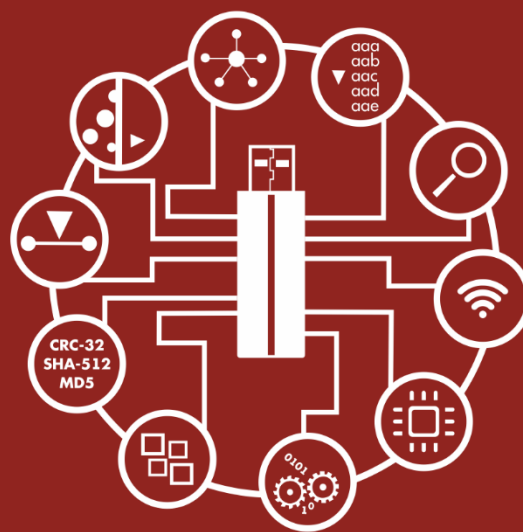




Сканер-ВС

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

О КОМПАНИИ	2
О РУКОВОДСТВЕ	3
1. НОВЫЙ ИНТЕРФЕЙС	5
2. ТЕСТИРОВАНИЕ ЗАЩИЩЕННОСТИ	8
2.1. Что такое проект. Создание проекта	8
2.2. Поиск целей	10
2.2.1. Краткое описание	10
2.2.2. Запуск	11
2.2.3. Поиск целей	11
2.2.4. Завершение работы	14
2.3. Поиск уязвимостей	16
2.3.1. Краткое описание	16
2.3.2. Начало работы	16
2.3.3. Поиск уязвимостей	17
2.3.4. Завершение работы	19
2.4. Эксплуатация	20
2.4.1. Краткое описание	20
2.4.2. Запуск	21
2.4.3. Поиск эксплойтов	21
2.4.4. Сетевой аудит паролей	23
2.4.5. Завершение работы	28
2.5. Отчеты	29
2.5.1. Краткое описание	29
2.5.2. Настройки отчета	29

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:

- проекты (на рисунке 2 выделена фиолетовой рамкой);
- инструменты (на рисунке 2 выделена красной рамкой);
- справочная информация (на рисунке 2 выделена зеленой 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

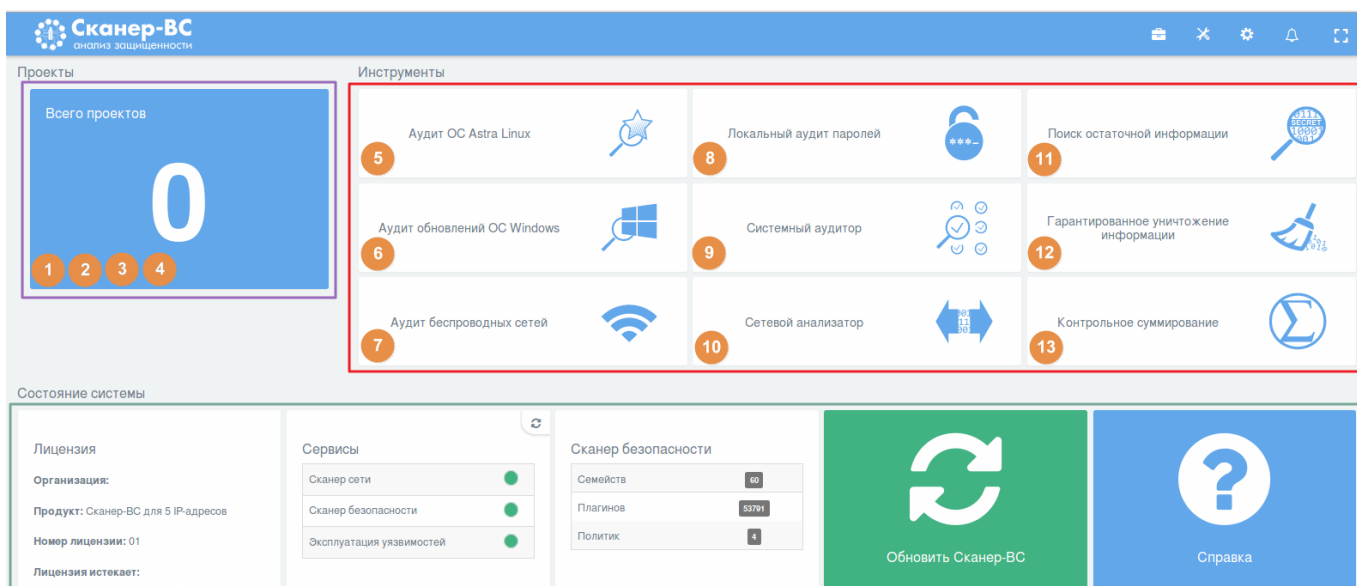


Рисунок 2 — Пользовательский веб-интерфейс «Сканер-ВС» новой версии

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).

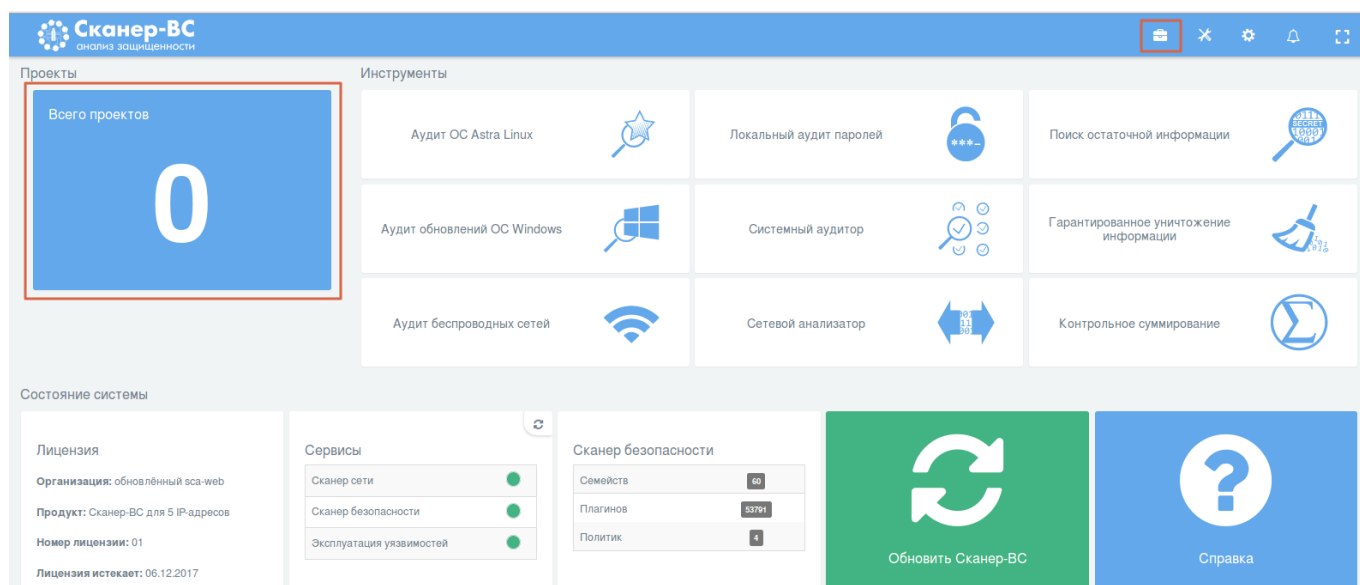


Рисунок 3 — Раздел «Проекты» веб-интерфейса «Сканер-ВС»

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

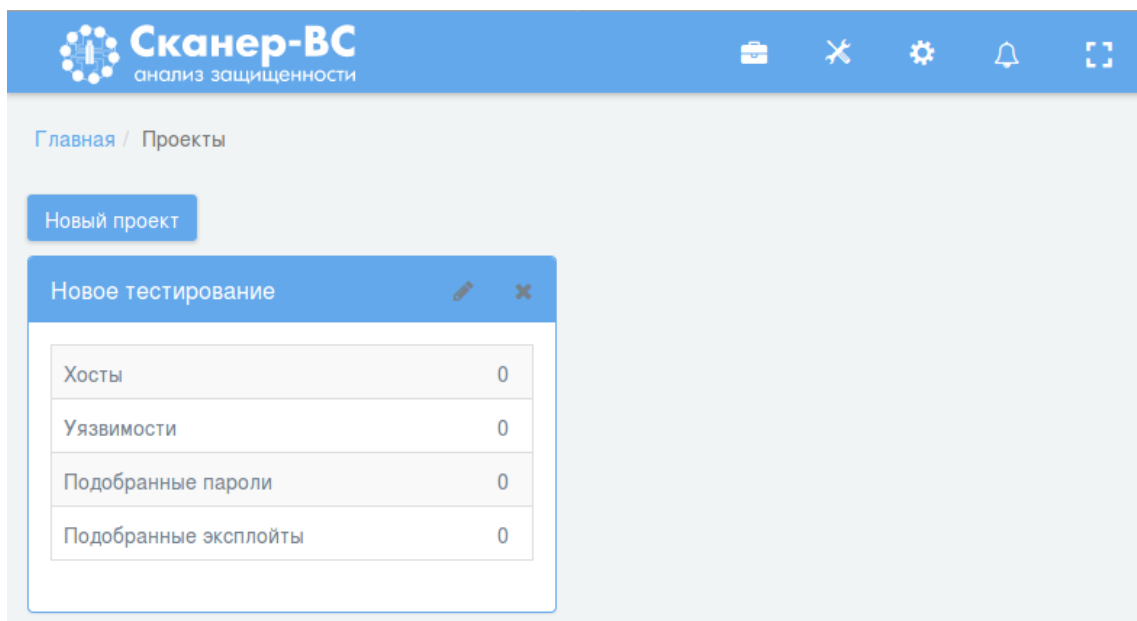


Рисунок 4 — Создание проекта

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

The screenshot shows the 'Сканер-ВС' web application with the breadcrumb trail 'Главная / Проекты / Новый проект'. The main content area is titled 'Добавление нового проекта'. It contains a form with the following fields:

- Имя ***: A text input field.
- Описание**: A large text area for a description.

At the bottom of the form are two buttons: 'Сохранить' (Save) and 'Отмена' (Cancel).

Рисунок 5 — Добавление нового проекта

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.

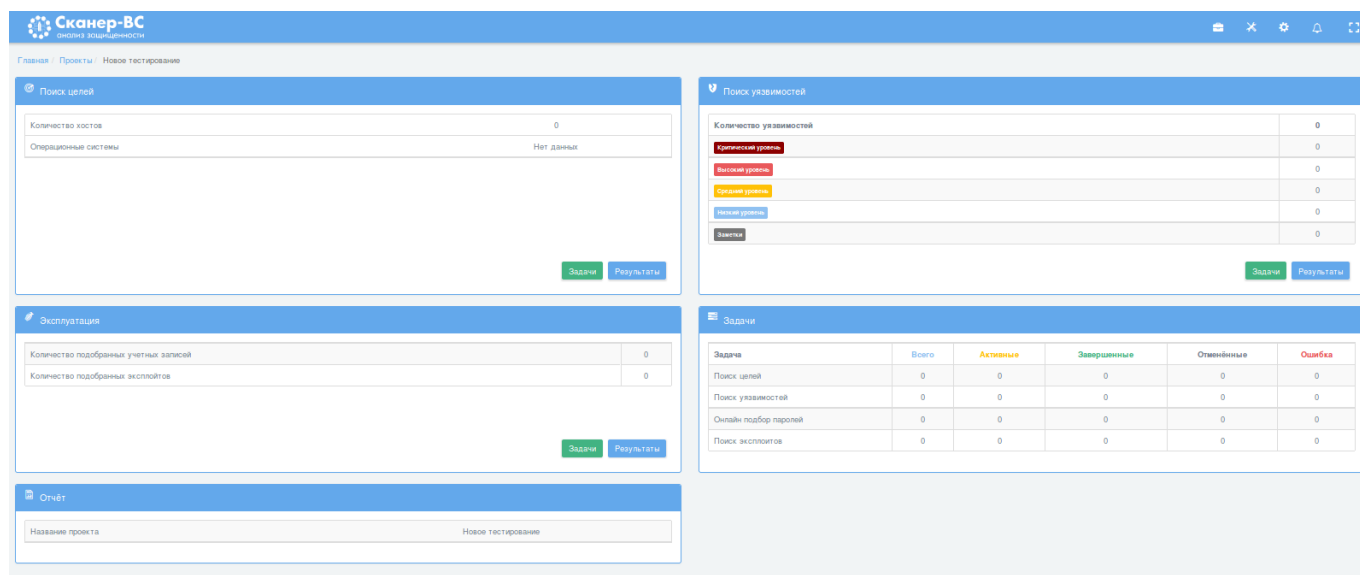


Рисунок 6 — Вид рабочего пространства проекта

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 кнопку **Задачи** в секторе «Поиск целей» (Рисунок 6).

Перейдите на вкладку «Задачи» и нажмите на кнопку **Новое сканирование** (Рисунок 7).

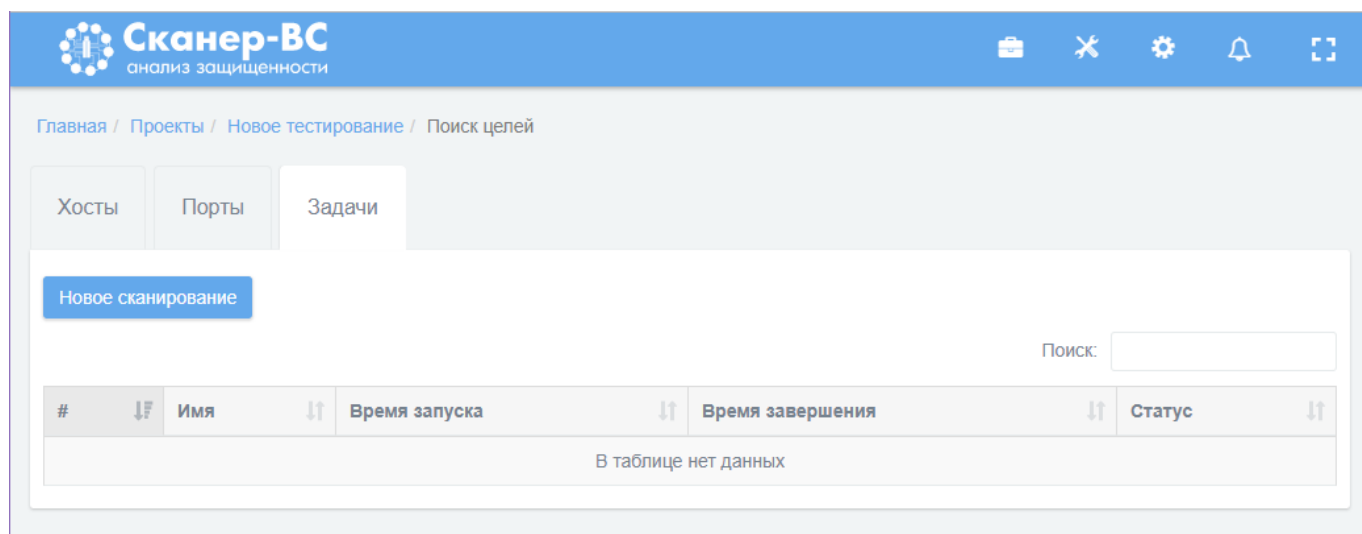


Рисунок 7 — Вкладка «Задачи»

2.2.3. Поиск целей

Настройки, необходимые для запуска сканирования сети, находятся на вкладке «Базовые» (Рисунок 8), где в поле «Цели» пользователь задает *цели сканирования*: конкретный IP-адрес, множество IP-адресов — сеть или подсеть.

Цели сканирования можно импортировать из активов или из файла.

Для загрузки целей из активов нажмите кнопку **Импорт целей из активов** и 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 из файла подготовьте соответствующий список целей в формате TXT, где одна строка должна содержать только один IP-адрес компьютера. Затем нажмите кнопку **Импорт целей из файла** и в открывшемся окне выберите файл с импортируемым списком, далее нажмите кнопку **Открыть**. Перечень целей сканирования появится в поле «Цели» (Рисунок 8).

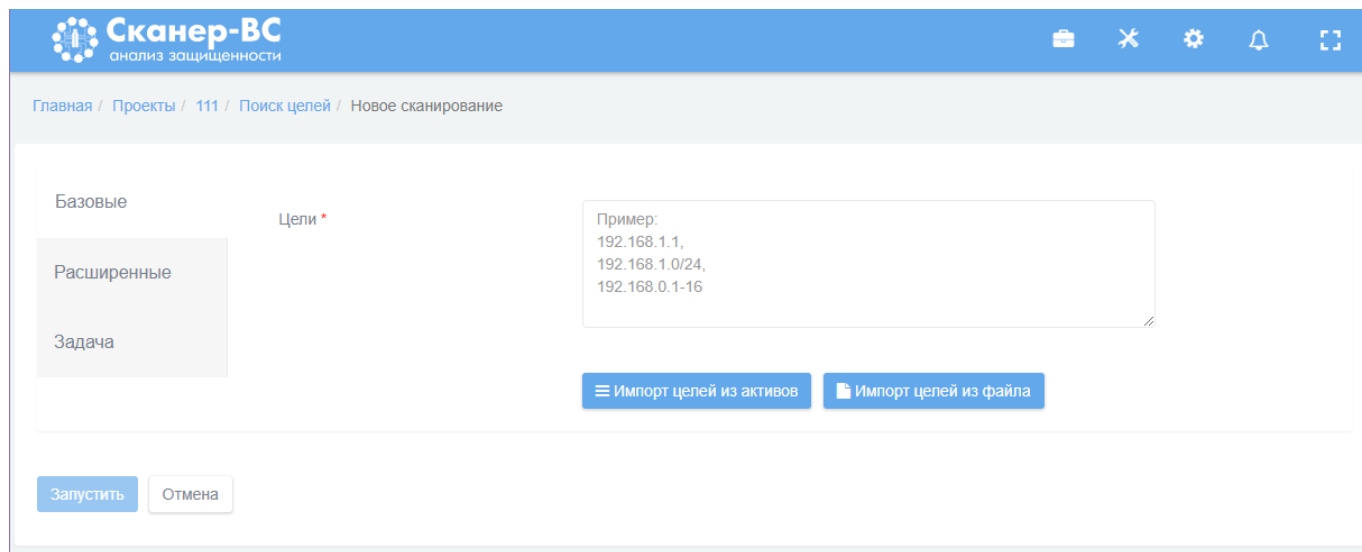


Рисунок 8 — Основные настройки сканирования

Дополнительные настройки сканирования сети расположены на вкладке «Расширенные» и используются пользователем при необходимости (Рисунок 9). Если результаты сканирования необходимо использовать в других фазах тестирования, необходимо включить функцию «Определять версию сервисов» (Рисунок 9).

The screenshot shows the 'Сканер-ВС' application interface. The top navigation bar includes the application logo and title, and a set of icons. The breadcrumb trail reads: Главная / Проекты / 111 / Поиск целей / Новое сканирование. On the left, there is a sidebar with three tabs: 'Базовые', 'Расширенные', and 'Задача'. The 'Задача' tab is selected. The main area contains the following settings:

- Сканировать конкретные TCP-порты: ☐
- Сканировать конкретные UDP-порты: ☐
- Скорость сканирования: Normal (dropdown menu)
- Таймаут сканирования, сек:
- Игнорировать результаты Ping: ☐
- Определять версию сервисов: ☐

At the bottom, there are two buttons: 'Запустить' (blue) and 'Отмена' (white).

Рисунок 9 — Дополнительные настройки сканирования

На вкладке «Задача» пользователь задает имя и описание текущего сканирования в соответствующие пустые поля (Рисунок 10). Если поля оставить пустыми, они будут заполнены автоматически, исходя из установленных настроек сканирования.

The screenshot shows the 'Сканер-ВС' application interface. The top navigation bar and breadcrumb trail are the same as in Figure 9. The sidebar tabs are 'Базовые', 'Расширенные', and 'Задача'. The 'Задача' tab is selected. The main area contains the following fields:

- Имя:
- Описание:

At the bottom, there are two buttons: 'Запустить' (blue) and 'Отмена' (white).

Рисунок 10 — Имя и описание сканирования

Для того, чтобы провести инвентаризацию ресурсов сети, нажмите кнопку **Запустить** (Рисунок 10).

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 11), красный — процесс сканирования завершен с ошибкой.

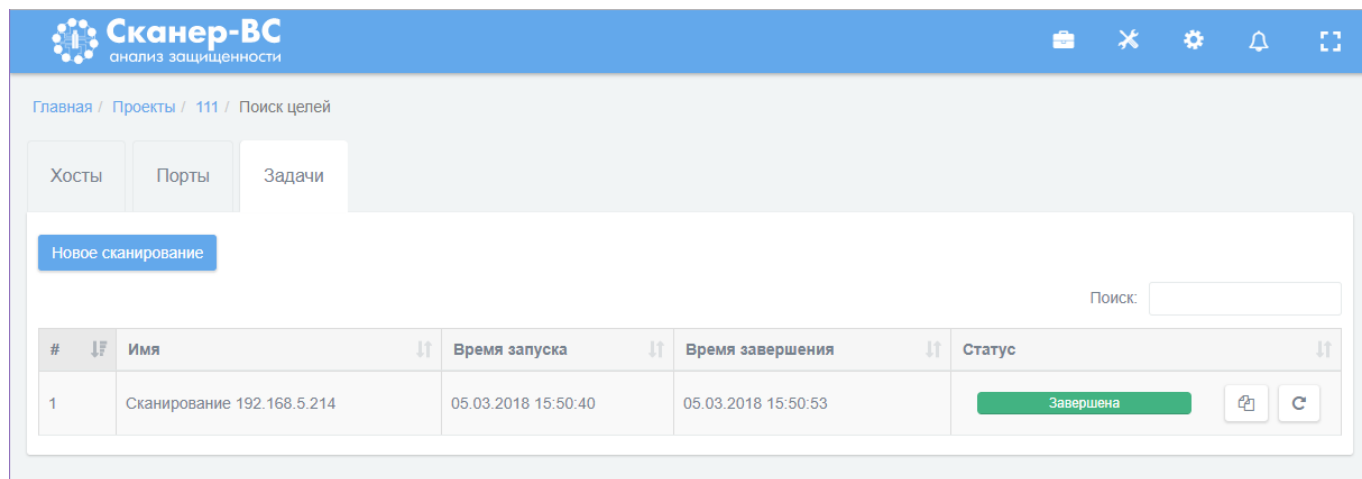


Рисунок 11 — Процесс сканирования

Независимо от результатов сканирования любую задачу можно перезапустить или дублировать. Для этого необходимо нажать на кнопки **Дублировать** или **Повторить** (Рисунок 11), расположенные справа от индикатора статуса сканирования. 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 выполнения задачи.

Изменение статуса выполнения задачи будет отражено в правом верхнем углу веб-интерфейса (кнопка Уведомления) (Рисунок 12) и в журнале событий (Рисунок 13).

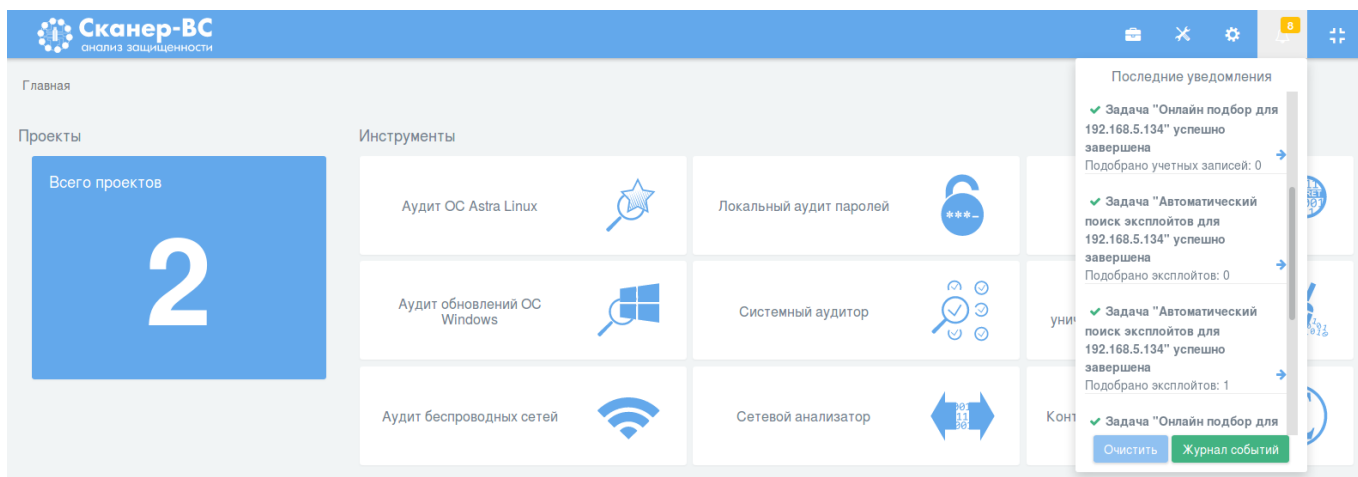


Рисунок 12 — Уведомления

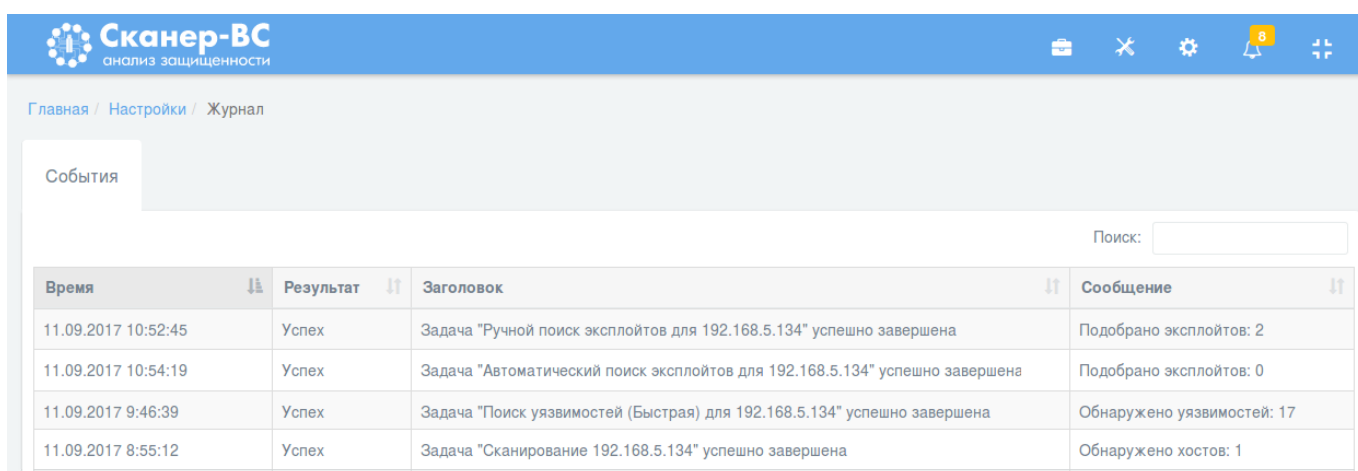


Рисунок 13 — Журнал событий

После завершения сканирования на вкладке «Порты» появятся данные об IP-адресах, которые будут сгруппированы в таблицу (Рисунок 14).

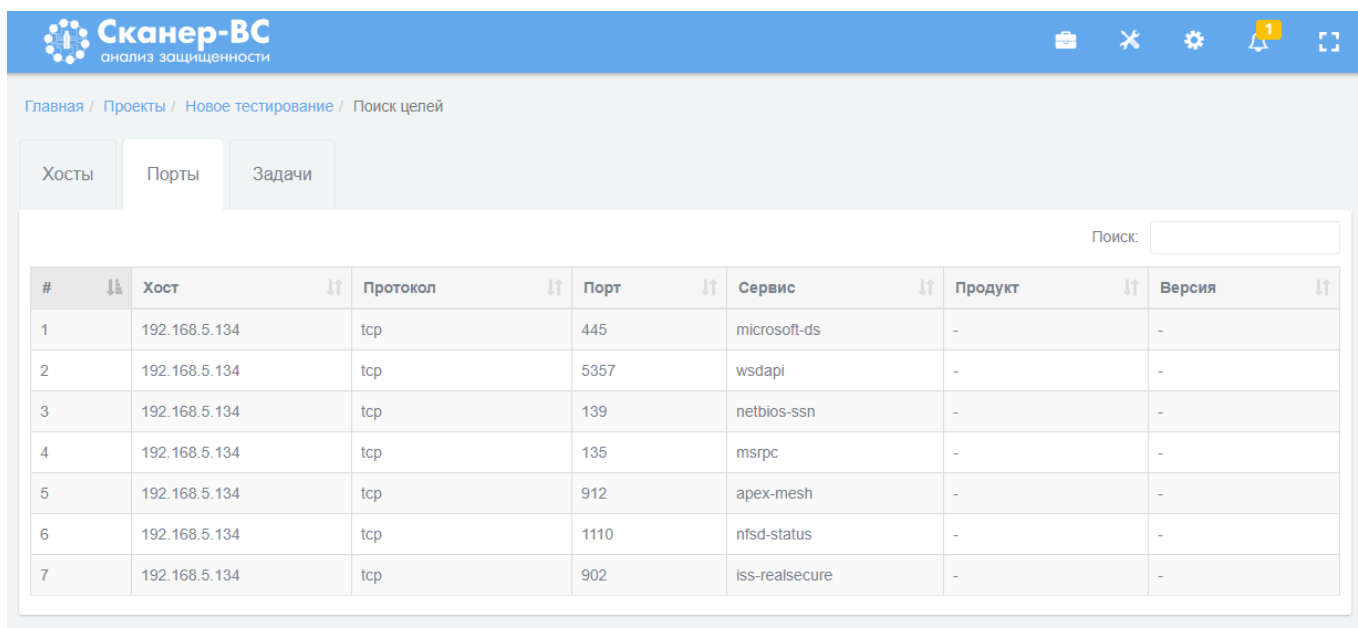


Рисунок 14 — Вкладка «Порты»

На вкладке «Хосты» в таблице показаны IP-адреса и операционные системы (далее — ОС), которые им соответствуют (Рисунок 15).

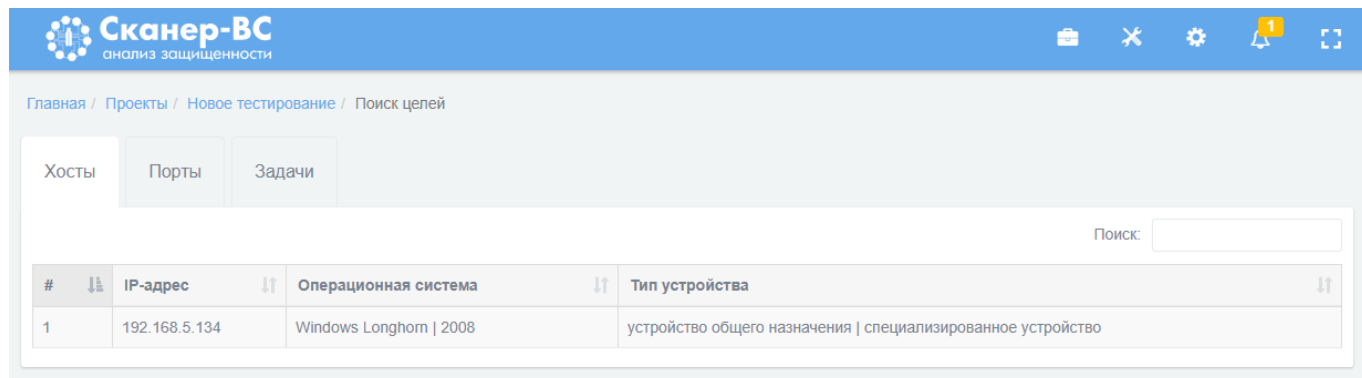


Рисунок 15 — Вкладка «Хосты»

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. Фаза тестирования Поиск уязвимостей направлена на обнаружение таких дефектов.

2.3.2. Начало работы

Чтобы начать поиск уязвимостей нажмите кнопку **Задачи** в секторе «Поиск уязвимостей», затем перейдите на вкладку «Задачи» и нажмите на кнопку **Новое сканирование** (Рисунок 16).

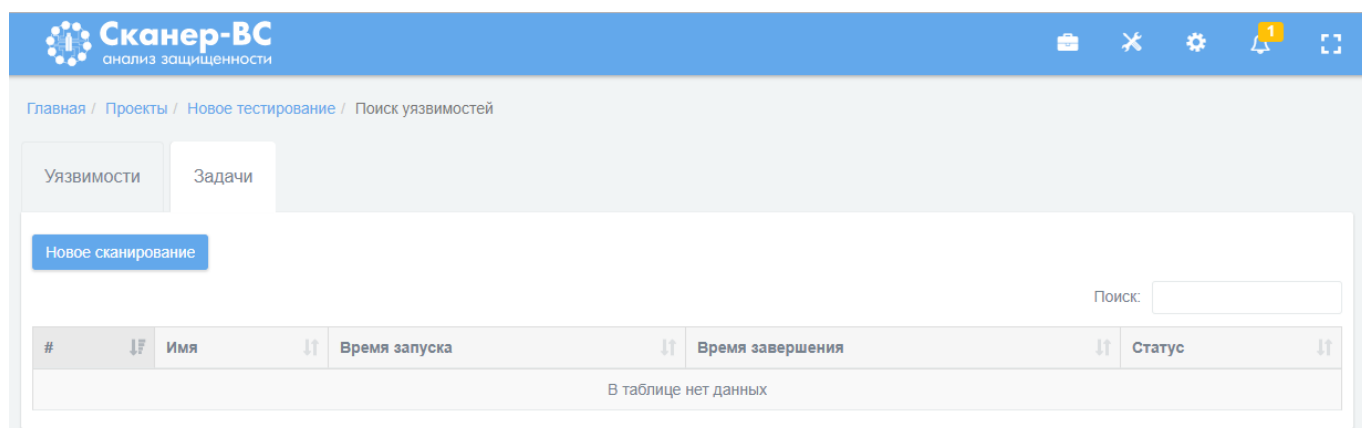


Рисунок 16 — Вкладка «Задачи»

2.3.3. Поиск уязвимостей

Настройки, необходимые для запуска поиска уязвимостей, находятся на вкладке «Базовые» (Рисунок 17), где пользователь задает цели поиска уязвимостей (IP-адреса проверяемых компьютеров, сетей или подсетей) и выбирает политику сканирования (набор правил сканирования): базовую (быструю, сканирование веб-сервисов, либо полное сканирование) или пользовательскую, настраиваемую пользователем. Создание пользовательской политики описано в документе «Программный комплекс «Средство анализа защищенности «Сканер-ВС» Руководство оператора».

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 нажмите кнопку **Импорт целей из активов**, 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 **Импорт целей из файла** и в открывшемся окне выберите файл с импортируемым списком, далее нажмите кнопку **Открыть**. Перечень целей сканирования появится в поле «Цели».

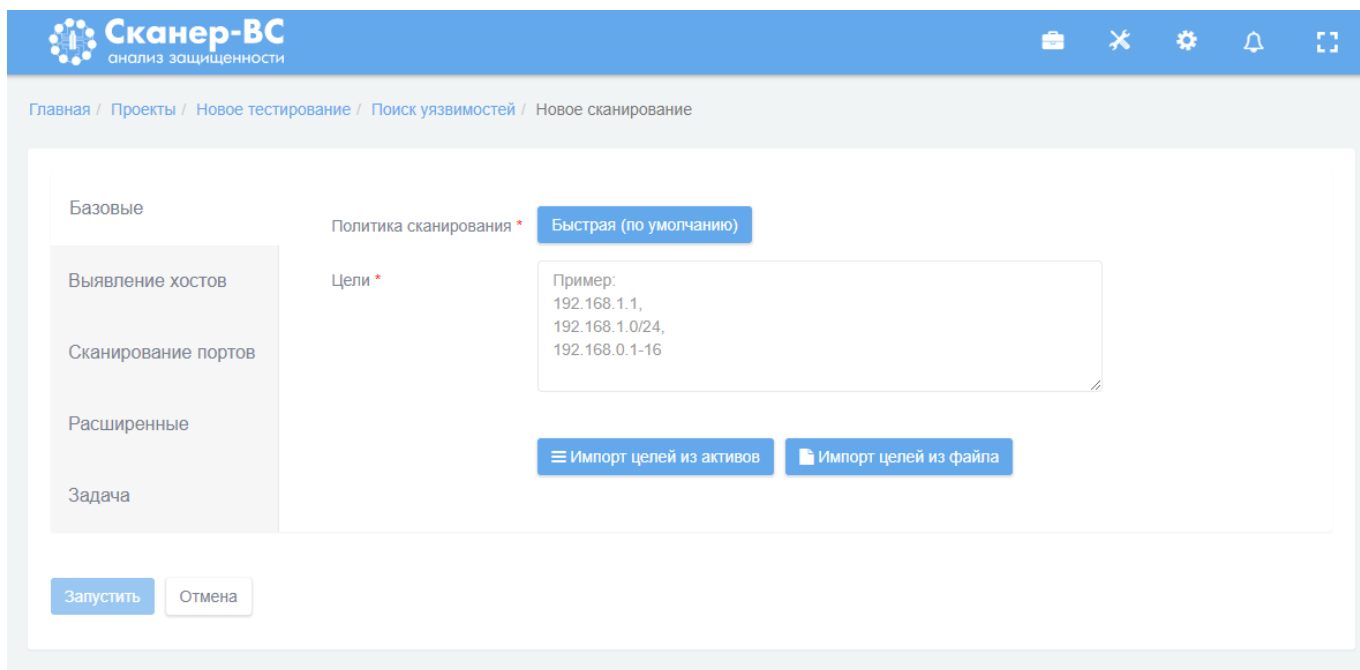


Рисунок 17 — Основные настройки сканирования

Далее выберите политику сканирования. По умолчанию установлена **Быстрая**. Если необходимо сменить политику сканирования, нажмите на кнопку **Быстрая (по умолчанию)** и выберите одну из базовых политик или создайте свою (Рисунок 18).

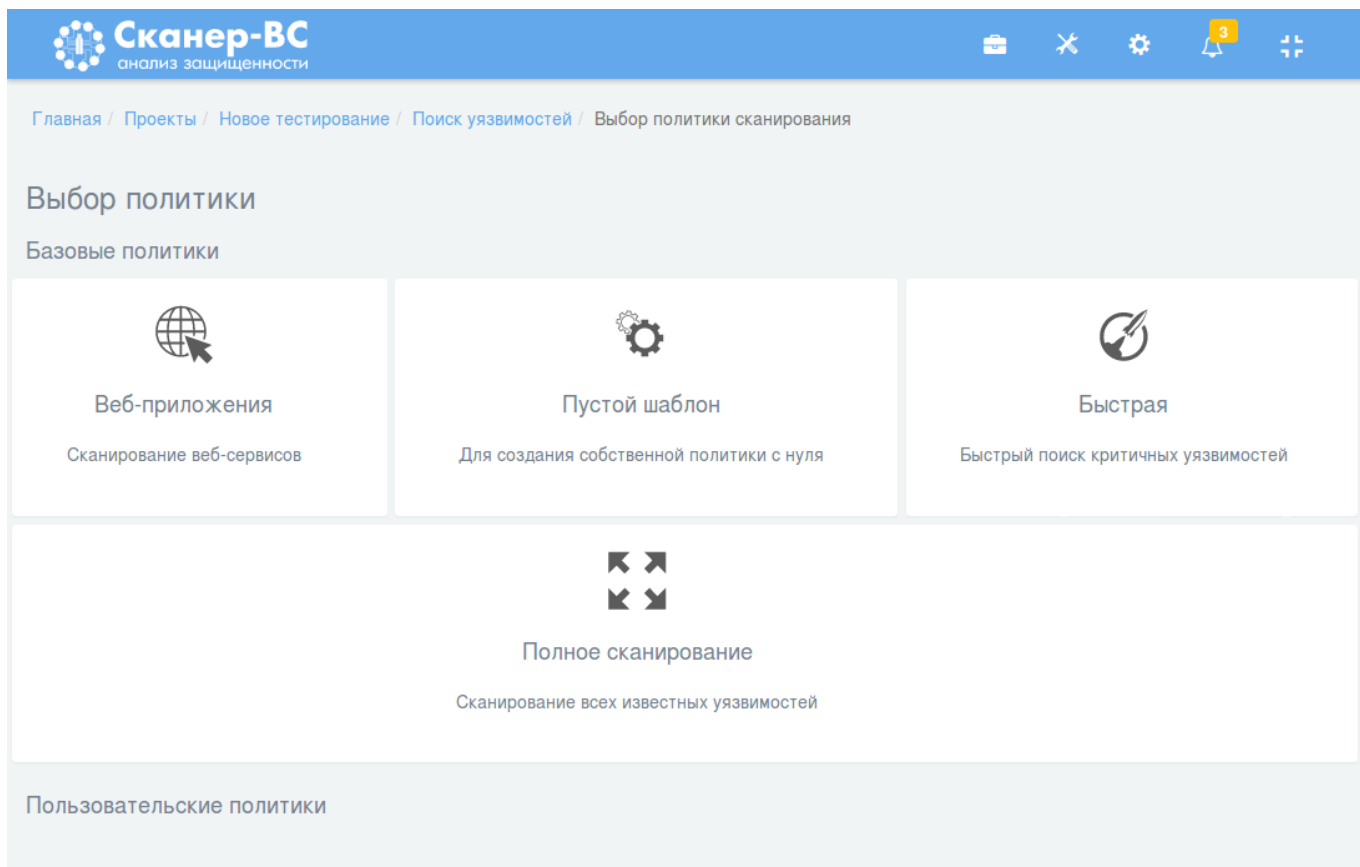


Рисунок 18 — Выбор политики сканирования

На вкладке «Задача» (Рисунок 19) пользователь задает имя и описание в соответствующие пустые поля. Если поля оставить пустыми, они будут заполнены автоматически, исходя из указанных настроек сканирования.

The screenshot shows the 'Сканер-ВС' (Scanner-ВС) web application. The header is blue with the application logo and name. Below the header is a breadcrumb trail: Главная / Проекты / Новое тестирование / Поиск уязвимостей / Новое сканирование. On the left is a sidebar with navigation options: Базовые, Выявление хостов, Сканирование портов, Расширенные, and Задача. The 'Задача' tab is selected. The main form area contains two input fields: 'Имя' (Name) with the placeholder 'Введите имя' and 'Описание' (Description) with the placeholder 'Введите описание'. At the bottom of the form are two buttons: 'Запустить' (Run) and 'Отмена' (Cancel).

Рисунок 19 — Имя и описание сканирования

Дополнительные настройки сканирования расположены на вкладках «Выявление хостов», «Сканирование портов», «Расширенные» (Рисунок 19) и используются пользователем при необходимости.

Для начала процесса сканирования нажмите кнопку **Запустить** (Рисунок 19).

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 20). Желтый цвет индикатора означает, что в текущий момент сканирование выполняется, зеленый — сканирование успешно завершено, красный — процесс сканирования завершен с ошибкой.

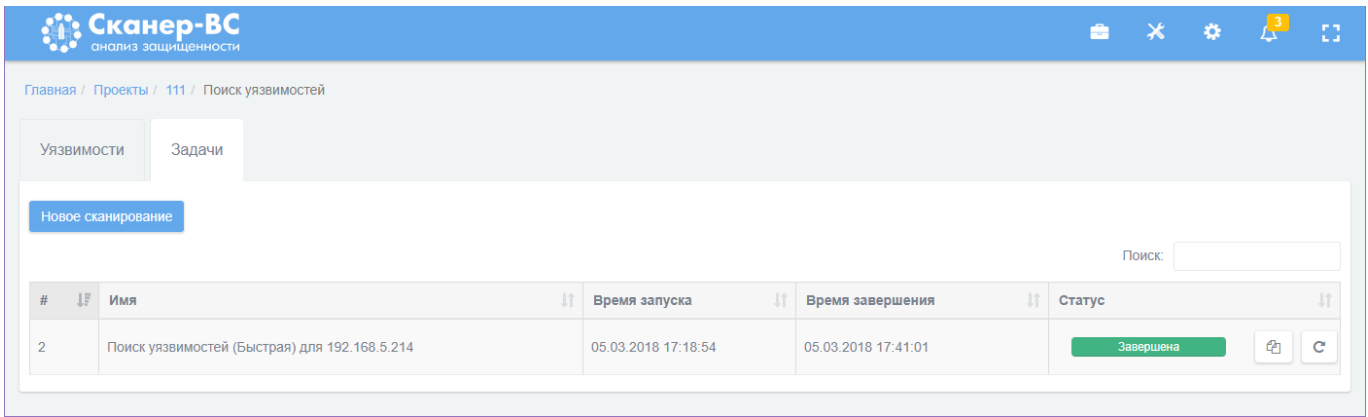


Рисунок 20 — Результат сканирования

После завершения сканирования на вкладке «Уязвимости» появятся данные об обнаруженных уязвимостях, которые будут сгруппированы в таблицу (Рисунок 21).

Сканер-ВС анализ защищенности						
Главная / Проекты / Новое тестирование / Поиск уязвимостей						
Уязвимости Задачи						
Поиск:						
#	Хост	Порт	Описание	CVE	Уровень риска	
1	192.168.5.134	135	Службы распределенной вычислительной среды / удаленных процедур (DCE / RPC) или MSRPC на удаленном хосте могут быть перечислены путем подключения к порту 135 и выполнения соответствующих запросов.		Средний	
2	192.168.5.134	445	Этот скрипт обнаруживает, что порт 445 и 139 открыты и если они запускают сервер CIFS / SMB.		Заметка	
3	192.168.5.134	0	Этот NVT обобщает техническую информацию о сканируемом хосте собранных во время сканирования.		Заметка	

Рисунок 21 — 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 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 нажмите кнопку **Задачи** в секторе «Эксплуатация» (Рисунок 6).

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 (с включенной функцией **Определять версии сетевых протоколов**) и поиск уязвимостей, то нажмите кнопку **Автоматический поиск эксплойтов**, в ином случае нажмите кнопку **Ручной поиск эксплойтов** (Рисунок 22).

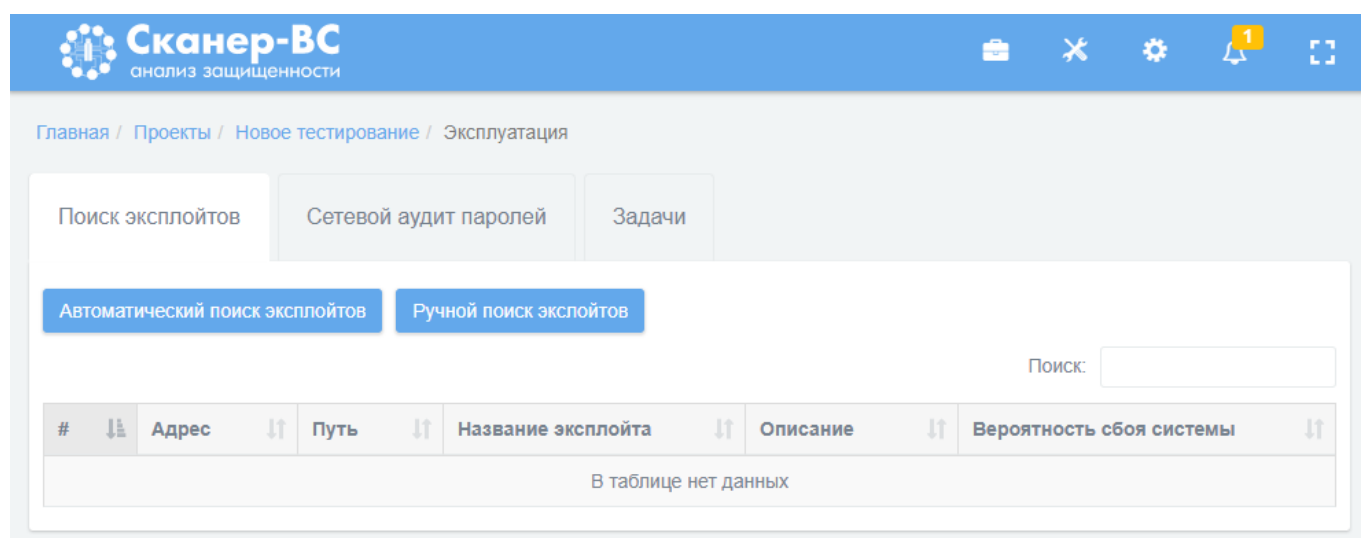


Рисунок 22 — Вкладка «Поиск эксплойтов»

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

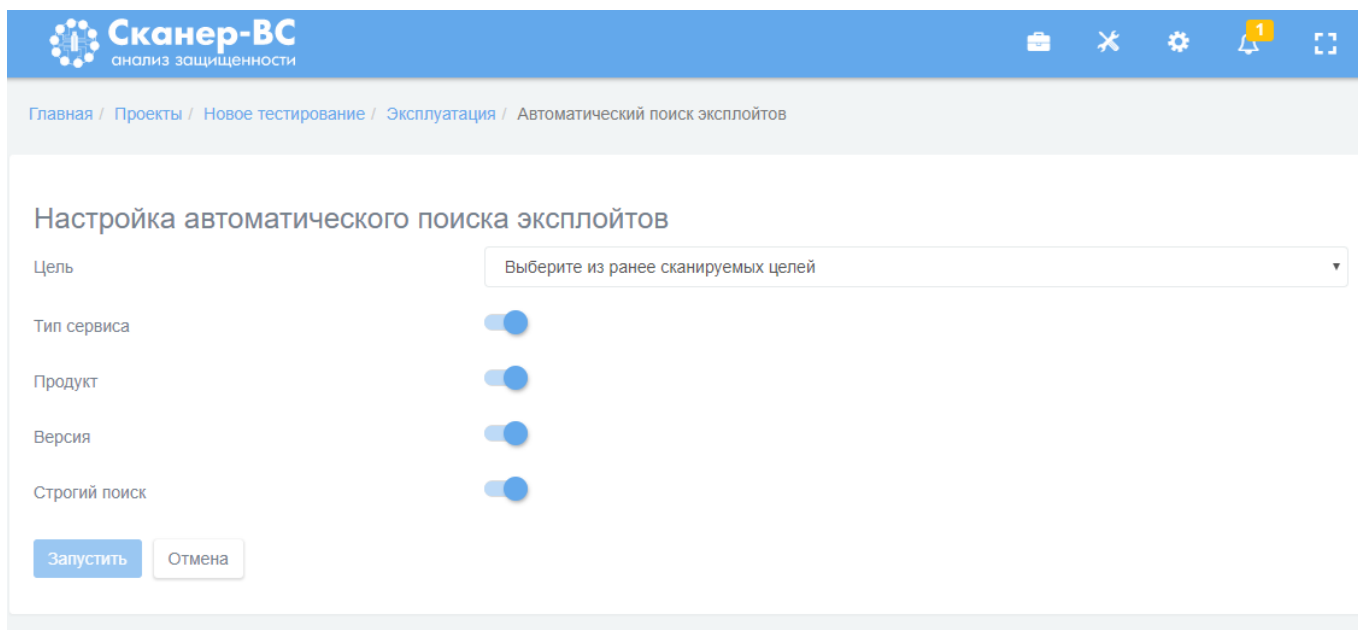


Рисунок 23 — Интерфейс настройки и запуска автоматического поиска эксплойтов

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 кнопку **Запустить**.

После нажатия кнопки **Ручной поиск эксплойтов** откроется окно «Настройка ручного поиска эксплойтов» (Рисунок 24).

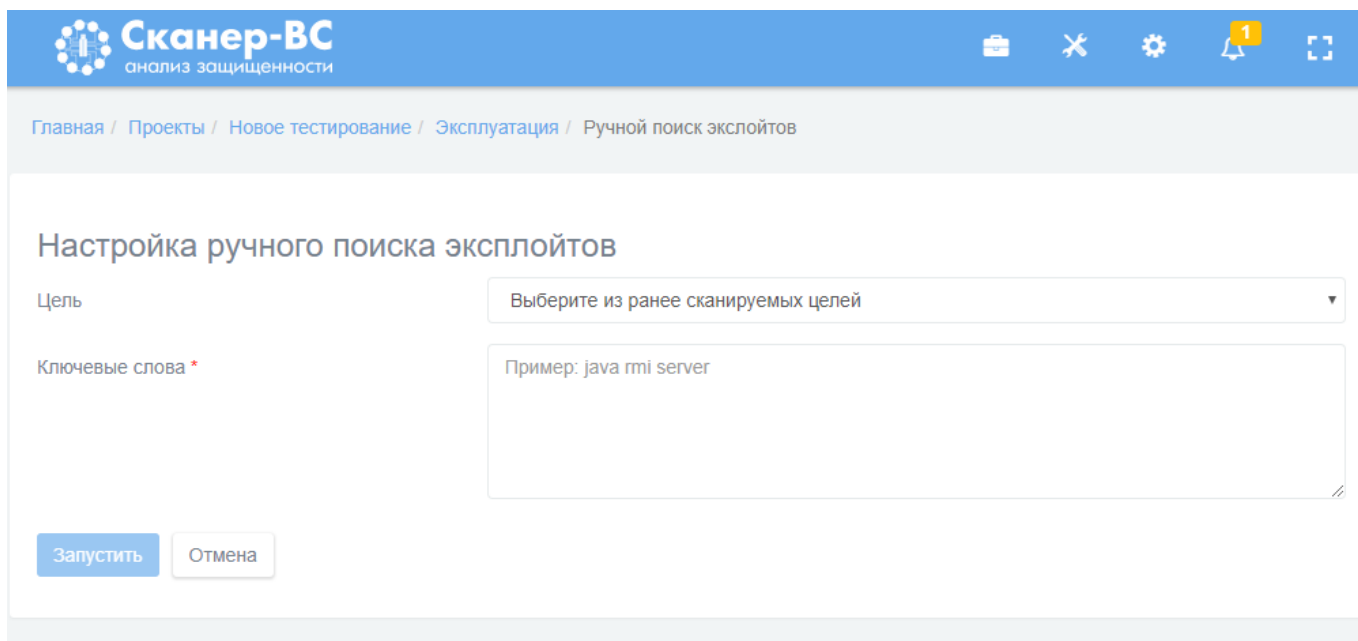


Рисунок 24 — Интерфейс настройки и запуска ручного поиска эксплойтов

В поле «Цель» укажите 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 кнопку **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 25).

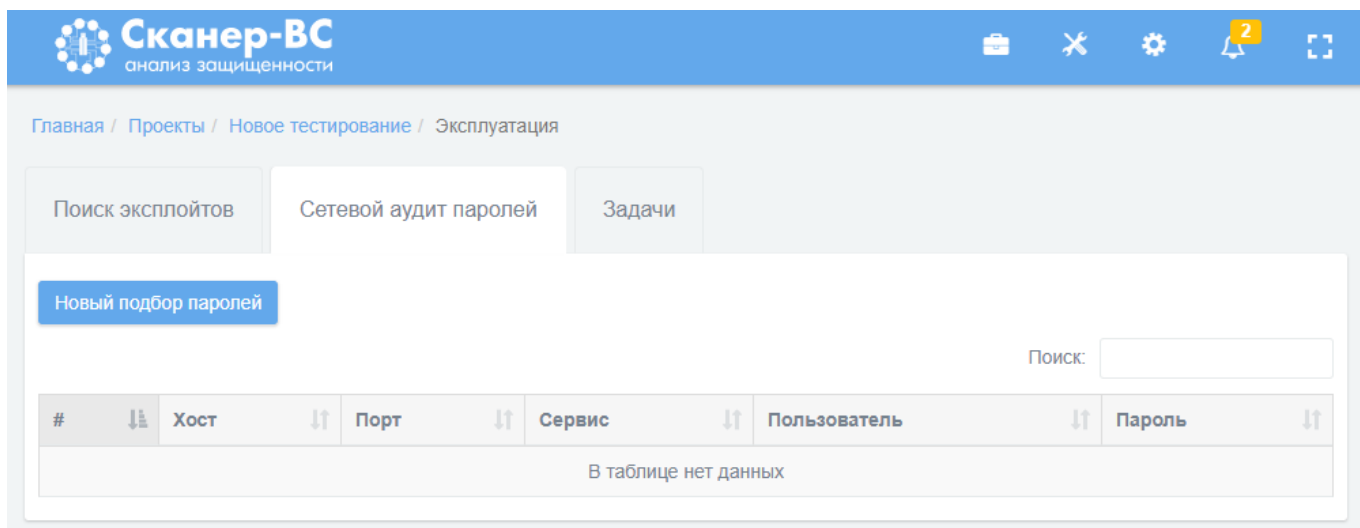


Рисунок 25 — Интерфейс запуска подбора паролей

На вкладке «Базовые» расположены базовые параметры сетевого аудита паролей (Рисунок 26): 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 из активов нажмите кнопку **Импорт целей из активов**, 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 **Импорт целей из файла** и в открывшемся окне выберите файл импортируемого списка. Нажмите кнопку **Открыть**. Перечень целей появится в поле «Цели».

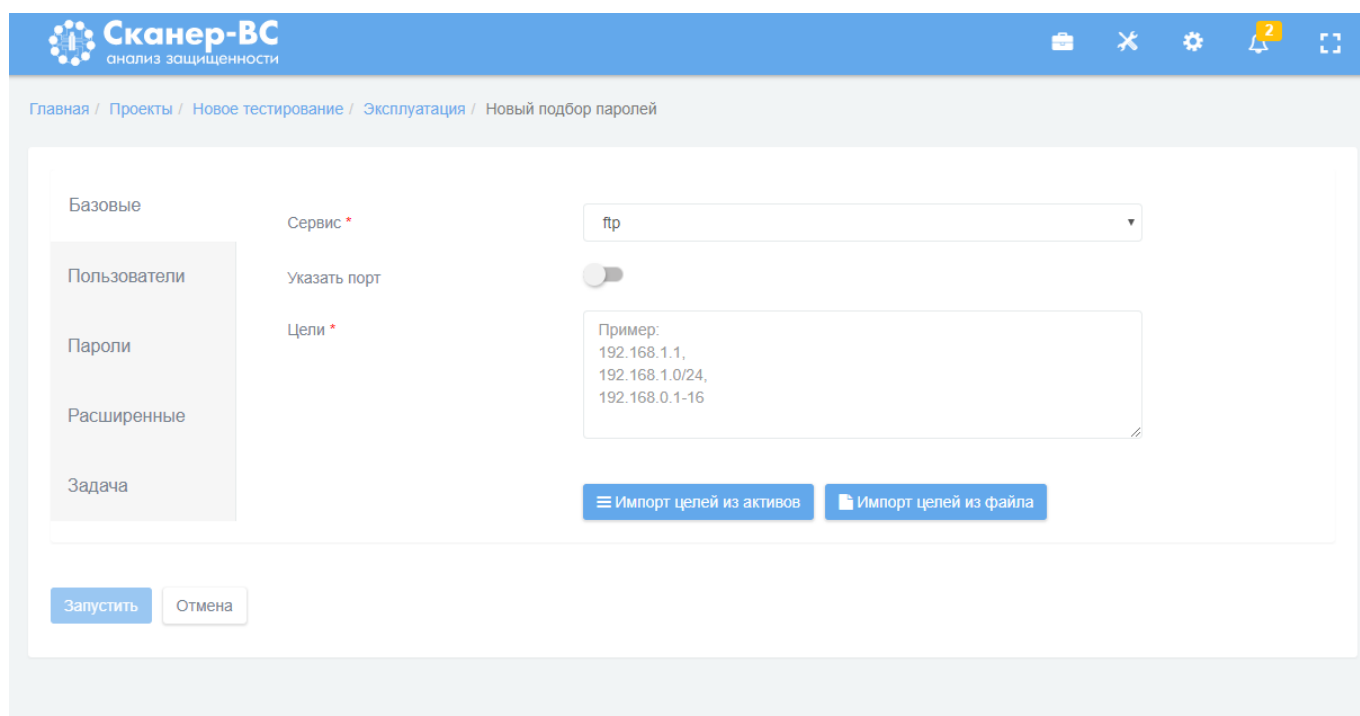


Рисунок 26 — Основные настройки подбора паролей

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

На вкладке «Пользователи» необходимо указать идентификаторы (имена, логин) пользователей проверяемых IP-адресов (Рисунок 27). 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.

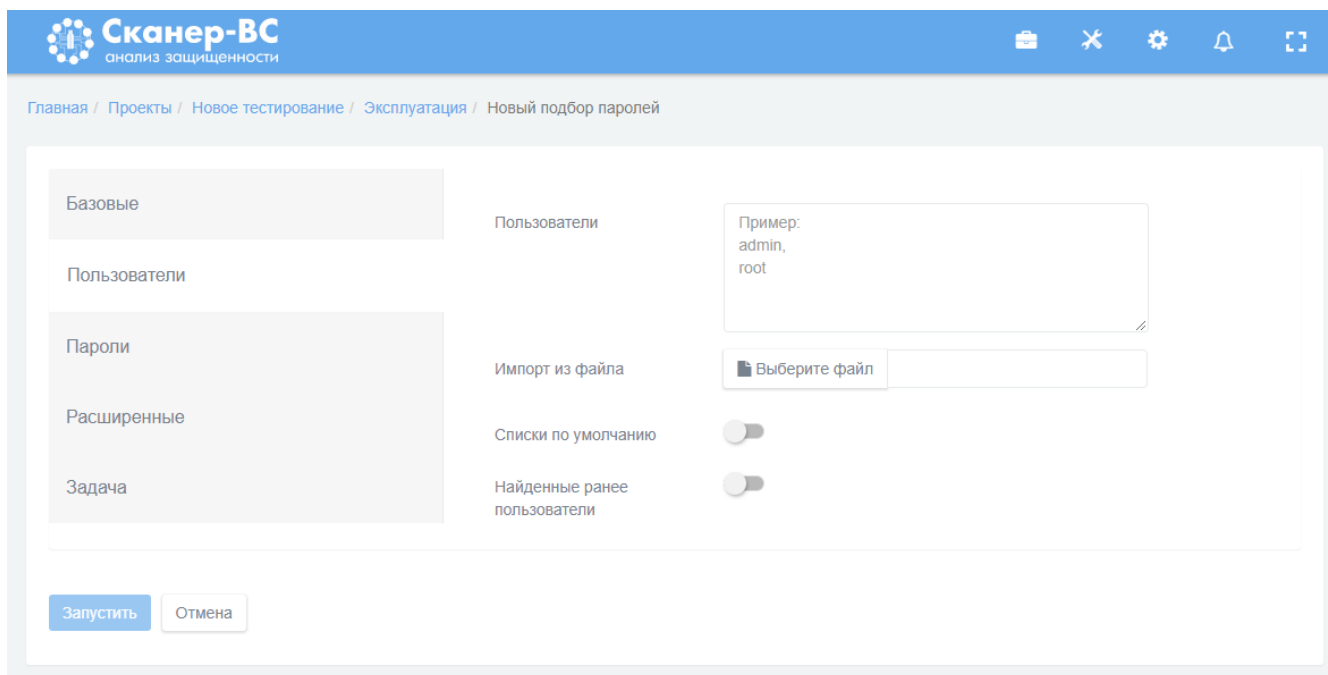


Рисунок 27 — Настройка подбора паролей, вкладка «Пользователи»

На вкладке «Пароли» в поле «Пароли» необходимо указать комбинации букв и цифр, которые будут использоваться в качестве аутентификационной информации (Рисунок 28). 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.

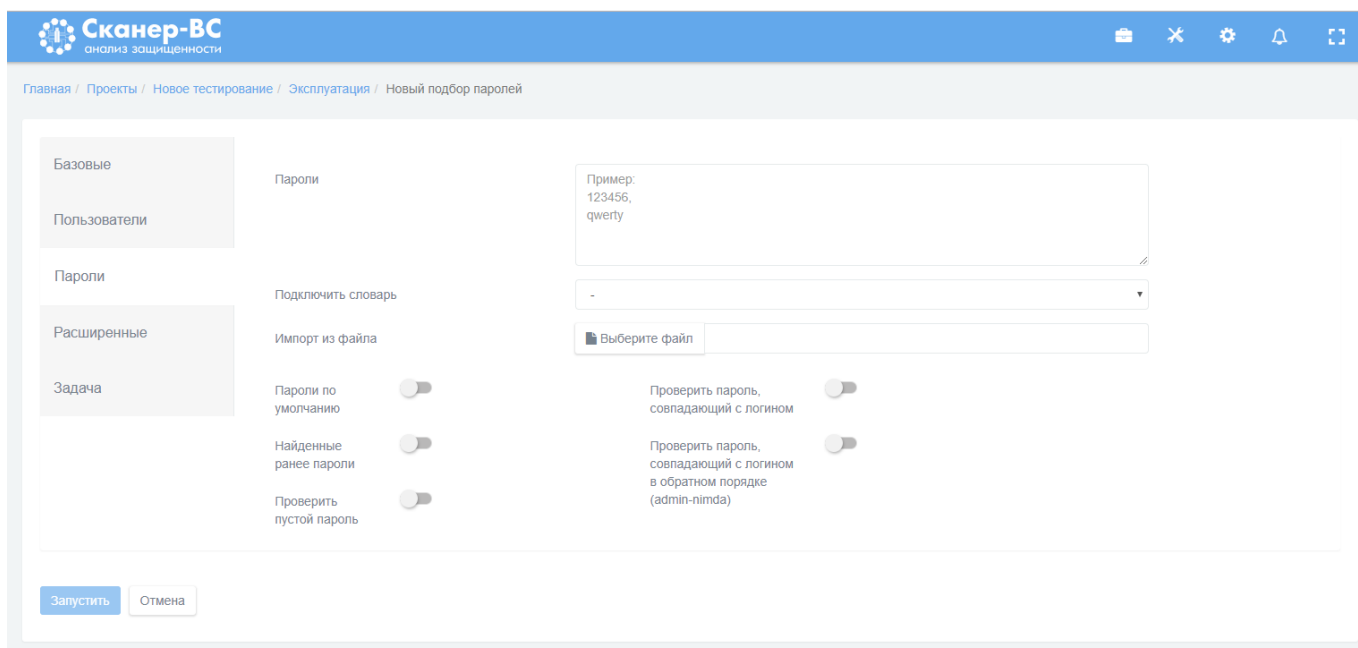


Рисунок 28 — Настройка подбора паролей

Для завершения подбора паролей при первой подобранной паре имя - пароль перейдите на вкладку «Расширенные» и активируйте «Закончить подбор при первом положительном результате» (Рисунок 29). При необходимости задайте параметр «Время ожидания между соединениями».

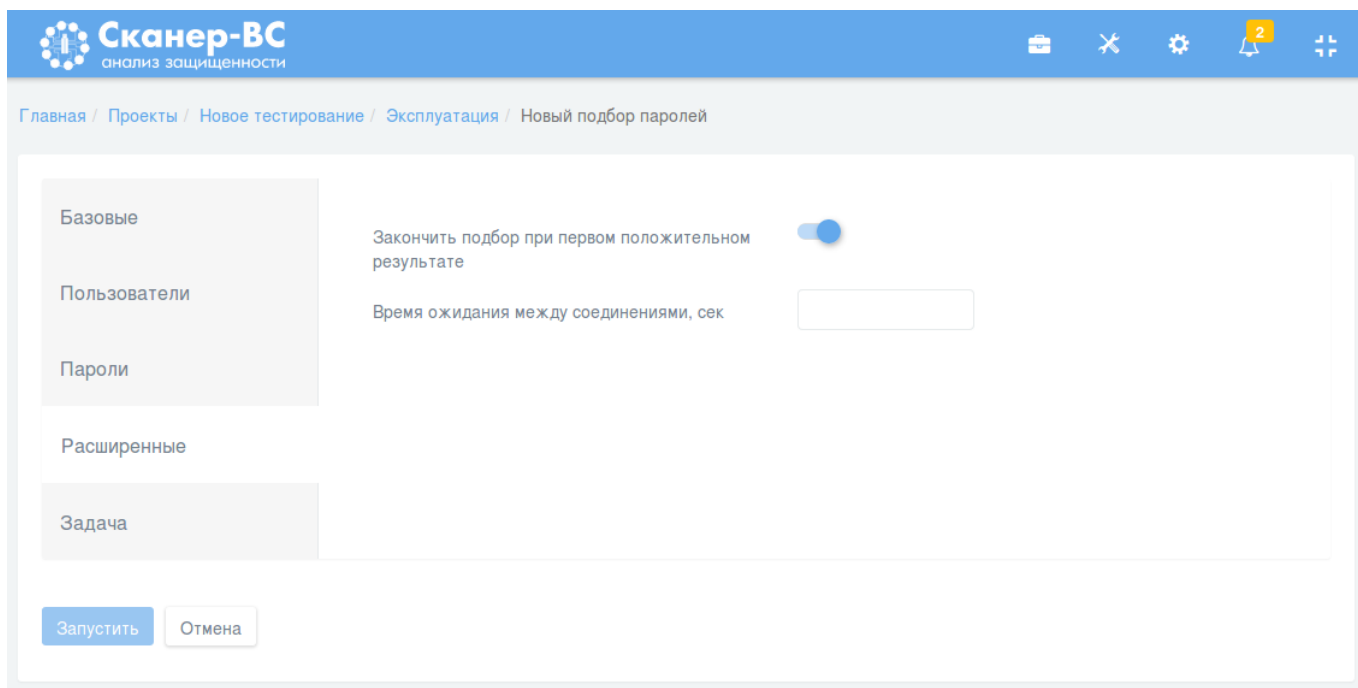


Рисунок 29 — Расширенные настройки подбора паролей

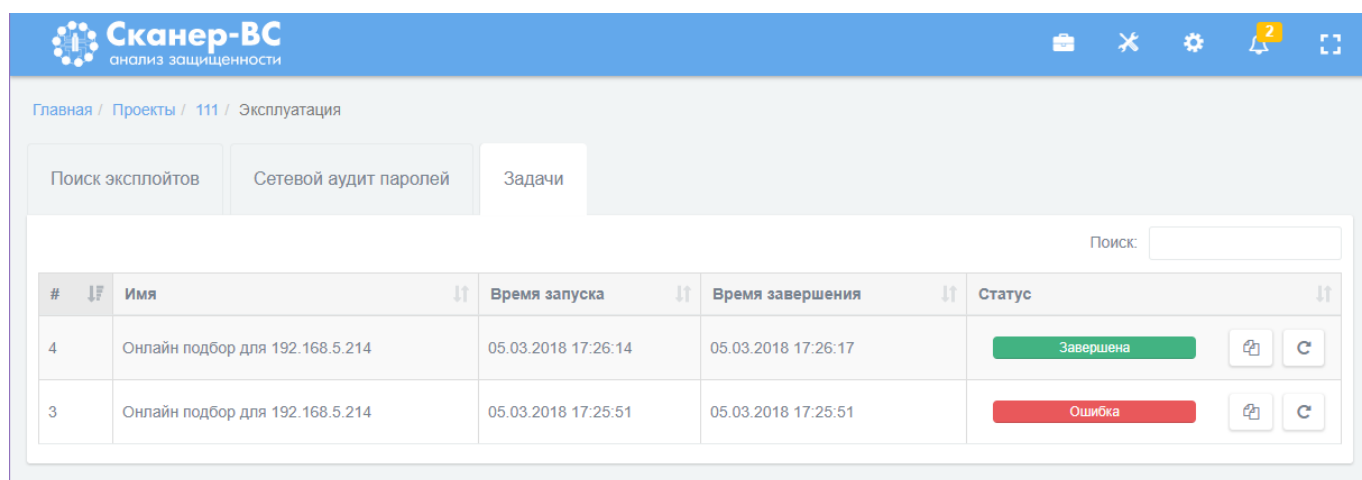
На вкладке «Задача» пользователь задает название и описание для задачи поиска в соответствующие пустые поля. Если поля оставить

пустыми, они будут заполнены автоматически, исходя из указанных настроек тестирования.

Нажмите кнопку **Запустить** (Рисунок 29).

2.4.5. Завершение работы

После нажатия кнопки **Запустить** на вкладке «Задачи» в таблице появится номер задачи, имя и индикатор статуса (Рисунок 30). Желтый цвет индикатора означает процесс сканирования, зеленый — завершение сканирования, красный — процесс сканирования выполнен с ошибкой.



#	Имя	Время запуска	Время завершения	Статус
4	Онлайн подбор для 192.168.5.214	05.03.2018 17:26:14	05.03.2018 17:26:17	Завершена
3	Онлайн подбор для 192.168.5.214	05.03.2018 17:25:51	05.03.2018 17:25:51	Ошибка

Рисунок 30 — Таблица задач

После завершения сканирования на вкладке «Сетевой аудит паролей» появятся данные о подобранных паролях (Рисунок 31), а на вкладке «Эксплойты» таблица с найденными эксплойтами (Рисунок 32).

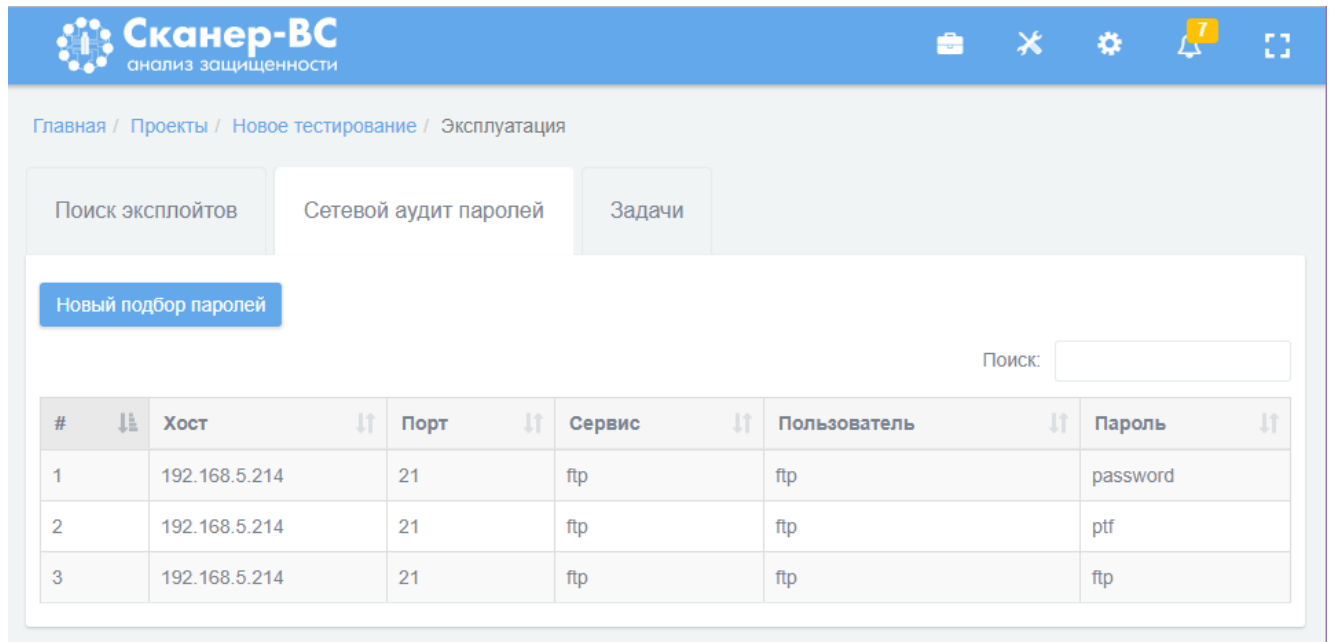


Рисунок 31 — Информация о подобранных паролях

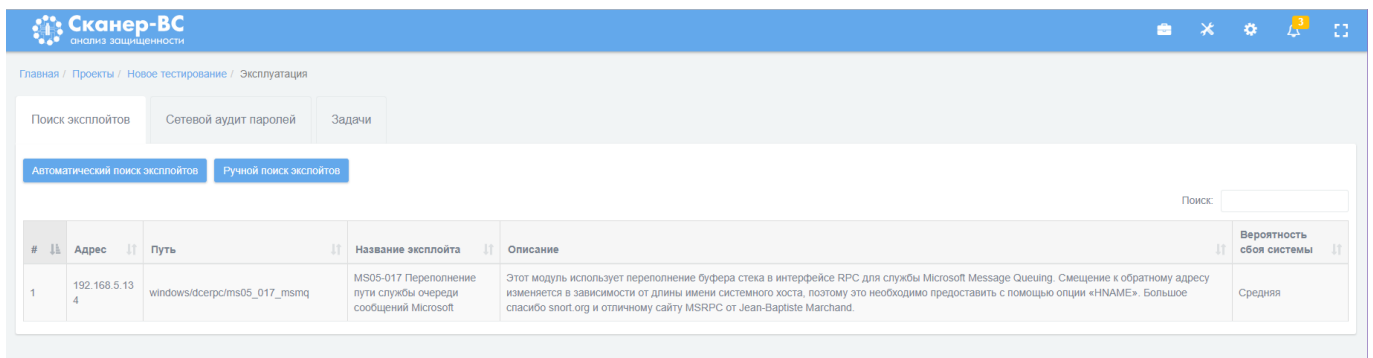


Рисунок 32 — Информация о найденных эксплойтах

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 33), который можно активировать с помощью кнопки **Настройки** (активирован по умолчанию).

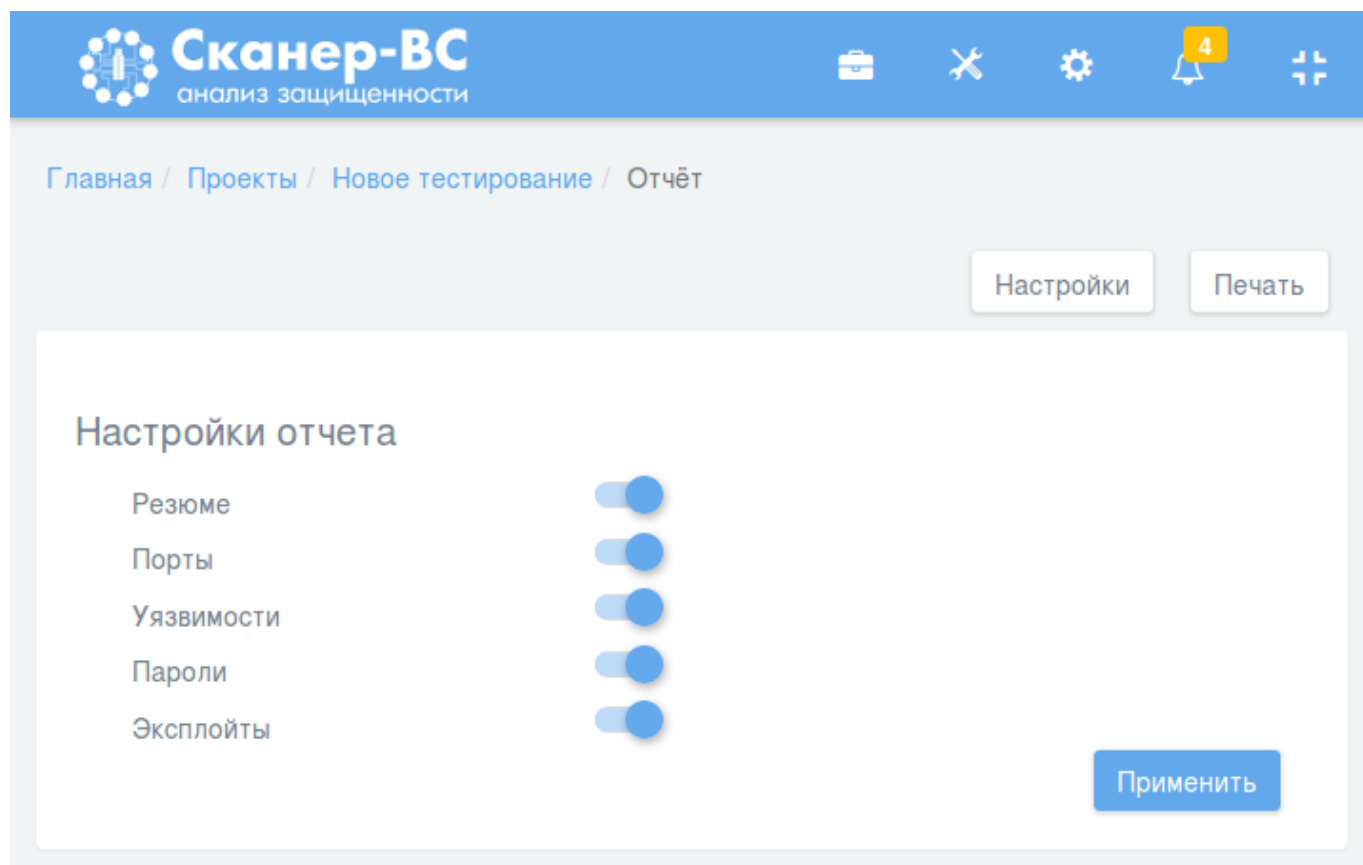


Рисунок 33 — Конструктор отчетов

Полный отчет состоит из следующих разделов: «Резюме», «Порты», «Уязвимости», «Подобранные пароли» и «Подобранные эксплойты». Раздел «Резюме» - краткая информация по всем этапам тестирования в виде диаграмм и общей таблицы распределения уязвимостей по хостам (Рисунок 34).

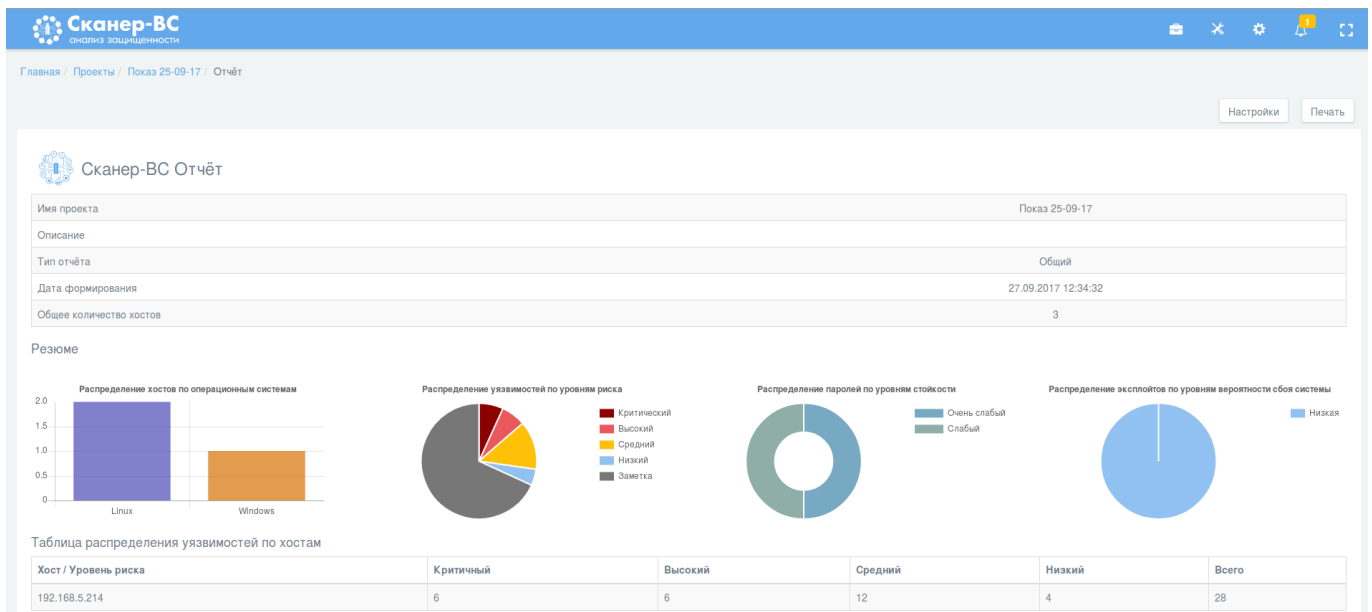


Рисунок 34 — Фрагмент отчета «Сканер-ВС»

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