
192.168.10.250	76239	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u95, 7u80, и 8u45 (CVE-2015-4760)	16.07.2015
192.168.10.250	84117	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4805)	21.10.2015
192.168.10.250	84131	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4835)	21.10.2015
192.168.10.250	84138	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4843)	21.10.2015
192.168.10.250	84140	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4844)	21.10.2015
192.168.10.250	84145	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4860)	21.10.2015
192.168.10.250	84161	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4881)	21.10.2015
192.168.10.250	84165	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u101, 7u85, и 8u60 (CVE-2015-4883)	21.10.2015
192.168.10.250	124586	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u105, 7u91, и 8u66 (CVE-2016-0494)	21.01.2016
192.168.10.250	124586	Устранено	Критический	10	Неопределённая уязвимость в Java SE, и JRockit компоненты в Oracle Java SE 6u105, 7u91 и 8u66 и JRockit R26.3.8 (CVE-2016-0493)	21.01.2016
192.168.10.250	141437	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u113, 7u99, и 8u77 (CVE-2016-0696)	21.04.2016
192.168.10.250	141439	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u113, 7u99, и 8u77 (CVE-2016-0687)	21.04.2016
192.168.10.250	141459	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u113, 7u99 и 8u77, JRockit R26.3.9 (CVE-2016-3427)	21.04.2016
192.168.10.250	141463	Устранено	Критический	10	Неопределённая уязвимость в Oracle Java SE 6u113, 7u99, и 8u77 (CVE-2016-3443)	21.04.2016

Страница 1 из 44

8.5 Анализ конфигураций

Данная форма аналитики позволяет оценить соответствие инфраструктуры правилам выбранной конфигурации.

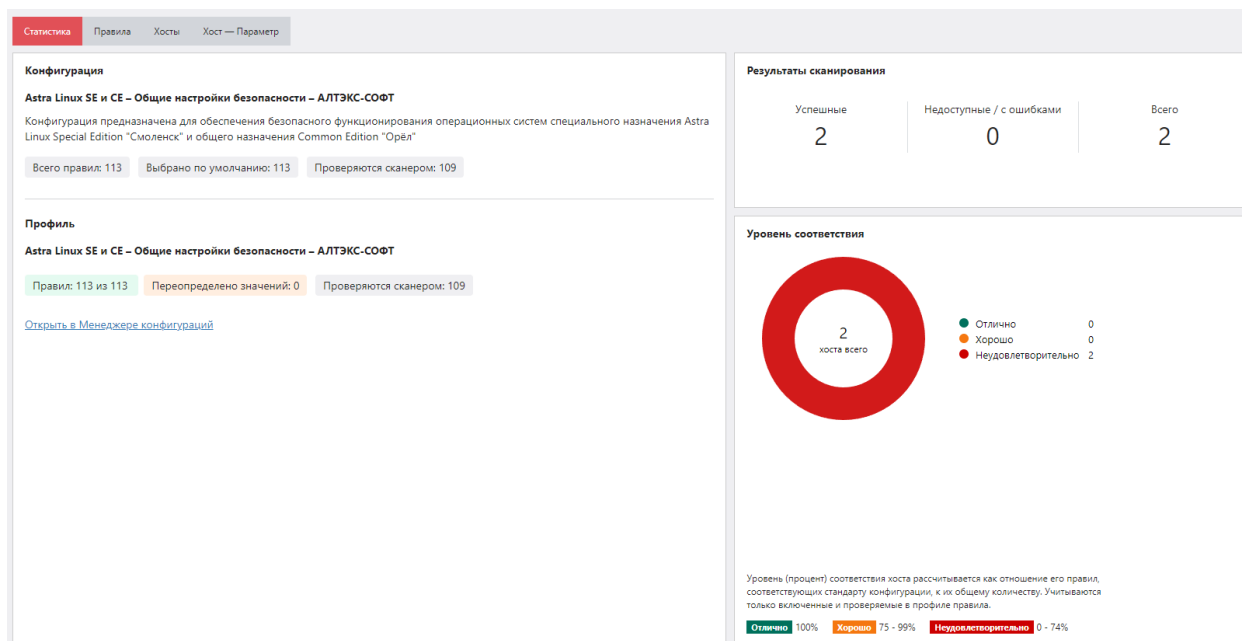
Для перехода на форму нажмите **Аналитика** → **Анализ конфигураций**

Содержание

- [8.5.1 Вкладка Статистика](#)
- [8.5.2 Вкладка Правила](#)
- [8.5.3 Вкладка Хосты](#)
- [8.5.4 Вкладка Хост – Параметр](#)

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.

Конфигурация

Astra Linux SE и CE – Общие настройки безопасности – АЛТЭК-СОФТ

Конфигурация предназначена для обеспечения безопасного функционирования операционных систем специального назначения Astra Linux Special Edition "Смоленск" и общего назначения Common Edition "Орёл"

Всего правил: 113

Выбрано по умолчанию: 113

Проверяются сканером: 109

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

Профиль

Astra Linux SE и CE – Общие настройки безопасности – АЛТЭК-СОФТ

Правил: 113 из 113

Переопределено значений: 0

Проверяются сканером: 109

[Открыть в Менеджере конфигураций](#)

- 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

Результаты сканирования

Успешные

1

[Недоступные / с ошибками](#)

1

Всего

2

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

Хост	Тип сканирования	Задание	Результат	Причина недоступности
> 192.168.80.32	Аудит конфигураций	1_27	Хост недоступен	Ошибка установления соединения.

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

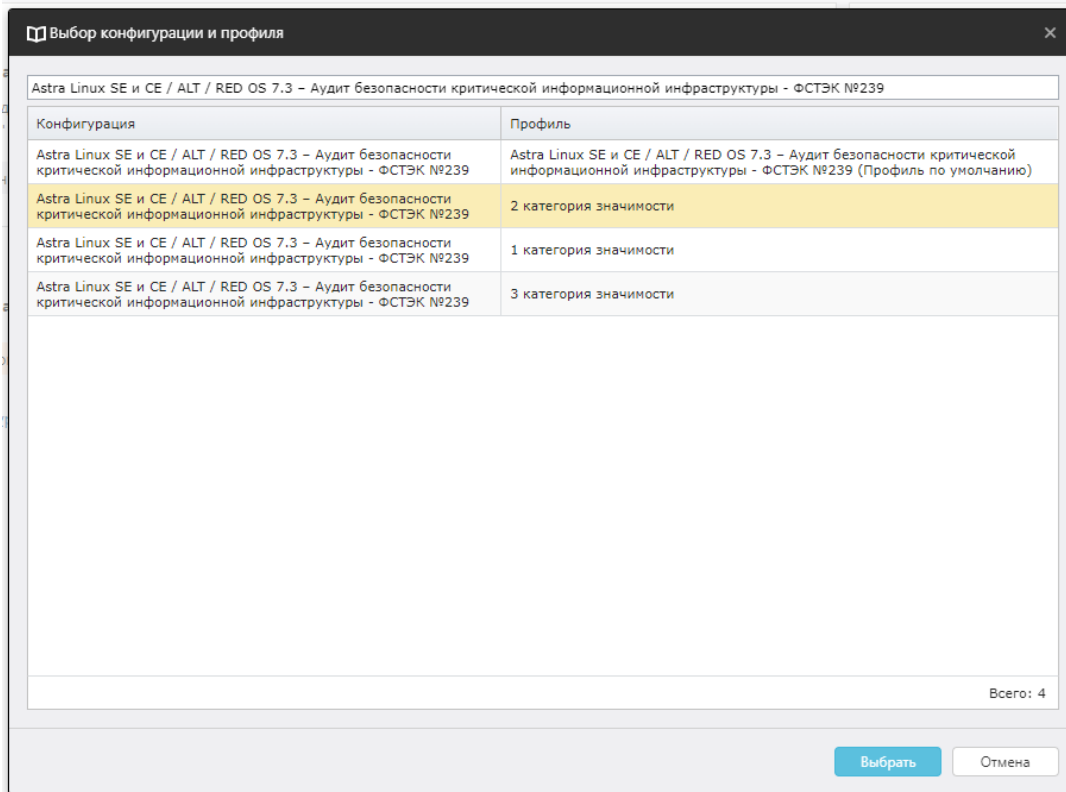


Общий фильтр

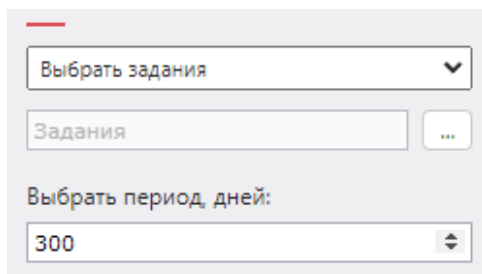
Анализ конфигураций

Конфигурация


- 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;

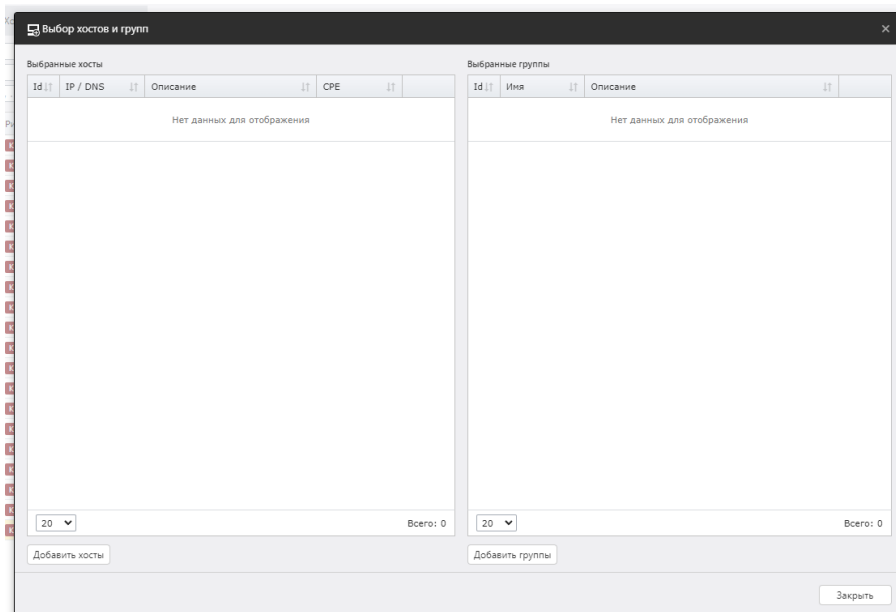


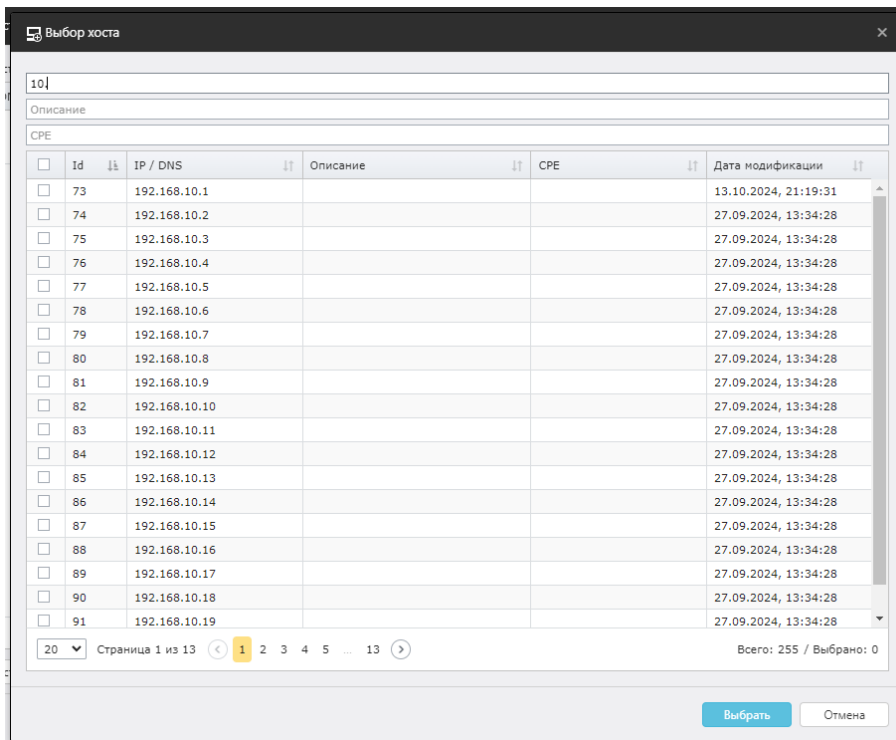
- Задания – можно выбрать задания, из результатов сканирования которых будет производиться анализ конфигураций. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится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



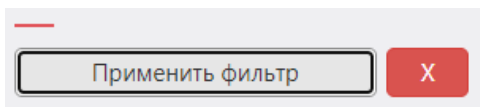
Нажмите на , после чего откроется окно выбора заданий;

- 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.

№ п/п	Правило	Риск	Хостов "Соответствие"	Хостов "Несоответствие"	Хостов "Ошибка" или "Неизвестно"	Хостов "Неприменимо"	Дополнительно
1	Директория /tmp располагается на отдельном разделе	Низкий	0 (0 %)	2 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
2	Директория /var располагается на отдельном разделе	Низкий	0 (0 %)	2 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
3	Директория /var/log располагается на отдельном разделе	Низкий	0 (0 %)	2 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
4	Директория /home располагается на отдельном разделе	Низкий	1 (50 %)	1 (50 %)	0 (0 %)	0 (0 %)	Значения на хостах
5	Добавление опции noexec для съемных носителей	Низкий	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
6	Добавление опции noexec для /home и /tmp разделов	Низкий	1 (50 %)	1 (50 %)	0 (0 %)	0 (0 %)	Значения на хостах
7	Ограничить права на crontab файл	Средний	0 (0 %)	2 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
8	Установить umask для пользователей по умолчанию	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
9	Проверка владельца shadow файла	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
10	Проверка группы владельца файла shadow	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
11	Проверка прав доступа файла shadow	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
12	Проверка владельца файла group	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
13	Проверка группы владельца файла group	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
14	Проверка прав доступа к файлу group	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
15	Проверка владельца файла passwd	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
16	Проверка группы владельца файла passwd	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
17	Проверка прав доступа к файлу passwd	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
18	Проверка прав доступа разделенных библиотек	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
19	Проверка, что владельцем разделенных библиотек является суперпользователь	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
20	Проверка прав доступа исполняемых файлов	Средний	0 (0 %)	2 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
21	Проверка, что владельцем системных исполняемых файлов является суперпользователь	Средний	2 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
22	Отсутствие ';' или Group/World-Writable Directory в \$PATH	Средний	0 (0 %)	2 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
23	Отключить данные памяти	Средний	0 (0 %)	2 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах

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;

№ п/п	Правило	Риск	Хостов "Соответствие"	Хостов "Несоответствие"	Хостов "Ошибка" или "Неизвестно"	Хостов "Непринято"	Дополнительно
> 1	Директория /tmp располагается на отдельном разделе	Низкий	0 (0 %)	2 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
▼ 2	Директория /var располагается на отдельном разделе	Низкий	0 (0 %)	2 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах

Правило partition_for_var
OVAL oval:ru.aitc-soft.nix:def:26021
Описание Директория /var используется службами и другими системными сервисами для хранения часто изменяющихся данных. Необходимо убедиться во время установки, что она располагается на отдельном разделе или логическом томе, либо перенести её позднее, используя LVM.

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.

Список правил

№	Правило	Уровень критичности
> 1	Все обновления ПО должны быть установлены	Высокий
> 2	Проверка валидности документа sources.list	Высокий
> 3	Проверка системы перед внесением изменений	Средний
▼ 4	Ограничение пользователям SSH доступа	Низкий

Правило sshd_limit_user_access
Описание По умолчанию SSH настроен разрешать любым пользовательским аккаунтам подключаться к системе. Для того, чтобы указать пользователей, которым разрешен вход через SSH и запрещать всем остальным пользователям, необходимо исправить или дополнить следующую строку в /etc/ssh/sshd_config:
DenyUsers USER1 USER2
Где USER1 и USER2 пользователи, которым запрещен вход.

Страница 1 из 1 1 Всего: 4

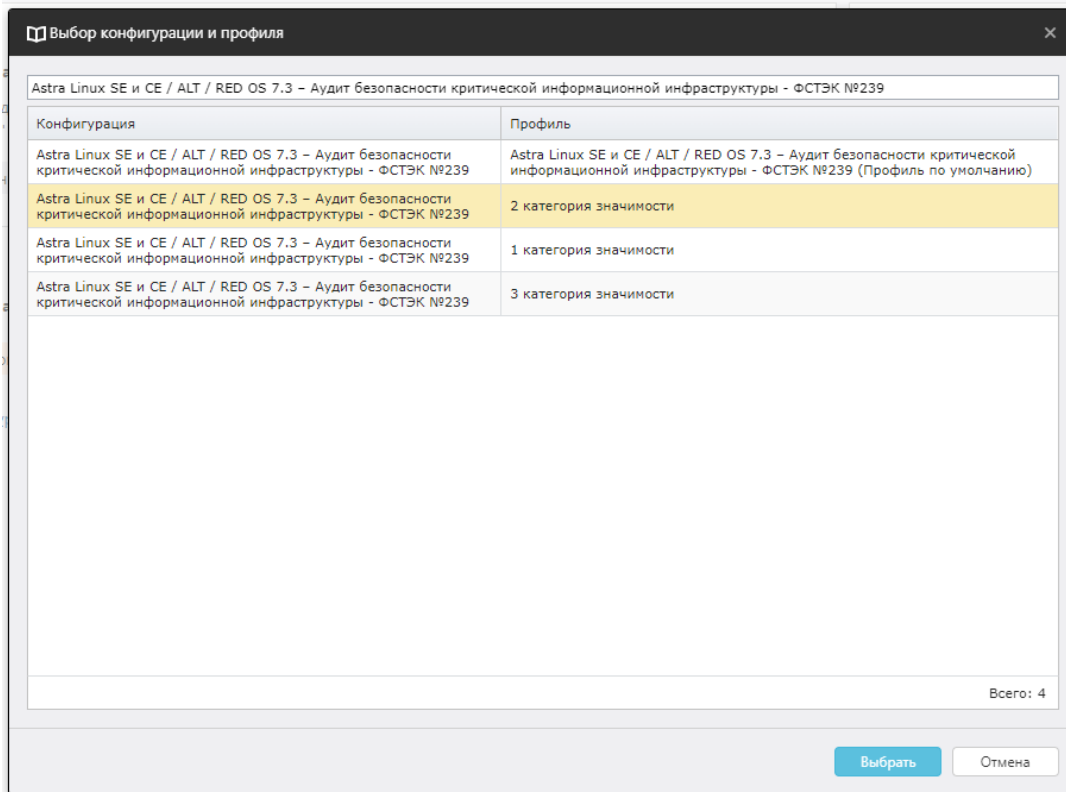
Закреть

Общий фильтр

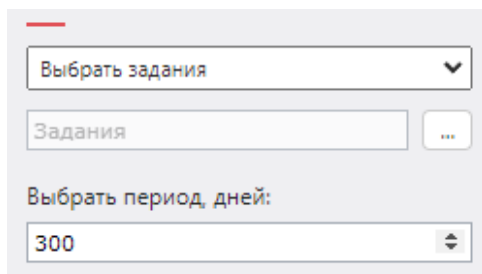
Анализ конфигураций

Конфигурация ...


- 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;

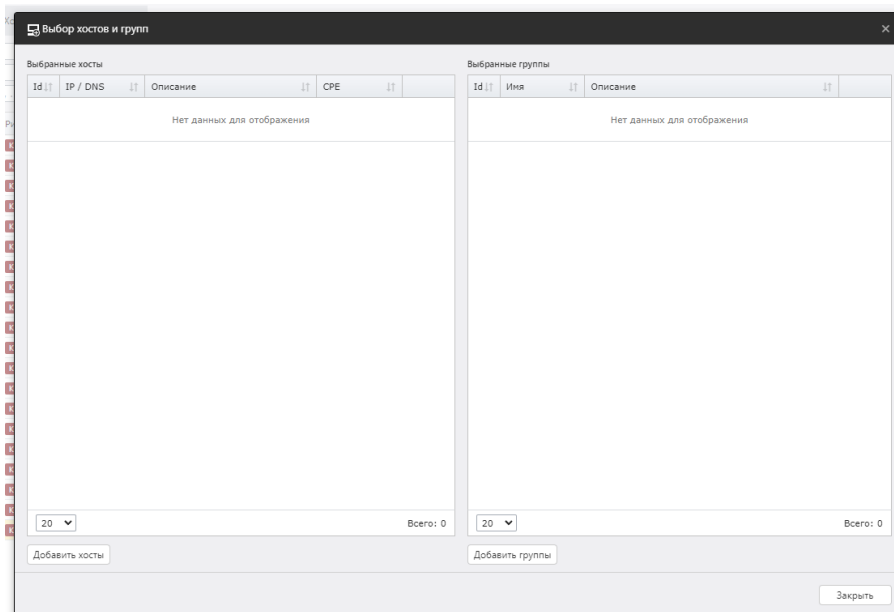


- Задания – можно выбрать задания, из результатов сканирования которых будет производиться анализ конфигураций. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится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



Выбор хоста

10]

Описание

CPE

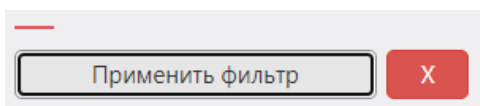
<input type="checkbox"/>	Id	IP / DNS	Описание	CPE	Дата модификации
<input type="checkbox"/>	73	192.168.10.1			13.10.2024, 21:19:31
<input type="checkbox"/>	74	192.168.10.2			27.09.2024, 13:34:28
<input type="checkbox"/>	75	192.168.10.3			27.09.2024, 13:34:28
<input type="checkbox"/>	76	192.168.10.4			27.09.2024, 13:34:28
<input type="checkbox"/>	77	192.168.10.5			27.09.2024, 13:34:28
<input type="checkbox"/>	78	192.168.10.6			27.09.2024, 13:34:28
<input type="checkbox"/>	79	192.168.10.7			27.09.2024, 13:34:28
<input type="checkbox"/>	80	192.168.10.8			27.09.2024, 13:34:28
<input type="checkbox"/>	81	192.168.10.9			27.09.2024, 13:34:28
<input type="checkbox"/>	82	192.168.10.10			27.09.2024, 13:34:28
<input type="checkbox"/>	83	192.168.10.11			27.09.2024, 13:34:28
<input type="checkbox"/>	84	192.168.10.12			27.09.2024, 13:34:28
<input type="checkbox"/>	85	192.168.10.13			27.09.2024, 13:34:28
<input type="checkbox"/>	86	192.168.10.14			27.09.2024, 13:34:28
<input type="checkbox"/>	87	192.168.10.15			27.09.2024, 13:34:28
<input type="checkbox"/>	88	192.168.10.16			27.09.2024, 13:34:28
<input type="checkbox"/>	89	192.168.10.17			27.09.2024, 13:34:28
<input type="checkbox"/>	90	192.168.10.18			27.09.2024, 13:34:28
<input type="checkbox"/>	91	192.168.10.19			27.09.2024, 13:34:28

20 Страница 1 из 13 1 2 3 4 5 ... 13

Всего: 255 / Выбрано: 0

Выбрать Отмена

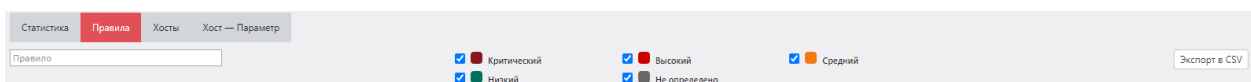
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



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-yyuu.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"

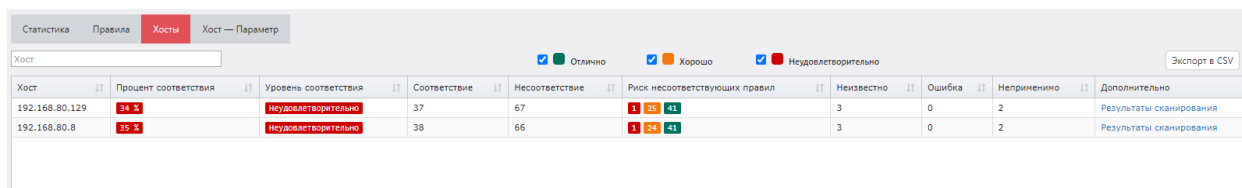
Количество хостов с результатом проверки правила Неприменимо	Хостов "Неприменимо"
Id правила	ID правила, например partition_for_tmp
OVAL определение	Ссылка на OVAL-определение правила
Описание	Описание правила

Пример:

Код
<p>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</p> <p>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."</p>

8.5.3 Вкладка Хосты

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



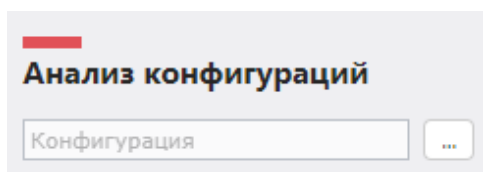
Хост	Процент соответствия	Уровень соответствия	Соответствие	Несоответствие	Риск несоответствующих правил	Неизвестно	Ошибка	Неприменимо	Дополнительно
192.168.80.129	34 %	Неудовлетворительно	37	67	1 25 41	3	0	2	Результаты сканирования
192.168.80.8	35 %	Неудовлетворительно	38	66	1 24 41	3	0	2	Результаты сканирования


Информация о правиле включает в себя:

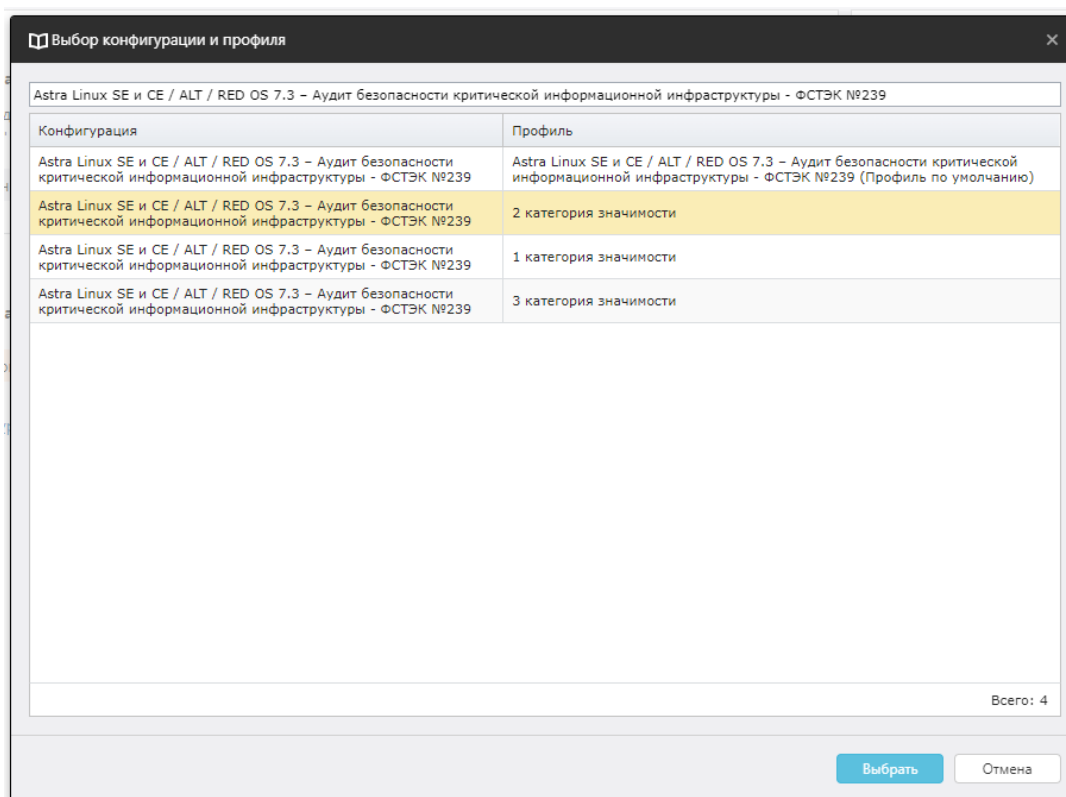
- Хост – IP-адрес или DNS-имя хоста;
- Процент соответствия – Уровень (процент) соответствия хоста рассчитывается как отношение его правил, соответствующих стандарту конфигурации, к их общему количеству. Учитываются только включенные и проверяемые в профиле правила.;
- Уровень соответствия – оценка соответствия:
 - 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:


Выбрать задания

Задания

Выбрать период, дней:

300

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:

Выбор хостов и групп

Выбранные хосты				Выбранные группы		
Id	IP / DNS	Описание	CPE	Id	Имя	Описание
Нет данных для отображения				Нет данных для отображения		

20 | Всего: 0 | 20 | Всего: 0

Добавить хосты | Добавить группы | Закрыть

Выбор хоста

10]

Описание

CPE

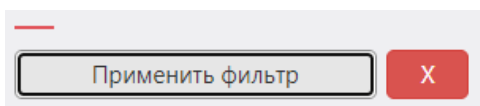
<input type="checkbox"/>	Id	IP / DNS	Описание	CPE	Дата модификации
<input type="checkbox"/>	73	192.168.10.1			13.10.2024, 21:19:31
<input type="checkbox"/>	74	192.168.10.2			27.09.2024, 13:34:28
<input type="checkbox"/>	75	192.168.10.3			27.09.2024, 13:34:28
<input type="checkbox"/>	76	192.168.10.4			27.09.2024, 13:34:28
<input type="checkbox"/>	77	192.168.10.5			27.09.2024, 13:34:28
<input type="checkbox"/>	78	192.168.10.6			27.09.2024, 13:34:28
<input type="checkbox"/>	79	192.168.10.7			27.09.2024, 13:34:28
<input type="checkbox"/>	80	192.168.10.8			27.09.2024, 13:34:28
<input type="checkbox"/>	81	192.168.10.9			27.09.2024, 13:34:28
<input type="checkbox"/>	82	192.168.10.10			27.09.2024, 13:34:28
<input type="checkbox"/>	83	192.168.10.11			27.09.2024, 13:34:28
<input type="checkbox"/>	84	192.168.10.12			27.09.2024, 13:34:28
<input type="checkbox"/>	85	192.168.10.13			27.09.2024, 13:34:28
<input type="checkbox"/>	86	192.168.10.14			27.09.2024, 13:34:28
<input type="checkbox"/>	87	192.168.10.15			27.09.2024, 13:34:28
<input type="checkbox"/>	88	192.168.10.16			27.09.2024, 13:34:28
<input type="checkbox"/>	89	192.168.10.17			27.09.2024, 13:34:28
<input type="checkbox"/>	90	192.168.10.18			27.09.2024, 13:34:28
<input type="checkbox"/>	91	192.168.10.19			27.09.2024, 13:34:28

20 Страница 1 из 13 1 2 3 4 5 ... 13

Всего: 255 / Выбрано: 0

Выбрать Отмена

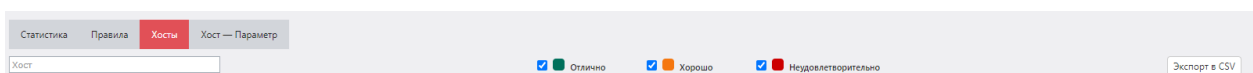
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



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-yyuu.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 определено
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;

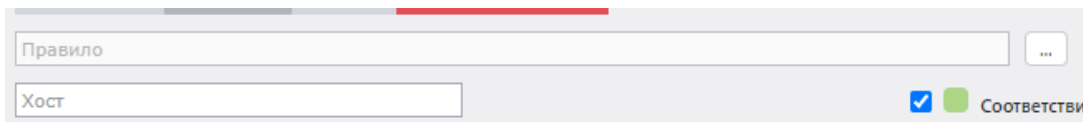
Неприменимо – данное правило неприменимо для проверяемой платформы;

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

The screenshot displays the 'Host - Parameter' tab in the RedCheck application. The interface is divided into several sections:

- Navigation:** 'Статистика', 'Правила', 'Хосты', 'Хост — Параметр'.
- Filtering:** 'Ограничить права на cronstab файл', 'Хост: [input]', and a legend for status: Соответствие, Несоответствие, Ошибка, Неизвестно, Неприменимо.
- Table:** A table with columns 'Хост', 'Результат', and 'Фактический параметр'. It lists two hosts: 192.168.80.129 and 192.168.80.8, both with a 'Несоответствие' status. The 'Фактический параметр' column contains detailed parameter values for files like /etc/crontab and /var/spool/cron.
- Right Panel:** Contains details for the selected rule: 'Ограничить права на cronstab файл'. It shows the profile 'Astra Linux SE и CE - Общие настройки безопасности - АЛТЭКС-СОФТ', status 'Включено', and criticality 'Средний'. It also includes a description of the rule's purpose and a list of system files it checks.

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 хсcdf** ([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.

Профиль ▾

Название Astra Linux SE и CE – Общие настройки безопасности – АЛТЭК-СОФТ

Отключено 0 правил

Изменено 0 правил

Правило ▾

Ограничить права на crontab файл

Статус правила Включено

Критичность ▾

Средний

Описание ▾

Системные файлы crontab доступны только демону cron (с привилегиями суперпользователя) и команде crontab (запускаемая от root). Если непривилегированным пользователям дать права на чтение или (что ещё хуже) модификацию системных crontab файлы, то это может привести к повышению привилегий локального пользователя. Для правильного задания прав и группы, необходимо выполнить команды:

```
# chmod 400 /etc/crontab
# chmod -R 770 /var/spool/cron/
# chown -R 0 /var/spool/cron/
```

Дополнительно ▾

ID *restrict_permissions_on__files*

OVAL ID *oval:ru.altx-soft.nix:def:26069*

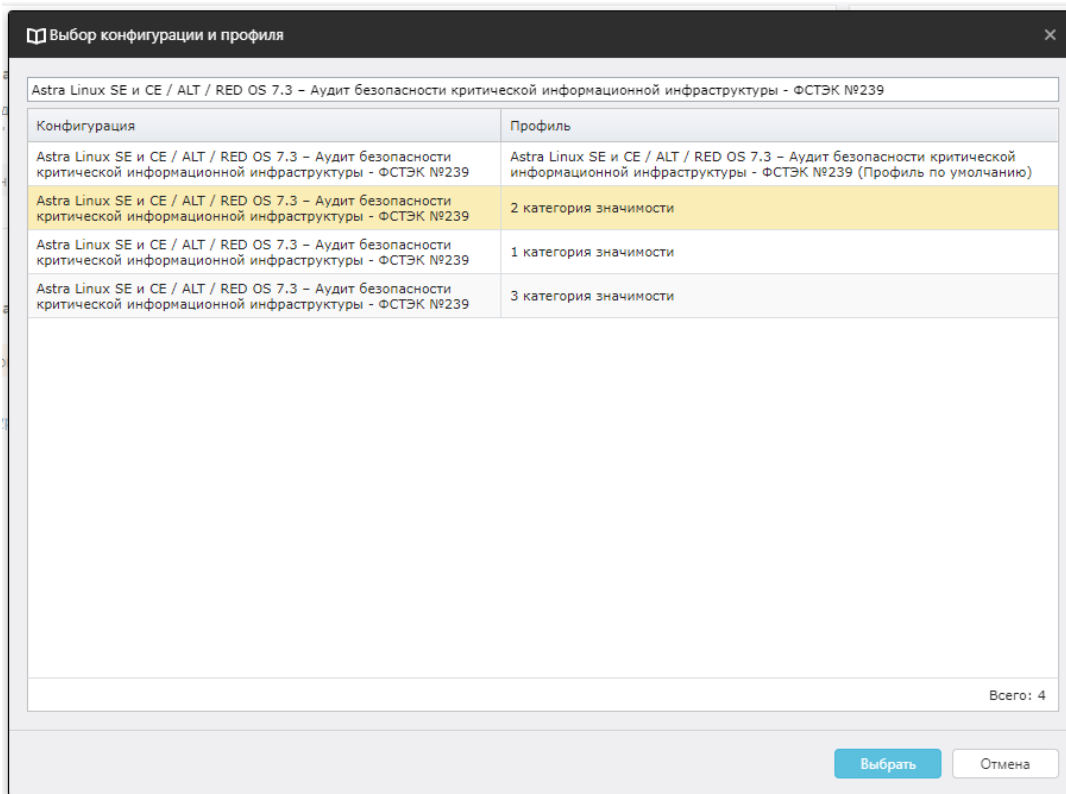
OVAL URL *ALTX-AstraLinux-oval.xml*

Общий фильтр

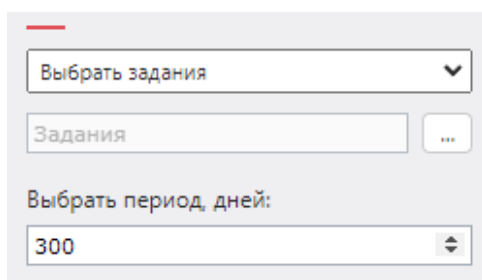
Анализ конфигураций

Конфигурация ...

- 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;




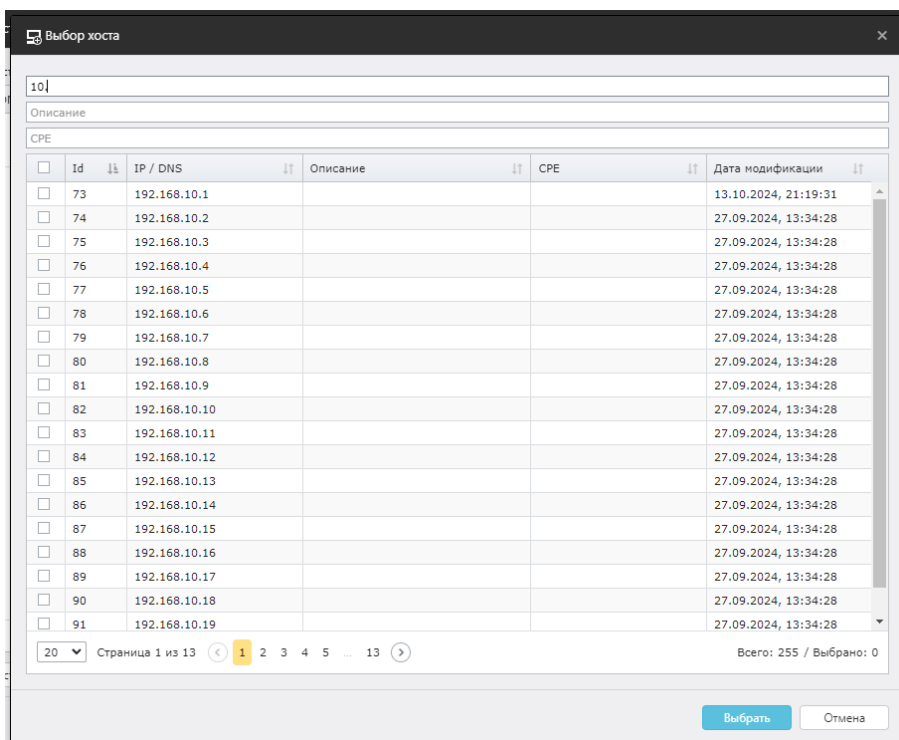
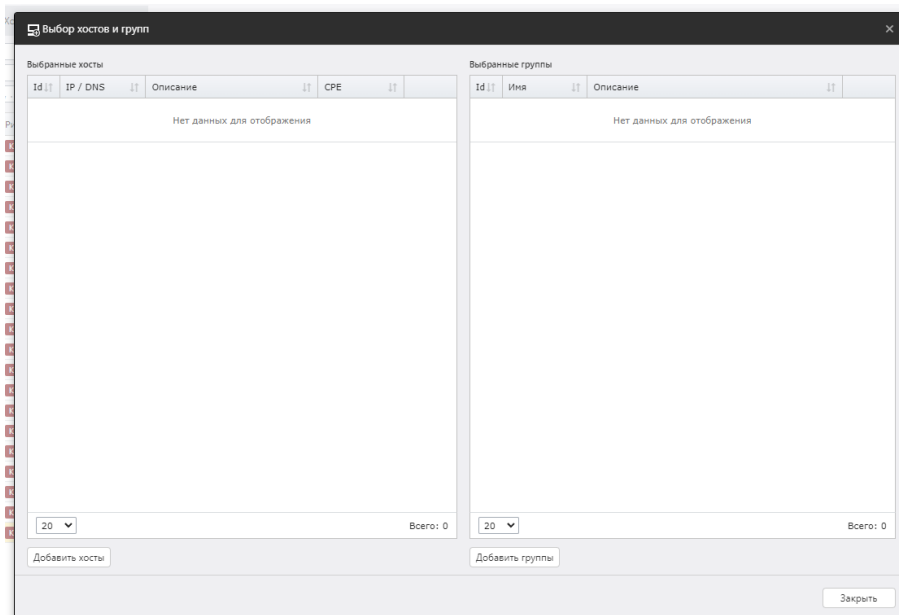
- Задания – можно выбрать задания, из результатов сканирования которых будет производиться анализ конфигураций. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится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



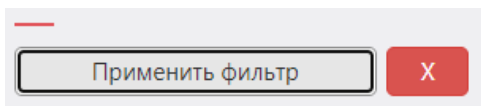
Нажмите на , после чего откроется окно выбора заданий;

- 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:



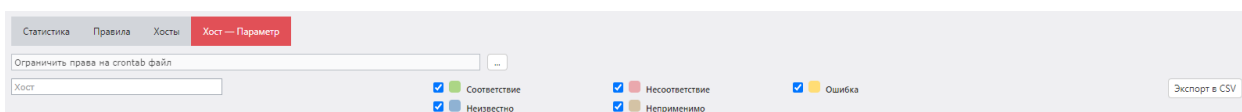
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



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-yyuu.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>uехес</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>gехес</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>оехес</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>uехес</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>gехес</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>оехес</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>uехес</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>gехес</b> для файла <b>/var/spool/cron/crontabs</b> =

```

True
Значение параметра **oread** для файла **/var/spool/cron/crontabs** = **False**
Значение параметра **owrite** для файла **/var/spool/cron/crontabs** = **False**
Значение параметра **oexec** для файла **/var/spool/cron/crontabs** = **False**
Значение параметра **user_id** для файла **/var/spool/cron/crontabs** = **0**

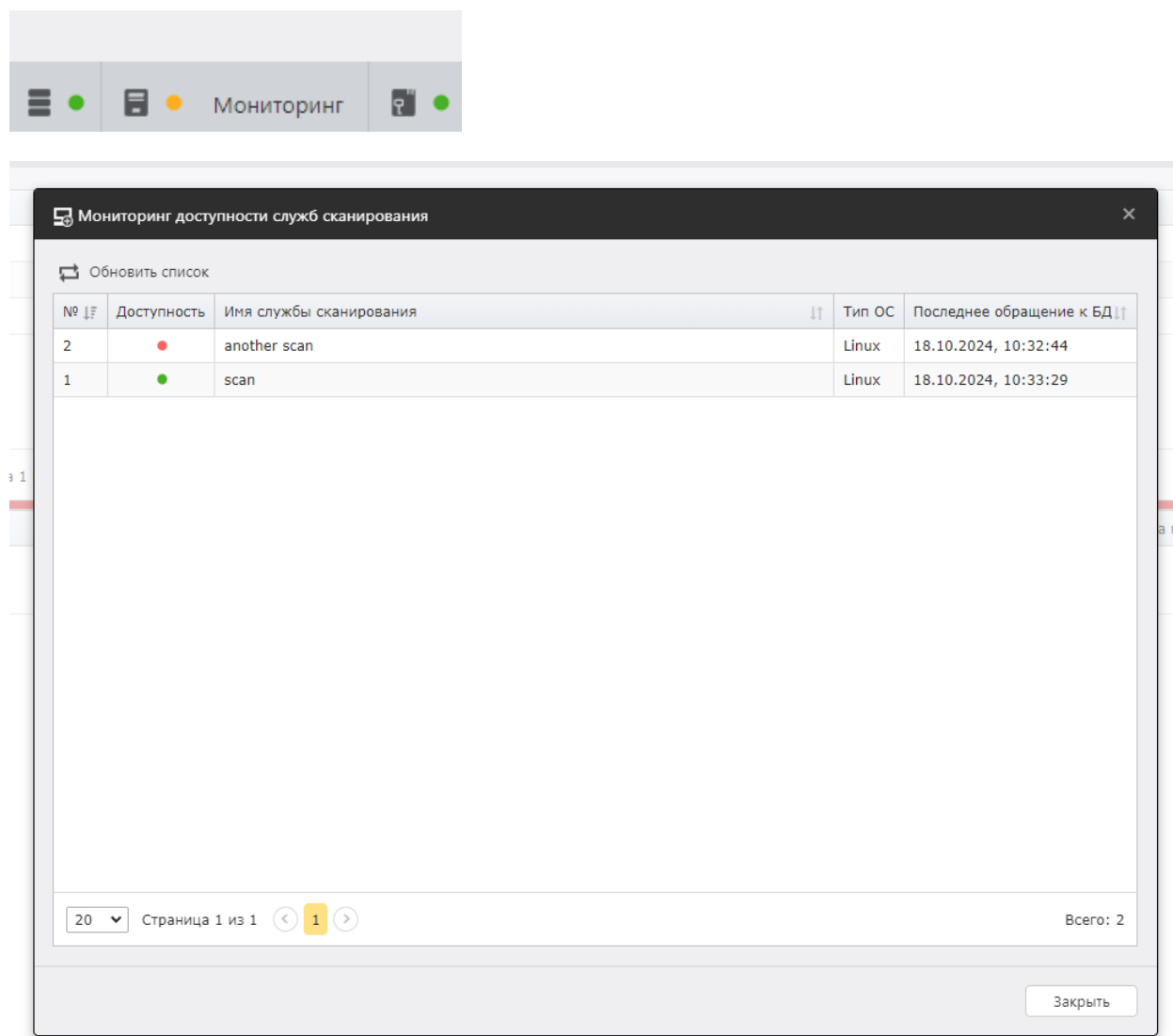
Дополнительные возможности

Содержание

- Мониторинг служб сканирования

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**:



The screenshot shows a window titled "Мониторинг доступности служб сканирования" (Monitoring of scan service availability). The window contains a table with the following data:

№	Доступность	Имя службы сканирования	Тип ОС	Последнее обращение к БД
2	●	another scan	Linux	18.10.2024, 10:32:44
1	●	scan	Linux	18.10.2024, 10:33:29

At the bottom of the window, there is a pagination control showing "Страница 1 из 1" and "Всего: 2". A "Закреть" (Close) button is located in the bottom right corner.

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**.

Подключенные службы сканирования										
Имя	UID	По умолчанию	Дата создания	Дата последнего запуска	Имя хоста	ОС	Версия ОС	Разрядность	Последнее обращение к БД	Версия SCAP процессора
another scan	a268e675-8442-4db3-940f-0005097cc829	Нет	07.10.2024, 09:41:15	18.10.2024, 06:34:01	redos	reods.7_3_x86-64-x64	5.4.0.54	64	18.10.2024, 10:46:50	8.0.0-scap-nlx.425
scan	a268e675-8442-4db3-940f-0005097cc829	Да	07.10.2024, 09:41:15	18.10.2024, 06:34:01	astra	astra.1.7_x86-64-x64	5.4.0.54	64	18.10.2024, 10:35:49	8.0.0-scap-nlx.425

Страница 1 из 1 1 Всего: 2