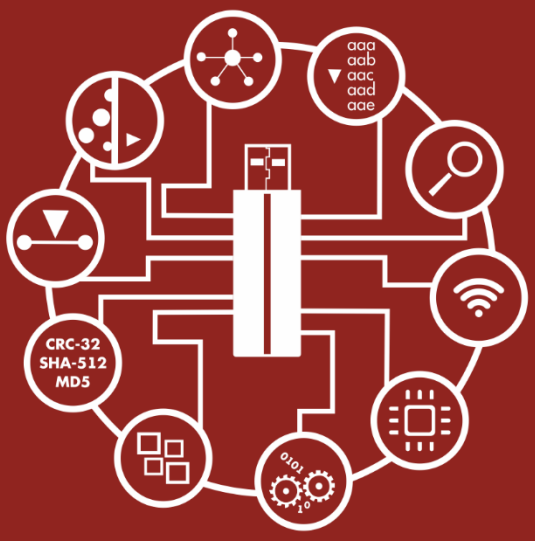
Эшелон
комплексная безопасность



Сканер-ВС

анализ защищенности

КРАТКОЕ РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

О КОМПАНИИ

АО «НПО «Эшелон» специализируется на комплексном обеспечении информационной безопасности.

Основными направлениями деятельности являются:

- проектирование, внедрение и сопровождение комплексных систем обеспечения информационной безопасности;
- сертификация средств защиты информации и систем в защищенном исполнении;
- аттестация объектов информатизации;
- лицензирование деятельности в области создания средств защиты информации;
- проведение анализа защищенности компьютерных систем;
- аудит информационной безопасности организаций;
- обучение сотрудников компаний по вопросам обеспечения информационной безопасности;
- поставка оборудования и средств защиты информации;
- разработка средств защиты информации, средств анализа эффективности защиты информации и устройств в защищенном исполнении;
- испытания, экспертизы, исследования в области безопасности информации;

Более детальную информацию о компании вы сможете найти на сайте npo-echelon.ru.

О РУКОВОДСТВЕ

Это руководство разработано с целью ознакомить пользователя с некоторыми возможностями обновленного средства анализа защищенности «Сканер-ВС» (далее – «Сканер-ВС»). Данный документ содержит только основные инструкции для начала использования «Сканер-ВС» и не является заменой руководства оператора.

СОДЕРЖАНИЕ

1. НОВЫЙ ИНТЕРФЕЙС

В предыдущей версии средства анализа защищенности «Сканер-ВС» (далее – «Сканер-ВС») все инструменты располагались на панели управления в нижней части рабочего стола (Рисунок 1). В новой версии «Сканер-ВС» на смену панели управления пришел пользовательский веб-интерфейс (Рисунок 2).

Одинаковыми цифрами на рисунках 1 и 2 обозначены элементы интерфейса, запускающие одни и те же инструменты.

Веб-интерфейс новой версии «Сканер-ВС» существенно отличается от панели управления предыдущей версии. Все графические элементы веб-интерфейса можно разделить на следующие группы:

– справочная информация (на рисунке 2 выделена зеленой рамкой);

– проекты (на рисунке 2 выделена фиолетовой рамкой);

– инструменты (на рисунке 2 выделена красной рамкой).

Пиктограмма настроек «Сканер-ВС» находится в верхней части веб-интерфейса. Для доступа к настройкам нужно нажать ее левой кнопкой мыши.

Пиктограммы запуска инструментальных программ, реализующих функции «Сканер-ВС», которые в прошлой версии продукта «Сканер-ВС» располагались на панели управления, теперь сгруппированы в двух областях веб-интерфейса:

– проекты;

– инструменты.

Функции «Сканер-ВС», включенные в разделы «Проекты» и «Инструменты», представлены в таблице 1.

Рисунок 1 – Панель управления «Сканер-ВС» предыдущей версии

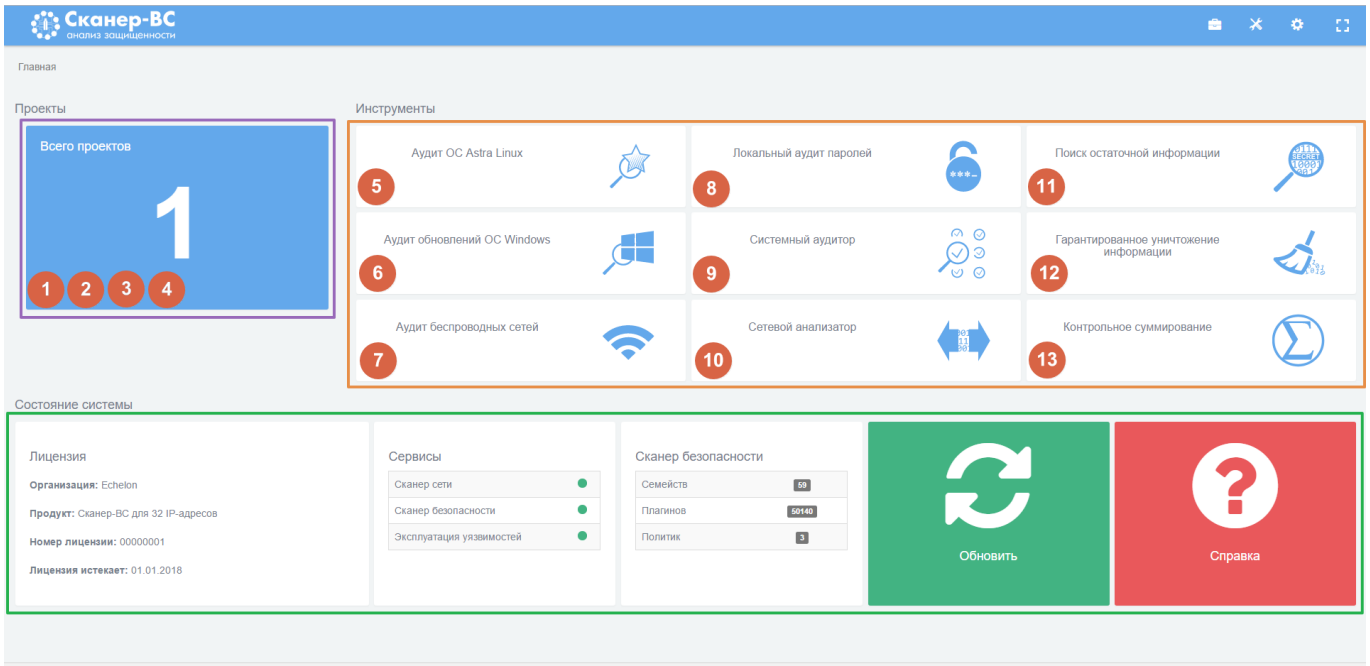


Рисунок 2 – Пользовательский веб-интерфейс «Сканер-ВС» новой версии

Таблица 1. Функции старой и новой версий программного комплекса «Сканер-ВС»

№	Было	Стало
Раздел «Проекты»		
1	Сканер сети	Поиск целей
2	Сканер безопасности	Поиск уязвимостей
3	Сетевой аудит паролей	Сетевой аудит паролей
4	Средство проведения тестирования на проникновение	Поиск эксплойтов
Раздел «Инструменты»		
5	—	Аудит ОС Astra Linux
6	Аудит обновлений ОС Windows	Аудит обновлений ОС Windows
7	Аудит беспроводных сетей	Аудит беспроводных сетей
8	Локальный аудит паролей	Локальный аудит паролей
9	Системный аудитор	Системный аудитор
10	Сетевой анализатор	Сетевой анализатор
11	Поиск остаточной информации	Поиск остаточной информации
12	Гарантированной уничтожение информации	Гарантированной уничтожение информации
13	ПИК Эшелон	Контрольное суммирование

2. ТЕСТИРОВАНИЕ ЗАЩИЩЕННОСТИ

2.1. Что такое проект. Создание проекта

В новой версии «Сканер-ВС» создана единая среда для проведения тестирования защищенности. Для каждого нового тестирования создается *проект*, представляющий собой совокупность всех данных, относящихся к текущему тестированию. Проект включает в себя исходные данные фаз тестирования (поиск целей, поиск уязвимостей, сетевой аудит паролей, поиск эксплойтов) и результаты тестирования в виде сгенерированного отчета. Для проведения тестирования пользователь может создать новый проект или, в случае продолжения начатого ранее и сохраненного тестирования, использовать его.

Для создания проекта в левой части веб-интерфейса нажмите левой кнопкой мыши по разделу «Проекты» или нажмите на кнопку **Проекты** в верхнем правом углу веб-интерфейса (Рисунок 3).

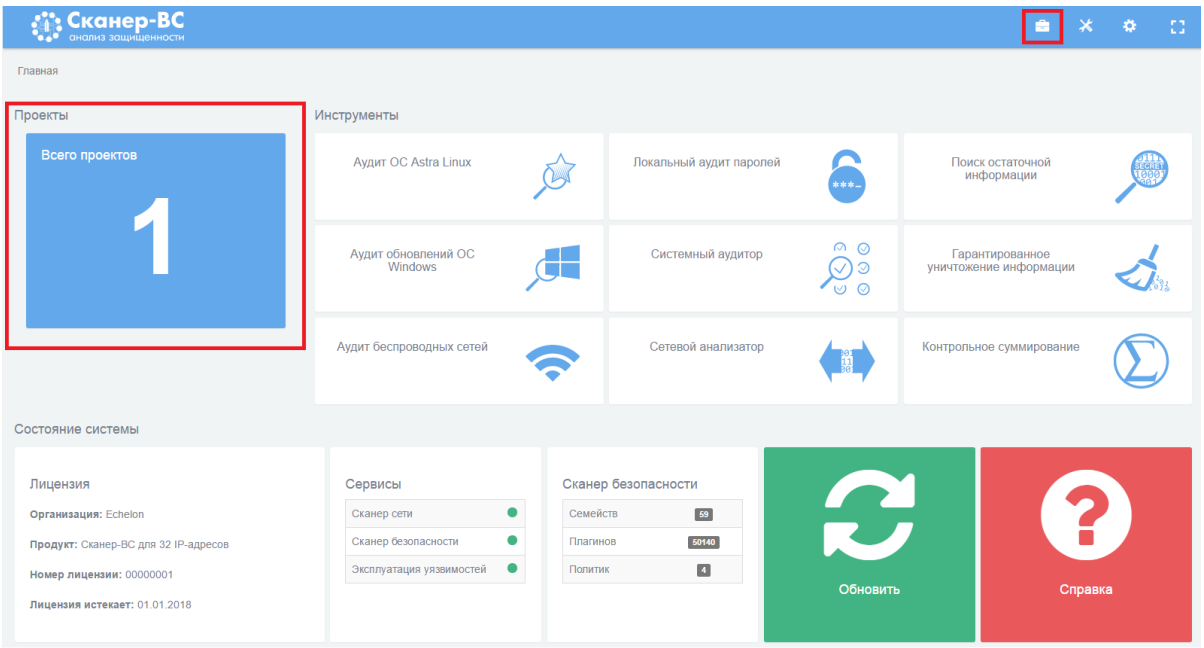


Рисунок 3 – Раздел «Проекты» веб-интерфейса «Сканер-ВС»

В открывшемся окне нажмите на кнопку **Новый проект** или выберите уже существующий проект из перечисленных в рабочей области (Рисунок 4).

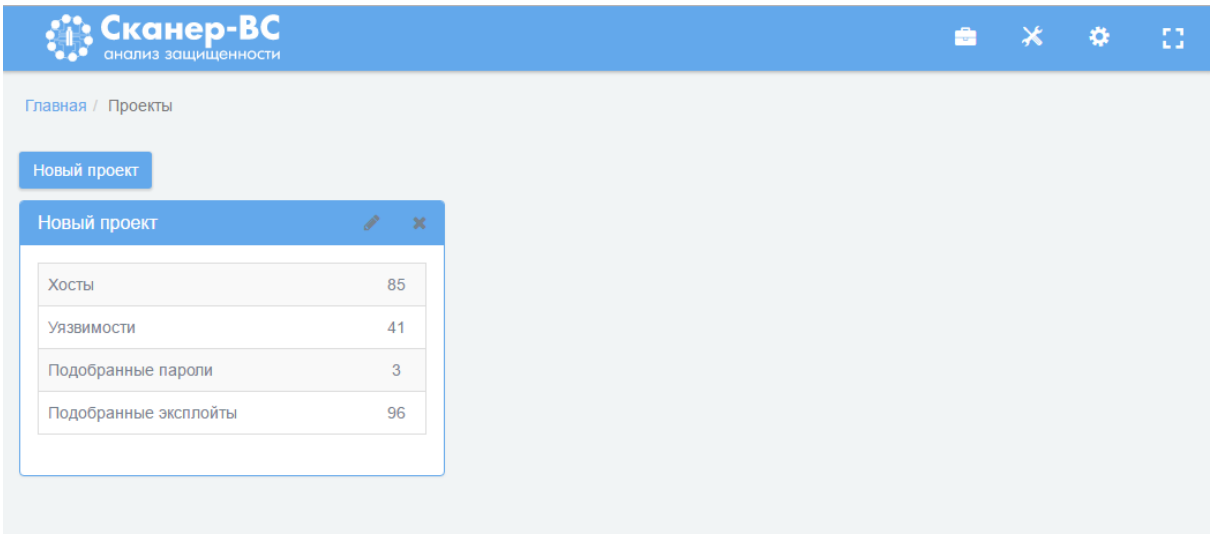


Рисунок 4– Создание проекта

При нажатии на кнопку **Новый проект** откроется окно (Рисунок 5):

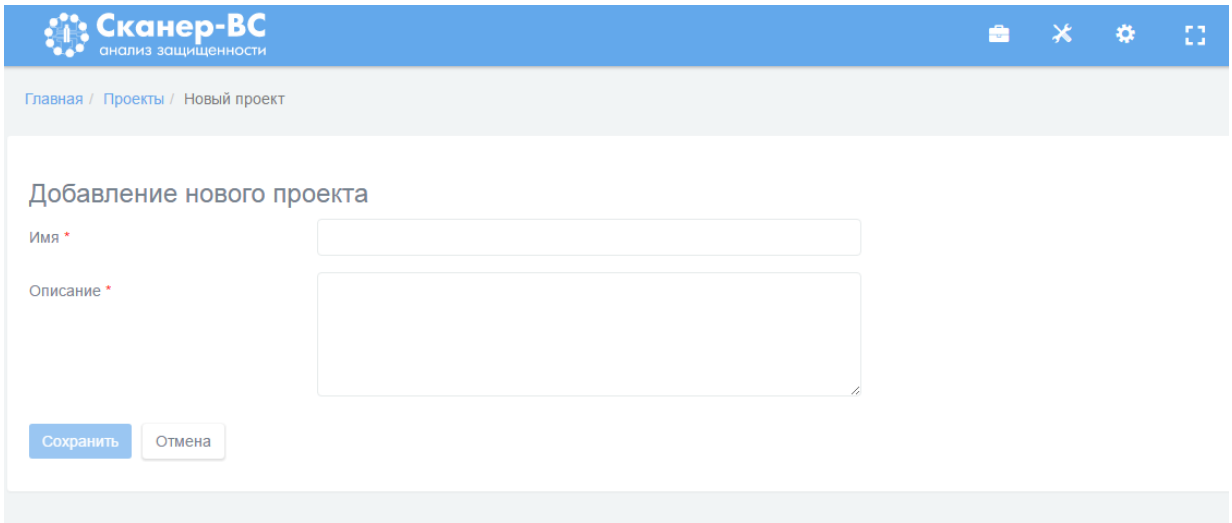


Рисунок 5 – Добавление нового проекта

Поля «Имя» (в него вводят название проекта) и «Описание» (в данное поле вводят краткое описание проекта) обязательны для заполнения. После заполнения полей для сохранения введенной информации о новом проекте нажмите кнопку **Сохранить**, если же по каким-либо причинам проект создавать не требуется, нажмите кнопку **Отмена**.

После нажатия кнопки **Сохранить** или после выбора ранее сохраненного проекта рабочее пространство примет вид, похожий на показанный на рисунке 6.

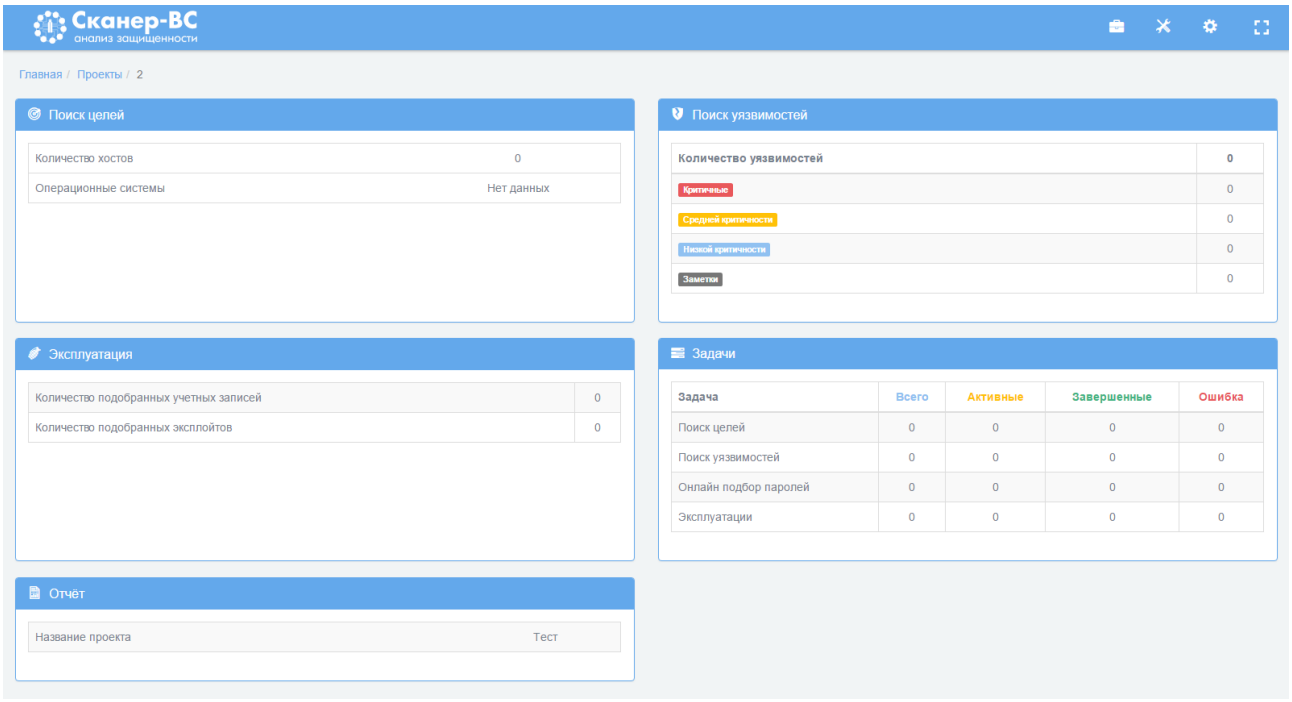


Рисунок 6 – Вид рабочего пространства проекта

Рабочее пространство разделено на сектора, каждый из которых соответствует определенной фазе тестирования. В разделах 2.2. - 2.5. описаны действия пользователя при проведении каждой фазы тестирования.

2.2. Поиск целей

2.2.1. Краткое описание

В начале тестирования обязательным является *поиск целей* - обзор локальной сети, к которой подключен «Сканер-ВС», с целью выявления объектов тестирования для следующих фаз проверки. Поиск целей производится путем сканирования IP-адресов и портов (TCP- и UDP-портов) компьютеров, присоединенных к локальной сети. Без поиска целей невозможно использовать все возможности «Сканер-ВС», в частности, невозможно производить поиск эксплойтов (см. п. 2.4. «Эксплуатация»). Найденные в результате поиска целей действующие подключения с

IP-адресами и задействованными TCP- и UDP-портами далее будем называть *активами*. Данные о них располагаются в секторе «Поиск целей» на вкладках «Хосты» и «Порты» в виде таблиц. Дополнительно поиск целей может быть использован для определения сервисов (служб), запущенных на включенном в сеть компьютере, для идентификации ОС и приложений.

2.2.2. Запуск

Нажмите левой кнопкой мыши по сектору «Поиск целей» (Рисунок 7).

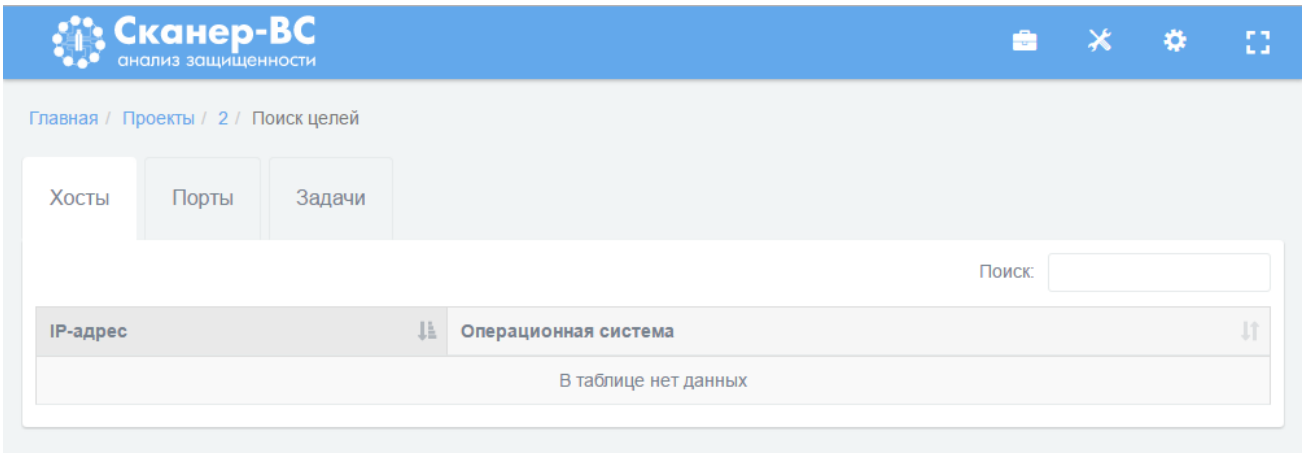


Рисунок 7 – Сектор «Поиск целей»

Перейдите на вкладку «Задачи» и нажмите на кнопку **Новое сканирование** (Рисунок 8).

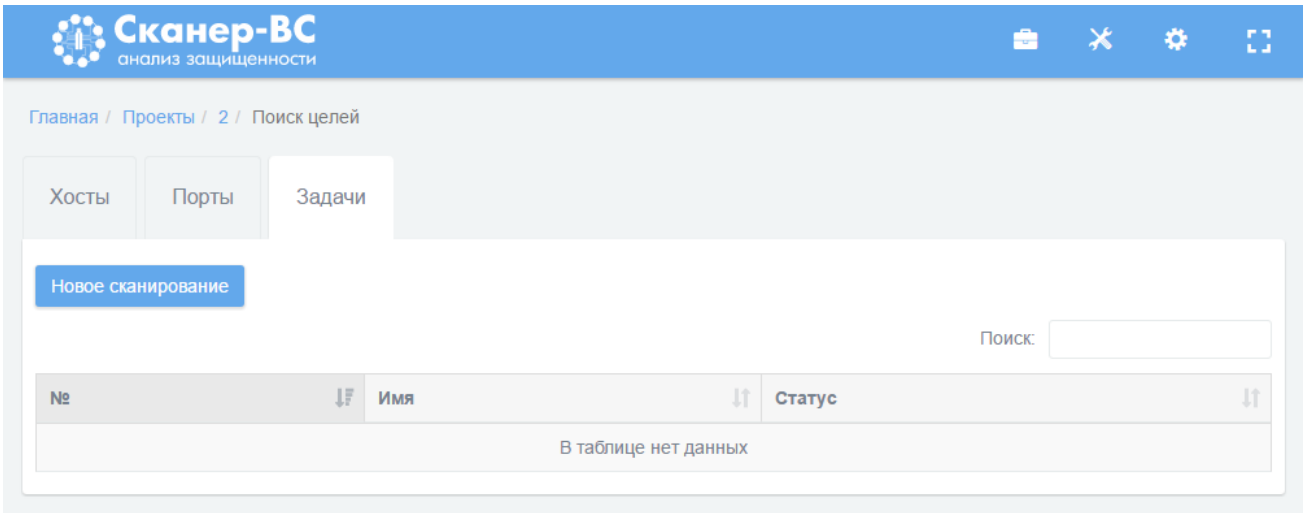


Рисунок 8 – Вкладка «Задачи»

2.2.3. *Поиск целей*

Настройки, необходимые для запуска сканирования сети, находятся на вкладке «Базовые» (Рисунок 9), где в поле «Цели» пользователь задает *цели сканирования:* конкретный IP-адрес, множество IP-адресов - сеть или подсеть.

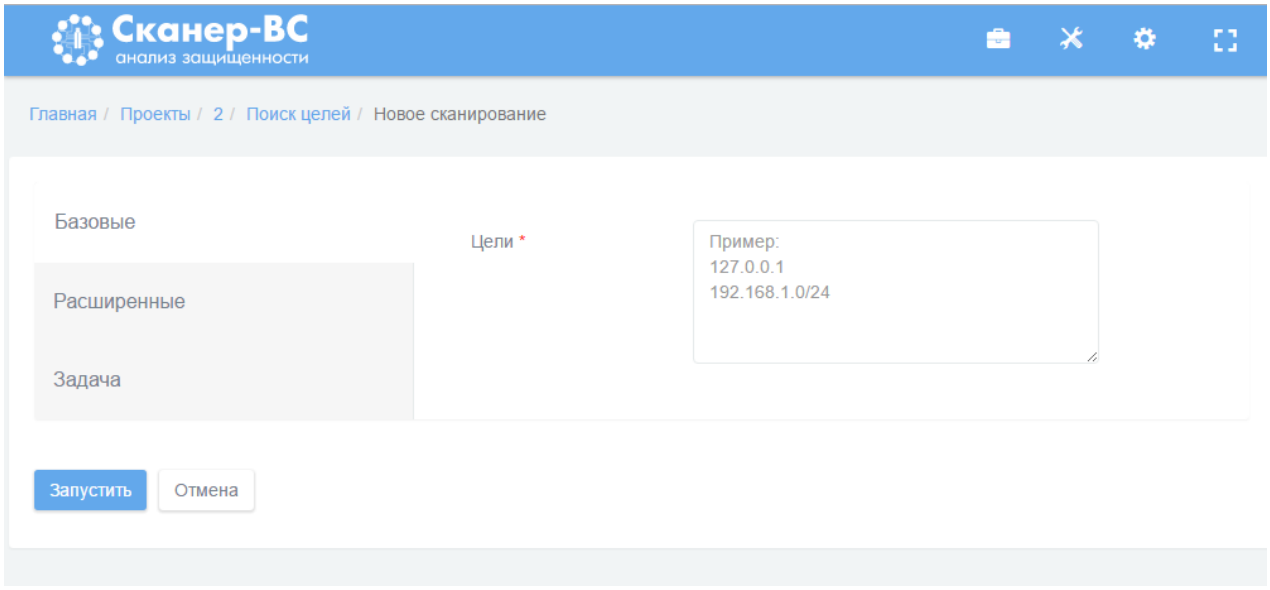


Рисунок 9 – Основные настройки сканирования

Дополнительные настройки сканирования сети расположены на вкладке «Расширенные» и используются пользователем при необходимости (Рисунок 10).

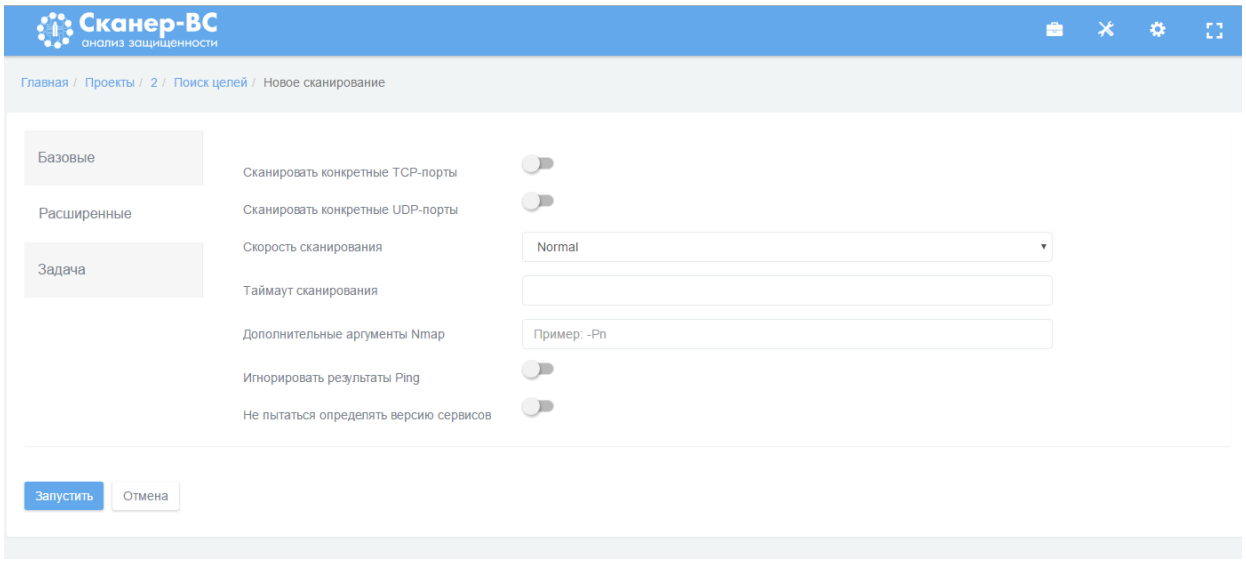


Рисунок 10 – Дополнительные настройки сканирования

На вкладке «Задача» пользователь задает имя и описание текущего сканирования в соответствующие пустые поля (Рисунок 11). Если поля

оставить пустыми, они будут заполнены автоматически, исходя из установленных настроек сканирования.

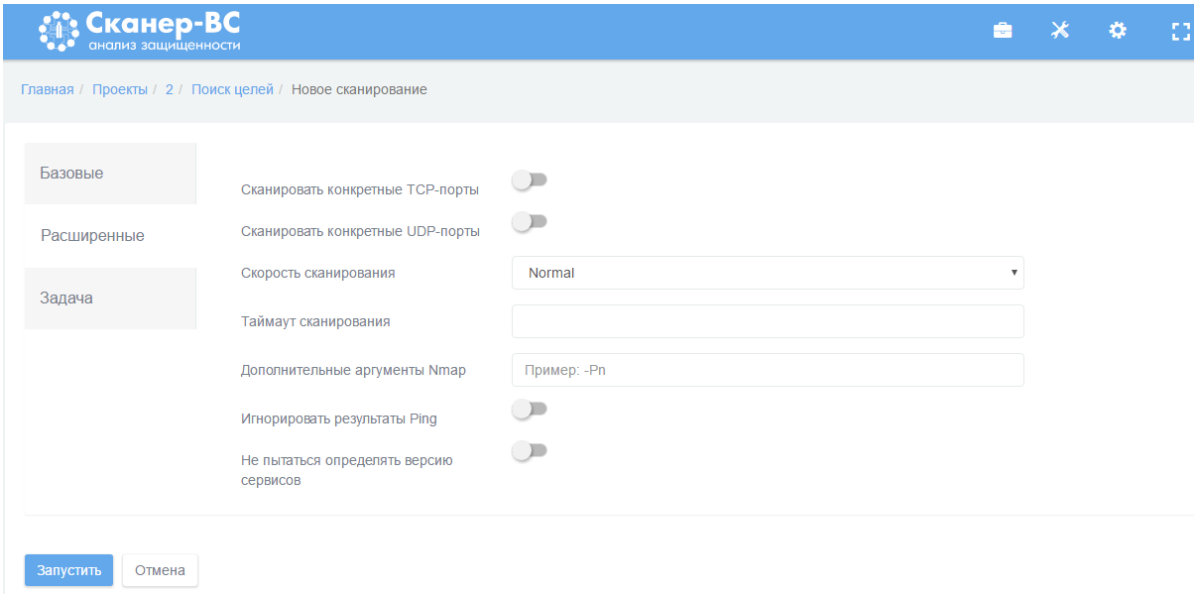


Рисунок 11 – Имя и описание сканирования

Чтобы начать сканирование нажмите кнопку **Запустить** (Рисунок 11).

2.2.4. Завершение работы

После запуска сканирования на вкладке «Задачи» в таблице появится номер задачи, ее имя, текущий статус (цветной индикатор). Желтый цвет индикатора означает, что в текущий момент сканирование выполняется, зеленый - сканирование успешно завершено (Рисунок 12), красный - процесс сканирования завершен с ошибкой.

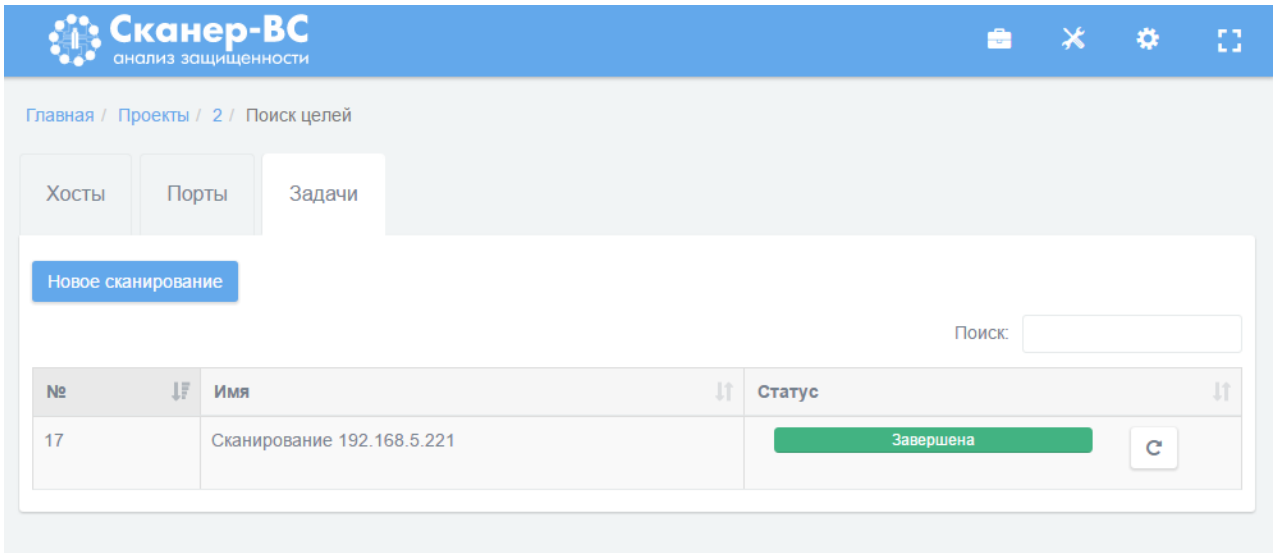
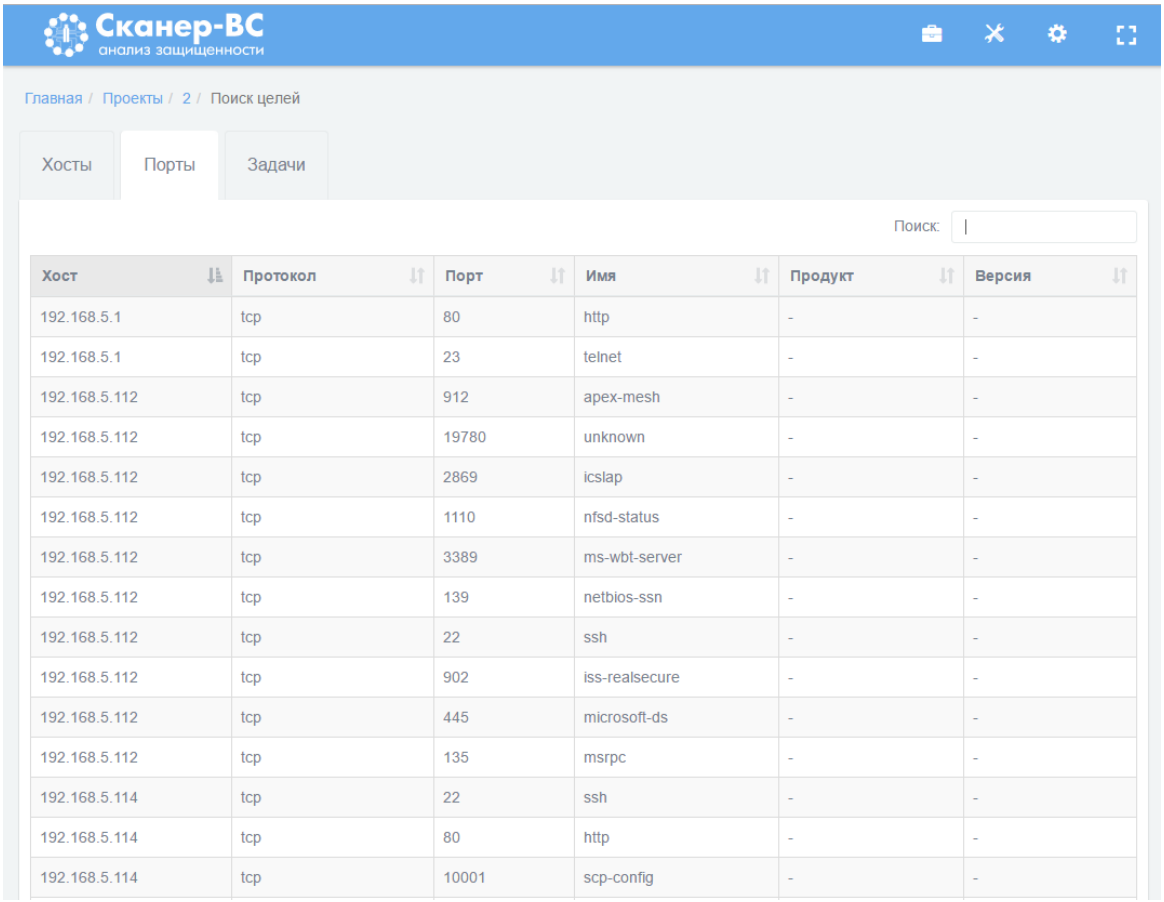


Рисунок 12 – Процесс сканирования

Независимо от результатов сканирования любую задачу можно перезапустить, нажав на кнопку **Повторить** (Рисунок 12), расположенную справа от индикатора статуса сканирования. Если сканирование завершено с ошибкой, для получения подробной информации об ошибке нажмите левой кнопкой мыши по индикатору статуса сканирования (в этом случае он красного цвета), после чего откроется новое окно с информацией о задаче, деталях запуска и ошибках во время запуска задачи.

После завершения сканирования во вкладке «Порты» появятся данные об IP-адресах, которые будут сгруппированы в таблицу (Рисунок 13).



Хост	Протокол	Порт	Имя	Продукт	Версия
192.168.5.1	tcp	80	http	-	-
192.168.5.1	tcp	23	telnet	-	-
192.168.5.112	tcp	912	apex-mesh	-	-
192.168.5.112	tcp	19780	unknown	-	-
192.168.5.112	tcp	2869	icslap	-	-
192.168.5.112	tcp	1110	nfsd-status	-	-
192.168.5.112	tcp	3389	ms-wbt-server	-	-
192.168.5.112	tcp	139	netbios-ssn	-	-
192.168.5.112	tcp	22	ssh	-	-
192.168.5.112	tcp	902	iss-realsecure	-	-
192.168.5.112	tcp	445	microsoft-ds	-	-
192.168.5.112	tcp	135	msrpc	-	-
192.168.5.114	tcp	22	ssh	-	-
192.168.5.114	tcp	80	http	-	-
192.168.5.114	tcp	10001	scp-config	-	-

Рисунок 13 – Вкладка «Порты»

Во вкладке «Хосты» в таблице показаны IP-адреса и операционные системы (далее – ОС), которые им соответствуют (Рисунок 14).

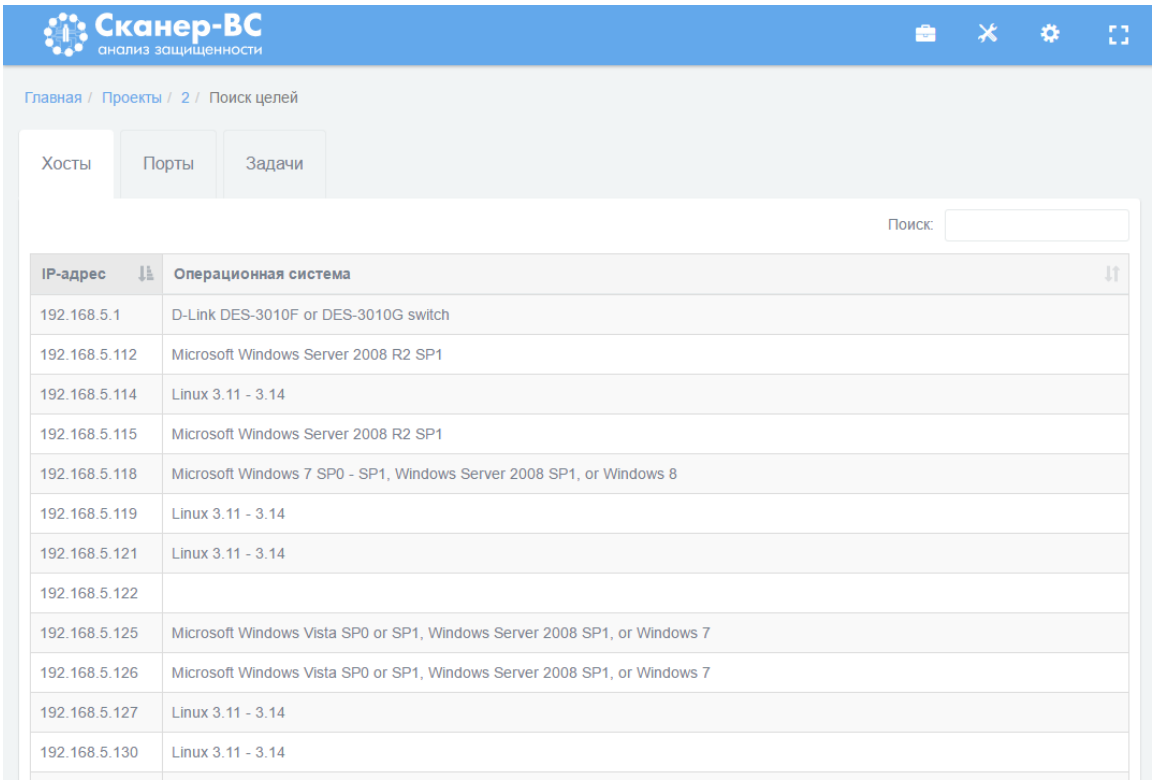


Рисунок 14 – Вкладка «Хосты»

2.3. Поиск уязвимостей

2.3.1. Краткое описание

Под уязвимостью программного обеспечения (далее – ПО) подразумевается дефект ПО, который может стать причиной нарушения информационной безопасности. Поиск уязвимостей - действия по обнаружению таких дефектов.

Поиск уязвимостей можно производить разными способами:

– запуская специальные инструментальные программы, как на одном компьютере, так и в пределах компьютерной сети;

– воздействуя специальными программами на работающие в сети компьютеры с помощью одного из компьютеров.

В данном случае описан второй вариант поиска.

2.3.2. Начало работы

Чтобы начать поиск уязвимостей нажмите левой кнопкой мыши по сектору «Поиск уязвимостей», затем перейдите на вкладку «Задачи» и нажмите на кнопку **Новое сканирование** (Рисунок 15).

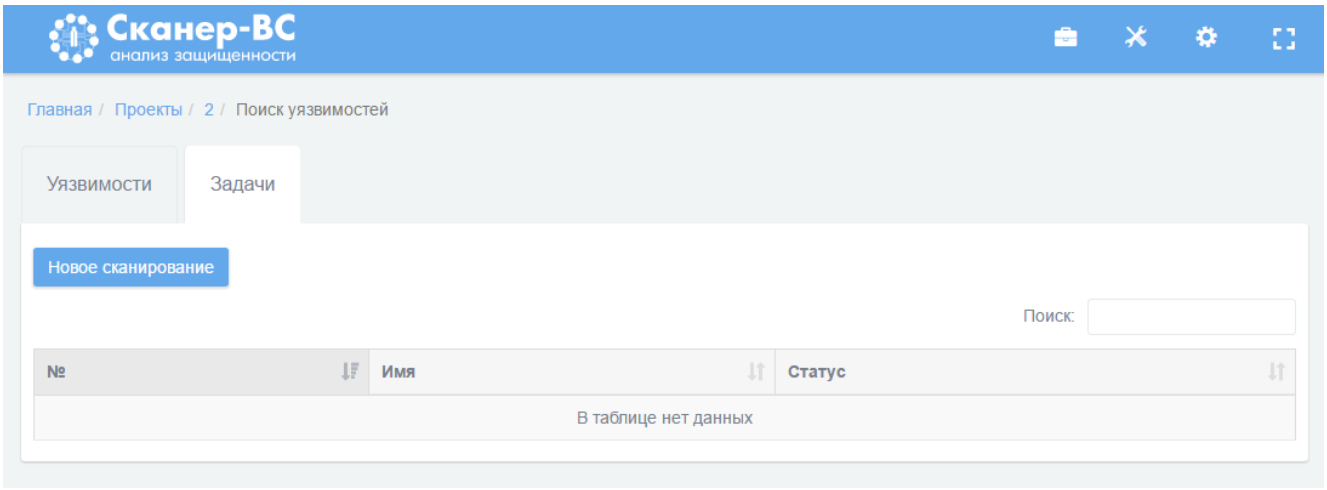


Рисунок 15– Сектор «Поиск уязвимостей»

2.3.3. Поиск уязвимостей

Настройки, необходимые для запуска поиска уязвимостей, находятся на вкладке «Базовые» (Рисунок 16), где пользователь задает *цели поиска уязвимостей* (IP-адреса проверяемых компьютеров, сетей или подсетей) и выбирает *политику сканирования* (набор правил сканирования): базовую (сканирование веб-сервисов, либо полное сканирование) или пользовательскую, настраиваемую пользователем. Цели поиска уязвимостей можно задавать несколькими способами: вводя вручную адреса в поле «Цели», импортируя цели из активов или загружая из файла.

Для загрузки из активов целей поиска уязвимостей в поле «Импорт целей из активов» нажатием левой кнопки мыши отметьте нужные IP-адреса (если IP-адрес выбран, рядом с ним в пустом квадрате появится галочка) или нажмите кнопку **Выделить все** (все IP-адреса в поле будут отмечены автоматически). Затем нажмите кнопку **Выбрать** и отмеченные IP-адреса появятся в поле «Цели».

Для загрузки целей сканирования из файла подготовьте соответствующий список целей поиска уязвимостей в формате .TXT, где одна строка должна содержать только один IP-адрес компьютера, сети или подсети. Затем нажмите кнопку **Выберите файл** и в

открывшемся окне отметьте имя файла с импортируемым списком, далее нажмите кнопку **Открыть**. Перечень целей сканирования появится в поле «Цели».

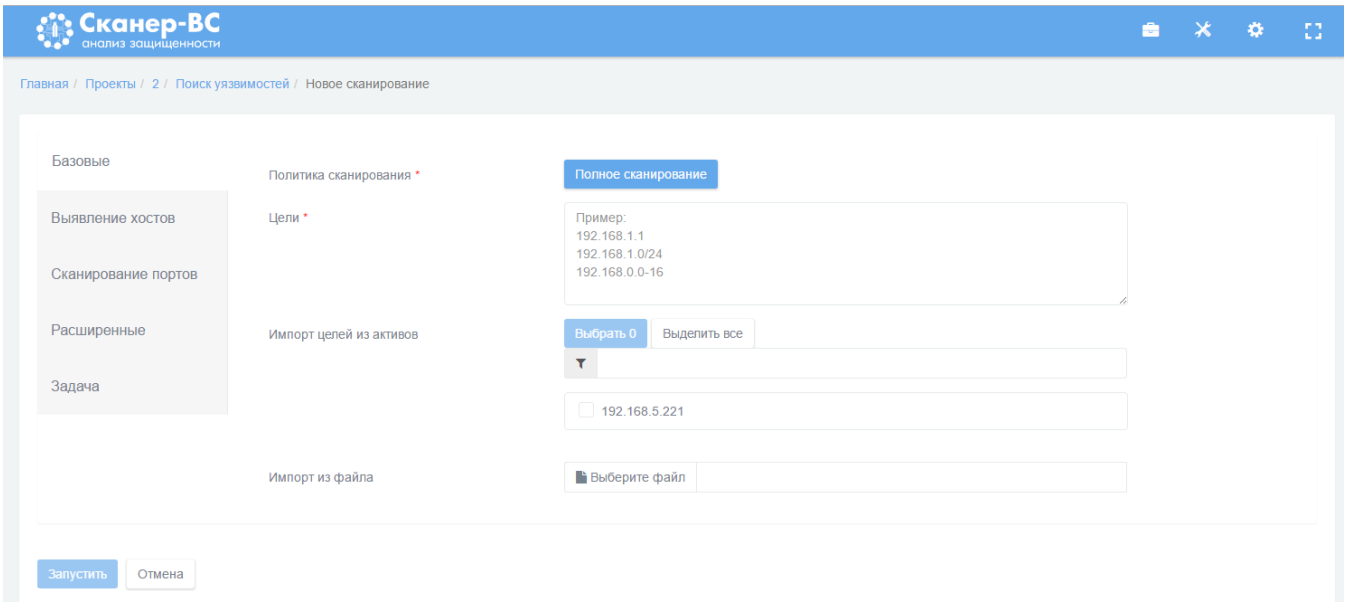


Рисунок 16 – Основные настройки сканирования

Далее выберите политику сканирования. По умолчанию установлено **Полное сканирование**. Если необходимо сменить политику сканирования, нажмите на кнопку **Полное сканирование** и выберите одну из базовых политик или создайте свою (Рисунок 17).

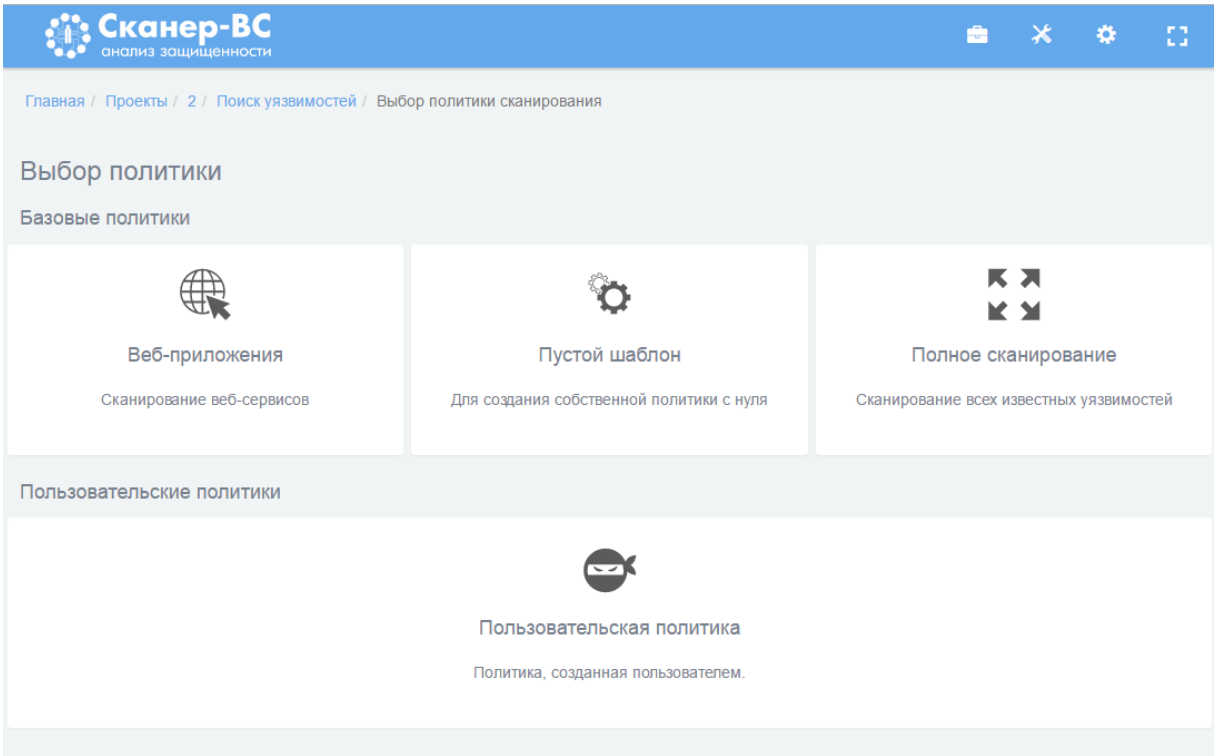


Рисунок 17 – Выбор политики сканирования

Дополнительные настройки сканирования расположены на вкладках «Выявление хостов», «Сканирование портов», «Расширенные» (Рисунок 16) и используются пользователем при необходимости.

На вкладке «Задача» (Рисунок 18) пользователь задает имя и описание в соответствующие пустые поля. Если поля оставить пустыми, они будут заполнены автоматически, исходя из указанных настроек сканирования.

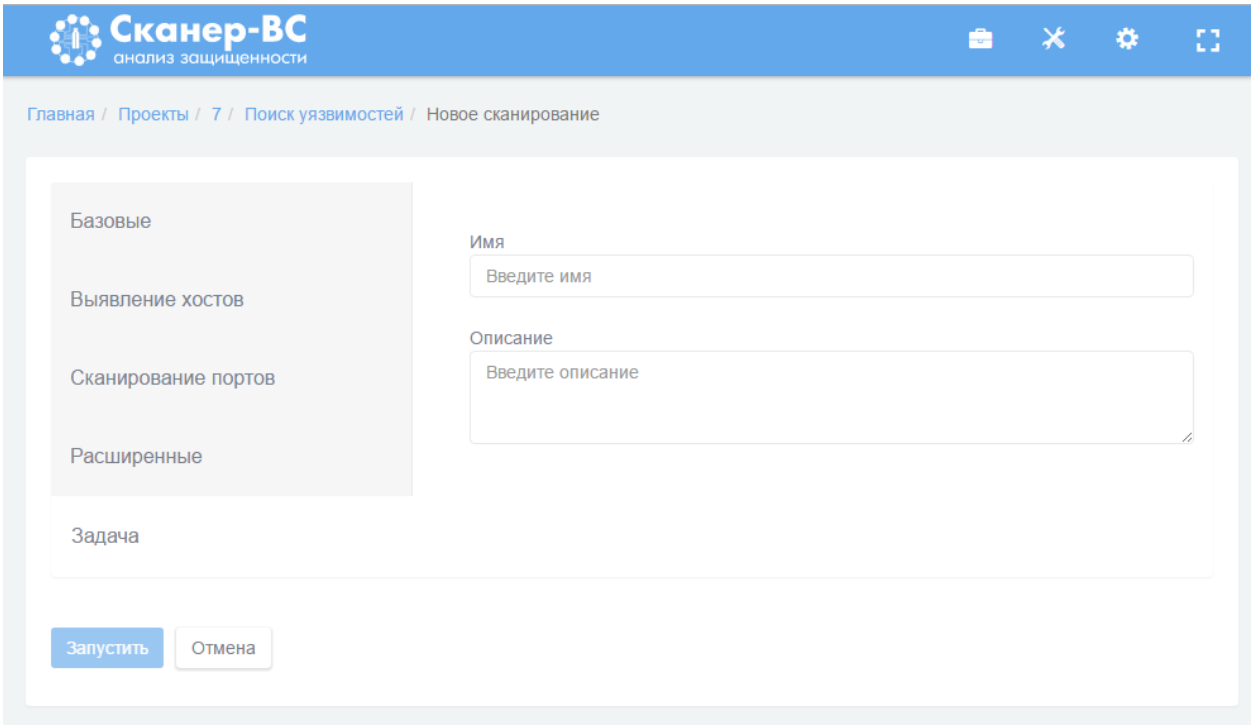


Рисунок 18 – Имя и описание сканирования

Для начала процесса сканирования нажмите кнопку **Запустить** (Рисунок 18).

2.3.4. Завершение работы

После запуска сканирования в таблицу на вкладке «Задачи» будет добавлена строка, содержащая номер задачи, ее имя и индикатор статуса (Рисунок 19). Желтый цвет индикатора означает, что в текущий момент сканирование выполняется, зеленый - сканирование успешно завершено, красный - процесс сканирования завершен с ошибкой.

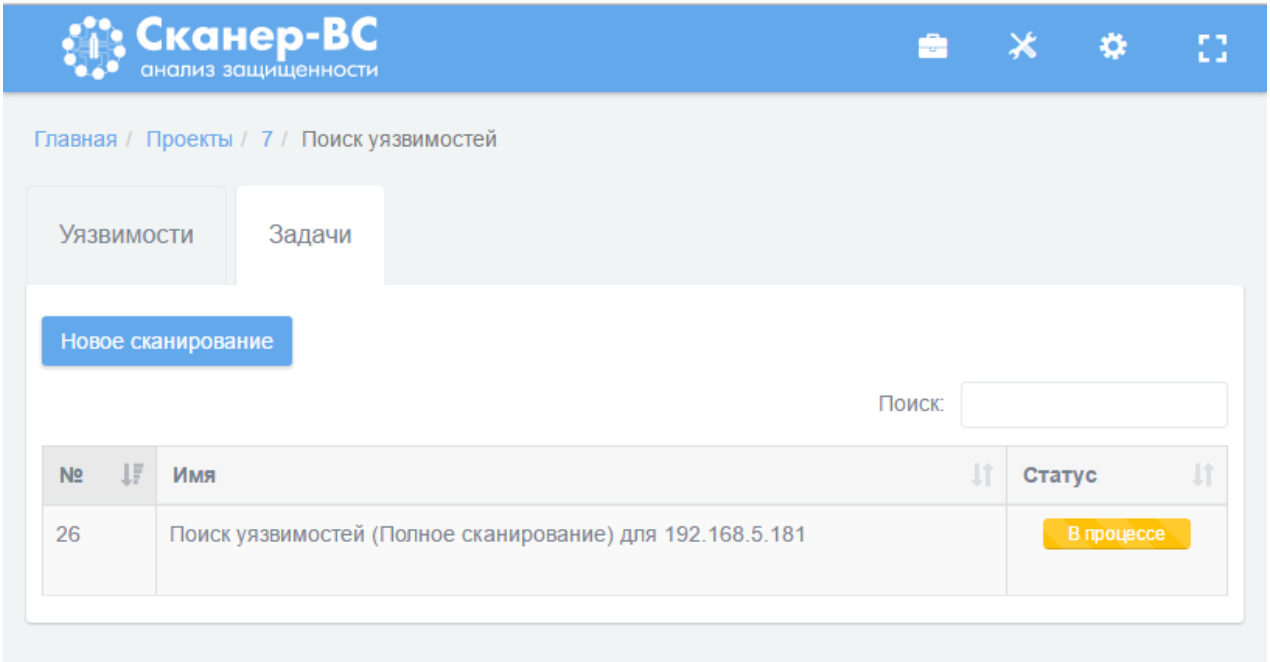
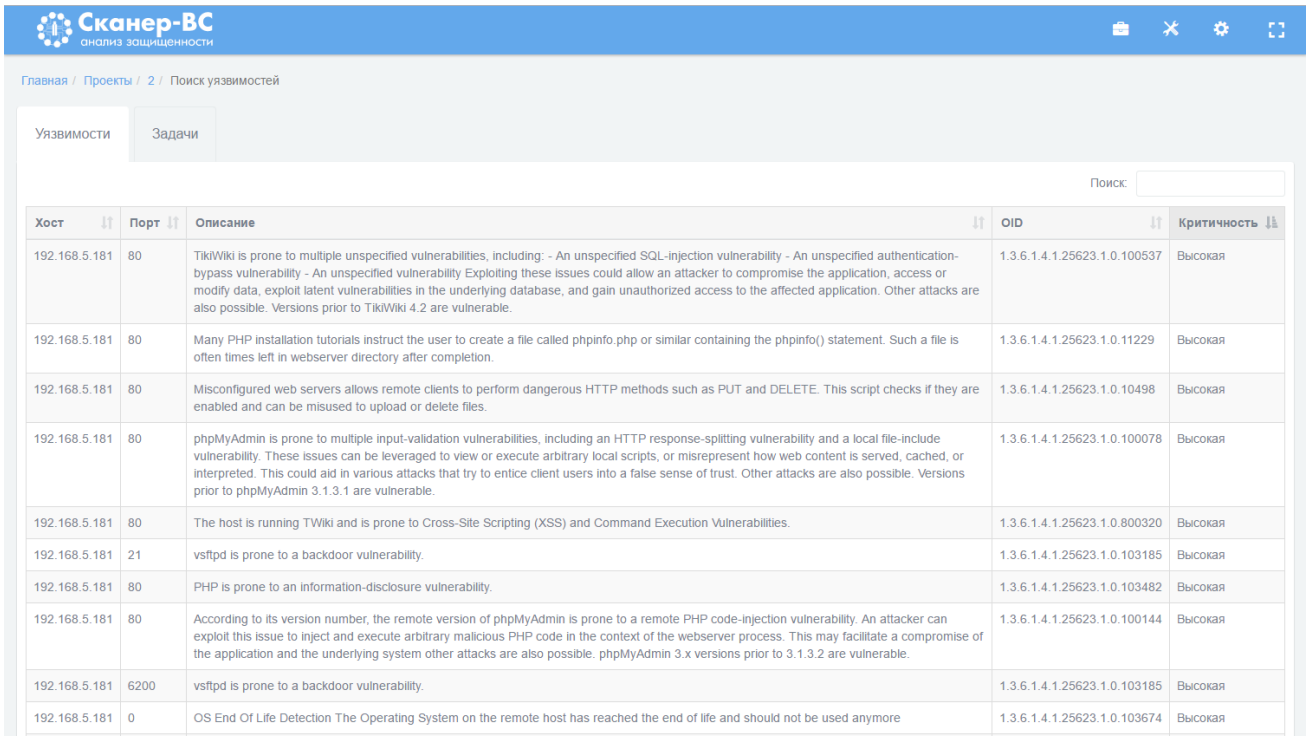


Рисунок 19 – Процесс сканирования

Независимо от результатов сканирования любую задачу можно перезапустить, нажав на кнопку **Повторить** (Рисунок 12), расположенную справа от индикатора статуса. Если сканирование завершено с ошибкой, для получения подробной информации об ошибке, нажмите левой кнопкой мыши по красному индикатору, после чего откроется новое окно с информацией о текущем сканировании, его основных параметрах, ошибках.

После завершения сканирования на вкладке «Уязвимости» появятся данные об обнаруженных уязвимостях, которые будут сгруппированы в таблицу (Рисунок 20).



Хост	Порт	Описание	OID	Критичность
192.168.5.181	80	TikiWiki is prone to multiple unspecified vulnerabilities, including: - An unspecified SQL-injection vulnerability - An unspecified authentication-bypass vulnerability - An unspecified vulnerability Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible. Versions prior to TikiWiki 4.2 are vulnerable.	1.3.6.1.4.1.25623.1.0.100537	Высокая
192.168.5.181	80	Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often times left in webserver directory after completion.	1.3.6.1.4.1.25623.1.0.11229	Высокая
192.168.5.181	80	Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files.	1.3.6.1.4.1.25623.1.0.10498	Высокая
192.168.5.181	80	phpMyAdmin is prone to multiple input-validation vulnerabilities, including an HTTP response-splitting vulnerability and a local file-include vulnerability. These issues can be leveraged to view or execute arbitrary local scripts, or misrepresent how web content is served, cached, or interpreted. This could aid in various attacks that try to entice client users into a false sense of trust. Other attacks are also possible. Versions prior to phpMyAdmin 3.1.3.1 are vulnerable.	1.3.6.1.4.1.25623.1.0.100078	Высокая
192.168.5.181	80	The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.	1.3.6.1.4.1.25623.1.0.800320	Высокая
192.168.5.181	21	vsftpd is prone to a backdoor vulnerability.	1.3.6.1.4.1.25623.1.0.103185	Высокая
192.168.5.181	80	PHP is prone to an information-disclosure vulnerability.	1.3.6.1.4.1.25623.1.0.103482	Высокая
192.168.5.181	80	According to its version number, the remote version of phpMyAdmin is prone to a remote PHP code-injection vulnerability. An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system other attacks are also possible. phpMyAdmin 3.x versions prior to 3.1.3.2 are vulnerable.	1.3.6.1.4.1.25623.1.0.100144	Высокая
192.168.5.181	6200	vsftpd is prone to a backdoor vulnerability.	1.3.6.1.4.1.25623.1.0.103185	Высокая
192.168.5.181	0	OS End Of Life Detection The Operating System on the remote host has reached the end of life and should not be used anymore	1.3.6.1.4.1.25623.1.0.103674	Высокая

Рисунок 20 – Результаты поиска

2.4. Эксплуатация

2.4.1. Краткое описание

Фаза «Эксплуатация» объединяет две задачи: сетевой аудит паролей и поиск *эксплойтов* - возможностей несанкционированного удаленного использования ресурсов компьютера (доступ к информации, эксплуатация вычислительных мощностей, возможность действовать от лица других пользователей) посредством специальных программ или без них. Часто эксплойтом называют программу, предоставляющую возможность использования ресурсов компьютера.

Задача сетевого аудита паролей - выявление возможности получения доступа к ресурсам компьютеров в проверяемой сети путем подбора имени и пароля пользователя. Задача поиска эксплойтов - тестирование компьютеров в проверяемой сети на возможность их использования описанными выше способами.

2.4.2. Запуск

Для запуска сетевого аудита паролей и поиска эксплойтов (Рисунок 21) нажмите левой кнопкой мыши по сектору «Эксплуатация».

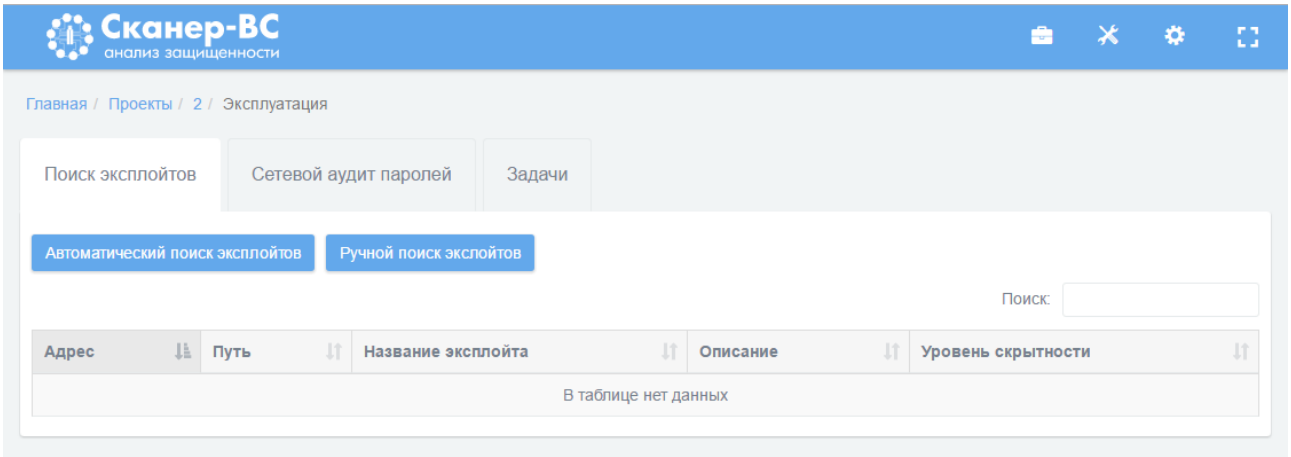


Рисунок 21 – Сектор «Эксплуатация»

2.4.3. Поиск эксплойтов

Для проведения тестирования возможности несанкционированного удаленного использования ресурсов компьютера выберите вкладку «Поиск эксплойтов». Если перед запуском поиска эксплойтов в проекте были проведены поиск целей и поиск уязвимостей, то нажмите кнопку **Автоматический поиск эксплойтов**, в ином случае нажмите кнопку **Ручной поиск эксплойтов**.

После нажатия кнопки **Автоматический поиск эксплойтов** откроется окно «Настройка автоматического поиска эксплойтов» (Рисунок 22).

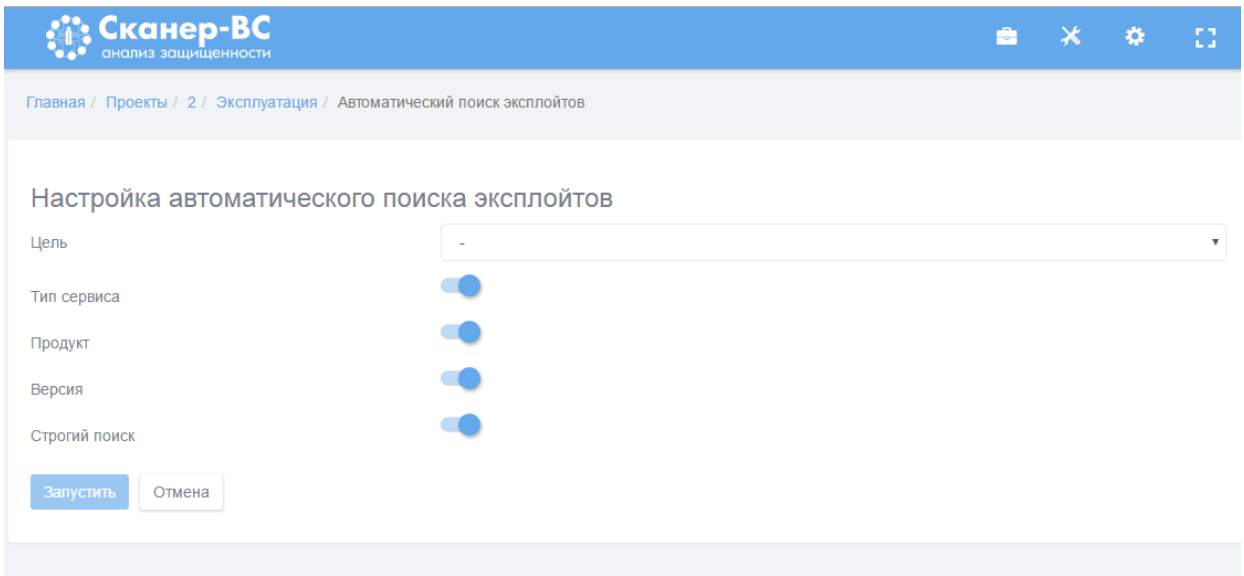


Рисунок 22 – Интерфейс настройки и запуска автоматического поиска эксплойтов

В поле «Цель» выберите IP-адрес. Запуск тестирования можно произвести только для одного IP-адреса. Далее указываются критерии поиска эксплойтов: «Тип сервиса», «Продукт», «Версия». Тумблер «Строгий поиск» добавляет условие, что по выбранным критериям будет проведен поиск эксплойтов, для которых все выбранные параметры поиска будут иметь заданные значения, если тумблер выключен, будет произведен поиск эксплойтов, для которых совпадает хотя бы один параметр поиска. После завершения настройки для запуска тестирования нажмите копку **Запустить.**

После нажатия кнопки **Ручной поиск эксплойтов** откроется окно «Настройка ручного поиска эксплойтов» (Рисунок 23).

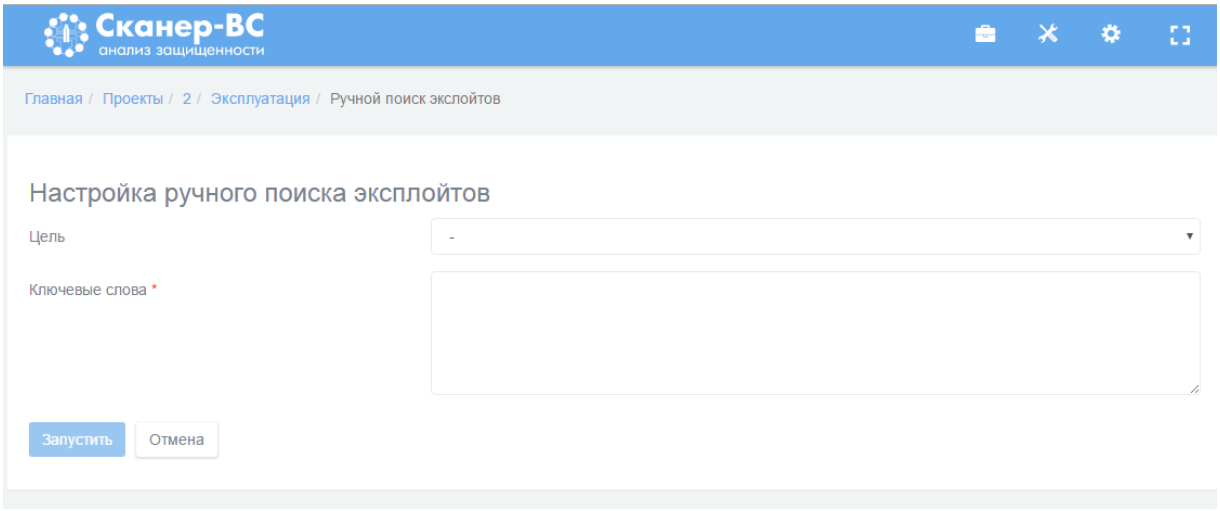


Рисунок 23 – Интерфейс настройки и запуска ручного поиска эксплойтов

В поле «Цель» введите IP-адрес. Запуск тестирования можно произвести только для одного IP-адреса. В многострочное поле «Ключевые слова» вводятся параметры поиска - фрагменты текста, которые должны обязательно присутствовать в названии, описании и других данных эксплойта из базы эксплойтов. Одна строка многострочного поля должна содержать только одно значение. Когда все параметры будут внесены, нажмите копку **Запустить**. Поиск будет производиться аналогично строгому поиску (см. п.2.4.3).

2.4.4. Сетевой аудит паролей

Перейдите на вкладку «Сетевой аудит паролей» и нажмите на кнопку **Новый подбор паролей** (Рисунок 24).

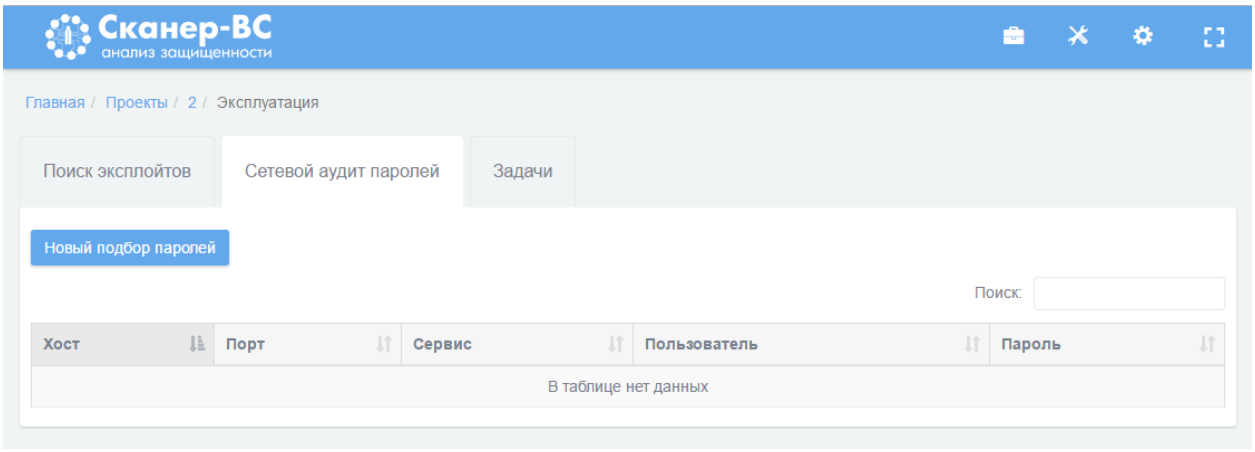


Рисунок 24 – Интерфейс запуска подбора паролей

На вкладке «Базовые» расположены базовые параметры сетевого аудита паролей, которые требуется задать (Рисунок 25): тестируемый сервис (протокол), порт (если используется порт не по умолчанию) и цели тестирования: IP-адрес, сеть или подсеть. Цели можно задать вручную, импортировать из поиска целей или загрузить из файла.

Для загрузки целей поиска уязвимостей из активов в поле «Импорт хостов из активов» нажатием на левую кнопку мыши отметьте нужные IP-адреса (если IP-адрес выбран, рядом с ним в пустом квадрате появится галочка) или нажмите кнопку **Выделить все** (все IP-адреса в поле будут отмечены автоматически). Затем нажмите кнопку **Выбрать** и отмеченные IP-адреса появятся в поле «Цели».

Для загрузки целей сканирования из файла подготовьте соответствующий список целей поиска уязвимостей в формате .TXT, где одна строка документа должна содержать только один IP-адрес, сети или подсети. Затем нажмите кнопку **Выберите файл** и в открывшемся окне отметьте имя импортируемого списка. Нажмите кнопку **Открыть**. Перечень целей сканирования появится в поле «Цели».

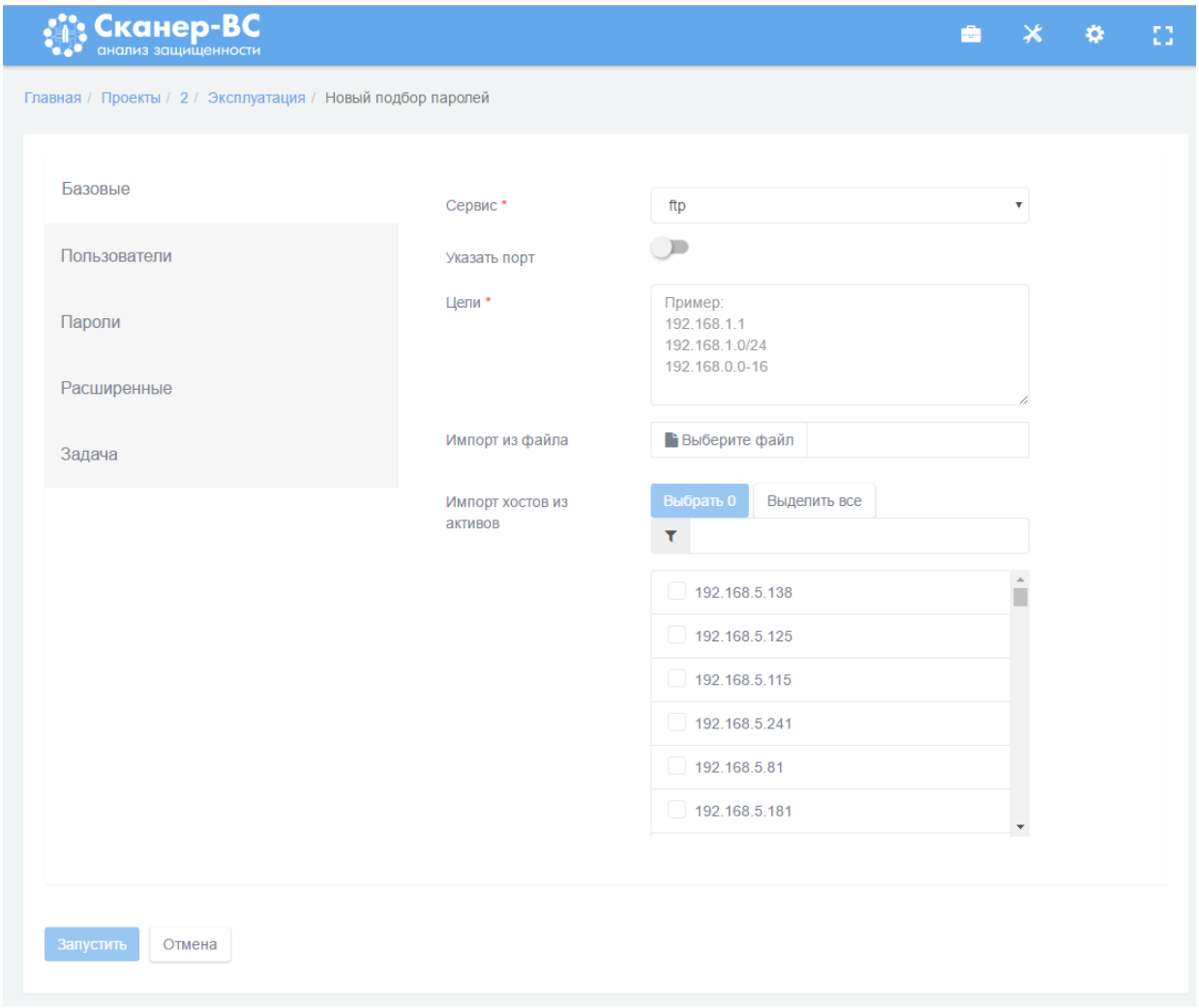


Рисунок 25 – Основные настройки подбора паролей

Для того, чтобы указать сервис (протокол), нажмите левой кнопкой мыши на выпадающий список напротив надписи «Сервис» и выберите нужное значение.

На вкладке «Пользователи» пользователь задает идентификаторы (имена, login) пользователей проверяемых IP-адресов (Рисунок 26). Задать их можно вручную в поле «Пользователи», или импортировать из файла в формате .TXT, где одна строка документа должна содержать только одно имя. Дополнительные настройки («Списки по умолчанию», «Найденные ранее пользователи») используются пользователем при необходимости.

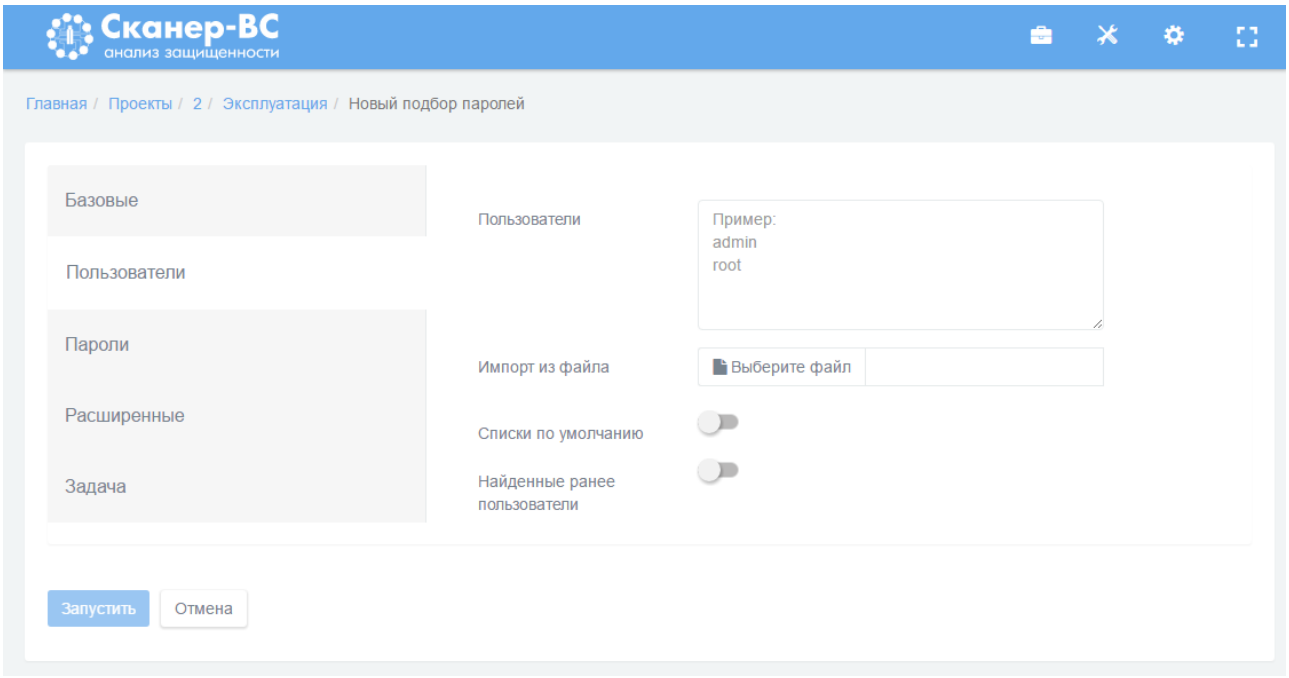


Рисунок 26 – Настройка подбора паролей, вкладка «Пользователи»

На вкладке «Пароли» в поле «Пароли» пользователь задает комбинации букв и цифр, которые будут использоваться в качестве аутентификационной информации (Рисунок 27). Каждая комбинация должна находиться на отдельной строке. Настройки программы поддерживают загрузку паролей из файла в формате .TXT, где одна строка документа должна содержать только один пароль. Дополнительные настройки («Пароли по умолчанию», «Найденные ранее пароли» и другие) используются пользователем при необходимости.

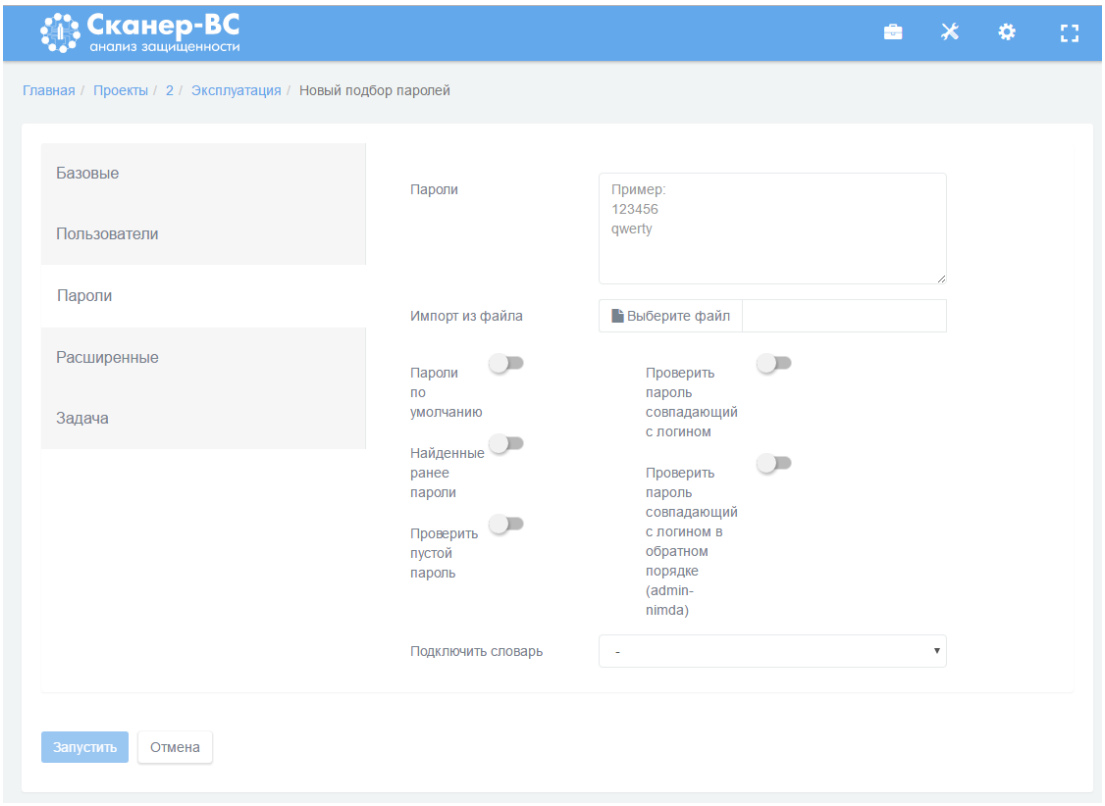


Рисунок 27 – Настройка подбора паролей

Для завершения подбора паролей при первой подобранной паре имя - пароль, перейдите на вкладку «Расширенные» и активируйте «Закончить подбор при первом положительном результате» (Рисунок 28).

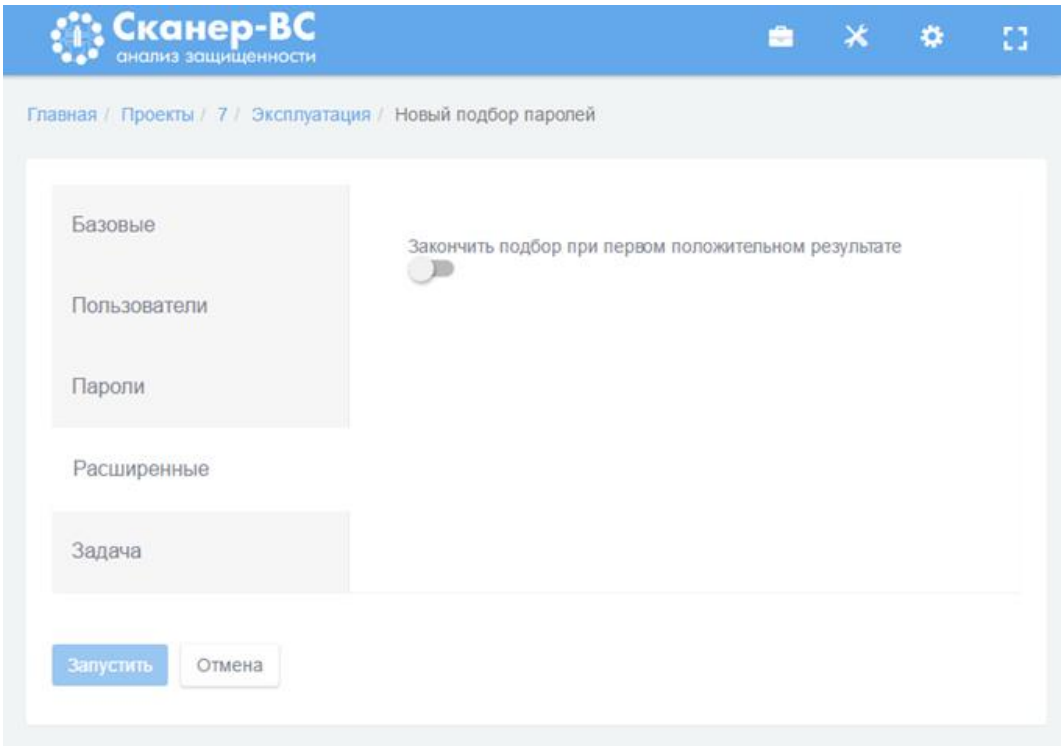


Рисунок 28 – Расширенные настройки подбора паролей

На вкладке «Задача» пользователь задает название и описание для задачи поиска в соответствующие пустые. Если поля оставить пустыми, они будут заполнены автоматически, исходя из указанных настроек тестирования.

Нажмите кнопку **Запустить** (Рисунок 28).

2.4.5. Завершение работы

После нажатия кнопки **Запустить** на вкладке «Задачи» в таблице появится номер задачи, имя и индикатор статуса (Рисунок 29). Желтый цвет индикатора означает процесс сканирования, зеленый - завершение сканирования, красный - процесс сканирования выполнен с ошибкой.

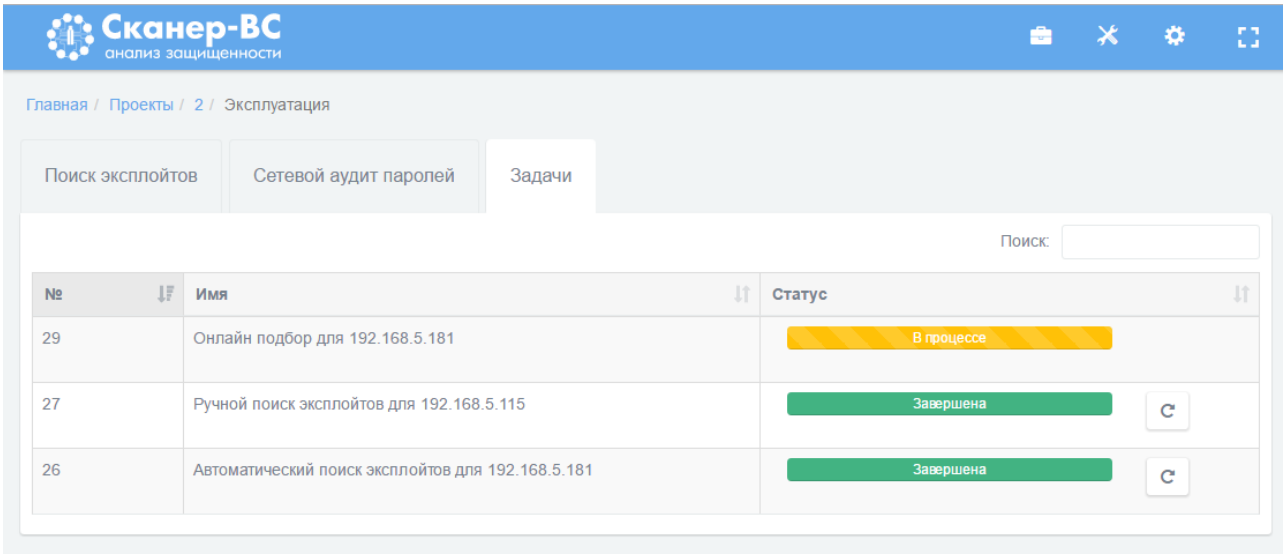


Рисунок 29 – Таблица задач поиска эксплойтов

После завершения сканирования в разделе «Онлайн подбор паролей» появятся данные о подобранных паролях (Рисунок 30), а в разделе «Эксплойты» таблица с найденными эксплойтами (Рисунок 31).

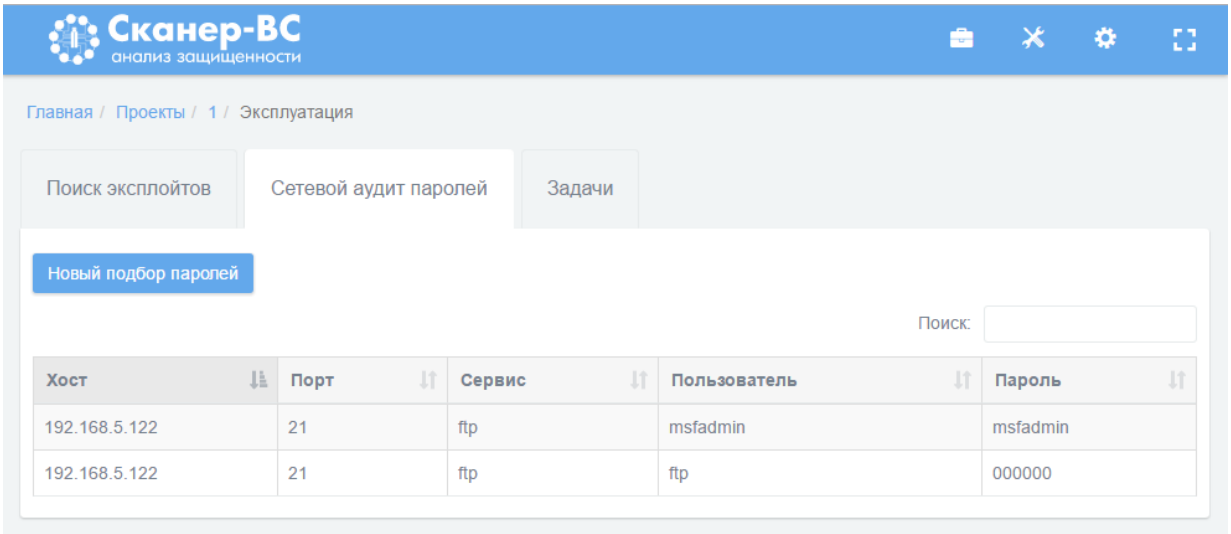


Рисунок 30 – Информация о подобранных паролях

Рисунок 31 – Информация о найденных эксплойтов

2.5. Отчеты

2.5.1. Краткое описание

Документирование является неотъемлемой частью анализа защищенности информационной системы. Для объединения результатов всех этапов тестирования в «Сканер-ВС» используется сектор «Отчет» (Рисунок 6), с помощью которого можно построить отчет с результатами тестирований.

2.5.2 Настройки отчета

После того как был выбран сектор «Отчет», в нем отображается страница с предварительно построенным полным отчетом, который можно просмотреть и экспортировать в формате .PDF или напечатать с помощью кнопки **Печать**.

Для настройки отчета можно воспользоваться конструктором отчета (Рисунок 32), который можно активировать с помощью кнопки **Настройки** (активирован по умолчанию).

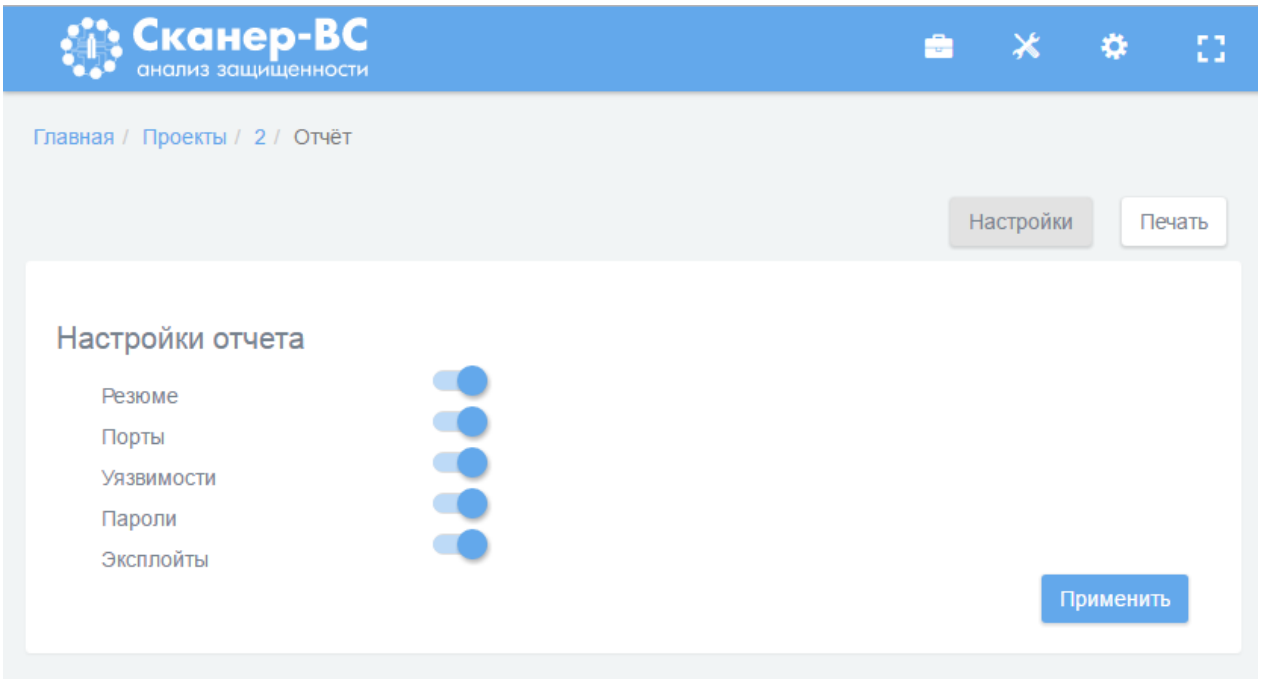


Рисунок 32 – Конструктор отчетов

Полный отчет состоит из следующих разделов: «Резюме», «Порты», «Уязвимости», «Пароли» и «Эксплойты». Раздел «Резюме» - краткая информация по всем этапам тестирования в виде диаграмм и общей таблицы распределения уязвимостей по хостам (Рисунок 33).

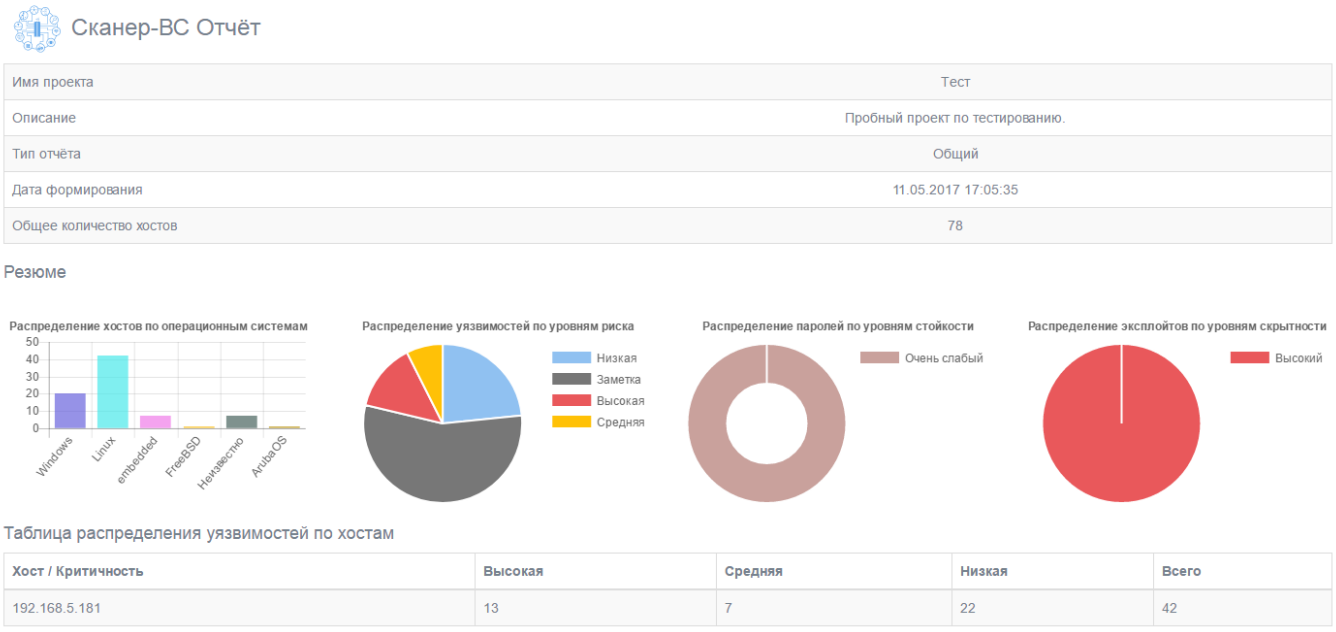


Рисунок 33 – Фрагмент отчета «Сканер-ВС»

Раздел «Порты» соответствует фазе «Поиск целей», раздел «Уязвимости» - фазе «Поиск уязвимостей», раздел «Пароли» и «Эксплойты» - фазе «Эксплуатация». При необходимости любой раздел отчета можно исключить из конечного отчета по тестированию, для этого необходимо с помощью левой кнопки мыши отключить тумблер напротив каждого исключаемого раздела отчета, затем нажать кнопку **Применить**. Отчет изменится согласно новым условиям.