ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "НТЦ КОНТАКТ"

УТВЕРЖДАЮ
Директор
Закрытого акционерного общества
"НТЦ КОНТАКТ"

_____ А.А. Тепляков
"___"_____ 2025

СРЕДСТВО ПРОГРАММНОЕ КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ BY.СЮИК.00473-01

Руководство оператора
ЛИСТ УТВЕРЖДЕНИЯ

BY.СЮИК.00473-01 34 01-ЛУ

Инженер

_____ М.М. Сорокин
"___"_____ 2025

Нормоконтролер

_____ В.А. Кондратенко
"___"_____ 2025

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

2025

№ изм.	*Подп.*	*Дата*

Литера O_1

УТВЕРЖДЕН
BY.СЮИК.00473-01 34 01-ЛУ

СРЕДСТВО ПРОГРАММНОЕ
КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ
BY.СЮИК.00473-01

Руководство оператора
BY.СЮИК.00473-01 34 01
Листов 58

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

2025

Изм.№	Подп.	Дата

Литера

АННОТАЦИЯ

Настоящее руководство оператора содержит сведения о назначении, функциях и особенностях эксплуатации средства программного контроля эффективности защищенности информации BY.СЮИК.00473-01 (далее – «Сканер уязвимостей»).

СОДЕРЖАНИЕ

1. Назначение программы 5
1.1. Общие сведения о программе 5
1.2. Функции программы 5
2. Условия выполнения программы 6
2.1. Аппаратные требования 6
2.2. Программные требования 6
2.3 Кнопки для управления 6
3. Выполнение программы 7
3.1. Комплектность «Сканер уязвимостей» 7
3.2. Установка «Сканер уязвимостей» 7
3.3. Подключение к веб-интерфейсу 8
3.4. Информационные панели и дисплеи 8
3.4.1. Добавление и удаление дисплеев панели мониторинга 9
3.4.2. Организация отображения на информационных панелях дисплеев 10
3.4.3. Добавление, редактирование, удаление информационной панели 10
3.5. Фильтрация содержимого страницы 11
3.5.1. Настройка параметров фильтрации 11
3.5.2. Управление фильтрами 12
3.6. Использование тегов 13
3.6.1. Создание и управление тегами 13
3.6.2. Привязка тега к отдельному объекту или нескольким объектам 14
3.7. Использование корзины 14
3.8. Отображение состояния канала 15
3.9. Изменение пользовательских настроек 15
3.10. Создание и управление пользователями 18
3.11. Создание и управление ролями 19
3.11.1. Создание роли с ограниченной и расширенной функциональностью 21
3.12. Создание и управление группами 21
3.13. Разрешения 21
3.13.1. Создание и управление разрешениями 22
3.13.2. Предоставление дополнительных разрешений 22
3.13.3. Создание разрешений на странице сведений о ресурсе 23
3.14.Настройка сканирования 24
3.14.1. Создание цели 24
3.14.2. Создание задачи 25
3.14.3. Запуск задачи 26
3.14.4. Процесс сканирования 27
3.15.Настройка проверки подлинности с использованием локальных проверок безопасности 27
3.15.1. Преимущества и недостатки аутентифицированных сканирований 28
3.15.2 Использование учетных данных 28
3.15.3 Управление учетными данными 29
3.16. Требования к целевым системам с Microsoft Windows 29
3.16.1. Настройка учетной записи домена для проверки подлинности при сканировании 30
3.16.2. Требования к целевым системам с Unix 31
3.17Настройка сканирования CVE 32
3.18Создание и управление списком портов 33

Изм.№	Подп.	Дата

3.19 Настройка и управление конфигураций сканирования 34
3.19.1 Конфигурации сканирования по умолчанию 35
3.19.2 Создание, редактирования конфигурации сканирования 35
3.19.3 Описание настроек сканера....37
3.19.4 Импорт конфигурации сканирования 38
3.20 Выполнение запланированного сканирования и управление расписанием....38
3.21 Использование оповещений 39
3.22 Параметры и внешние факторы влияющие на процесс сканирования....40
3.23 Настройка форматов и управление отчетами 42
3.23.1 Импорт формата отчета 42
3.23.2 Использование и управление отчетами 42
3.23.3 Результаты отчета 43
3.23.4 Анализ отчета 44
3.23.5 Фильтрация отчета 45
3.23.6 Экспорт отчета....45
3.23.7 Импорт отчета....46
3.23.8 Запуск Уведомления для отчета 46
3.23.9 Создание дельта-отчета 47
3.24 Отображение уязвимостей....47
3.25 Динамика уязвимостей....48
3.26 Создание и использование примечаний 48
3.27 Использование переопределений и ложных срабатываний 49
3.27.1 Создание переопределения с помощью результата сканирования 49
3.27.2 Создание переопределения на веб-странице «Переопределения»…..……50
3.28 Управление и создание хостов 51
3.29 Создание цели с набором хостов 52
3.30 Управление операционными системами 52
3.31 Выход из веб-интерфейса 52
3.32 Регламент обновлений 53
4. Сообщения оператору 54
Перечень терминов....55
Перечень сокращений 57

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Общие сведения о программе

«Сканер уязвимостей» предназначен для автоматизированного анализа защищенности узлов вычислительной сети и выявления уязвимостей.

Устройство в «Сканер уязвимостей» является типом активов. Устройство – это персональная электронная вычислительная машина (ПЭВМ), сервер, активное сетевое оборудование или иной узел, который подключен к вычислительной сети и подвержен сканированию.

Основными входными данными для «Сканер уязвимостей» являются:

– IP-адрес целевого устройства (системы) для сканирования. Для определения целевых устройств может быть указан перечень (диапазон) IP-адресов либо IP-адрес сети, в которой такие устройства находятся;

– список портов для сканирования;

– база знаний.

Основными выходными данными для «Сканер уязвимостей» являются отчеты. Отчеты содержат перечень уязвимостей, выявленных на целевых устройствах, и рекомендации по их устранению. Отчеты могут быть получены администратором или оператором на экране ПЭВМ или экспортированы.

1.2 Функции программы

«Сканер уязвимостей» реализует следующие функции:

– поиск уязвимостей на узлах вычислительной сети;

– выполнение локального поиска уязвимостей с прохождением аутентификации в целевой системе;

– предоставление рекомендаций для устранения обнаруженных уязвимостей;

– создание отчетов.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Аппаратные требования

«Сканер уязвимостей» устанавливается на ПЭВМ и серверы, удовлетворяющие следующим минимальным аппаратным характеристикам:

1) процессор: количество ядер 4 или более с частотой 2,5 ГГц или более;
2) оперативное запоминающее устройство: 8 ГБ или выше;
3) свободное пространство на жестком диске: SSD 100 ГБ или более;
4) сетевая карта: 100 Мбит/с Ethernet или более;
5) операционная система (ОС): Ubuntu 24.04 x64.

2.2 Программные требования

«Сканер уязвимостей» предназначен для применения на ПЭВМ и серверах, работающих под управлением семейства Unix-подобных ОС на базе ядра Linux.

«Сканер уязвимостей» совместим с системами виртуализации VirtualBox, Hyper-V, Proxmox Virtual Environment, VMware.

2.3 Кнопки для управления

Перечень кнопок, используемый для управления в «Сканер уязвимостей», приведен в таблице 1.

Таблица 1

Кнопка	Описание кнопки
	Удалить
	Обновить
	Вернуть параметры
	Сведения об объекте
	Показать страницу со списком всех объектов
	Создать
	Клонировать
	Редактировать
	Экспортировать объект в формате XML-документа
	Импортировать
	Переместить в корзину
	Запустить
	Продолжить
	Проверить сканер
	Дельта-отчет
	Примечание
	Тип решения
	Показать соответствующие хосты

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1 Комплектность «Сканер уязвимостей»

«Сканер уязвимостей» поставляется на компакт-диске BY.СЮИК.00473-01.

3.2 Установка «Сканер уязвимостей»

3.2.1 Работа с программой «Сканер уязвимостей» включает следующие этапы:
– установка (инсталляция);
– штатная работа.

3.2.2 Для корректной установки «Сканер уязвимостей» необходимо соблюдение следующих условий:
– наличие на ПЭВМ доступа к сети Интернет;
– наличие у пользователя ОС прав супер-пользователя.

Перед установкой «Сканер уязвимостей» необходимо переместить любым доступным способом на ПЭВМ установочные пакеты. Дальнейшие действия выполняются из директории, в которой находятся установочные пакеты (далее – рабочая директория).

Для установки необходимо выполнить следующие действия:

1) Скопировать архив с носителя в рабочую директорию, создать папку в корневой директории и извлечь его в папку:

```
# mkdir /scanner
# tar -C /scanner -xvzf <рабочая директория>/scanner.tar.gz
```

2) разрешить выполнение скрипта установки, выполнив в терминале следующую команду:

```
# chmod +x /scanner/install.sh
```

3) запустить установку, выполнив в терминале следующую команду с правами администратора:

```
# ./install.sh
```

Если установка завершена успешно, в терминале будет отображено сообщение «*Установка завершена*».

В случае возникновения ошибок при инсталляции и невозможности устранить их с помощью средств администрирования ОС необходимо обратиться к разработчику.

После завершения установки обновление базы знаний уязвимостей продолжится в фоновом режиме. Для отслеживания статуса обновления базы необходимо получить доступ к веб-интерфейсу «Сканер уязвимостей» от имени администратора, созданного при начальном конфигурировании, и перейти «Администрирование» → «Состояние базы знаний» (рис. 3.1).

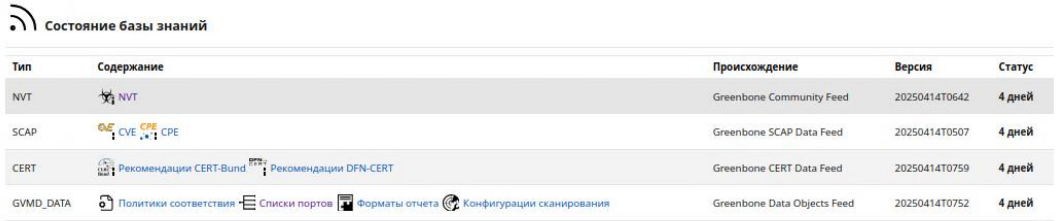

Рис. 3.1

В процессе установки «Сканер уязвимостей» дополнительно будут автоматически установлены необходимые свободно распространяемые пакеты, приведенные в таблице 1а.

Таблица 1 а

Наименование	Версия*	Наименование	Версия*
redis-server	7.0.15	libmicrohttpd12	0.9.75-3ubuntu1
postgresql	16.8	libxml2	2.9.13+dfsg-1ubuntu0.4
plymouth	0.9.5+git20211018	libglib2.0-0	2.72.4-0ubuntu2.3
plymouth-themes	0.9.5+git20211018	libgnutls30	3.7.3-4ubuntu1.5
libical3	3.0.14-1build1	libsnmp40	5.9.1+dfsg-1ubuntu2.6
libpq5	14.13-0ubuntu0.22.04.1	xml-twig-tools	1:3.52-1
libpaho-mqttpp3-1	1.2.0-2	libnet1	1.1.6+dfsg-3.1build3
libradcli4	1.2.11-1build1	libgssapi3-heimdal	7.7.0+dfsg-3ubuntu1
libssh-gcrypt-4	0.9.6-2ubuntu0.22.04.3	libhdb9-heimdal	7.7.0+dfsg-3ubuntu1
libhiredis0.14	0.14.1-2	xsltproc	1.1.34-4ubuntu0.22.04.1
python3	3.12.3	mosquitto	2.0.11-1ubuntu1.1
python3-pip	24.0	texlive-lang-other	2021.20220204-1
python3-wrapt	1.13.3-1build1	texlive-latex-extra	2021.20220204-1
python3-cffi	1.15.0-1build2	texlive-fonts-recommended	2021.20220204-1
python3-psutil	5.9.0-1build1	plymouth-x11	0.9.5+git20211018
python3-lxml	4.8.0-1build1	texlive-lang-cyrillic	2021.20220204-1
python3-defusedxml	0.7.1-1	net-tools	1.60+git20181103.0
python3-paramiko	2.9.3-0ubuntu1.2	htop	3.0.5-7build2
python3-redis	3.5.3-2	nmap	7.91+dfsg1+really7.80
python3-gnupg	0.4.8-1	apache2	2.4.52-1ubuntu4.12
python3-paho-mqtt	1.5.1-1	dialog	1.3-20211214-1
* Версии пакетов указаны по состоянию на 16.10.2024			

Версии пакетов могут отличаться при каждой инсталляции в зависимости от используемого репозитория пакетов и даты установки. Для корректной работы «Сканер уязвимостей» рекомендуется использовать пакеты версий не ниже указанных.

В организации, эксплуатирующий «Сканер уязвимостей» должны быть приняты организационные и (или) технические меры по защите физической целостности СВТ, на котором функционирует «Сканер уязвимостей».

Перед началом работы с «Сканер уязвимостей» Администратор ОС Linux должен выполнить настройку средств защиты от вредоносного программного обеспечения, стандартными средствами ОС выполнить работы по регистрации Пользователей в ОС, созданию требований к аутентификационным данным пользователей, таким образом, чтобы каждый Пользователь сменил свои аутентификационные данные (пароль) при следующем входе в ОС, и их прав. В качестве аутентификационных данных необходимо использовать сложные пароли длиной не менее 8 символов. Администратор не должен допускать возможности работы пользователей с недостаточно стойкими паролями.

Обычно для работы «Сканер уязвимостей» не требуется дополнительных настроек среды, отличных от настроек, определенных в ОС Linux, по умолчанию.

По умолчанию пользователям ограничен доступ к конфигурационным и иным файлам «Сканер уязвимостей», которые влияют на функционирование отдельных сервисов или «Сканер уязвимостей» в целом; к журналам регистрации событий безопасности «Сканер уязвимостей».

В ОС Linux должно быть установлено и поддерживаться точное время.

3.3 Подключение к веб-интерфейсу

Веб-интерфейс доступен по адресу «*https://<IP-адрес сканера>:9392»* (рис. 3.2).

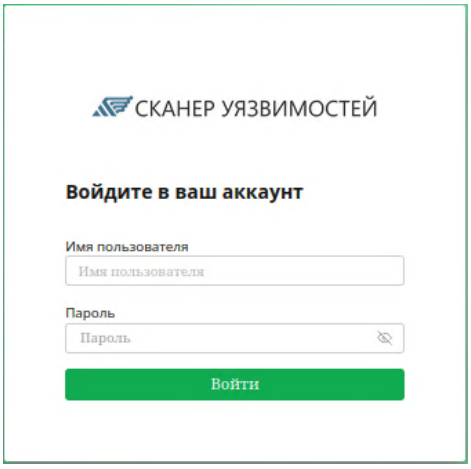

Рис. 3.2

По умолчанию, при установке «Сканер уязвимостей» создается пользователь с именем «**admin**», паролем «**admin**» и ролью администратора («Admin»).

3.4 Информационные панели и дисплеи

Панель управления веб-интерфейса «Сканер уязвимостей» отображается в верхней части страницы, в зависимости от содержимого страницы.

Существует два типа дисплеев панели мониторинга: диаграммы и таблицы. Для каждой страницы существует настройка отображения по умолчанию.

3.4.1 Добавление и удаление дисплеев панели мониторинга

Для добавления «Нового дисплея» необходимо:

1) нажать кнопку справа над дисплеями для создания нового дисплея;
2) выбрать дисплей в раскрывающемся списке (рис. 3.4);
3) нажать кнопку «Добавить».

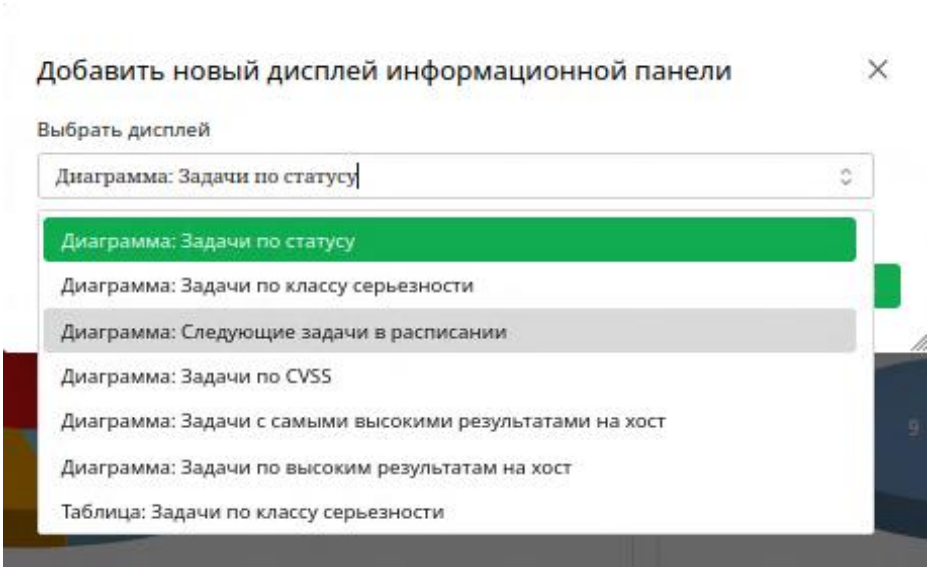

Рис. 3.3

Для удаления дисплея необходимо нажать кнопку (рис. 3.5).

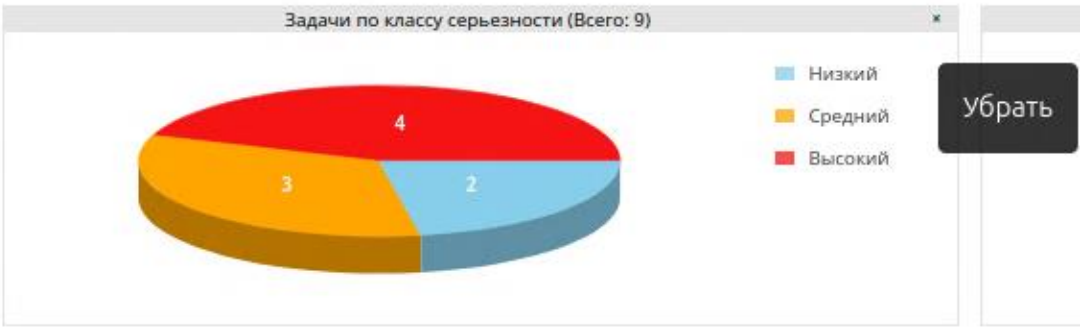

Рис. 3.4

В зависимости от дисплея существует несколько вариантов дополнительных параметров отображения. Переместить манипулятор типа «мышь» к правому краю дисплея, после чего появятся следующие параметры (рис. 3.5):

– применить фильтр к дисплею. Фильтр должен быть настроен для типа объекта, отображаемого на дисплее;

– загрузить диаграмму в формате SVG – файла (только для диаграмм);

– скрыть или показать легенду (только для диаграмм);

– переключить между 2D и 3D представлением (только для диаграмм).

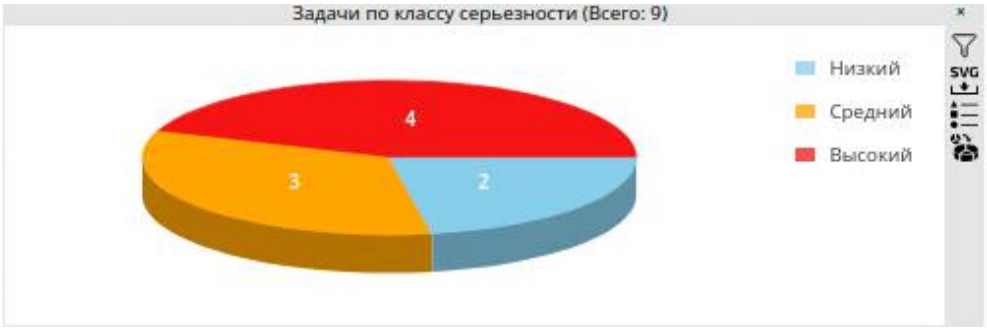

Рис. 3.5

3.4.2 Организация отображения на информационных панелях дисплеев

Вид дисплеев информационных панелей:

– отдельные наборы дисплеев;

– предопределенные панели мониторинга.

– обзорная панель мониторинга, дающая краткий обзор задач, CVE и NVT (рис. 3.6).

Рис. 3.6

3.4.3 Добавление, редактирование, удаление информационной панели

3.4.3.1 Для создание новой информационной панели необходимо:

1) нажать кнопку на вкладке «Информационные панели» (рис. 3.7);

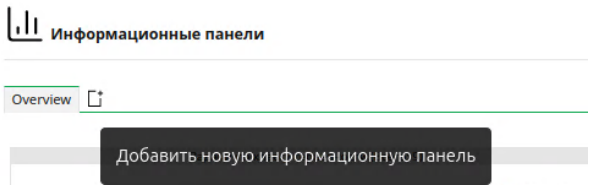

Рис. 3.7

2) ввести название информационной панели в поле ввода «Название информационной панели» (рис. 3.8);

3) выбрать дисплеи, в раскрывающемся списке «Начальные дисплеи» (рис. 3.8);

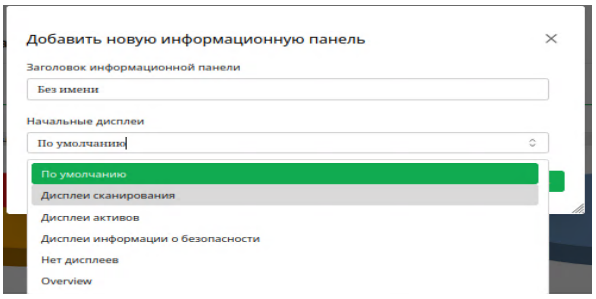

Рис. 3.8

4) нажать кнопку «Добавить».

3.4.3.2 Для изменения отображаемой «Панели мониторинга» необходимо:

1) нажать кнопку для редактирования данных;
2) изменить наименование;
3) нажать кнопку «Сохранить».

3.4.3.3 Для удаления «Информационные панели» необходимо нажать ×.

3.5 Фильтрация содержимого страницы

3.5.1 Настройка параметров фильтрации

Настройка параметров фильтрации осуществляется в верхней части большинства страниц «Сканер уязвимостей» и зависит от отображаемого контекста на текущей открытой веб-странице.

Для создания фильтра необходимо

1) выбрать в строке меню «Конфигурация» → «Фильтры»;
2) нажать кнопку для создания фильтра;
3) ввести наименование фильтра;
4) определить параметры фильтрации;
5) выбрать тип объекта, к которому необходимо применить фильтр, в раскрывающемся списке «Тип» (рис. 3.9);
6) нажать кнопку «Сохранить».

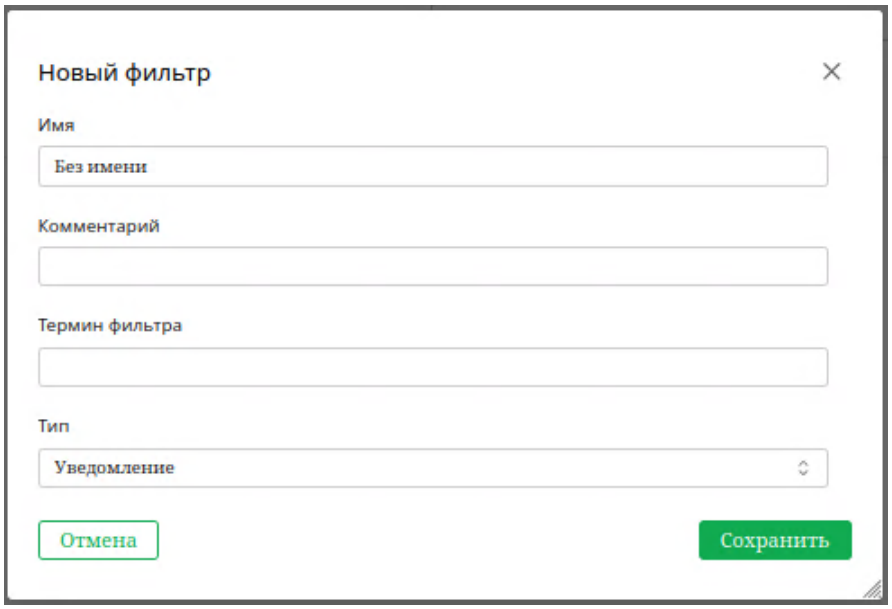

Рис. 3.9

Параметры фильтрации можно ввести в поле «Фильтр» (рис. 3.10) или изменить следующим образом:

1) нажать кнопку на панели фильтров для редактирования фильтра (рис. 3.10);

Рис. 3.10

2) в окне «Обновить фильтр» (рис. 3.11) изменить параметры фильтрации заполнив необходимые данные;

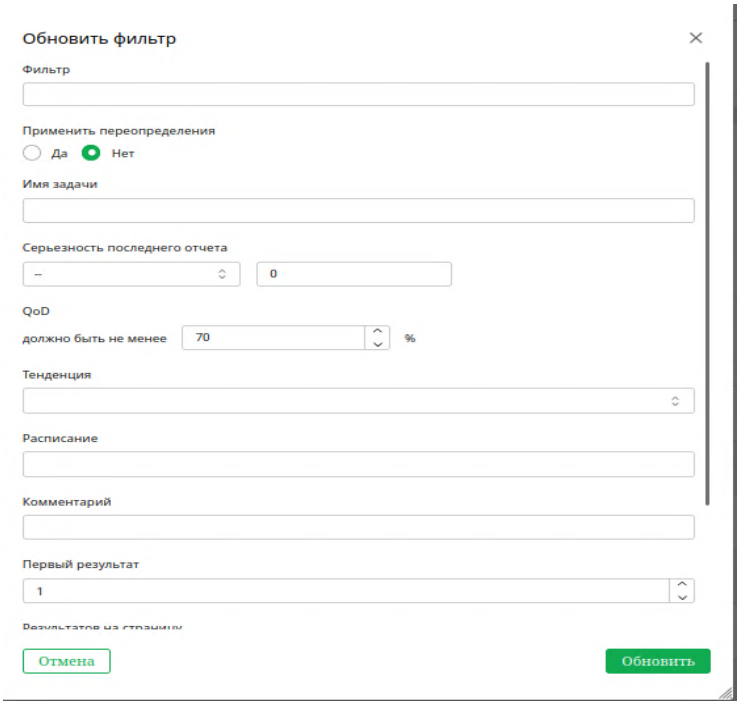

Рис. 3.11

3) нажать кнопку «Обновить».

Изм.№	Подп.	Дата

Для вводимых символов в поле «Фильтр» (см. рис. 3.12) не учитывается регистр. Все прописные буквы преобразуются в строчные перед применением фильтра.

Для параметров фильтрации доступны действия: ✕, ⟳, ↺.

Сохраненные параметры фильтрации окна «Фильтр» будут отображены в раскрывающемся списке фильтров выбранного раздела (страницы) (рис. 3.12).

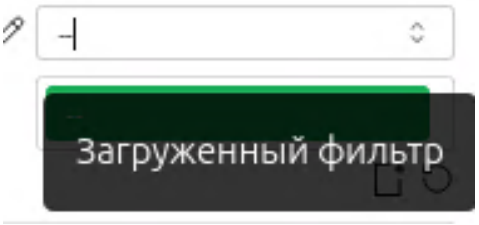

Рис. 3.12

3.5.2 Управление фильтрами

Все существующие фильтры отображаются в виде списка на странице «Конфигурация» → «Фильтры» (рис. 3.13).

Рис. 3.13

Для всех «Фильтров» отображается следующая информация:

– «Имя» – наименование фильтра;
– «Термины фильтра» – параметры фильтрации;
– «Тип» – тип объекта, к которому может быть применен «Фильтр»;

Доступные действия»: 🗑, ✎, 👁, ⇪.

Для отображения подробной информацию о фильтре необходимо нажать по наименованию фильтра. Для получения сведений о фильтре необходимо нажать кнопку 🔍.

3.6 Использование тегов

Теги – это информация, которая может быть связана с любым объектом. «Теги» создаются непосредственно с объектами и могут быть связаны только с типом объекта, для которого они созданы.

Теги можно использовать для фильтрации объектов.

При фильтрации по тегу должен быть установлен конкретный тег. В противном случае желаемый результат не будет найден.

3.6.1 Создание и управление тегами

Для создания и управления тегами необходимо:

1) выбрать в строке меню «Конфигурация» → «Теги»;
2) нажать кнопку 🗋+ для создания нового тега;
3) в открывшемся окне (рис. 3.14) определить наименование тега, выбрать тип ресурса, для которого может быть присвоен тег, в раскрывающемся списке «Тип ресурса»;

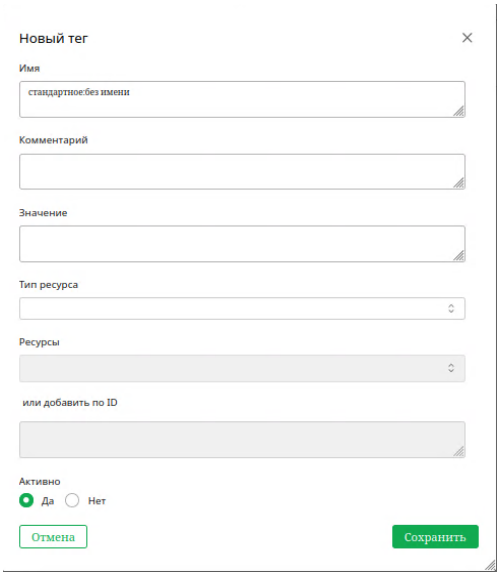

Рис. 3.14

4) нажать кнопку «Сохранить».

Все существующие теги отображаются при выборе в строке меню «Конфигурация» → «Теги» (рис. 3.15).

Рис. 3.15

3.6.2 Привязка тега к отдельному объекту или нескольким объектам

Для создания тега к отдельному объекту необходимо:

1) нажать по наименованию объекта и нажав кнопку открыть страницу сведений об объекте;

2) перейти во вкладку «Пользовательские теги», нажать кнопку для создания или нажать кнопку для редактирования;

3) выбрать «Тег» из раскрывающегося списка или создать новый, нажав на кнопку (рис. 3.16);

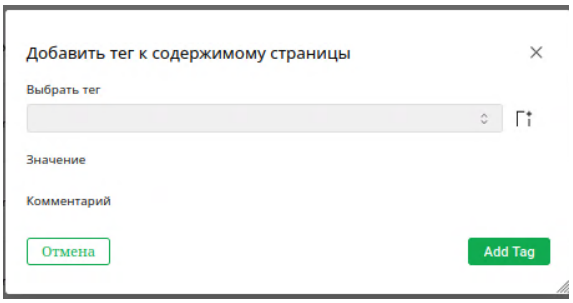

Рис. 3.16

4) нажать кнопку «Добавить».

Для добавления тега к нескольким объектам одного типа необходимо:

1) открыть страницу списка типов объектов, отфильтровать список так, чтобы

отображались только те объекты, у которых должен быть данный «Тег»;

2) в раскрывающемся списке под перечнем объектов выбрать наименование объектов, к которым необходимо добавить «Тег»;

3) нажать кнопку «Добавить тег к выделению»;

4) в появившемся окне (см. рис. 3.16) выбрать «Тег», который необходимо применить ко всем отфильтрованным объектам страницы;

5) нажать кнопку «Добавить».

3.7 Использование корзины

Для перехода на страницу «Корзина» в строке меню выбрать «Администрирование» → «Корзина». На странице перечислены все объекты, которые в данный момент находятся в корзине, сгруппированные по типу данных.

Содержимое сводной таблицы показывает все возможные типы удаленных объектов с указанием количества объектов. При нажатии по наименованию объекта отобразится перечень удаленных объектов для данного типа данных (рис. 3.17).

Объекты на странице «Корзина» окончательно удаляются только при ручном удалении их из корзины или при нажатии на кнопку «Очистить корзину» в верхнем правом углу страницы (рис. 3.17).

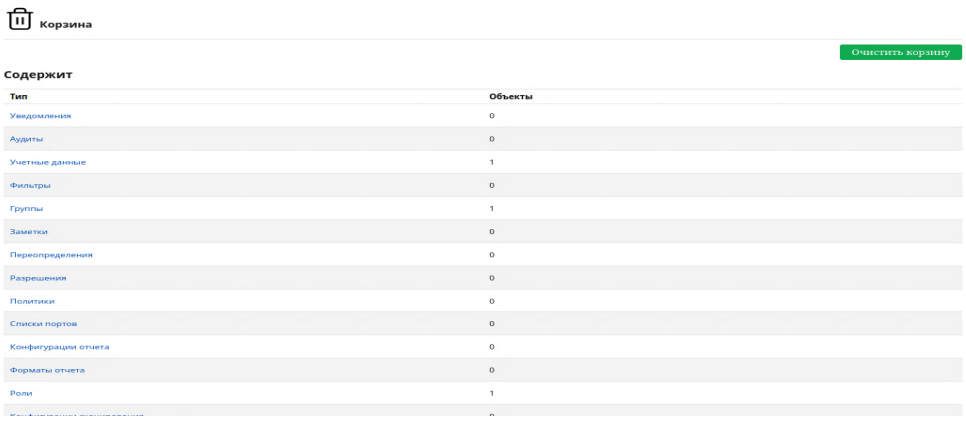

Рис. 3.17

В разделе «Тип» допускается управление отдельными объектами:

– восстановление данных из корзины (объект не может быть восстановлен, если он зависит от другого объекта в корзине);

– безвозвратно удалить объект (объект не может быть удален, если от него зависит другой объект в корзине).

3.8 Отображение состояния канала

Для отображения статуса синхронизации канала необходимо выбрать в строке меню «Администрирование» → «Состояние базы знаний».

На странице отобразится следующая информация (рис. 3.18):

– «Тип» – NVT, SCAP, CERT или GVMD_DATA;

– «Содержание» – тип информации, предоставляемой каналом;

– «Происхождение» – имя службы синхронизации канала;

– «Версия» – номер версии данных;

– «Статус» – информация о состоянии канала, время, прошедшее с момента последнего обновления.

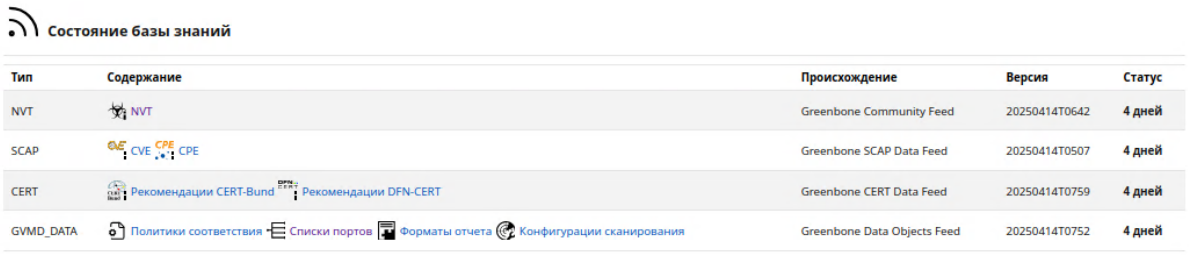

Рис. 3.18

3.9 Изменение пользовательских настроек

В «Сканер уязвимостей» каждому пользователю предоставляется управление настройками веб-интерфейса в зависимости от назначенных прав ролевой модели. Для доступа к настройкам необходимо в правом верхнем углу нажать на кнопку и выбрать раздел «Настройки» (рис. 3.19).

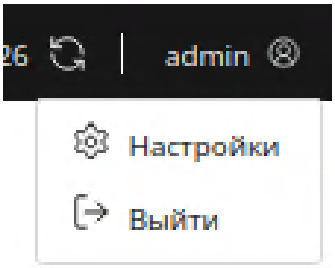

Рис. 3.19

При открытии раздела «Мои настройки» отображаются основные параметры настройки «Сканер уязвимостей» установленные пользователем или используемые по умолчанию (рис. 3.20).

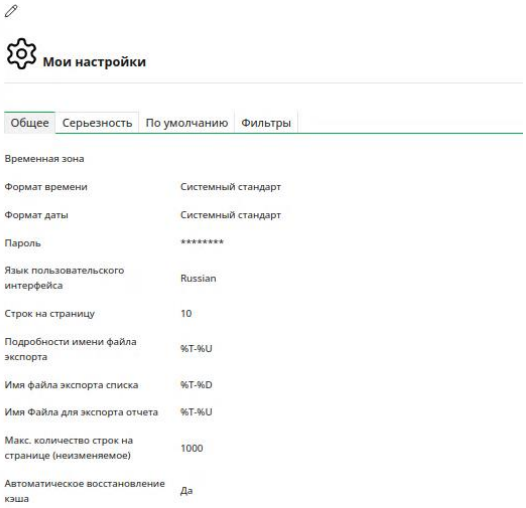

Рис. 3.20

Для изменения настроек нажать на кнопку в левом верхнем углу. В открывшемся окне предоставляется возможность редактировать настройки учетной записи (рис. 3.21):

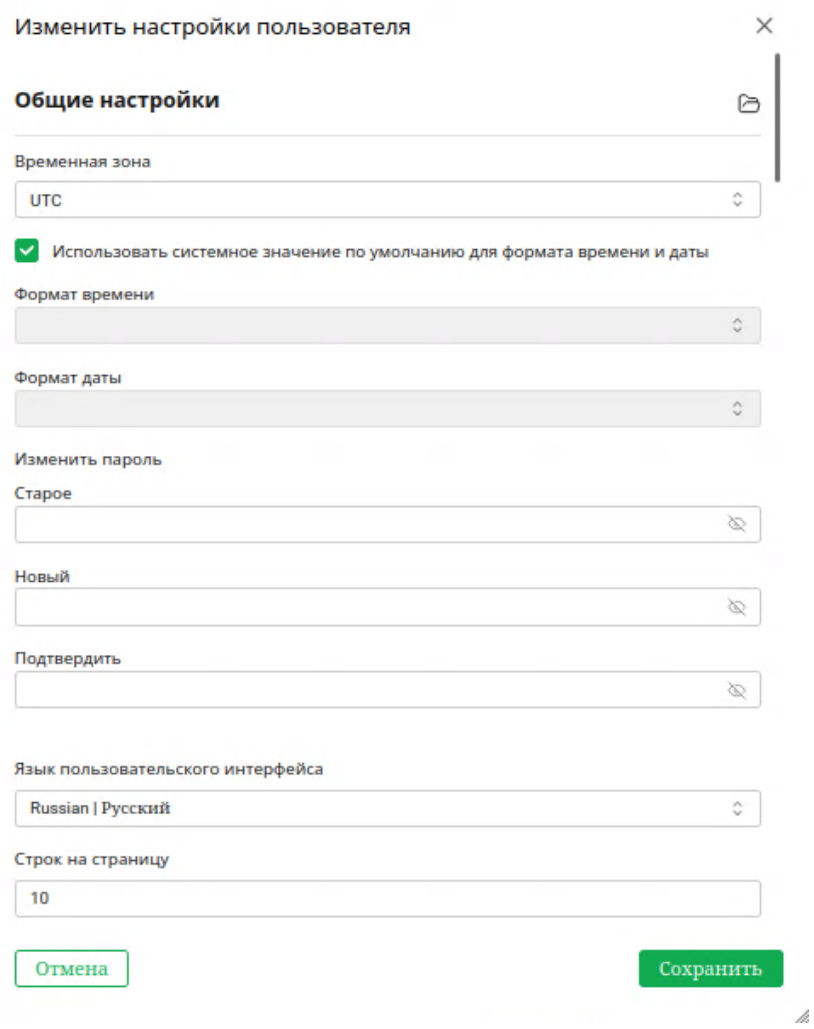

Рис. 3.21

1) «Общие настройки»:
   - «Временная зона» – «Сканер уязвимостей» сохраняет всю информацию в часах реального времени внутри устройства;
   - «Изменить пароль» – изменение пароля пользователя;
   - «Язык пользовательского интерфейса» – отображение текстовой информации интерфейса на выбранном языке;
   - «Строк на странице» – отображение выбранного количества объектов по умолчанию на странице списка в веб-интерфейсе;
   - «Подробности экспорта имени файла» – формат имени файла, содержащего экспортируемый объект;
   - «Список имен файлов экспорта» – формат имени файла, содержащего экспортируемый список объектов;
   - «Имя файла экспорта отчета» – формат имени файла, содержащего экспортируемый отчет;
   - «Автоматическое восстановление кэша» – предоставляет возможность включить или отключить автоматическое кэширование действий, выполняемых в программном обеспечении (ПО), включая действия пользователя. При выполнении нескольких действия подряд (например, удаление нескольких объектов) с включенной автоматической перестройкой кэша, каждое действие запускает перестройку кэша, что приводит к

замедлению процесса. В таких случаях автоматическое восстановление кэша может быть временно отключено;

2) «Настройка серьезности»:
   – «Динамическая серьезность» – определяет, изменяется ли серьезность существующего результата при изменении базового NVT. В противном случае новая степень серьезности повлияет только на будущие проверки;
   – «Уровень серьезности по умолчанию» – допустимый уровень серьезности;
3) «Настройки по умолчанию»:
   – «Уведомления по умолчанию» – уведомления по умолчанию согласно заданных параметров. В случае, если для NVT не назначена серьезность, используется параметры по умолчанию;
   – «Учетные данные ESXi по умолчанию» – выбор учетной записи;
   – «Конфигурация сканирования сканера по умолчанию» – выбор конфигурации сканирования;
4) «Настройки фильтра» – фильтры по умолчанию для каждой страницы.

3.10 Создание и управление пользователями

«Сканер уязвимостей» в зависимости от ролевой модели позволяет создавать и управлять пользователями.

После установки ПО «Сканер уязвимостей», по умолчанию создается пользователь с правами администратора и возможностями создания и управления пользователями системы.

Роль – описание набора полномочий пользователей или групп. Система управления пользователями устройства поддерживает концепцию разрешений на основе ролевой модели при доступе к веб-интерфейсу. Дополнительные роли могут быть созданы и назначены администратором системы. Роль определяет, какие параметры веб-интерфейса могут быть предоставлены пользователям. Принудительное выполнение ролей реализовано не в веб-интерфейсе, а скорее в базовом протоколе управления и, таким образом, влияет на всех клиентов GMP. Права на чтение и запись могут быть назначены ролям отдельно.

Группы – назначение определенных прав на доступ к ресурсам ПО.

Группы и роли предоставляют возможность для назначения прав на доступ к ресурсам ПО для нескольких пользователей.

Каждому пользователю присваивается диапазон IP-адресов, содержащий разрешенные или запрещенные целевые адреса. Доступ к определенным интерфейсам устройства может быть разрешен или запрещен.

Для создания «Пользователя» необходимо:

1) войти в систему с ролью «Администратор»;
2) выбрать в строке меню «Администрирование» → «Пользователи»;
3) создать нового пользователя, нажав кнопку ;
4) ввести логин пользователя, комментарий, пароль, определить роль, группу и хост-доступ для доступа к ресурсам ПО (рис. 3.22):
   – «Имя пользователя» – это имя, используемое для аутентификации в системе. Имя должно содержать буквы и цифры, но не более 80 символов;
   – «Комментарий» – поле пояснительных заметок или критических замечаний о пользователе;
   – «Аутентификация» – пароль, используемый для входа в систему. Пароль может содержать символы любого типа, но не более 40 символов;
   – «Роли» – права пользователя при использовании. Каждый пользователь может иметь несколько ролей. Доступны роли администратора и пользователя. Кроме того, можно добавлять и настраивать пользовательские роли;
   – «Группы» – членство пользователя в рамках системы. Пользователь может

принадлежать к нескольким группам. Управление разрешениями также может выполняться с помощью групп;

– «Хост-доступ» – хосты, на которых пользователю разрешено запускать сканирование. Ограничения распространяются и на администраторов системы, но им разрешено снимать их самостоятельно. Пользователь (User) и роли, не имеющие доступа к управлению учетными данными пользователей, не могут обойти ограничения. В зависимости от ролевой модели пользователю назначаются доступные ресурсы с помощью параметров: «запретить все и разрешить»/«разрешить все и запретить»;

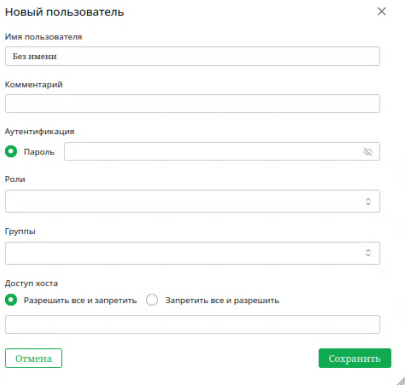

Рис. 3.22

5) нажать кнопку «Сохранить».

Все существующие пользователи отображаются при входе в систему под ролью администратора, для этого необходимо выбрать в строке меню «Администрирование» → «Пользователи».

Доступные действия»: , , (доступно удаление пользователей, которые в данный момент не вошли в систему), , , .

Для отображения подробной информацию о пользователе необходимо нажать на имя пользователя. Для отображения страницы сведений о пользователе необходимо нажать кнопку (рис. 3.23).

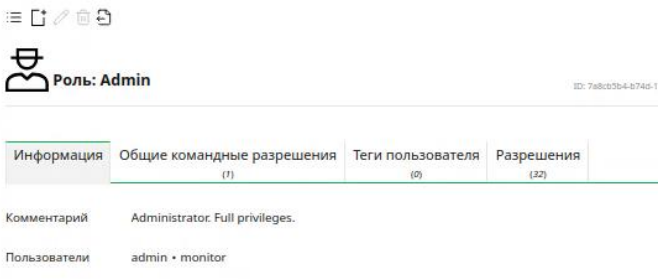

Рис. 3.23

В «Сканер уязвимостей» присутствует ограничение на одновременный вход в систему с одного локального ПЭВМ. При необходимости вход в систему должен выполняться с другого ПЭВМ или с другого браузера. Повторный вход в систему в том же браузере деактивирует открытую сессию пользователя.

3.11 Создание и управление ролями

Веб-интерфейс предоставляет возможность создания и настройки собственных ролей пользователей. По умолчанию доступны следующие роли:

«Admin» – роль по умолчанию имеет все разрешения. В частности, разрешено создавать других пользователей, роли и группы и управлять ими;

«User» – по умолчанию, роль имеет все разрешения на доступ к ресурсам ПО, кроме управления пользователями, ролями и группами. Роль не имеет разрешений синхронизировать каналы и управлять ими.

«Observer» — обозреватель. Имеет права только на просмотр. Обозревателю запрещается создавать, удалять, редактировать или использовать любые задачи, цели и т.д. Обозреватель имеет доступ только к тем объектам, доступ к которым был явно разрешен;

«Info» — информационный обозреватель. Имеет доступ только на чтение данных на информационной панели базы знаний. Вся остальная информация недоступна. Имеет права на редактирование параметров собственной учетной записи (например, изменение пароля);

«Guest» — гость. Аналогично роли информационного обозревателя («Info»). Не имеет прав на редактирование параметров собственной учетной записи;

«Monitor» — наблюдатель. Роль предназначена для осуществления мониторинга производительности. Имеет права на просмотр ответов о производительности системы.

Изменить роли по умолчанию невозможно, но их можно скопировать (клонировать) и впоследствии редактировать.

3.11.1 Создание роли с ограниченной и расширенной функциональностью

Для создания роли с ограниченной функциональностью необходимо:

1) войти в систему с ролью «Администратор»;
2) выбрать в строке меню «Администрирование» → «Роли»;
3) создать новую роль, нажав кнопку ;
4) определить параметры роли пользователя:

– «Имя» – наименование роли, содержащее буквы и цифры, но не более 80 символов;

– «Комментарий» – дополнительная информация о роли;

– «Пользователи» – список пользователей с этой ролью выбирается из раскрывающегося списка «Пользователи»;

5) нажать кнопку «Сохранить».

Роль с ограниченной функциональностью создана и отображается на странице «Роли».

Для создания роли с расширенной функциональностью в профиле пользователя необходимо:

1) в строке роли нажать кнопку и отредактировать параметры пользователя;
2) добавить разрешение, выбрав его наименование в раскрывающемся списке и нажав кнопку «Создать разрешение», при необходимости удалить разрешение, нажав кнопку в списке разрешений;
3) нажать кнопку «Сохранить».

Для всех ролей доступны действия: (в корзину перемещаются только роли, созданные от имени данного пользователя), (редактировать можно только роли, созданные от имени данного пользователя), , .

Для отображения сведений о роли нажать на наименование роли и в раскрывшемся перечне кнопку .

На странице «Роли» доступны следующие действия: , , (в корзину перемещаются только роли, созданные от имени данного пользователя), (редактировать можно только самостоятельно созданные роли), , .

Роли распределяются при создании нового пользователя (рис. 3.24).

При назначении пользователю более одной роли, права доступа для этих ролей будут добавлены автоматически.

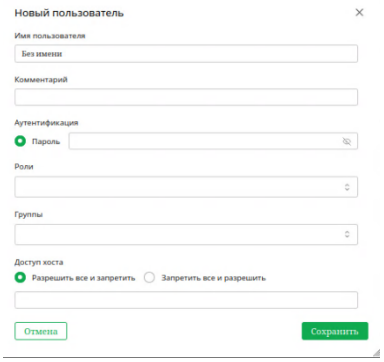

Рис. 3.24

3.12 Создание и управление группами

Группы используются для назначения определенных прав на доступ к ресурсам ПО. Количество групп для создания неограниченно. Группам могут быть назначены разрешения. По умолчанию группы не настроены.

Для создания группы необходимо:

1) войти в систему с ролью «Администратор»;
2) выбрать в строке меню «Администрирование» → «Группы»;
3) создать новую группу, нажав кнопку ;
4) определить параметры группы (рис. 3.26):

– «Имя» – наименование группы содержит буквы и цифры, но не более 80 символов;

– «Комментарий» – дополнительная информация о группе;

– «Пользователи» – список пользователей группы допускается выбрать в раскрывающемся списке «Пользователи». Пользователями группы возможно управлять в профиле пользователя;

– «Особые группы» – установить флажок, если все участники группы должны иметь доступ на чтение и запись ко всем ресурсам группы;

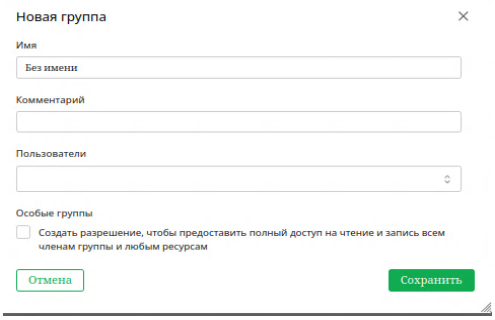

Рис. 3.26

5) нажать кнопку «Сохранить».

Для всех групп доступны следующие действия: , , , , .

Для отображения подробной информацию о группе необходимо нажать по наименованию группы. Для получения сведений о группе нажать кнопку .

3.13 Разрешения

Для просмотра всех разрешений, назначенных в системе, в строке меню выбрать «Администрирование» → «Разрешения». Если создано несколько ролей, то могут существовать множественные разрешения.

Каждое разрешение относится только к одному объекту. Разрешение позволяет субъекту выполнить связанное с ним действие (рис. 3.27).

Субъекты могут быть следующих типов:

– Пользователи;
– Роли;
– Группы.

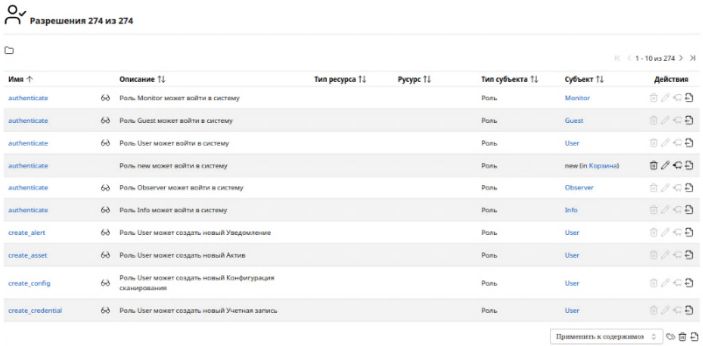

Рис. 3.27

3.13.1 Создание и управление разрешениями

Для создания нового разрешения необходимо:

1) выбрать в строке меню «Администрирование» → «Разрешения»;
2) создать новое разрешение, нажав кнопку ;
3) определить параметры разрешения (рис. 3.28):

– «Имя» – разрешение из списка, которое должно быть предоставлено;
– «Комментарий» – в комментарии разрешение описывается более подробно;
– «Субъект» – субъект (пользователь, роль или группа), которому должно быть предоставлено разрешение;
– «Тип ресурса» – доступные разрешения для роли пользователя;
– «ID ресурса» – данные ID ресурса для сканирования;
– «Описание» – описание;

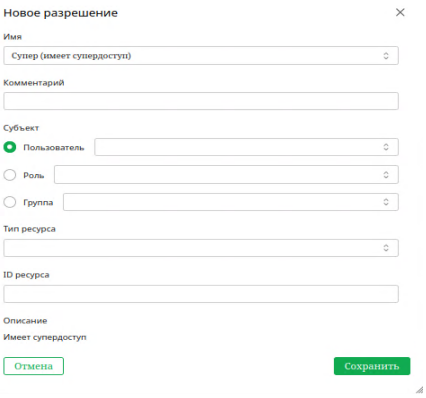

Рис. 3.28

4) нажать кнопку «Сохранить».

Для всех разрешений доступны действия: , , , , .

Нажать по названию разрешения, чтобы отобразить подробную информацию о разрешении. Нажать кнопку , для открытия страницы сведений о разрешении.

3.13.2 Предоставление дополнительных разрешений

Любой ресурс на устройстве (например, пользователь, задача) принадлежит определенному пользователю.

Ресурсы могут просматриваться и использоваться только их владельцем. Для

предоставления ресурсов другим пользователям необходимы дополнительные разрешения.

Администратор назначает супер разрешения для:

– Пользователь;
– Роль;
– Группа;
– Любая.

Супер разрешения обеспечивают полный доступ к любому ресурсу соответствующего пользователя, роли, группы.

Только супер администратор может предоставлять супер разрешения любому другому пользователю, роли или группе.

Для создания супер разрешения необходимо:

1) нажать на имя пользователя/роли/группы на странице «Пользователи»/«Роли»/«Группы», для которых должны быть назначены супер разрешения;
2) открыть страницу сведений, нажав кнопку ;
3) записать или скопировать идентификатор;
4) выбрать в строке меню «Администрирование» → «Разрешения»;
5) нажать кнопку для создания нового разрешения;
6) выбрать параметры в раскрывающемся списке «Новое разрешение» (см. рис. 3.29);
7) в раскрывающемся списке выбрать пользователя/роль/группу, у которых должны быть супер разрешения;
8) выбрать в раскрывающемся списке «Тип ресурса», для которого назначаются супер разрешения;
9) ввести или вставить ранее определенный идентификатор в поле ввода «ID пользователя»;
10) нажать кнопку «Сохранить».

3.13.3 Создание разрешений на странице сведений о ресурсе

Для создания разрешений на странице сведений о ресурсе необходимо:

1) открыть страницу сведений о ресурсе выбрав «Сканирование» → «Задачи»;
2) нажать по наименованию задачи;
3) нажать кнопку , для открытия страницы сведений о задаче;
4) нажать на кнопку «Разрешения»;
5) нажать кнопку , для создания нового разрешения (раздел «Разрешения»);
6) в появившемся окне (рис. 3.29) установить:

– тип разрешения: «Читать» (предоставление разрешения на чтение информации) или «Писать» (предоставление разрешения на просмотр и запись информации);
– к кому применять данное разрешение: Пользователь/Роль/Группа;
– параметр задачи;

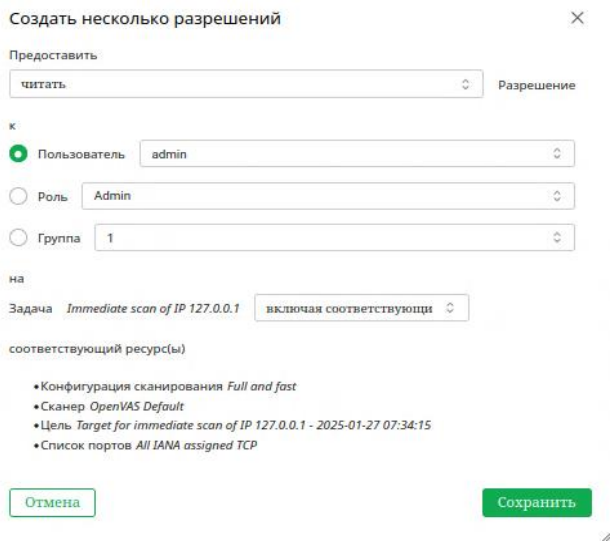

Рис. 3.29

7) нажать кнопку «Сохранить».

Созданное разрешение отображается в разделе «Разрешения» на странице сведений о ресурсе.

3.14 Настройка сканирования

3.14.1 Создание цели

Для создания цели сканирования необходимо:

1) выбрать в строке меню «Конфигурация» → «Цели»;
2) нажать кнопку для создания новой цели;
3) заполнить параметры о цели (рис. 3.30);

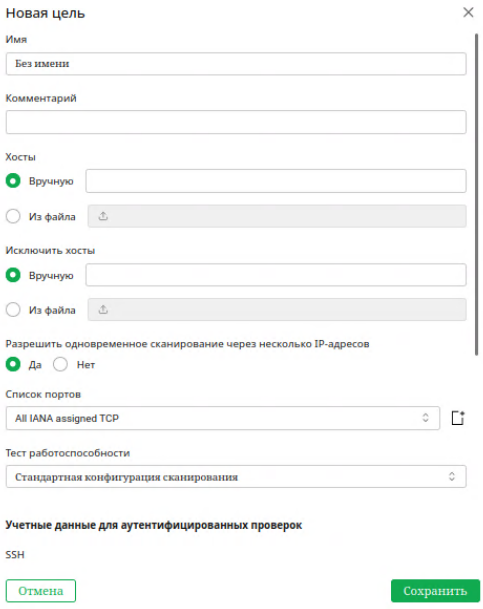

Рис. 3.30

4) нажать кнопку «Сохранить».

Добавленная цель будет отображена в разделе «Цель». Для всех целей доступны действия: , , , , .

3.14.2 Создание задачи

Для создания и настройки задачи необходимо выбрать в строке меню «Сканирование» → «Задачи», нажать кнопку .

Существуют следующие варианты создания задачи:

– «Новая задача»;

– «Новая задача контейнер».

3.14.2.1 При выборе создания «Новая задача» откроется форма (рис. 3.31), в которой необходимо заполнить следующие поля:

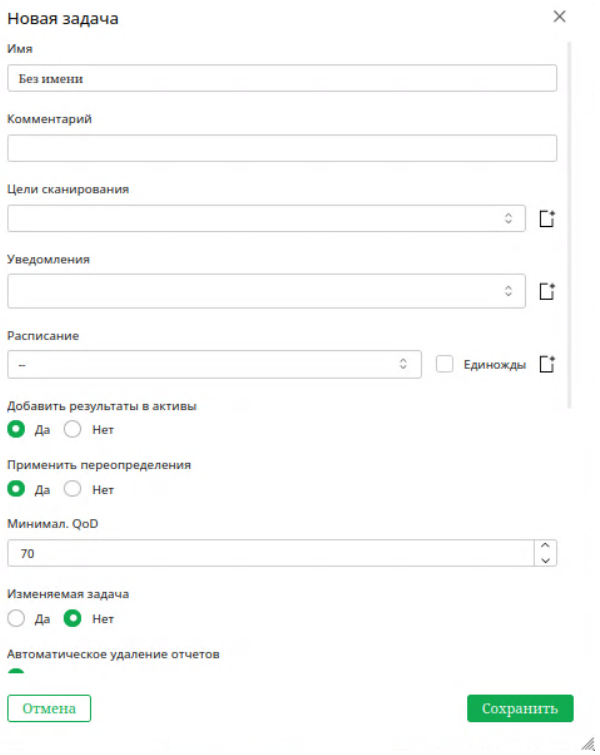

Рис. 3.31

1) «Имя» – наименование задачи;

2) «Комментарий» – дополнительный комментарий (при необходимости);

3) «Цель сканирования» – поле для выбора ранее созданной цели сканирования. При необходимости создать новую цель сканирования, необходимо нажать кнопку ;

4) «Уведомления» – настройка уведомления по заданным параметрам для данной задачи. Использование и создание оповещений согласно 3.23;

5) «Расписание» – задание времени сканирования. Управление и создание расписания согласно 3.22;

6) «Добавить результаты в активы» – добавление результатов сканирования в базу данных активов;

7) «Применить переопределения» – применение переопределений при добавлении результатов в базу данных активов;

8) «Минимальное QoD» – минимально допустимый уровень достоверности обнаружения уязвимости для добавления результатов в базу данных активов. Значение и типы QoD приведены в таблице 5;

9) «Изменяемая задача» – разрешение или запрет на изменение создаваемой задачи;

10) «Автоматическое удаление отчетов» – разрешение или запрет на автоматическое удаление старых отчетов при достижении указанного количества отчетов;

10) «Сканер» – поле для выбора вида сканера;

11) «Конфигурация сканирования» – поле для выбора конфигурации сканирования;

12) «Порядок сканирования хостов» – выбор очередности сканирования хостов. Доступны следующие варианты: «Последовательный», «Случайный», «Обратный»;

13) «Максимальное количество одновременно выполняемых NVT на хост» – количественный показатель одновременно выполняемых NVT на хост;

14) «Максимальное количество одновременно сканируемых хостов» – количественный показатель одновременно сканируемых хостов.

Для завершения создания новой задачи необходимо нажать «Сохранить», после чего задача будет отображена в списке задач в разделе «Задачи».

3.14.2.2 При выборе создания «Новая контейнерная задача» откроется форма (рис. 3.32), в которой необходимо заполнить имя и комментарий (при необходимости).

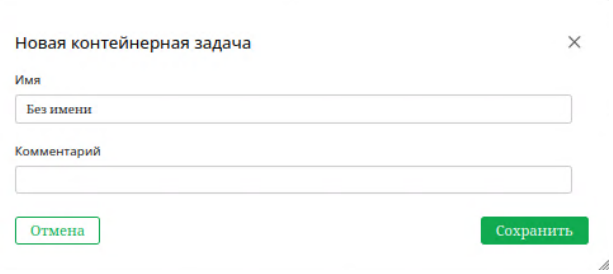

Рис. 3.32

Задача контейнера предназначена исключительно для хранения импортированных отчетов.

Для импортирования отчетов необходимо в разделе «Задачи» в строке с именем задачи контейнера нажать кнопку ⇲ в столбце «Действия». В появившемся окне

«Импортировать отчет» (рис. 3.33) выбрать файл отчета, указать задачу контейнера, в поле «Добавить в активы» выбрать «Да», для завершения процесса нажать кнопку «Импортировать».

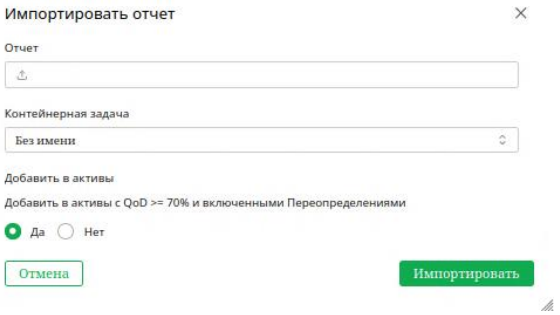

Рис. 3.33

3.14.3 Запуск задачи

Для запуска задачи сканирования необходимо в строке вновь созданной задачи нажать кнопку ▷. Задача добавится в очередь ожидания. После этого «Сканер уязвимостей» начнет сканирование по поставленной задаче.

Отчет о задаче доступен для отображения сразу после запуска задачи, нажав на строку в столбце «Статус».

Как только статус сканирования изменится на «Завершено», будет доступен полный отчет. В любой момент промежуточные результаты сканирования могут быть пересмотрены.

3.14.4 Процесс сканирования

На странице «Задачи» (рис. 3.34) отображены текущие задачи и их текущее состояние.

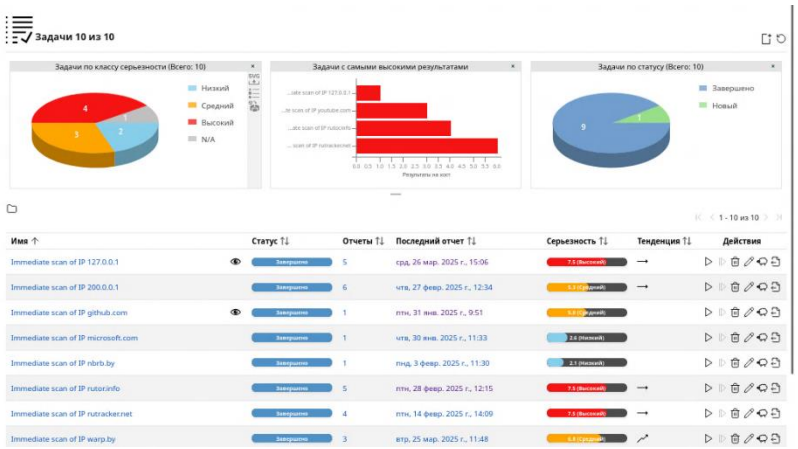

Рис. 3.34

Статус сканирования отображается в столбце «Статус» с индикаторами и уровнями заполнения:

Новый – задача не выполнялась с момента ее создания;

6 % – задача запущена и выполнена на 6 %. Процент выполнения соответствует количеству завершенных тестов NVT;

Запрошено – задача только что была запущена, подготавливается сканирование;

Удаляется – выдана команда на удаление задачи. Процесс удаления может занимать некоторое время, так как необходимо удаление отчетов;

Stop Requested – выдана команда на остановку задачи;

Остановлено на 0 % – процент выполнения задачи до ее остановки. Формирование отчета, вероятно, не завершено. Данное состояние может быть вызвано перезагрузкой «Сканер уязвимостей» или отсутствием электропитания. Задача будет возобновлена автоматически после перезапуска «Сканер уязвимостей»;

Прервано на 0 % – ошибка;

Завершено – задача выполнена успешно;

Контейнер – задача является задачей контейнером.

В крайнем правом столбце расположены кнопки для управления задачами: , , , , , , (создание отчета на момент нажатия при условии, что запушено сканирование).

3.15 Настройка проверки подлинности с использованием локальных проверок безопасности

Аутентифицированное сканирование может предоставить более подробную информацию об уязвимости в сканируемой системе. Во время проверки подлинности цель сканируется как извне, с использованием сети, так и изнутри, с использованием действительных аутентификационных данных пользователя.

Во время проверки подлинности «Сканер уязвимостей» входит в целевую систему для выполнения локальных проверок безопасности.

Для проверки требуется предварительная настройка учетных данных пользователя. Эти учетные данные используются для аутентификации в различных службах целевой системы. В некоторых случаях результаты могут быть ограничены разрешениями используемых пользователей.

VTS в соответствующих семействах NVT (локальные проверки безопасности) будут выполняться только в том случае, если «Сканер уязвимостей» смог авторизоваться в целевую систему. Локальные контрольные точки безопасности в результирующем сканировании минимально инвазивны.

«Сканер уязвимостей» только определяет уровень риска, но не вносит никаких изменений в целевую систему. Однако вход в систему с помощью устройства, вероятно, регистрируется в протоколах целевой системы.

«Сканер уязвимостей» может использовать различные учетные данные в зависимости от характера цели. Наиболее важными из них являются:

– «SMB» – в системе Microsoft Windows, «Сканер уязвимостей» может проверять уровень исправлений и локально установленное программное обеспечение, такое как Adobe Acrobat Reader или Java suite;

– «SSH» – используется для проверки уровня исправлений в системах Unix и Linux;

– «ESXi» – используется для локального тестирования серверов VMware ESXi;

– «SNMP» – сетевые компоненты, такие как маршрутизаторы и коммутаторы, могут быть протестированы через SNMP.

3.15.1 Преимущества и недостатки аутентифицированных сканирований

Объем и успешность процедур тестирования в значительной степени зависят от разрешений используемой учетной записи.

Локальные проверки безопасности – метод поиска сведений об уязвимости.

Аутентифицированное сканирование аналогично подходу «Белого ящика». «Сканер уязвимостей» имеет доступ к предварительной информации и может получить доступ к цели изнутри: доступный реестр, версии ПО.

Удаленное сканирование аналогично подходу «Черного ящика». «Сканер уязвимостей» использует те же методы и протоколы, что и потенциальный злоумышленник для доступа к цели извне. Во время тестирования «Сканер уязвимостей» может вызвать сбои в работе для извлечения любой доступной информации об используемом ПО, например, сканер может отправить неверно сформированный запрос в службу для запуска ответа, содержащего дополнительную информацию о развернутом продукте.

Во время удаленного сканирования с использованием конфигурации полного и быстрого сканирования все удаленные проверки безопасны.

3.15.2 Использование учетных данных

Учетные данные для локальных проверок безопасности необходимы, чтобы позволить VTS входить в целевые системы.

Для создания новой учетной записи необходимо:

1) выбрать в строке меню «Конфигурация» → «Учетные данные»;
2) нажать кнопку ;
3) в появившемся окне (рис. 3.35) определить сведения об учетных данных.

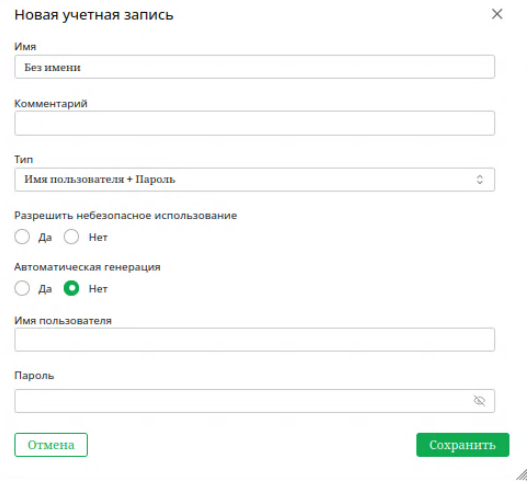

Рис. 3.35

4) нажать кнопку «Сохранить».

3.15.3. Управление учетными данными

Для отображения учетных данных выбрать в строке меню «Конфигурация» → «Учетные данные» (рис. 3.36).

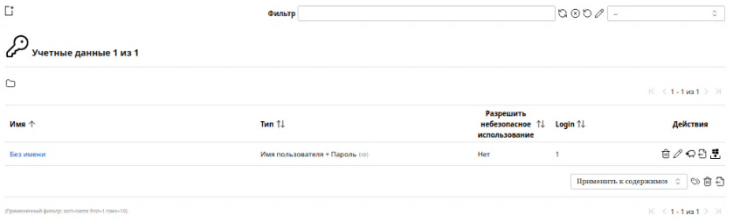

Рис. 3.36

Для всех учетных записей доступны действия: , , , , (в корзину можно переместить только те учетные данные, которые в данный момент не используются).

В зависимости от выбранного типа учетных данных могут быть доступны дополнительные действия:

– загрузить EXE-пакет для Microsoft Windows (доступно, если выбран тип аутентификации «Имя пользователя + пароль»);

– загрузить RPM-пакет для Red Hat Enterprise Linux и его производных (доступно, если выбран тип аутентификации «Имя пользователя + SSH-ключ»);

– загрузить пакет Debian для Debian GNU / Linux и производных от него (доступно, если выбран тип аутентификации «Имя пользователя + SSH-ключ»);

– загрузить открытый ключ (доступно, если выбран тип аутентификации «Имя пользователя + SSH–ключ или сертификат клиента»).

3.16 Требования к целевым системам с Microsoft Windows

Для доступа к реестру необходимо запустить службу «Удаленного реестра».

Если автоматический запуск нежелателен, можно настроить ручной запуск. В этом случае служба запускается во время сканирования системы устройством, а затем снова отключается. Чтобы обеспечить такое поведение, необходимо учитывать следующую информацию о LocalAccountTokenFilterPolicy.

Необходимо, чтобы для всех сканируемых систем был активирован общий доступ к файлам и принтерам. При использовании Microsoft Windows XP, позаботьтесь об отключении параметра «Использовать простой общий доступ к файлам».

Для отдельных систем, не привязанных к домену, должен быть установлен следующий раздел реестра:

HKLM\ПРОГРАММНОЕОБЕСПЕЧЕНИЕ\Microsoft\Windows\CurrentVersion\ Политики\Система\DWORD: LocalAccountTokenFilterPolicy= 1

В системах с контроллером домена используемая учетная запись пользователя должна принадлежать к группе Domain Администраторы для достижения наилучших результатов. Из-за концепции разрешений невозможно обнаружить все уязвимости с помощью локального администратора или администраторов, назначенных доменом.

Если выбран локальный администратор, что явно не рекомендуется, то обязательно также установить следующий раздел реестра:

HKLM\ПРОГРАММНОЕОБЕСПЕЧЕНИЕ\Microsoft\Windows\CurrentVersion\ Политики\Система\ DWORD: LocalAccountTokenFilterPolicy = 1

Сгенерированный установочный пакет для учетных данных: программа установки переводит службу удаленного реестра в режим автоматического запуска.

Создать правило исключения для устройства в брандмауэре Microsoft Windows. Кроме того, на системах XP для общего доступа к служебным файлам и принтерам должно быть установлено значение включено.

Сгенерированный установочный пакет для учетных данных: во время установки программа установки предлагает диалоговое окно для ввода IP-адрес устройства. Если запись подтверждена, правило брандмауэра настроено. Общий доступ к служебному файлу и принтеру будет включен в правилах брандмауэра.

Для проверок соответствия требованиям, ориентированных на операционные системы Windows, рекомендуется установить максимальное значение одновременно выполняемые VTS на узел / максимальное количество одновременно сканируемых узлов равно 1, чтобы максимизировать точность результатов.

3.16.1 Настройка учетной записи домена для проверки подлинности при сканировании

Для проверки подлинности целевых систем Microsoft Windows настоятельно рекомендуется использовать доменную учетную запись с доменной политикой, предоставляющей права локального администратора.

Политику домена необходимо создать только один раз, а затем ее можно применить или отменить для разных учетных записей пользователей;

Локальное редактирование реестра Microsoft Windows больше не требуется. Таким образом, администрирование пользователей осуществляется централизованно, что экономит время в долгосрочной перспективе и снижает количество возможных ошибок конфигурации.

С точки зрения оценки уязвимости, только учетная запись домена позволяет обнаруживать связанные с доменом результаты сканирования, связанные с доменом. Эти результаты будут отсутствовать при использовании локальной учетной записи пользователя.

Использование учетной записи домена в соответствии с рекомендациями по политике домена также имеет ряд преимуществ в плане безопасности: соответствующий пользователь может не входить в систему локально или через протокол удаленного рабочего стола (RDP), что ограничивает возможные векторы атак.

Для того чтобы использовать учетную запись домена для удаленного аудита на базе хоста в целевой системе Microsoft Windows, необходимо выполнить следующую конфигурацию в Windows XP Professional, Windows Vista, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, Windows 8.1 или Windows 10. Система также должна быть частью домена.

3.16.2 Требования к целевым системам с Unix

Для аутентифицированного сканирования в системах Unix достаточно доступа пользователя. Вход в систему осуществляется через SSH. Аутентификация осуществляется либо с помощью паролей, либо с помощью закрытого SSH-ключа, хранящегося на устройстве.

Удаленный SSH-сервер должен иметь следующие настройки по умолчанию, настроенные в файле sshd_config:

Максимальное количество сеансов: 10

Максимальное количество попыток: 6

При использовании значений описанных выше могут возникать сбои при входе в систему.

Сгенерированный установочный пакет для учетных данных: установочный пакет для дистрибутивов Linux на основе Debian представляет собой DEB–файл, установочный пакет для дистрибутивов Linux на основе Red Hat представляет собой RPM-файл. Оба установочных пакета создают нового пользователя без каких–либо определенных разрешений. Открытый SSH-ключ, созданный на устройстве, хранится в домашней папке пользователя. Для пользователей других дистрибутивов Linux или производных от Unix, открытый ключ предлагается для скачивания.

В обоих случаях необходимо убедиться, что SSH не запрещает аутентификацию по открытому ключу. Строка «PubkeyAuthentication no» не должна присутствовать.

Также могут быть использованы существующие пары ключей SSH. Пары ключей SSH могут быть сгенерированы с помощью команды «ssh–keygen» в Linux или puttygen.exe при использовании PuTTY в Microsoft Windows. Чтобы использовать существующую пару ключей SSH для аутентификации, закрытый ключ должен быть предоставлен при создании учетных данных.

Закрытый ключ SSH должен быть либо в формате PEM, либо OpenSSH. Поддерживаются типы ключей Ed25519, ECDSA, RSA и DSA.

Для проверок, которые включают тестирование политик, может потребоваться разрешение «root» или членство в определенных группах. Файлы конфигурации доступны для чтения только опытным пользователям или членам определенных групп.

Чем больше разрешений у пользователя, тем больше результатов и настроек может быть обнаружено в системе. В некоторых случаях может потребоваться доступ пользователя «root».

Следующие команды выполняются с правами «root» пользователя во время проверки подлинности.

Новый или измененный VTS может добавлять новые команды в любое время.

В зависимости от найденного программного обеспечения могут выполняться дополнительные команды.

Выполняемые команды зависят от дистрибутива Linux и выбранной конфигурации сканирования.

Рекомендуется установить пакет «locate» (альтернативно «mlocate») для предоставления команды «locate /mlocate» в целевой системе. Использование этой команды сокращает количество вызовов команды «find», используемой для поиска файлов, и, таким образом, повышает производительность поиска и снижает использование ресурсов целевой системы.

Для работы команд могут потребоваться соответствующие разрешения базы данных

и регулярные обновления базы данных.

3.17 Настройка сканирования CVE

Не каждая уязвимость оправдывает новое сканирование сети или отдельных систем. Если устройство уже получило информацию об уязвимостях в результате предыдущих проверок, оно может составить прогноз того, какие угрозы безопасности могут существовать в настоящее время.

Использование сканера CVE позволяет быстро спрогнозировать возможные угрозы безопасности без необходимости проведения еще одного сканирования уязвимостей. Чтобы выполнить это, сканер CVE проверяет CPE целевых хостов, присутствующих в ресурсах хоста, на наличие назначенных CVE.

Это особенно оправдано для сред, в которых большинство уязвимостей было удалено или исправлено с помощью устройства. Если прогнозируются новые угрозы безопасности, можно запустить фактическое сканирование уязвимостей для проверки.

Существуют некоторые предварительные условия для успешного запуска сканирования CVE:

Чтобы быть обнаруженным, CVE должен иметь CPE, присвоенный в Национальной базе данных уязвимостей (NVD)

Для базы данных активов требуются текущие данные для сканера CVE. Для обнаружения продуктов перед запуском сканирования CVE необходимо выполнить полное сканирование.

Для полного сканирования необходимо активировать опцию задачи «Добавить результаты в ресурсы», чтобы результаты были добавлены в базу данных активов и доступны сканеру CVE.

Выполнение полного сканирования с аутентификацией может увеличить результаты, обнаруженные при сканировании CVE.

Необходимо регулярно проводить полное сканирование систем.

Сканирование CVE может выполняться следующим образом:

1) выбрать в строке меню «Сканирование» → «Задачи»;
2) нажать кнопку ;
3) в появившемся окне (рис. 3.37) заполнить параметры задачи. В графе «Сканер» в раскрывающемся списке выбрать CVE;

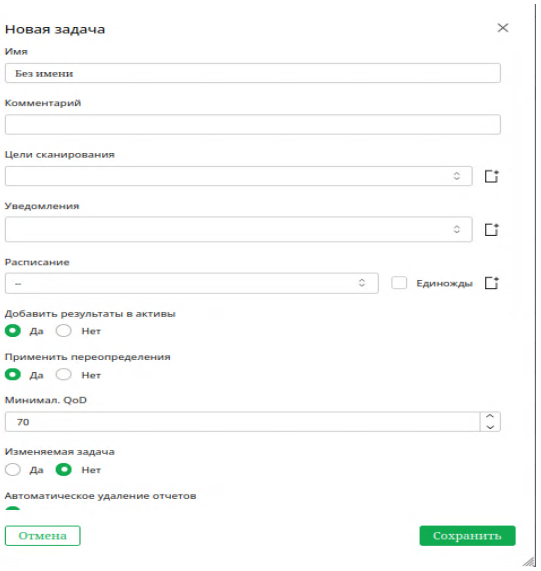

Рис. 3.37

4) нажать «Сохранить»;

5) в разделе «Задачи» в строке с задачей нажать «Запустить». Сканирование запущено. Как только статус изменится на «Готово», будет доступен полный отчет. В любой момент промежуточные результаты могут быть пересмотрены. Завершение сканирования может занять некоторое время. Страница обновляется автоматически, если доступны новые данные;

6) по завершении сканирования выбрать в строке меню «Сканирование» → «Отчеты». В строке отчета нажать на дату составления отчета для отображения результатов. В отчете каждая найденная CVE показана как уязвимость (рис. 3.38).

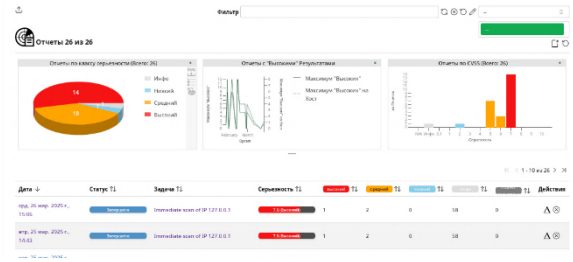

Рис. 3.38

3.18 Создание и управление списком портов

При наличии в сканируемой системе приложений, работающих на портах отличных от портов, прописанных по умолчанию, их необходимо отслеживать и тестировать с помощью «Сканер уязвимостей». При необходимости может быть создан индивидуальный список портов, включающий необходимый порт.

Все списки портов по умолчанию являются объектами данных, которые распространяются через канал. Они загружаются и обновляются с каждым обновлением канала.

Если списки портов по умолчанию недоступны, может потребоваться обновление канала или установить владельца импорта канала.

В дополнение к спискам портов по умолчанию могут быть созданы пользовательские списки портов или импортированы из файла.

Для создания списка портов необходимо:

1) выбрать в стоке меню «Конфигурация» → «Списки портов» → кнопка ;
2) в открывшемся окне (рис. 3.39) указать следующие сведения о списках портов:

– «Имя» – наименование списка портов;

– «Комментарий» – дополнительный комментарий (при необходимости);

– «Диапазоны портов» – ручной ввод диапазонов портов или импорт списка диапазонов портов. При вводе портов вручную, диапазоны портов разделяются запятыми. При импорте из файла записи могут разделяться запятыми или разрывами строк. В файле должна использоваться кодировка символов ASCII. Каждое значение в списке может быть отдельным портом (например, 7) или диапазоном портов (например, 9 – 11). Эти параметры могут быть смешанными (например, 5, 7, 9 – 11, 13).

Записи в списке может предшествовать спецификатор протокола (T: для TCP, U: для UDP), например, T:1–3, U:7, 9–11 (TCP-порты 1, 2 и 3, UDP-порты 7, 9, 10 и 11). Если спецификатор не указан, по умолчанию – TCP;

Рис. 3.39

3) нажать кнопку «Сохранить».

Список портов может быть импортирован следующим образом:

1) выбрать в строке меню «Конфигурация» → «Списки портов»;
2) нажать «Обзор» и выбрать XML-файл в списке портов;
3) нажать кнопку «Импортировать».

Все существующие списки портов можно отобразить, выбрав в строке меню «Конфигурация» → «Списки портов».

Для всего списка портов доступны действия: ✎ (редактировать можно только самостоятельно созданные списки портов, которые в данный момент не используются), 🗨, ⇪, 🗑 (в корзину можно переместить только списки портов, которые в данный момент не используются. Если список портов не удален из корзины, он не загружается заново во время следующего обновления канала).

3.19 Настройка и управление конфигураций сканирования

«Сканер уязвимостей» поставляется с различными предопределенными конфигурациями сканирования. Их можно настраивать и создавать новые конфигурации сканирования.

Для отображения существующих конфигураций сканирования необходимо выбрать в строке меню «Конфигурация» → «Конфигурации сканирования» (рис. 3.40).

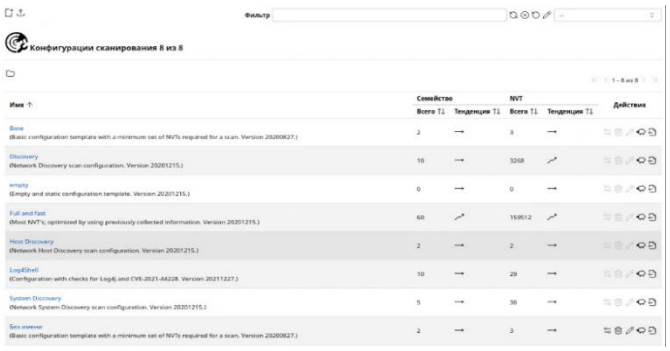

Рис. 3.40

Для всех конфигураций сканирования отображается следующая информация:

– «Имя» – имя конфигурации сканирования;
– «Семейство»:
– «Общий» – количество активированных семейств NVT для конфигурации сканирования;
– «Тренд» – Тенденция семейств NVT.

Примечание. Новые семейства NVT не включаются автоматически после обновления;

– «NVT»:
– «Общий» – количество активированных VTS для конфигурации сканирования;
– «Тренд» – тенденции VTS.

Для всех конфигураций доступны действия: ✎, 🗨, ⇪, 🗑 (в корзину можно

переместить только те конфигурации сканирования, которые в данный момент не используются. Если конфигурация сканирования не удалена из корзины, она не загружается заново при следующем обновлении канала).

3.19.1 Конфигурации сканирования по умолчанию

Все конфигурации сканирования по умолчанию представляют собой объекты данных, которые распространяются через канал. Они загружаются и обновляются с каждым обновлением канала.

Если недоступны настройки сканирования по умолчанию, может потребоваться обновление канала или может потребоваться установить владельца импорта канала.

Настройки сканирования по умолчанию редактировать нельзя. Кроме того, они могут быть временно удалены только владельцем канала импорта или администратором. Во время следующего обновления ленты они будут загружены снова.

В дополнение к конфигурациям сканирования по умолчанию могут быть созданы пользовательские конфигурации сканирования или импортированы.

По умолчанию доступны следующие конфигурации сканирования:

1) «Empty» – конфигурация сканирования представляет собой пустой шаблон, не содержащий VTS. Его можно клонировать и использовать для полностью индивидуальной конфигурации сканирования. Семейства NVT являются статическими, т.е. Новые NVT выбранных семейств NVT не добавляются и не используются автоматически;

2) «Base» – в этой конфигурации сканирования используются только VTS, которые собирают информацию о целевой системе. Его можно клонировать и использовать для создания полностью индивидуальной конфигурации сканирования. «Используемый сканер портов» – проверка активности целевого хоста. Дополнительно собирается информация об ОС. Семейства NVT являются статическими, т.е. новые NVT выбранных семейств VT не добавляются и не используются автоматически;

3) «Discovery» – в этой конфигурации сканирования используются только VTS, которые предоставляют информацию о целевой системе. Ошибок нет – неисправности не обнаружены. Среди прочего, собранная информация содержит информацию об открытых портах, используемом оборудовании, противопожарных стенах, используемых сервисах, установленном программном обеспечении и сертификатах. Система полностью инвентаризирована. Семейства NVT являются динамическими, т.е. новые NVT выбранных семейств NVT добавляются и используются автоматически;

4) «Host Discovery» – конфигурация сканирования используется для обнаружения целевых систем. «Используемый сканер портов» – проверка активности целевого хоста. Семейства NVT являются статическими, т.е. новые NVT выбранных семейств NVT не добавляются и не используются автоматически;

5) «System Discovery» – конфигурация сканирования используется для обнаружения целевых систем, включая установленные ОС тем и используемого оборудования. Никаких уязвимостей обнаружено не было. «Используемый сканер портов» – проверка активности целевого хоста. Семейства NVT являются статическими, т.е. новые NVT выбранных семейств NVT не добавляются и не используются автоматически;

6) «Full and fast» – конфигурация сканирования основана на информации, собранной при предыдущем сканировании портов, и использует почти все виртуальные машины. VTS оптимизированы наилучшим образом способ снизить вероятность ложных срабатываний особенно низко. Другие «Полные» конфигурации обеспечивают большую ценность только в редких случаях, но с гораздо большими усилиями. Семейства NVT являются динамическими, т.е. новые NVT выбранных семейств NVT добавляются и используются автоматически.

3.19.2 Создание, редактирования конфигурации сканирования

Для создания новой конфигурации сканирования необходимо:

1) выбрать в строке меню «Конфигурация» → «Сканировать» → нажать кнопку ;
2) в открывшемся окне (рис. 3.41) указать:
   – «Имя» – наименование конфигурации;
   – «Комментарий» – дополнительная информация (при необходимости);
   – «База» – выбрать переключатель базы, который необходимо использовать;

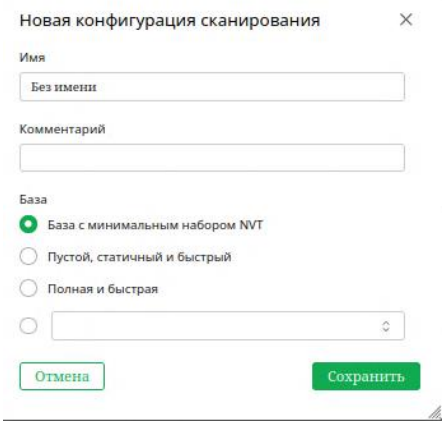

Рис. 3.41

3) нажать кнопку «Сохранить».

Для редактирования «Конфигурации сканирования» открыть в строке меню «Конфигурации» → «Конфигурации сканирования» и нажать кнопку в строке конфигурации (см. рис. 3.40) откроется веб-страница редактирования конфигураций сканирования с доступом к разделу «Редактировать семейство тестов сетевых уязвимостей» (рис. 3.42).

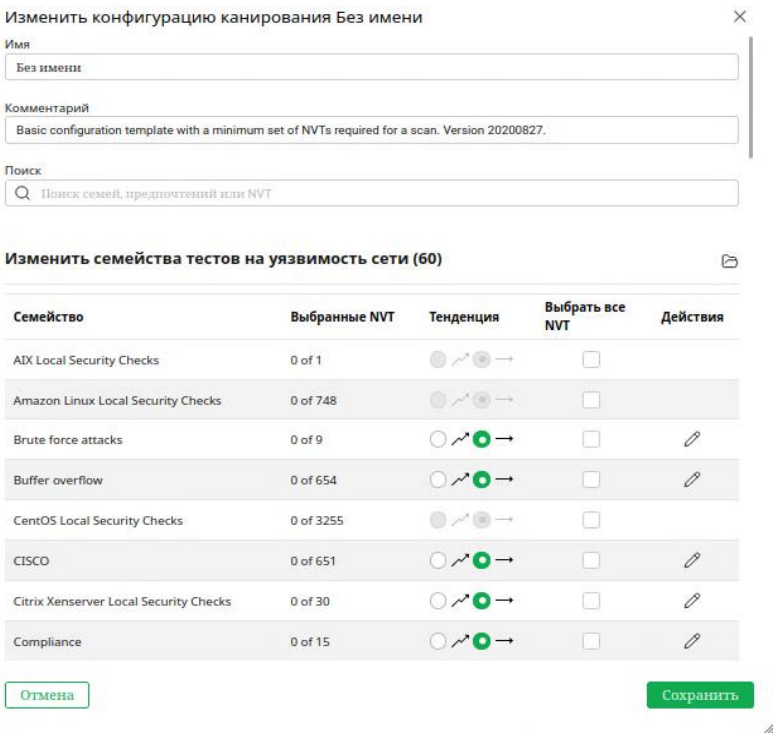

Рис. 3.42

Редактирование NVT включает загрузку текстового файла, в файле должна использоваться текстовая кодировка UTF-8.

Не допускается редактирование следующих семейств NVT:

- локальные проверки безопасности CentOS;
- локальные проверки безопасности Debian;
- локальные проверки безопасности Fedora;
- локальные проверки безопасности Huawei EulerOS;
- локальные проверки безопасности Oracle Linux;
- локальные проверки безопасности Red Hat;
- локальные проверки безопасности SuSE;
- локальные проверки безопасности Ubuntu.

3.19.3 Описание настроек сканера

Для редактирования настроек сканера необходимо открыть в строке меню «Конфигурации» → «Конфигурации сканирования» и нажать кнопку в строке конфигурации (см. рис. 3.40) откроется веб-страница редактирования конфигураций сканирования с доступом к разделу «Редактирование настроек сканера» (рис. 3.43).

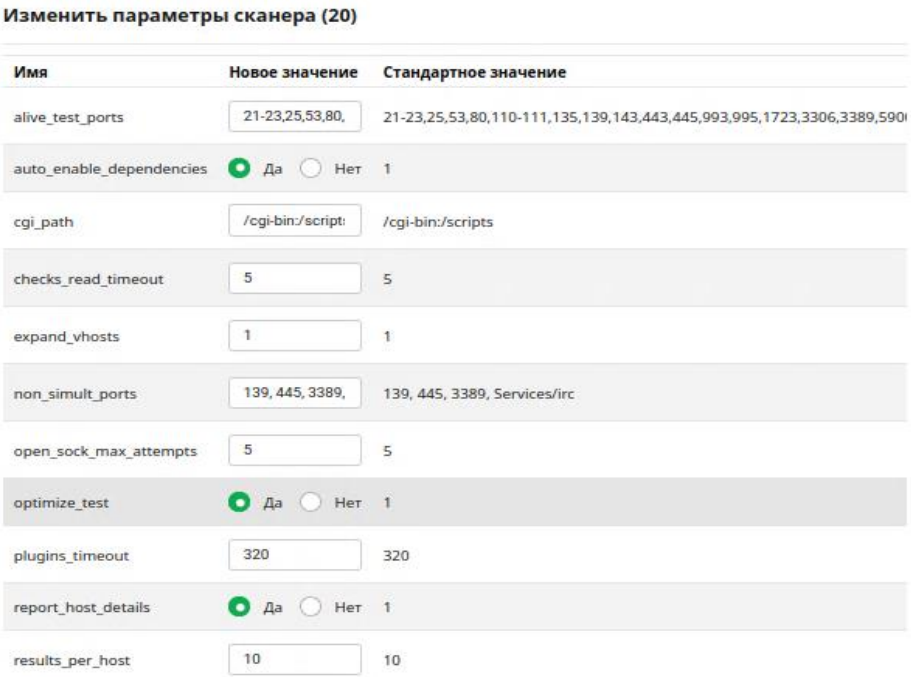

Рис. 3.43

Описание настроек сканера представлено в таблице 2.

Таблица 2

Наименование настройки	Определение
auto_enable_dependencies	определяет, будут ли VTS, требуемые другими VTS, активироваться автоматически
cgi_path	путь, используемый VTS для доступа к CGI-скриптам
checks_read_timeout	время ожидания сетевых сокетов во время сканирования
test_empty_vhost	сканер также сканирует целевой объект, используя пустые значения vhost в дополнение к связанным с целевым объектом значениям vhost
max_sysload	максимальная нагрузка на устройство. После достижения этой нагрузки дальнейшие VTS не запускаются до тех пор, пока нагрузка снова не упадет ниже этого значения

Наименование настройки	Определение
min_free_mem	минимальная доступная память (в МБ), которая должна быть свободна на устройстве. После того, как этот предел достигнут, дополнительные виртуальные машины не запускаются до тех пор, пока снова не будет доступно достаточное количество памяти
non_simult_ports	эти порты не тестируются VTS одновременно
optimize_test	VTS запускается только при выполнении определенных предварительных условий (например, при открытии портов или обнаружении приложения)
plugins_timeout	максимальное время выполнения NVT
safe_checks	некоторые виртуальные машины могут привести к повреждению хост-системы. Этот параметр отключает соответствующие виртуальные машины
scanner_plugins_timeout	максимальное время выполнения (в секундах) для всех виртуальных машин семейства NVT для сканирования портов. Если NVT работает дольше, он завершается
expand_vhosts	список vhosts целевого хоста расширяется значениями, собранными из таких источников, как запросы обратного поиска и проверки NVT на наличие сертификатов SSL / TLS
time_between_request	время ожидания (в миллисекундах) между двумя действиями, такими как открытие TCP–сокета, отправка запроса через открытый tcp-сокет и закрытие TCP-сокета
timeout_retry	количество повторных попыток, если время ожидания при попытке подключения к сокету истекло
unscanned_closed	определяет, необходимо ли рассматривать TCP-порты, которые не были проверены, как закрытые порты
unscanned_closed_udp	определяет, необходимо ли рассматривать порты UDP, которые не были проверены, как закрытые порты

3.19.4 Импорт конфигурации сканирования

Для импорта конфигурации сканирования необходимо:
1) выбрать в строке меню «Конфигурация» → «Сканировать»;
2) нажать «Обзор» и выбрать XML-файл конфигурации сканирования;
3) нажать кнопку «Импортировать» (рис.3.44).

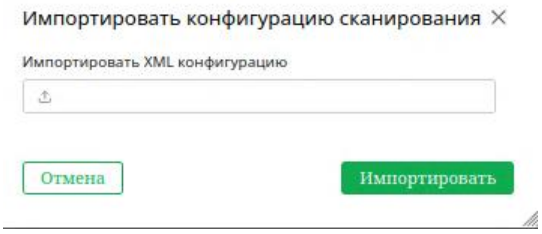

Рис. 3.44

3.20 Выполнение запланированного сканирования и управление расписанием

«Сканер уязвимостей» поддерживает планирование задач для их автоматизации и ссылается на расписания как на автоматические проверки в определенное время. Они могут выполняться один или несколько раз.

По умолчанию «Сканер уязвимостей» не предоставляет никаких расписаний.

Для создания нового расписания необходимо:

1) выбрать в строке меню «Конфигурация» → «Расписание» → ;
2) в открывшемся окне (рис. 3.45) указать детали расписания:

– «Имя» – наименование расписания;

– «Комментарий» – дополнительная информация (при необходимости);

– «Временная зона» – определение часового пояса. По умолчанию используется UTC±00:00;

– «Первый запуск» – определение даты и времени начала первого сканирования.

– «Продолжительность» – определение максимальной продолжительности, которую задача может занять для своего выполнения. Продолжительность зависит от указанного времени начала и окончания. Если определено время окончания и назначенное время истекло, задача прерывается и будет приостановлена до тех пор, пока не станет доступен следующий запланированный временной интервал. Таким образом, можно гарантировать, что сканирование всегда будет выполняться с определенным временным интервалом (обслуживания).

– «Повторение» – определение частоты повторения задачи: однократная, почасовая, ежедневная, еженедельно, ежемесячно, ежегодно, по рабочим неделям (с понедельника по пятницу) или на заказ. Если выбран параметр

– «Пользовательский», можно выбрать частоту повторения и дни, в которые должна выполняться задача;

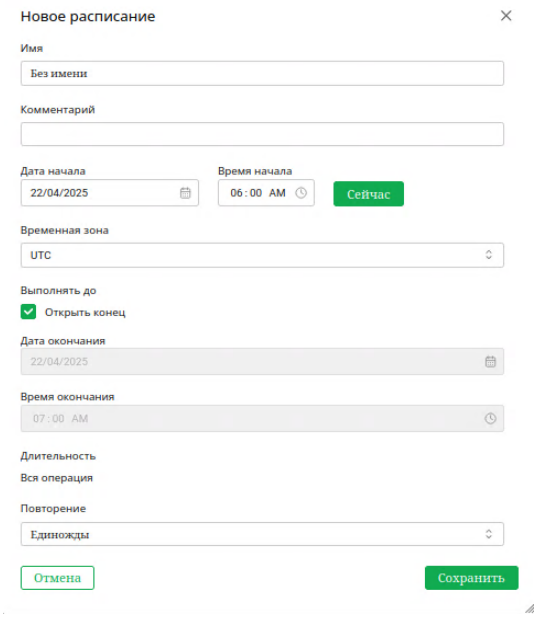

Рис. 3.45

3) нажать кнопку «Сохранить».

Расписание создано, и его можно выбрать при создании новой задачи.

Для всех расписаний доступны следующие действия: , , , , .

3.21 Использование оповещений

При настроенном событии (например, выполнение задачи), проверяется указанное условие (например, обнаружена уязвимость с высокой категорией серьезности). Если условия выполнены, то выполняется заданное действие по оповещению (например, электронное письмо отправляется на определенный адрес).

Для создания нового Уведомления необходимо:

1) выбрать в строке меню «Конфигурация» → «Уведомления»;
2) создать новое оповещение;
3) определить параметры Уведомления (рис. 3.46);

4) нажать кнопку «Сохранить».

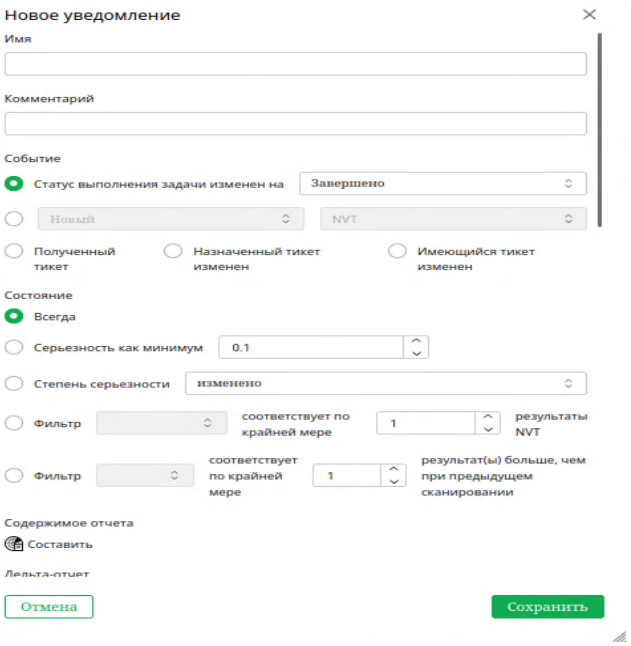

Рис. 3.46

Для использования созданного Уведомления необходимо:

1) выбрать в строке меню «Сканирование» → «Задачи»;
2) создать задачу согласно 3.14.2.1;
3) выбрать оповещение из раскрывающегося списка или создать новое (рис. 3.47);
4) нажать кнопку «Сохранить».

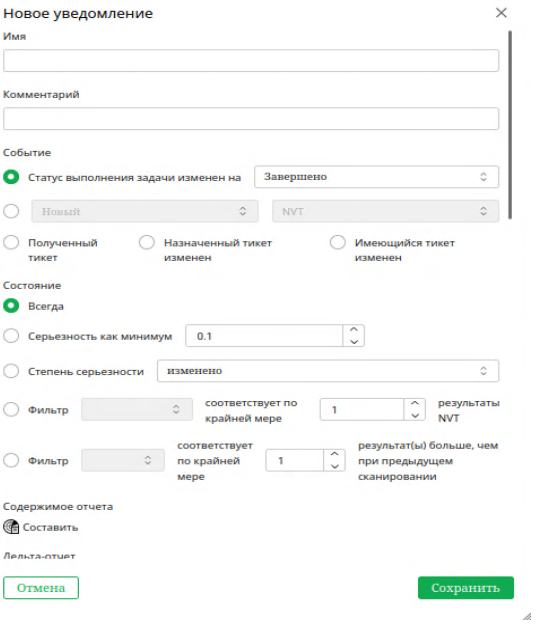

Рис. 3.47

3.22 Параметры и внешние факторы влияющие на процесс сканирования

Существует ряд проблем, которые могут возникнуть во время сканирования с использованием значений устройства по умолчанию, в зависимости от реальной среды и конфигурации сканируемых узлов потребуются дополнительные настройки:

1) хосты не найдены.

Во время сканирования устройство по умолчанию сначала использует команду «ping» для проверки доступности настроенных целей. Если хост не отвечает на запрос «ping», предполагается, что он отключен и не будет сканироваться сканером портов или каким-либо NVT.

В большинстве локальных сетей это не создает никаких проблем, поскольку все устройства будут отвечать на запрос «ping».

В некоторых случаях локальные брандмауэры или другая конфигурация могут подавлять ответ «ping». Следовательно цель не будет сканироваться и не будет включена в результаты и отчет о сканировании.

Для устранения проблемы конфигурация сканирования поддерживает настройку теста, который уже выполняется.

Если цель не отвечает на запрос «ping», может быть протестирован TCP-ping. Если цель находится в том же широковещательном домене, также может быть предпринята попытка ARP-«ping»;

2) длительные периоды сканирования.

Как только с помощью команды «ping» будет обнаружено, что цель активна, «Сканер уязвимостей» использует сканер портов для сканирования хоста. По умолчанию используется список портов TCP, содержащий около 5000 портов. Если цель защищена локальным брандмауэром, блокирующим часть этих пакетов, при проверке портов потребуется дождаться истечения времени ожидания для каждого отдельного порта. Если хосты защищены локальными брандмауэрами, списки портов или брандмауэры могут быть настроены. Если брандмауэр не блокирует запрос, а отклоняет его, то сканеру портов нет необходимости ждать истечения тайм-аута завершения сеанса;

3) не используется VTS.

Это происходит особенно часто, если используются NVT на основе UDP, такие как NVT, использующие протокол SNMP. Если используется полная и быстрая конфигурация по умолчанию, включаются NVT SNMP. Но если хост настроен с использованием списка портов по умолчанию, VTS не выполняются. Это происходит потому, что список портов по умолчанию не включает UDP-порты. Следовательно, порт 161/udp (SNMP) не обнаружен и исключен из дальнейших проверок. Как обнаруженные сканирования, так и рекомендуемая конфигурация сканирования полностью и быстро оптимизируют сканирование на основе обнаруженных служб. Если UDP-порт не обнаружен, виртуальные машины SNMP не проявляют активность.

Не включать все порты по умолчанию в списках портов. Это значительно продлит сканирование. Рекомендуется настраивать списки портов на порты, которые используются в среде и поддерживаются брандмауэрами;

4) сканирование vhosts.

«Сканер уязвимостей» способен находить все взаимосвязи между именами хостов и IP-адресами без необходимости дополнительного ввода данных пользователем.

В средах с виртуальными хостами отчеты о проверке будут давать меньше результатов, поскольку это позволяет избежать дублирования. Для локального сканирования используются настройки:

– «test_empty_vhost» – при включенном параметре, сканер проверяет цель, используя пустые значения «vhost» в дополнение к связанным с целью значениям «vhost»;

– «expand_vhosts» – при включенном параметре, список «vhosts» целевого хоста расширяется за счет собранных значений из таких источников, как запросы обратного поиска и проверки NVT на наличие сертификатов SSL / TLS.

3.23 Настройка форматов и управление отчетами

Форматы отчетов определяются как форматы, из которых создается отчет на основе результатов сканирования.

Форматы отчетов можно использовать для экспорта информации отчета в другие форматы документов.

Наименование экспортируемого отчета настраивается в настройках пользователя.

Все форматы отчетов по умолчанию представляют собой объекты данных, которые распространяются через канал, загружаются и обновляются с каждым обновлением ленты.

Форматы отчетов по умолчанию недоступны, может потребоваться обновление ленты или установить владельца импорта ленты.

Форматы отчетов по умолчанию недоступны редактированию. Более того, они могут быть временно удалены только пользователем импорта ленты, владельцем или супер администратором. Во время следующего обновления ленты они будут загружены снова.

Все существующие форматы отчетов можно отобразить, выбрав в строке меню «Конфигурация» → «Форматы отчетов» (рис. 3.48).

Для сканеров доступны действия: , .

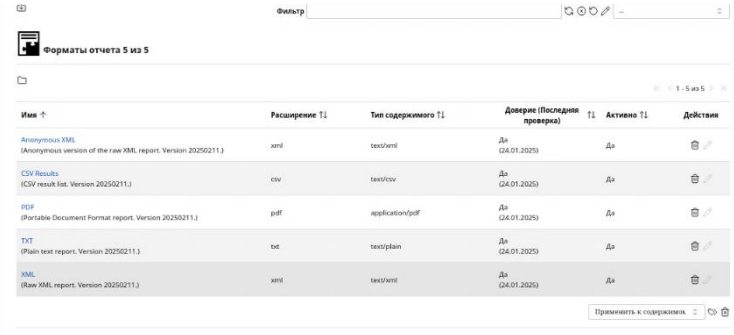

Рис. 3.48

3.23.1 Импорт формата отчета

Для импортирования формата отчета необходимо:

1) выбрать в строке меню «Конфигурация» → «Форматы отчетов»;
2) нажать кнопку (рис. 3.49);
3) в поле «Импортировать формат отчета XML» выбрать файл импорта;
4) нажать кнопку «Сохранить»;

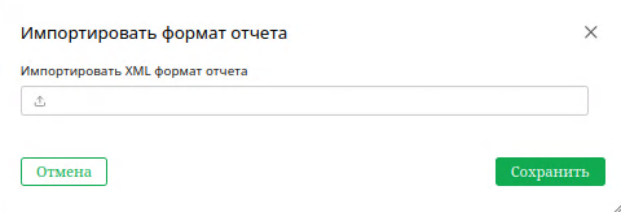

Рис. 3.49

3.23.2 Использование и управление отчетами

Для просмотра существующих отчетов по всем проверкам необходимо выбрать в строке меню «Сканирование» → «Отчеты» (рис. 3.50).

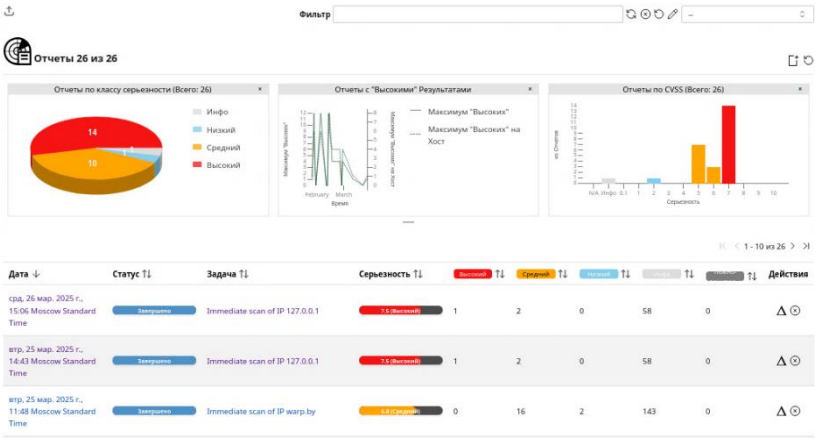

Рис. 3.50

Для просмотра отчетов по задаче необходимо:

1) выбрать в строке меню «Сканирование» → «Задачи»;
2) в столбце «Отчеты» нажать на общее количество отчетов;
3) выбрать отчет.

Для всех отчетов доступны следующие действия: Δ, ×.

Для чтения отчета нажать по дате отчета, чтобы отобразить подробную информацию Содержимое отчета можно отсортировать по выбранному столбцу, нажав на заголовок столбца. Содержимое может быть отсортировано по возрастанию или по убыванию:

▲ – в заголовке столбца показано, что объекты отсортированы по возрастанию;
▼ – в заголовке столбца показано, что объекты отсортированы по убыванию.

В левом верхнем углу отчета доступны следующие действия:

– «Показать страницу со списком всех форматов отчетов»;

– «Добавить содержимое отчета» с QoD не менее 30 % и разрешенными переопределениями ресурсов. Значение и типы QoD приведены в таблице 5;

– «Удалить содержимое отчета из ресурсов»;

– «Показать соответствующую задачу»;

– «Открыть страницу результатов». Фильтр применяется для отображения только результатов для этого отчета;

– «Открыть страницу уязвимости». Фильтр применяется для отображения только уязвимостей в этом отчете;

– «Открыть страницу TLS-сертификаты». Фильтр применяется для отображения только сертификатов TLS в этом отчете;

– «Открыть страницу отображения производительности системы за время сканирования»;

– «Загрузить отфильтрованный отчет»;

– «Запускает оповещение для отправки отчета».

3.23.3 Результаты отчета

Результаты сканирования содержат список всех уязвимостей, обнаруженных «Сканером уязвимостей» (рис. 3.51).

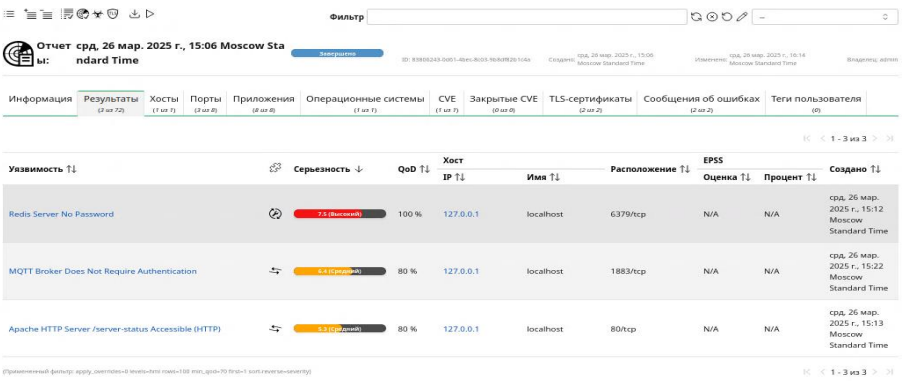

Рис. 3.51

Для каждой найденной уязвимости отображается следующая информация (см. рис. 3.51):

1) «Уязвимость» – наименование найденной уязвимости. При нажатии на наименование уязвимости отображаются подробные сведения о возможности взлома.

Уязвимости, к которым прилагается примечание, отмечены знаком .

2) («Тип решения») – решение для обнаруженной уязвимости. Возможны следующие решения:

– «Доступен обходной путь»;

– «Доступно смягчение в зависимости от конфигурации»;

– «Никакого исправления нет и не будет»;

– «Исправление предоставляется поставщиком»;

– «Решения не существует».

3) «Серьезность» – уровень опасности уязвимости;

4) «QoD» («Качество обнаружения») – это значение в диапазоне от 0 % до 100%, описывающее надежность выполняемой операции обнаружения уязвимостей. По умолчанию отображаются только результаты, которые были обнаружены VTS с QoD 30 % или выше. Фильтр можно настроить для отображения результатов с более низким QoD. Значение и типы QoD приведены в таблице 5;

5) «Хост» – IP-адрес и имя хоста, для которого был найден результат;

6) «Расположение» – номер порта и тип протокола, используемые для обнаружения уязвимости на хосте;

7) «Создание» – дата и время создания отчета.

3.23.4 Анализ отчета

Для анализа результатов необходимо обратить внимание на следующую информацию:

1) «Ложные срабатывания» – результат, описывающий проблему, которая не является критической при сканировании:

- сообщение о потенциально несуществующей уязвимости (ложноположительный результат);
- игнорирование сообщения о потенциально существующей уязвимости (ложноотрицательный результат);

2) «Множественные находки» – установлен устаревший программный пакет, часто существует множество уязвимостей. Каждая из этих уязвимостей тестируется отдельным NVT и вызывает предупреждение. Установка текущего пакета удалит сразу множество уязвимостей;

3) Высокий и средний уровни серьезности являются наиболее важными, и их следует рассматривать в приоритетном порядке. Прежде чем рассматривать результаты среднего

уровня, следует рассмотреть результаты высокого уровня. Только в исключительных случаях от этого подхода следует отказаться, например, если известно, что результаты высокого уровня не требуют особого внимания, поскольку доступ к службе невозможен через брандмауэр;

4) Результаты низкого уровня и «Инфо» в основном интересны для детального понимания. Эти результаты по умолчанию отфильтровываются, но могут содержать полезную информацию. Их рассмотрение повысит безопасность сети и систем. Результат с серьезностью «Инфо» заключается в том, что сервис использует баннер с его названием и номером версии.

3.23.5 Фильтрация отчета

Поскольку отчет часто содержит много результатов, предоставляется возможность отобразить и загрузить как полный отчет, так и только отфильтрованные результаты. Отчет можно отфильтровать следующим образом:

1) на странице «Отчеты» на панели фильтров нажать кнопку ;
2) в появившемся окне (рис. 3.52) установить параметры отчета, в поле «Фильтр» ввести ключевое слово, в поле «Применить переопределения» выбрать переключатель «Да» для включения переопределения;

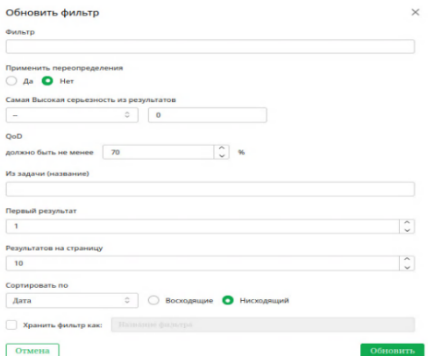

Рис. 3.52

3) нажать кнопку «Обновлять».

3.23.6 Экспорт отчета

Для экспорта отчета необходимо:

1) выбрать в строке меню «Сканирование» → «Отчеты»;
2) нажать по дате отчета, открыть страницу сведений об отчете;
3) нажать кнопку «Скачать отфильтрованный отчет»;
4) в появившемся окне (рис .3.53) выполнить следующее:
   – в поле «Включить» активировать флажок «Примечания», «Переопределение» (при необходимости);
   – выбрать формат отчета в раскрывающемся списке «Формат отчета»;
   – установить флажок «Сохранить по умолчанию»;

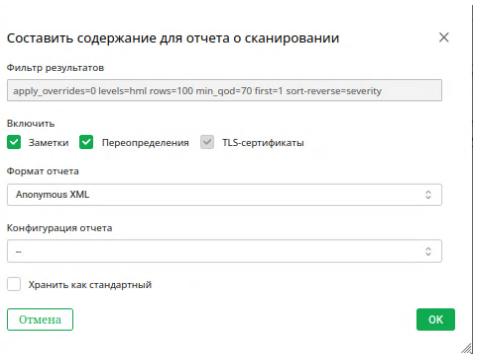

Рис. 3.53

5) нажать кнопку «ОК».

3.23.7 Импорт отчета

Для импорта отчета необходимо:

1) выбрать в строке меню «Сканирование» → «Отчеты»;
2) нажать кнопку «Загрузить отчет»;
3) в появившемся окне (рис. 3.54) в поле «Отчет» выбрать XML-файл отчета, в поле «Задача контейнера» в раскрывающемся списке выбрать контейнерную задачу, к которой необходимо добавить отчет, установить переключатель «Да», чтобы добавить отчет в активы;
4) нажать кнопку «Импортировать».

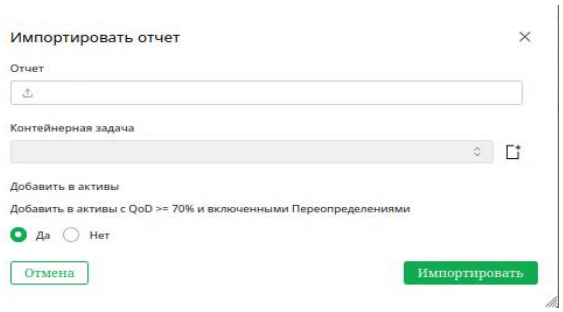

Рис. 3.54

3.23.8 Запуск Уведомления для отчета

Для отправления отчета оповещением необходимо отфильтровать данные отчета. При запуске Уведомления для отчета добавляется второй фильтр, созданный пользователем отчета.

Для запуска Уведомления для отчета о сканировании необходимо:

1) выбрать в строке меню «Сканирование» → «Отчеты»;
2) нажать по дате отчета;
3) отфильтровать данные отчета для отображения результатов, которые будут отправлены в оповещении;
4) нажать кнопку ▷;
5) в появившемся окне «Активировать оповещение для отчета о сканировании» (рис. 3.55):

– в поле «Включить» активировать флажок «Примечания», «Переопределение» (при необходимости);
– выбрать оповещение в раскрывающемся списке;
– установить флажок «Сохранить по умолчанию»;
– нажать кнопку «ОК».

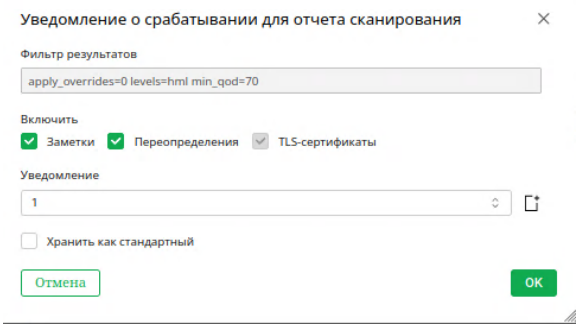

Рис. 3.55

3.23.9 Создание дельта- отчета

Если доступно более одного отчета по одной задаче, можно создать дельта–отчет следующим образом:

1) выбрать в строке меню «Сканирование» → «Задачи»;
2) нажать на общее количество отчетов в столбце «Отчеты».
3) при открытии страницы «Отчеты» применить фильтр для отображения только отчетов по выбранной задаче;
4) выбрать первый отчет и нажать Δ в столбце «Действия» (рис. 3.56);
5) выбрать второй отчет и нажать Δ в столбце «Действия»;
6) отобразится дельта-отчет с дельта-результатами, который можно экспортировать.

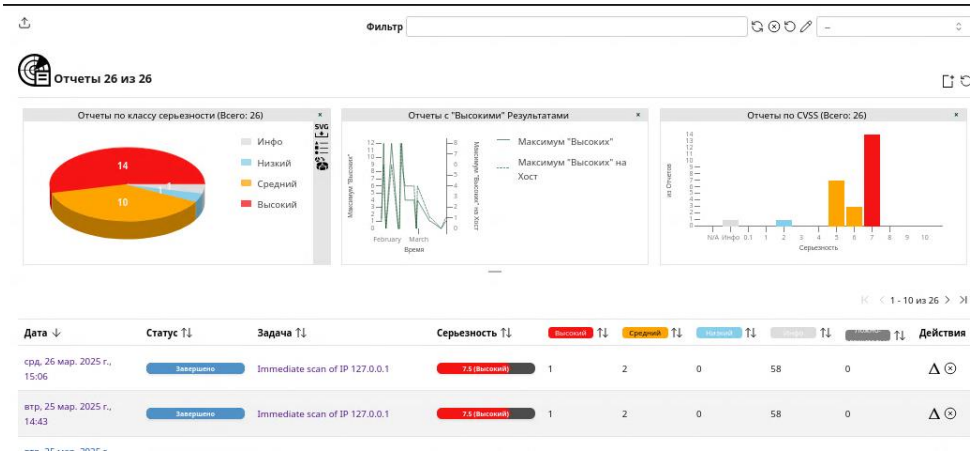

Рис. 3.56

Тип дельта-результата отображается в столбце «Действия». Существует четыре типа дельта-результатов:

– «Пропал [–]» – результат существует в первом отчете, но отсутствует во втором отчете (в соответствии с порядком выбора);

– «Новое [+]» – результат существует во втором отчете, но отсутствует в первом отчете (в соответствии с порядком выбора);

– «Одинаковый [=]» – результат существует в обоих отчетах и одинаков;

– «Изменено [~]» – результат присутствует в обоих отчетах, но отличается.

3.24 Отображение уязвимостей

Для просмотра уязвимостей во внутренней базе данных необходимо выбрать в строке меню «Сканирование» → «Уязвимости» (рис. 3.57).

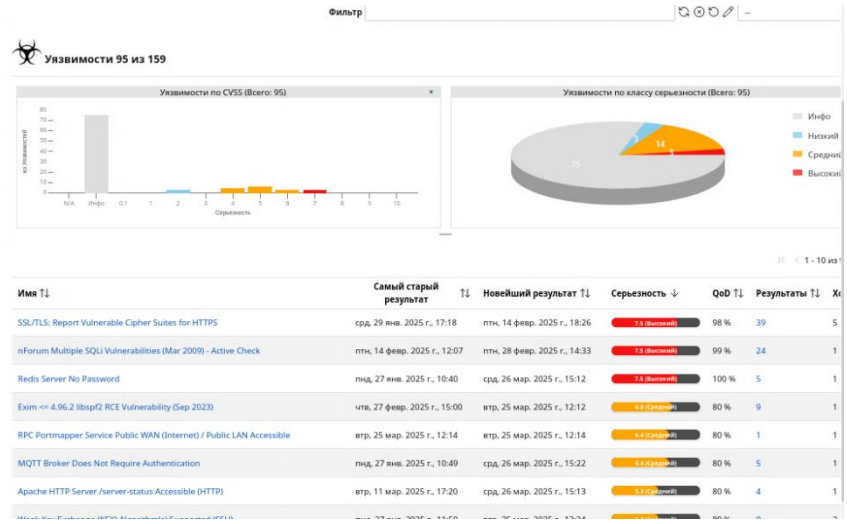

Рис. 3.57

3.25 Динамика уязвимостей

При повторном выполнении задачи на странице «Задачи» отображается динамика устранения выявленных уязвимостей в столбце «Тренд» (рис. 3.58).

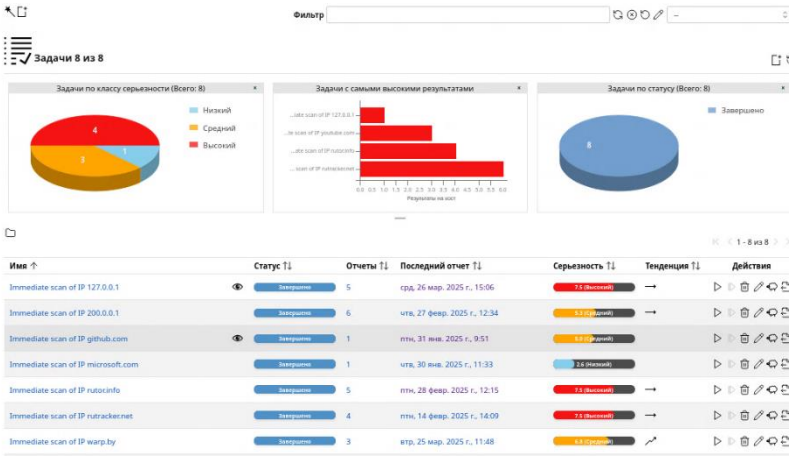

Рис. 3.58

Динамика обнаружения уязвимостей отображает изменение найденных уязвимостей между последним и предыдущим отчетом:

– ↗ общая степень серьезность найденных уязвимостей увеличилась;
– ↗ количество найденных уязвимостей увеличилось;
– → количество найденных уязвимостей и их степень серьезности одинаковые;
– ↘ количество найденных уязвимостей уменьшилось;
– ↘ общая степень серьезность найденных уязвимостей уменьшилась.

3.26 Создание и использование примечаний

Примечание может быть добавлено к конкретному результату, задаче, серьезности, порту или хосту и отображаться только в определенных отчетах.

Для создания примечания к отчету необходимо:

1) выбрать в строке меню «Сканирование» → «Отчеты»;
2) нажать по дате отчета, чтобы отобразить результаты;
3) выбрать результаты;
4) столбце «Уязвимость» нажать по наименованию уязвимости для отображения

подробного описания результатов;

5) в разделе «Результаты обнаружения продукта» → «Инфо» → «Просмотр подробностей обнаружения продукта»;

6) добавить примечание (рис. 3.59);

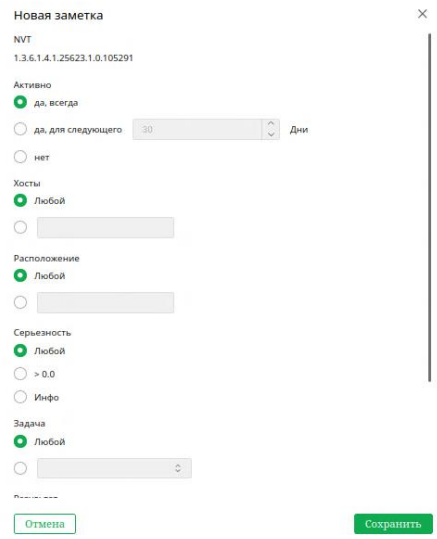

Рис. 3.59

7) нажать кнопку «Сохранить».

Для создания примечания к определенному NVT необходимо:

1) выбрать в строке меню «Сканирование» → «Заметки»;
2) создать примечание;
3) ввести данные примечание;
4) нажать кнопку «Сохранить».

Созданные примечание отобразятся в разделе «Заметки» (рис. 3.60).

Рис. 3.60

Для всех примечаний доступны следующие действия: , , , , .

3.27 Использование переопределений и ложных срабатываний

Серьезность результата может быть изменена. Это называется переопределением.

Переопределения полезны для управления результатами, которые были обнаружены как ложноположительные и которым была присвоена критическая степень, но в будущем им необходимо присвоить другую степень серьезности.

То же самое относится и к результатам, к которым необходимо присвоить более высокий уровень серьезности локально.

Переопределения используются для управления уровнем серьезности уязвимостей.

3.27.1 Создание переопределения с помощью результата сканирования

Для создания переопределения с помощью соответствующего результата сканирования в

отчете необходимо:

1) выбрать в строке меню «Сканирование» → «Отчеты»;
2) нажать на дату составления отчета, отобразить результаты;
3) выбрать результаты;
4) нажать по результату в столбце «Уязвимость»;
5) открыть страницу сведений о результате (рис.3.61);
6) определить переопределение нажав «Создать новое переопределение» (рис. 3.65);
7) нажать кнопку «Сохранить».

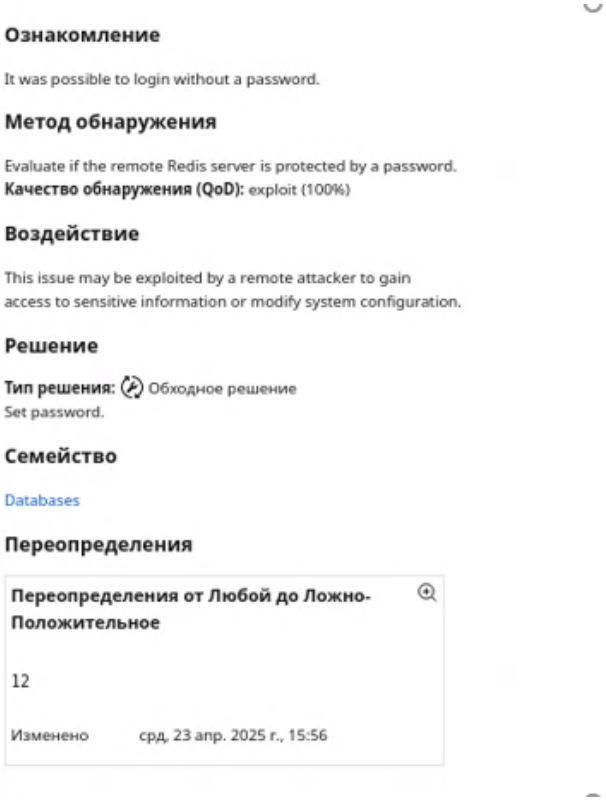

Рис. 3.61

3.27.2 Создание переопределения на веб-странице «Переопределения»

Для создания переопределения необходимо:

1) выбрать в строке меню «Сканирование» → «Переопределения»;
2) создать новое переопределение нажав ;
3) в появившемся окне (рис.3.62) ввести идентификатор NVT в поле ввода «NVT OID» и заполнить необходимые параметры переопределения. При необходимости включения переопределения в поле «Активный» установить переключатель «Да всегда» или «Да, в следующие дни». Для отключения переопределения установить переключатель «Нет»;
4) нажать кнопку «Сохранить».

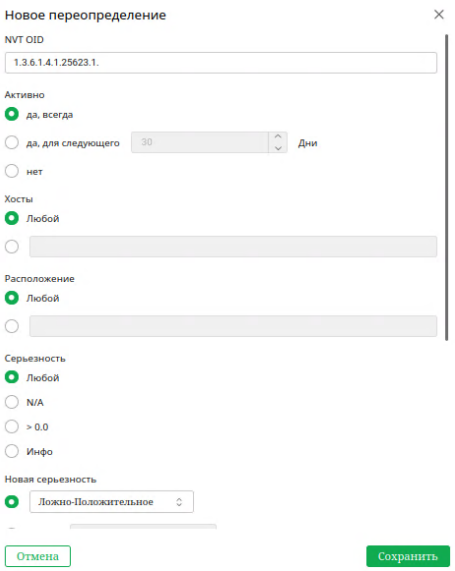

Рис. 3.62

Для всех переопределений доступны следующие действия: , , , , .

3.28 Управление и создание хостов

Хосты обеспечивают краткий обзор найденных и просканированных устройств, ОС, найденных уязвимостей и их уровень значимости.

Для добавления хоста в систему управления активами необходимо:

1) выбрать в строке меню «Ресурсы» → «Хосты»;
2) создать новый хост, нажав в верхнем левом углу страницы;
3) в появившемся окне (рис. 3.63) ввести IP-адрес хоста и комментарий (при необходимости);

Рис. 3.63

4) нажать кнопку «Сохранить».

Для отображения всех хостов необходимо выбрать в строке меню «Активы» → «Хосты» (рис. 3.64).

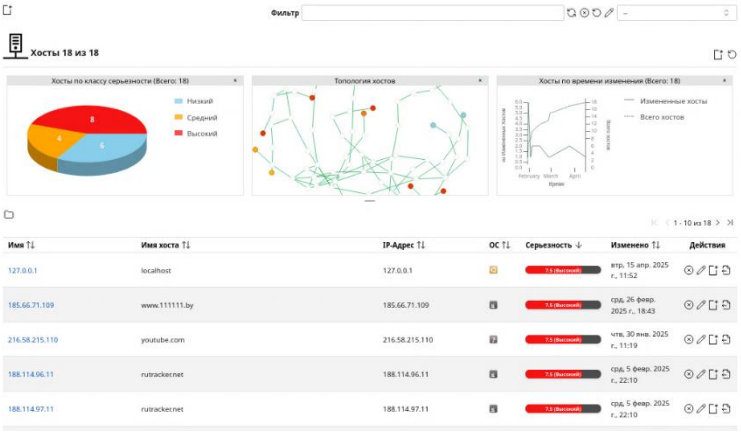

Рис. 3.64

Для всех хостов доступны следующие действия: ✕, ☐+, ✎, ⇪.

3.29 Создание цели с набором хостов

Для создания цели с набором хостов необходимо:

1) выбрать в строке меню «Ресурсы» → «Хосты»;
2) в строке хоста нажать «Создать цель из хоста»;
3) заполнить данные о цели;
4) нажать кнопку «Сохранить»;

Если при дальнейших проверках обнаружатся дополнительные подходящие хосты, они не будут добавлены к цели.

Для хостов доступны действия: ✕, ☐+, ✎, ⇪.

3.30 Управление операционными системами

Для отображения списка ОС необходимо перейти в строке меню «Ресурсы» → «Операционные системы» (рис. 3.65).

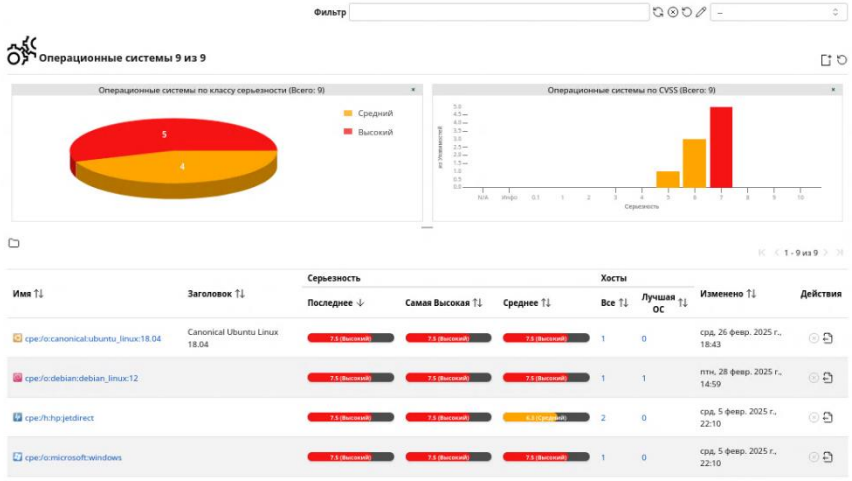

Рис. 3.65

Для всех ОС доступны следующие действия: ✕ (можно удалить только ОС, которые в данный момент не используются), ⇪, ≣, 🖳.

3.31 Выход из веб-интерфейса

Для выхода из веб-интерфейса необходимо нажать на кнопку 👤 в правом верхнем углу и выбрать «Выйти» (рис. 3.66).

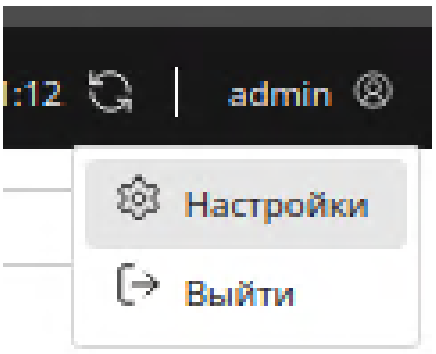

Рис. 3.66

При отсутствии действий в «Сканер уязвимостей» со стороны пользователя в течении 15 мин, происходит автоматический выход из системы.

Время, оставшееся до автоматического выхода пользователя из системы, отображается в сведеньях учетной записи при нажатии на кнопку «Тайм-аут сеанса».

3.32 Регламент обновлений

Обновление базы знаний на «Сканер уязвимостей» выполняется в режиме «онлайн» обновление (требует подключение «Сканера уязвимостей» к сети Интернет).

Для обновления базы знаний «Сканера уязвимостей» пользователю необходимо на «Сканер уязвимостей» в терминале выполнить следующую команду:

```
# sudo feed-sync
```

После выполнения команды «Сканер уязвимостей» подключится к серверу обновлений, указанному при установке, и выполнит обновление базы знаний при необходимости.

Обновление базы знаний рекомендуется выполнять не реже одного раза в месяц.

Для обновления «Сканера уязвимостей» пользователю необходимо загрузить с ftp ресурса производителя патч или новую версию и выполнить установку в соответствии с прилагаемыми инструкциями.

4. СООБЩЕНИЯ ОПЕРАТОРУ

При сканировании «Сканер уязвимостей» предполагает уведомление оператора об ошибках. Перечень основных ошибок представлен в таблице 3.

Таблица 3

Текст сообщения	Причина сообщения	Действия оператора
Ошибка входа. Неверный пароль или имя пользователя	Введен неверный пароль или имя пользователя	Ввести пароль или имя пользователя
Given host was invalid	Указанные хосты были недействительными	Ввести верный хост или диапазон хостов
Поле Текст обязательно для заполнения	Не заполнено поле «Текст»	Заполнить поле «Текст»
User with name exists already	Пользователь с таким именем уже существует	Присвоить новое имя пользователю
Empty password	Не заполнено поле «Пароль»	Заполнить поле «Пароль»
A TEXT entity is required	Не заполнено поле «Текст» при вводе параметров	Заполнить поле «Текст»
Validation of email address failed	Указанный адрес электронной почты не действителен	Ввести верный адрес электронной почты
Selected type requires a login username	Не верно указан тип учетных данных	Заполнить параметры в соответствии с типом учетных данных
Role exists already	Указанная роль существует	Создать роль с другим именем

ПЕРЕЧЕНЬ ТЕРМИНОВ

В настоящем руководстве применяются следующие термины и определения:

– значимость – значение в диапазоне от 0 до 10, которое соответствует уровню значимости (информационный, низкий, средний или высокий уровень).

– исправление – внесение изменений с целью нейтрализации уязвимостей.

«Сканер уязвимостей» автоматически отображает рекомендации для устранения обнаруженных уязвимостей. Возможны следующие типы исправлений представлены в таблице 4.

Таблица 4

Тип	Применение
Временное решение	Применяется для нейтрализации новой уязвимости до того момента, пока официальным разработчиком (производителем) не будет выпущен патч
Минимизация последствий	Данное решение не устраняет уязвимость, а позволяет минимизировать последствия от использования обнаруженной уязвимости. Исправление может быть выпущено не только официальным разработчиком данного продукта
Специализированное исправление, выпущенное официальным разработчиком	Если не указано иное, предполагается, что это исправление полностью устраняет уязвимость
Решение отсутствует	В настоящее время нет доступных исправлений. Будут отображены сведения о причине отсутствия исправления
Решение отсутствует	Исправления отсутствуют и выпущены не будут. Будут отображены сведения о причине отсутствия исправления. Зачастую такая ситуация характерна для случаев, когда продукт устарел или прекращена поддержка

– качество обнаружения – QoD (Quality of Detection) – это значение из диапазона от 0 % до 100 %, характеризующее степень достоверности обнаружения уязвимости. Значения и типы QoD приведен в таблице 5.

Таблица 5

QoD	Тип QoD	Описание
100 %	exploit	Обнаружение осуществлено посредством использования exploit, поэтому оно является достоверным
99 %	remote_vul	Обнаружение осуществлено в ходе активных удаленных проверок (исполнение кода, обход директорий и т.д.), результат которых явно указывает на наличие уязвимости
98 %	remote_app	Обнаружение осуществлено в ходе активных удаленных проверок (исполнение кода, обход директорий и т.д.), результат которых явно указывает наличие уязвимого приложения
97 %	package	Проверки ОС семейства Linux, основанные на аутентификации в системе и анализе установленных пакетов
97 %	registry	Проверки ОС семейства Windows с прохождением аутентификации в системе и анализе информации из реестра

QoD	Тип QoD	Описание
95 %	remote_active	Обнаружение осуществлено в ходе активных удаленных проверок (исполнение кода, обход директорий и т.д.), результат которых вероятно свидетельствует о наличии уязвимости или уязвимого приложения. «Вероятно» означает, что в редких случаях возможна ошибка
80 %	remote_banner	Приветственное сообщение от приложений содержит сведения об уровне значимости исправлений в идентификаторе версии. Это характерно для большинства коммерческих продуктов
80 %	executable_version	Проверки ОС семейства Linux или семейства Windows с прохождением аутентификации в системе, в которой сведения об уровне значимости исправлений указаны в идентификаторах версий приложений
75 %		Значение присваивается всем результатам, которым не присвоен уровень значимости
70 %	remote_analysis	Удаленные проверки, результаты которых не всегда являются достоверными
50 %	remote_probe	Удаленные проверки, в которых промежуточные устройства (межсетевой экран), может препятствовать корректному определению, поступил ли ответ непосредственно от приложения
30 %	remote_banner_unreliable	Приветственное сообщение от приложений не содержит сведений об уровне значимости исправлений в идентификаторе версии
30 %	executable_version_unreliable	Проверки ОС семейства Linux с прохождением аутентификации в системе, в которой сведения об уровне значимости исправлений не указаны в идентификаторах версий приложений
1 %	general_note	Информационная заметка о потенциальном наличии уязвимости, не имеющих подтверждений

– уровень значимости – определяется субдиапазонами основного диапазона значимости (от 0 до 10). Оператором могут быть выбраны различные классификации. Уровень значимости может изменяться с течением времени. В случае регулярного обновления базы знаний оператором может быть выбран динамический режим определения уровня значимости. В таком случае «Сканер уязвимостей» всегда будет использовать наиболее актуальную информацию об уровнях значимости.

– цель (целевое устройство, целевая система) – устройство или ОС данного устройства, которая подвергается сканированию.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе приняты следующие сокращения:

ОС	–	операционная система;
ПО	–	программное обеспечение;
«Сканер уязвимостей»	–	средство программное контроля эффективности защищенности информации BY.СЮИК.00473-01;
ПЭВМ	–	персональная электронная вычислительная машина;
CPE	–	перечень общеизвестных платформ (Common Platform Enumeration);
CVE	–	перечень общеизвестных уязвимостей информационной безопасности (Common Vulnerabilities and Exposures);
NVD	–	национальная база данных уязвимостей (National Vulnerability Database);
NVT	–	тест сетевых уязвимостей (Network Vulnerability Tests);
VTS	–	виртуальные машины;
QoD	–	качество обнаружения (Quality of Detection).

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	ныыовых	аннулированных					

Изм.№	Подп.	Дата