

Сканер-ВС

анализ защищенности

Руководство пользователя

АННОТАЦИЯ

В документе содержатся сведения о назначении, функциях и особенностях эксплуатации программного комплекса «Средство анализа защищенности «Сканер-ВС» (далее – ПК «Сканер-ВС», программный комплекс).

СОДЕРЖАНИЕ

| | |
|--|----|
| АННОТАЦИЯ | 2 |
| СОДЕРЖАНИЕ | 3 |
| 1. НАЗНАЧЕНИЕ ПРОГРАММЫ..... | 6 |
| 1.1. НАЗНАЧЕНИЕ ПРОГРАММЫ | 6 |
| 1.2. ОСНОВНЫЕ КОМПОНЕНТЫ..... | 6 |
| 2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ..... | 8 |
| 3. ВЫПОЛНЕНИЕ ПРОГРАММЫ | 9 |
| 3.1. ПОДГОТОВИТЕЛЬНЫЙ ЭТАП..... | 9 |
| 3.1.1. Установка программы..... | 9 |
| 3.1.2. Запуск программы ПК «Сканер-ВС». Настройка BIOS для загрузки ПК «Сканер-ВС» | 9 |
| 3.1.3. BIOS типа AMI | 10 |
| 3.1.4. BIOS типа AWARD..... | 11 |
| 3.1.5. Загрузка ПК «Сканер-ВС»..... | 13 |
| 3.2. РАБОТА С ПРОЕКТАМИ | 14 |
| 3.3. ПОИСК ЦЕЛЕЙ | 22 |
| 3.3.1. Краткое описание | 22 |
| 3.3.2. Запуск | 23 |
| 3.3.3. Поиск целей | 23 |
| 3.3.4. Завершение работы | 25 |
| 3.4. ПОИСК УЯЗВИМОСТЕЙ | 27 |
| 3.4.1. Краткое описание | 27 |
| 3.4.2. Начало работы | 27 |
| 3.4.3. Поиск уязвимостей..... | 28 |
| 3.4.4. Завершение работы | 31 |
| 3.5. ЭКСПЛУАТАЦИЯ | 32 |
| 3.5.1. Краткое описание | 32 |
| 3.5.2. Запуск | 33 |
| 3.5.3. Поиск эксплойтов..... | 33 |
| 3.5.4. Сетевой аудит паролей | 34 |
| 3.5.5. Завершение работы | 38 |
| 3.6. ОТЧЕТЫ..... | 39 |
| 3.6.1. Краткое описание | 39 |

| | |
|--|----|
| 3.6.2. Настройки отчета | 39 |
| 3.7. РАБОТА С ИНСТРУМЕНТАМИ..... | 40 |
| 3.7.1. Средство аудита ОС Astra Linux | 40 |
| 3.7.1.1. Запуск модуля | 40 |
| 3.7.1.2. Работа с модулем | 41 |
| 3.7.1.3. Завершение работы с модулем | 49 |
| 3.7.2. Средство локального аудита паролей | 49 |
| 3.7.2.1. Запуск модуля | 49 |
| 3.7.2.2. Работа с модулем | 50 |
| 3.7.2.3. Завершение работы с модулем | 53 |
| 3.7.3. Средство поиска остаточной информации | 53 |
| 3.7.3.1. Запуск модуля | 54 |
| 3.7.3.2. Работа с модулем | 54 |
| 3.7.3.3. Завершение работы с модулем | 57 |
| 3.7.4. Средство аудита обновлений ОС Windows | 57 |
| 3.7.4.1. Запуск модуля | 57 |
| 3.7.4.2. Работа с модулем | 58 |
| 3.7.4.3. Завершение работы с модулем | 59 |
| 3.7.5. Системный аудитор..... | 59 |
| 3.7.5.1. Запуск модуля | 59 |
| 3.7.5.2. Работа с модулем | 60 |
| 3.7.5.3. Работа с отчетами системного аудита | 63 |
| 3.7.5.4. Завершение работы с модулем | 66 |
| 3.7.6. Средство гарантированного уничтожения информации..... | 66 |
| 3.7.6.1. Запуск модуля | 66 |
| 3.7.6.2. Работа с модулем | 69 |
| 3.7.6.3. Завершение работы с модулем | 72 |
| 3.7.7. Средство аудита беспроводных сетей..... | 72 |
| 3.7.7.1. Запуск средства аудита беспроводных сетей..... | 72 |
| 3.7.7.2. Прослушивание сети, использующей WEP шифрование | 73 |
| 3.7.7.3. Прослушивание сети, использующей WPA шифрование..... | 76 |
| 3.7.7.4. Выход из средства аудита беспроводных сетей | 77 |
| 3.7.8. Сетевой анализатор..... | 77 |
| 3.7.8.1. Запуск модуля | 77 |
| 3.7.8.2. Начало работы с модулем | 78 |

| | |
|--|-----|
| 3.7.8.3. Работа с модулем в обычной сети | 90 |
| 3.7.8.4. Атаки типа MITM | 90 |
| 3.7.8.5. Работа с модулем в коммутируемой сети..... | 93 |
| 3.7.8.6. Завершение работы с модулем | 94 |
| 3.7.9. Средство контрольного суммирования..... | 94 |
| 3.7.9.1. Запуск модуля | 94 |
| 3.7.9.2. Работа с модулем | 95 |
| 3.7.9.3. Контрольное суммирование | 95 |
| 3.7.9.4. Завершение работы с модулем | 101 |
| 3.8. ДОПОЛНИТЕЛЬНЫЕ МОДУЛИ | 101 |
| 3.8.1. Менеджер сетевых подключений «Wicd Network Manager» | 101 |
| 3.8.2. Менеджер обновлений..... | 104 |
| 3.9. ЗАВЕРШЕНИЕ РАБОТЫ С ПК «СКАНЕР-ВС» | 106 |
| ПРИЛОЖЕНИЕ 1. СПИСОК АДАПТЕРОВ | 108 |

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение программы

ПК «Сканер-ВС» предназначен для поиска уязвимостей сетей, исследования структуры сетевых сервисов, сетевого и локального аудита паролей, поиска остаточной информации и анализа сетевого трафика.

ПК «Сканер-ВС» предназначен для автоматизированного анализа (контроля) защищенности информации, обрабатываемой в информационных системах (далее – ИС) и не содержащей сведений, составляющих государственную тайну.

ПК «Сканер-ВС» реализует следующие функции:

- инвентаризация ресурсов ИС;
- выявление и анализ уязвимостей ИС;
- обеспечение локального и сетевого аудита стойкости паролей;
- обеспечение перехвата и анализа сетевого трафика;
- обеспечение аудита программной и аппаратной конфигураций локальной системы;
- обеспечение контроля уничтожения информации на различных носителях;
- обеспечение поиска остаточной информации на машинных носителях;
- обеспечение контроля целостности информации;
- обеспечение контроля использования беспроводных сетей в ИС;
- контроль установки обновлений операционных систем (далее – ОС) семейства Microsoft

Windows.

1.2. Основные компоненты

ПК «Сканер-ВС» состоит из следующих основных модулей:

- поиск целей;
- поиск уязвимостей;
- средство сетевого аудита паролей;
- поиск эксплойтов;
- средство аудита ОС Astra Linux;
- средство локального аудита паролей;
- сетевой анализатор;
- системный аудитор;
- средство поиска остаточной информации;
- средство аудита беспроводных сетей;
- средство гарантированного уничтожения информации;
- средство контрольного суммирования;

– средство аудита обновлений ОС Windows.

1.2.1. Поиск целей – средство анализа локальной сети с целью инвентаризации ресурсов и выявления объектов тестирования.

1.2.2. Поиск уязвимостей – средство поиска уязвимостей программного обеспечения (далее – ПО), установленного на рабочей станции.

1.2.3. Средство сетевого аудита паролей предназначено для удаленного поиска и выявления паролей, содержащих легко подбираемые символьные комбинации.

1.2.4. Поиск эксплойтов – средство поиска возможностей несанкционированного использования ресурсов рабочей станции.

1.2.5. Средство аудита ОС Astra Linux предназначено для аудита настроек комплекса средств защиты ОС специального назначения «Astra Linux Serial Edition» по требованиям безопасности.

1.2.6. Средство локального аудита паролей предназначено для поиска и выявления на локальной рабочей станции неустойчивых к взлому паролей.

1.2.7. Сетевой анализатор предназначен для перехвата, анализа и фильтрации сетевого трафика.

1.2.8. Системный аудитор предназначен для сканирования рабочей станции на предмет определения параметров установленных ОС, системных, коммуникационных и периферийных устройств, в том числе USB-устройств.

1.2.9. Средство поиска остаточной информации предназначено для поиска по ключевым словам остаточной информации на носителях данных (жестких дисках, дискетах, оптических дисках и USB-накопителях).

1.2.10. Средство аудита беспроводных сетей предназначено для обнаружения, сканирования и проведения пассивных и активных атак на подбор паролей в беспроводных сетях с WEP, WPA, WPA-2 шифрованием.

1.2.11. Средство гарантированного уничтожения информации предназначено для удаления информации путем затирания файла случайным набором символов для предотвращения восстановления данных.

1.2.12. Средство контрольного суммирования предназначено для контроля целостности информации.

1.2.13. Средство аудита обновлений ОС Windows предназначено для определения списка неустановленных обновлений ОС семейства Microsoft Windows.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. ПК «Сканер-ВС», устанавливается на рабочие станции, удовлетворяющие рекомендуемым аппаратным и программным требованиям, представленным в таблице 1.

Таблица 1 – Требования к среде функционирования ПК «Сканер-ВС»

| Параметр | Значение |
|--------------------------|---|
| Операционная система | Не предъявляется |
| Процессор | Intel Pentium 4 2,2 ГГц |
| Объем оперативной памяти | 4 Гбайт |
| Привод/порт USB | Привод DVD-ROM/USB 2.0 |
| Видеоадаптер | SVGA видеоадаптер, совместимый со стандартом VESA 2.0 |

2.2. ПК «Сканер-ВС» обеспечивает выполнение функциональных возможностей при реализации потребителем следующих предварительных организационно-распорядительных мер:

- обеспечение сохранности оборудования и физической целостности системных блоков компьютеров;
- обеспечение свободной от вирусов программной среды компьютеров;
- обеспечение контроля изменения прикладной программной среды, исключение ввода в компьютер программных средств без гарантированной проверки;
- обеспечение организационно-технических мер защиты каналов передачи данных ПК «Сканер-ВС», расположенных в пределах контролируемой зоны.

Для защиты каналов передачи данных ПК «Сканер-ВС», в том числе выходящих за пределы контролируемой зоны, должны применяться сертифицированные в установленном порядке методы и средства, устойчивые к пассивному и/или активному прослушиванию сети, или должен быть запрещен удаленный доступ для администрирования ПК «Сканер-ВС» по незащищенным каналам связи.

2.3. Ограничения при применении отсутствуют.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Подготовительный этап

3.1.1. Установка программы

Установка программы не требуется.

3.1.2. Запуск программы ПК «Сканер-ВС». Настройка BIOS для загрузки ПК «Сканер-ВС»

Для успешной загрузки ПК «Сканер-ВС» необходимо установить в BIOS приоритет загрузки компьютера с CD-ROM/USB-накопителя перед загрузкой с жесткого диска.

При загрузке компьютера BIOS выводит результаты тестирования оборудования на экран. В этот момент можно увидеть название клавиши или сочетания клавиш, нажатие которых в этот момент позволит зайти в меню BIOS для дальнейших настроек (Рисунок 1).

Обычно это клавиши Delete или F2, или Alt+F2 (можно попробовать все три варианта).

Дальнейшие инструкции зависят от той версии BIOS, которая установлена на рабочей станции: BIOS типа AMI или BIOS типа Award. Их легко можно различить по внешнему виду интерфейса (Рисунок 1 и Рисунок 2).

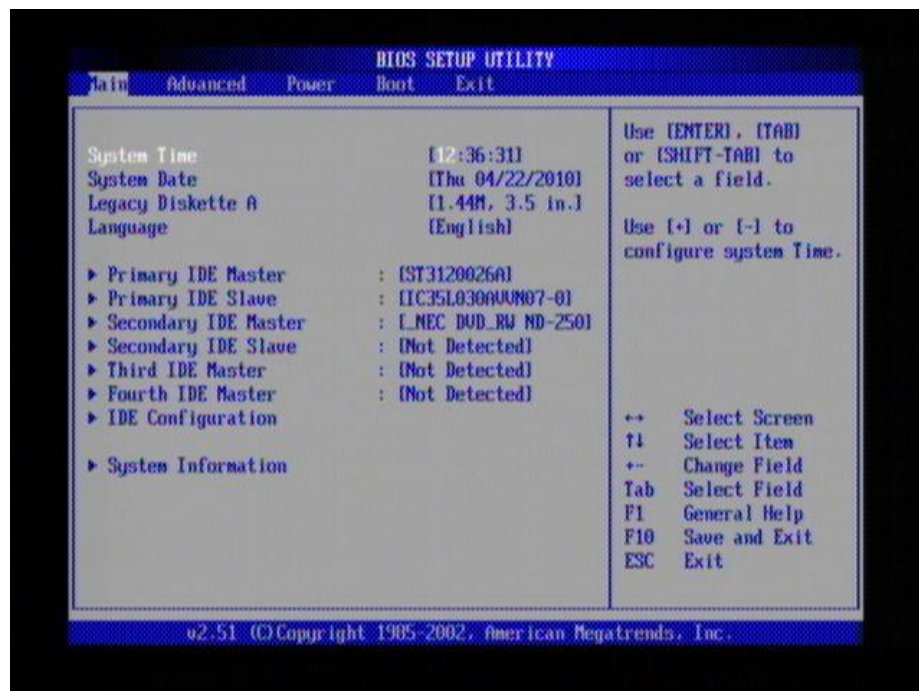


Рисунок 1 —BIOS типа AMI

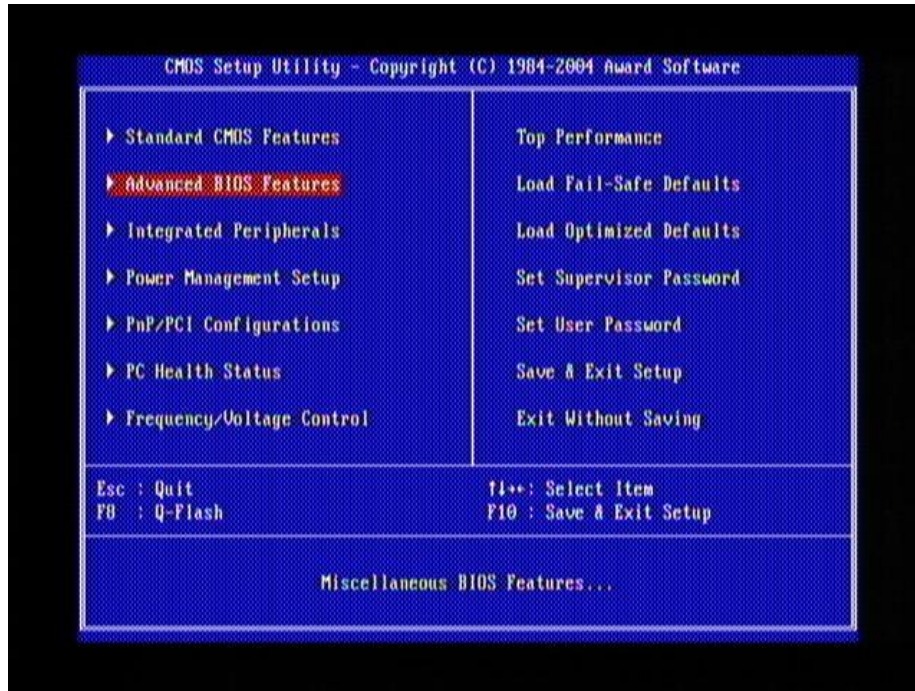


Рисунок 2 — BIOS типа Award

3.1.3. BIOS типа AMI

Если используется BIOS версии AMI, необходимо перейти в раздел **Boot** (Загрузка) (Рисунок 3).

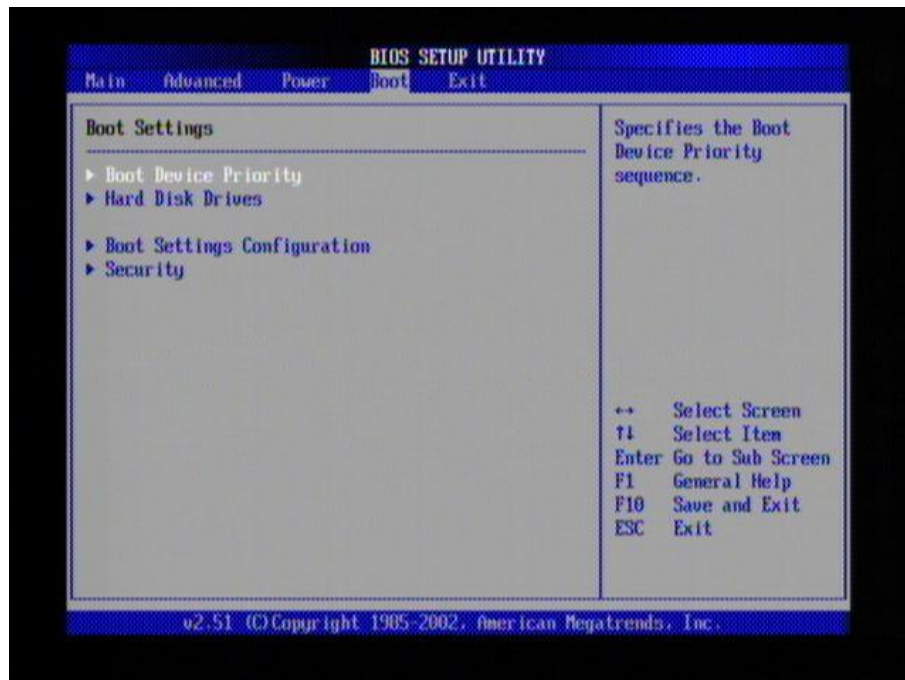


Рисунок 3 — Раздел «Boot»

Далее необходимо в разделе **Boot Device Priority** (Приоритет загрузки устройств) в поле **First Boot Device** (первое загрузочное устройство) указать дисковод, с которого планируется загрузка ПК «Сканер-ВС» (Рисунок 4).

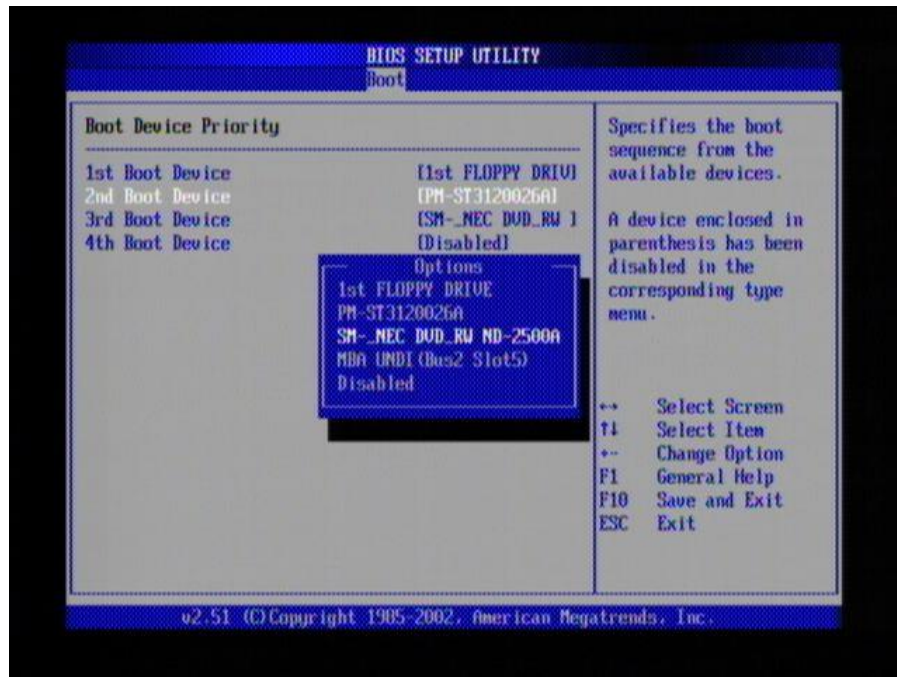


Рисунок 4 – Раздел «Boot Device Priority»

После этого можно перейти в раздел **Exit** (Выход) и выбрать пункт **Exit & Save Changes** (Выйти и сохранить изменения) (Рисунок 5).

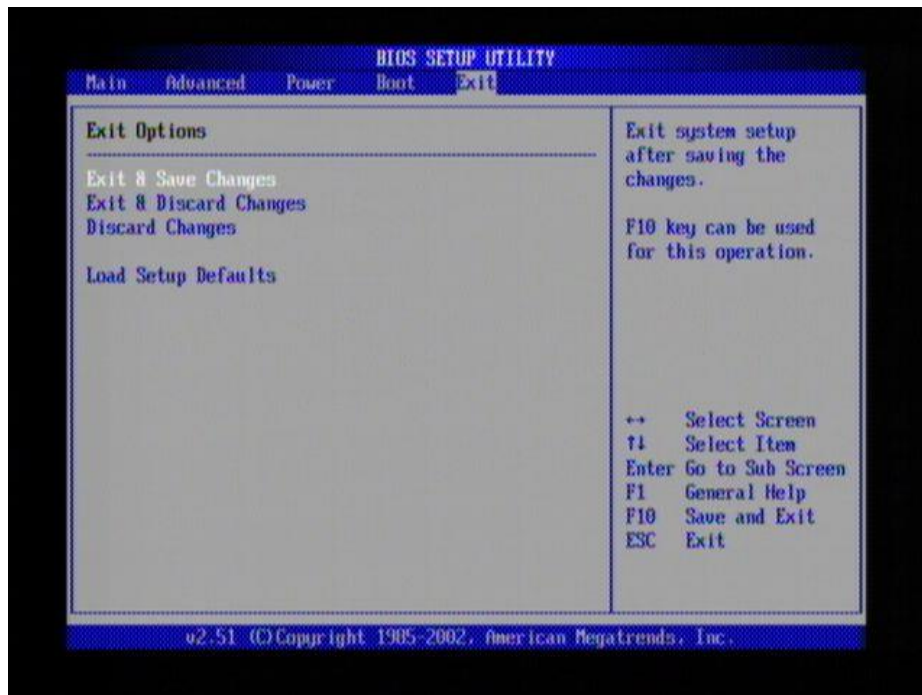


Рисунок 5 — Раздел «Exit»

3.1.4. BIOS типа AWARD

Для настройки необходимо выбрать пункт меню **Advanced BIOS Features** (Рисунок 6), и перейти к редактированию **First boot device**, в котором необходимо указать дисковод, с которого планируется загрузка ПК «Сканер-ВС» (Рисунок 7).

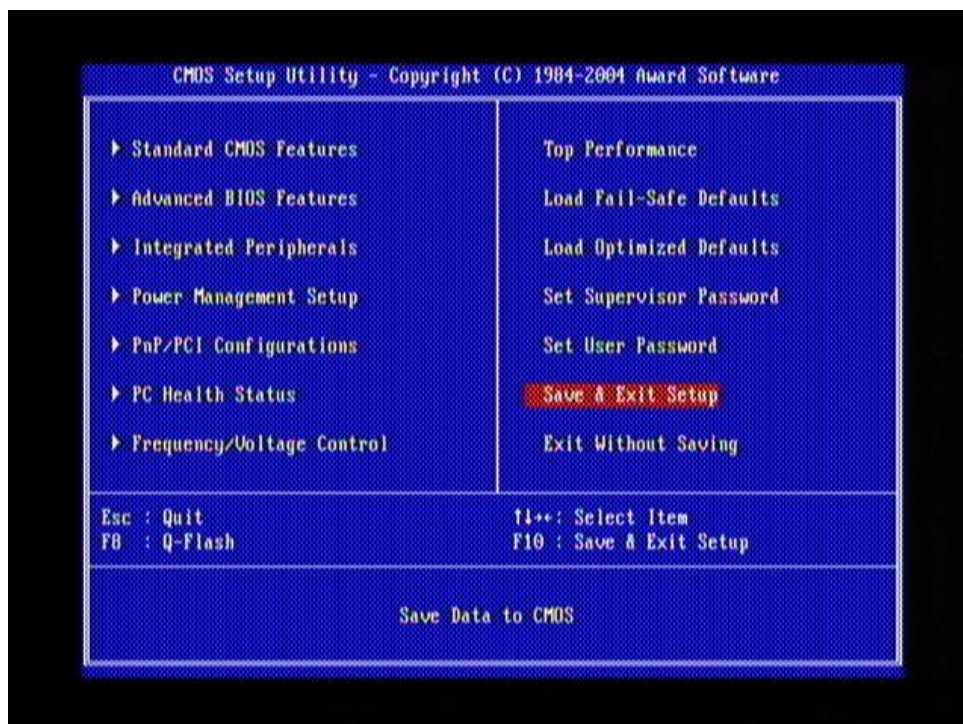


Рисунок 8 — Раздел «Save & Exit Setup»

3.1.5. Загрузка ПК «Сканер-ВС»

Загрузка ПК «Сканер-ВС» осуществляется непосредственно с диска или USB-накопителя по технологии LiveCD/LiveUSB.

Для загрузки ПК «Сканер-ВС» необходимо выполнить следующие действия:

- 1) включить рабочую станцию;
- 2) до загрузки основной ОС подключить носитель с ПО к рабочей станции.

На первом этапе появляется меню загрузчика, в котором представлены варианты загрузки, позволяющие запускать программу в различных режимах совместимости (Рисунок 9).

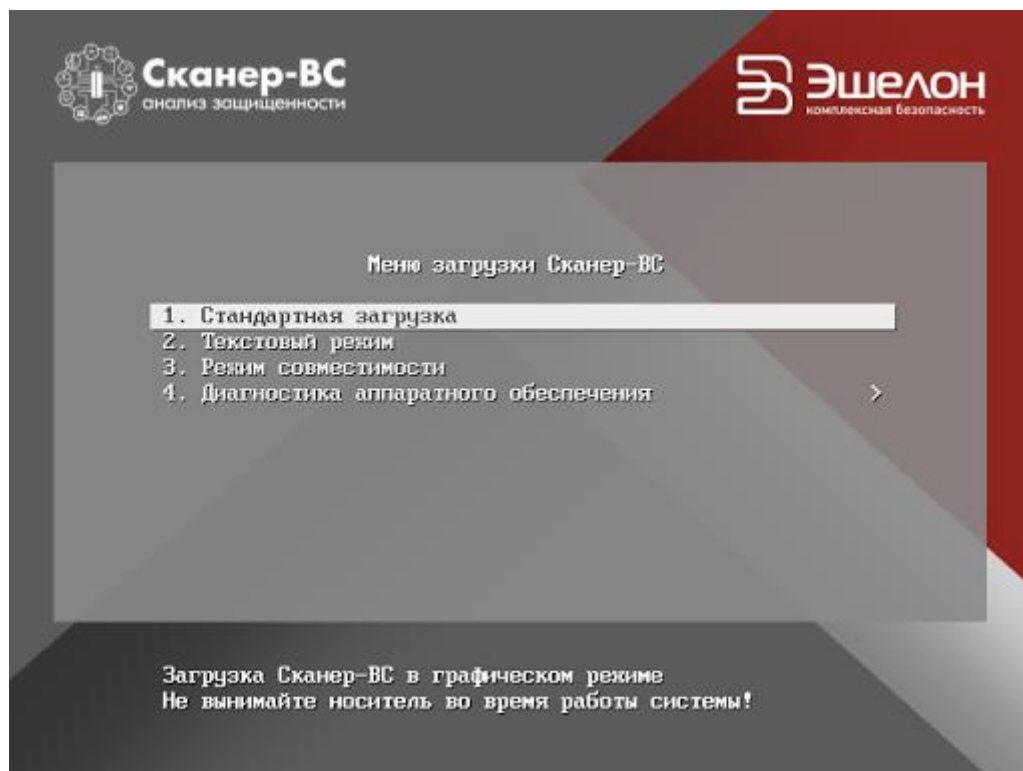


Рисунок 9 — Меню загрузчика ПК «Сканер-ВС»

Варианты загрузки:

- стандартная загрузка;
- текстовый режим;
- режим совместимости;
- диагностика аппаратного обеспечения.

Используйте стандартную загрузку, если при ее использовании у вас не возникает проблем с совместимостью.

В текстовом режиме ПК «Сканер-ВС» загружается в консольном режиме без графического интерфейса. Для запуска в текстовом режиме воспользуйтесь парой логин-пароль – root-toor.

Следует выбрать режим совместимости, если программный комплекс не запускается в режиме стандартной загрузки.

Запустите диагностику аппаратного обеспечения для уточнения проблем с совместимостью при загрузке ПК «Сканер-ВС».

Для настройки сети необходимо воспользоваться сетевым менеджером (запускается из меню ПК «Сканер-ВС» **Остальные приложения** → **Интернет** → **Wicd Network Manager**). Подробно настройка сети описана в п. 3.8.1. Менеджер сетевых подключений «Wicd Network Manager».

3.2. Работа с проектами

После загрузки ПК «Сканер-ВС» откроется пользовательский веб-интерфейс программного комплекса (Рисунок 12).

Если срок действия лицензии истек, то в верхнем правом углу рабочего окна ПК «Сканер-ВС» будет отражено соответствующее сообщение (Рисунок 10).

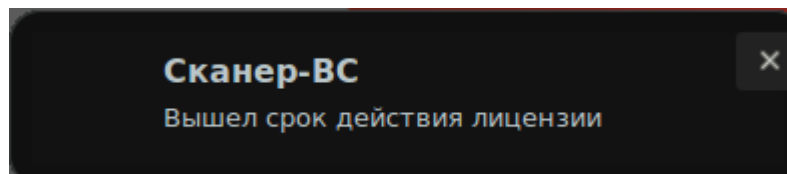


Рисунок 10 – Сообщение

Все графические элементы пользовательского веб-интерфейса можно разделить на следующие группы:

- справочная информация (на рисунке 12 выделена зеленой рамкой);
- проекты (на рисунке 12 выделена фиолетовой рамкой);
- инструменты (на рисунке 12 выделена красной рамкой).

В группе справочной информации содержатся:

- пиктограмма **Обновить Сканер-ВС** для обновления программного комплекса;
- пиктограмма **Справка**, в которой содержатся документы: «Руководство оператора», «Краткое руководство пользователя», «Технические условия»;
- информация о лицензии;
- информация о состоянии сервисов программного комплекса. При изменении доступности сервиса индикатор напротив него изменит цвет (Рисунок 11). Желтый цвет индикатора означает, что сервис загружается, красный – сервис недоступен, зеленый – сервис работает.

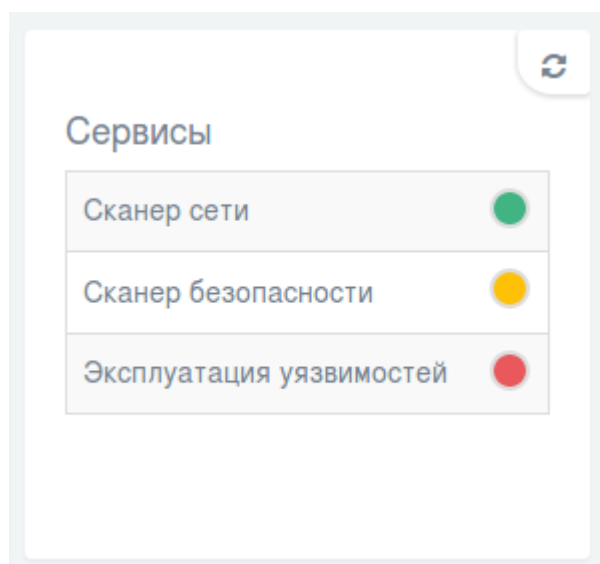


Рисунок 11 – Индикаторы доступности сервисов

Пиктограммы запуска инструментальных программ, реализующих функции ПК «Сканер-ВС» сгруппированы в двух областях веб-интерфейса:

- проекты;
- инструменты.

Для быстрого доступа к списку инструментов необходимо нажать левой кнопкой мыши на пиктограмму **Инструменты**, расположенную в верхнем правом углу пользовательского веб-интерфейса.



Рисунок 12 – Пользовательский веб-интерфейс

Пиктограмма настроек ПК «Сканер-ВС» находится в верхней части веб-интерфейса. Для доступа к настройкам нужно нажать ее левой кнопкой мыши. Окно настроек (Рисунок 13) содержит следующие вкладки: **Поиск уязвимостей**, **Журнал ошибок**, **Лицензия**, **Информация о продукте**.

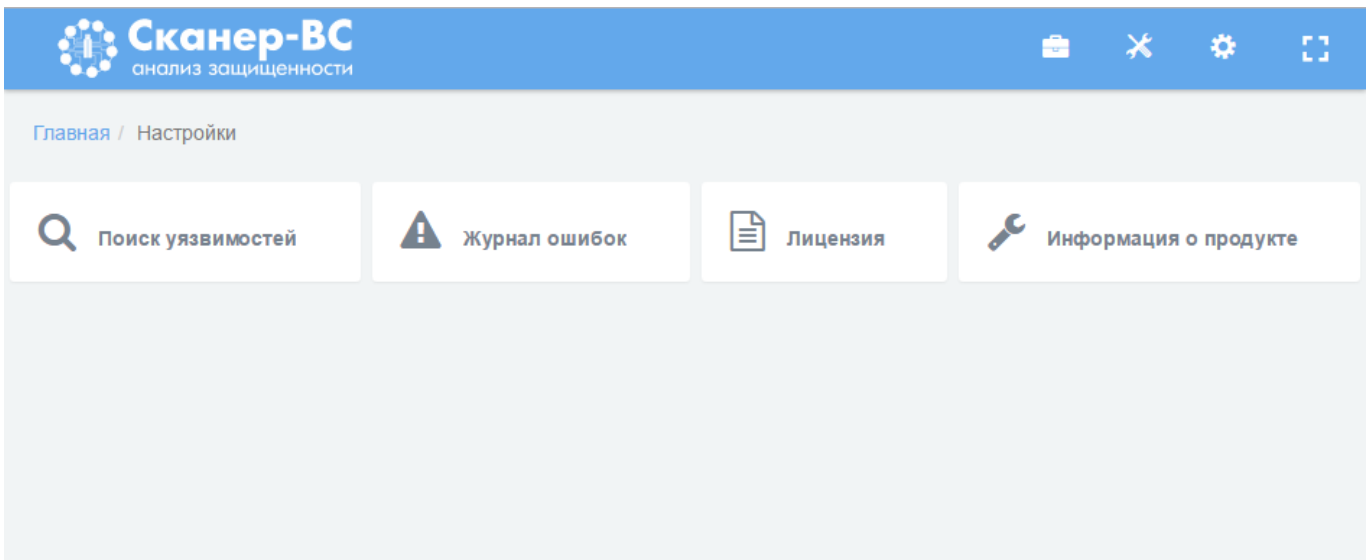


Рисунок 13 – Окно «Настройки»

На вкладке **Журнал ошибок** содержится информация об ошибках, возникших в процессе тестирования. На вкладках **Лицензия** и **Информация о продукте** содержится информация о лицензии и версии ПК «Сканер-ВС», а также контакты технической поддержки.

На вкладке **Поиск уязвимостей**, нажав левой кнопкой мыши на кнопку **Политики сканирования** будет отражена информация о политиках, используемых для поиска уязвимостей (Рисунок 14, Рисунок 15).

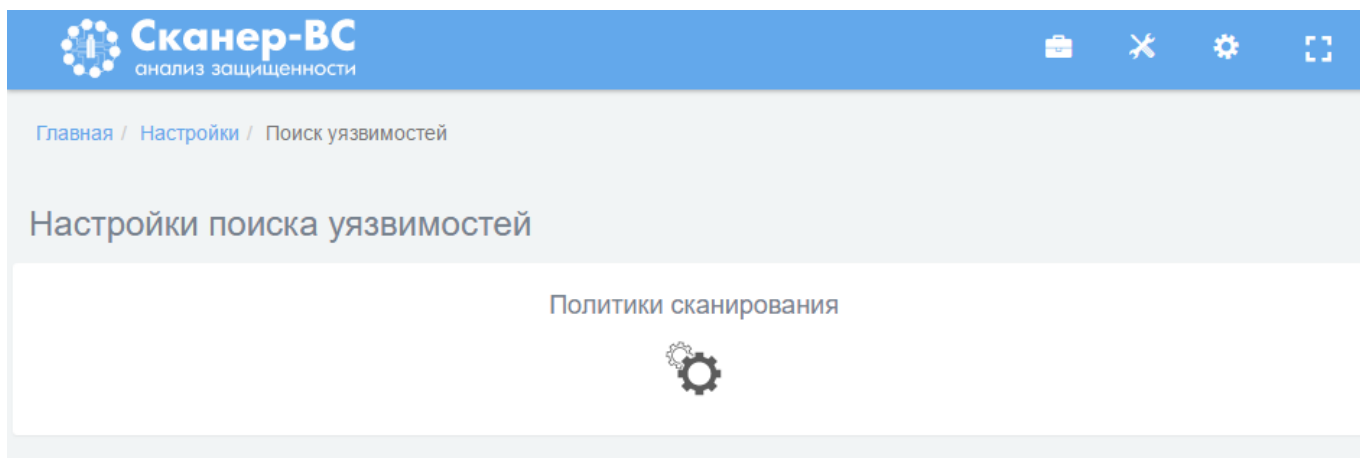


Рисунок 14 – Вкладка «Поиск уязвимостей»

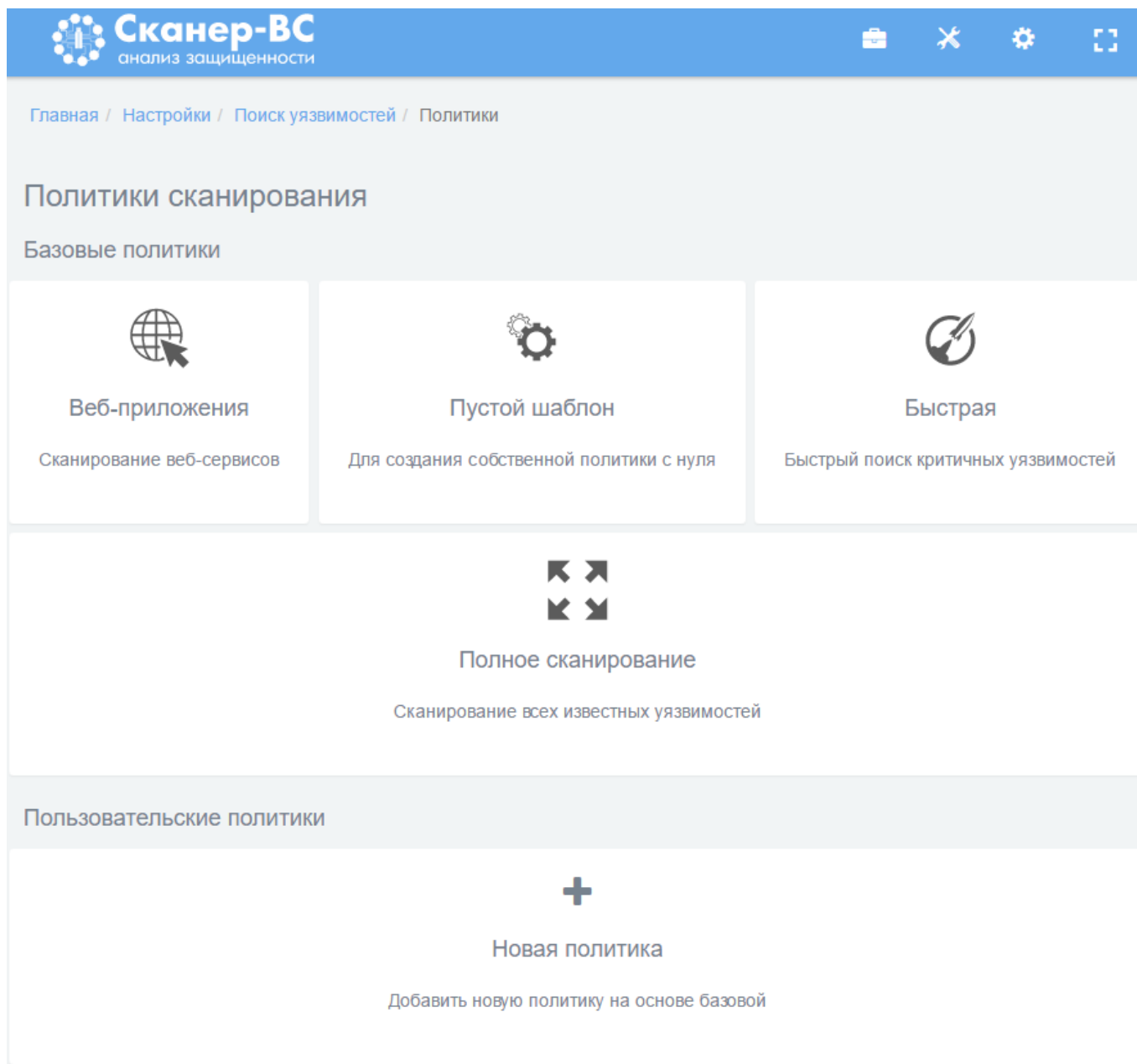


Рисунок 15 – Перечень политик сканирования

Для создания пользовательской политики нажмите левой кнопкой мыши на кнопку **Новая политика** на вкладке **Политики** (Рисунок 15). На открывшейся вкладке выберите шаблон на основании, которого необходимо создать новую политику: **Веб-приложения**, **Полное сканирование**, **Пустой шаблон** (Рисунок 16).

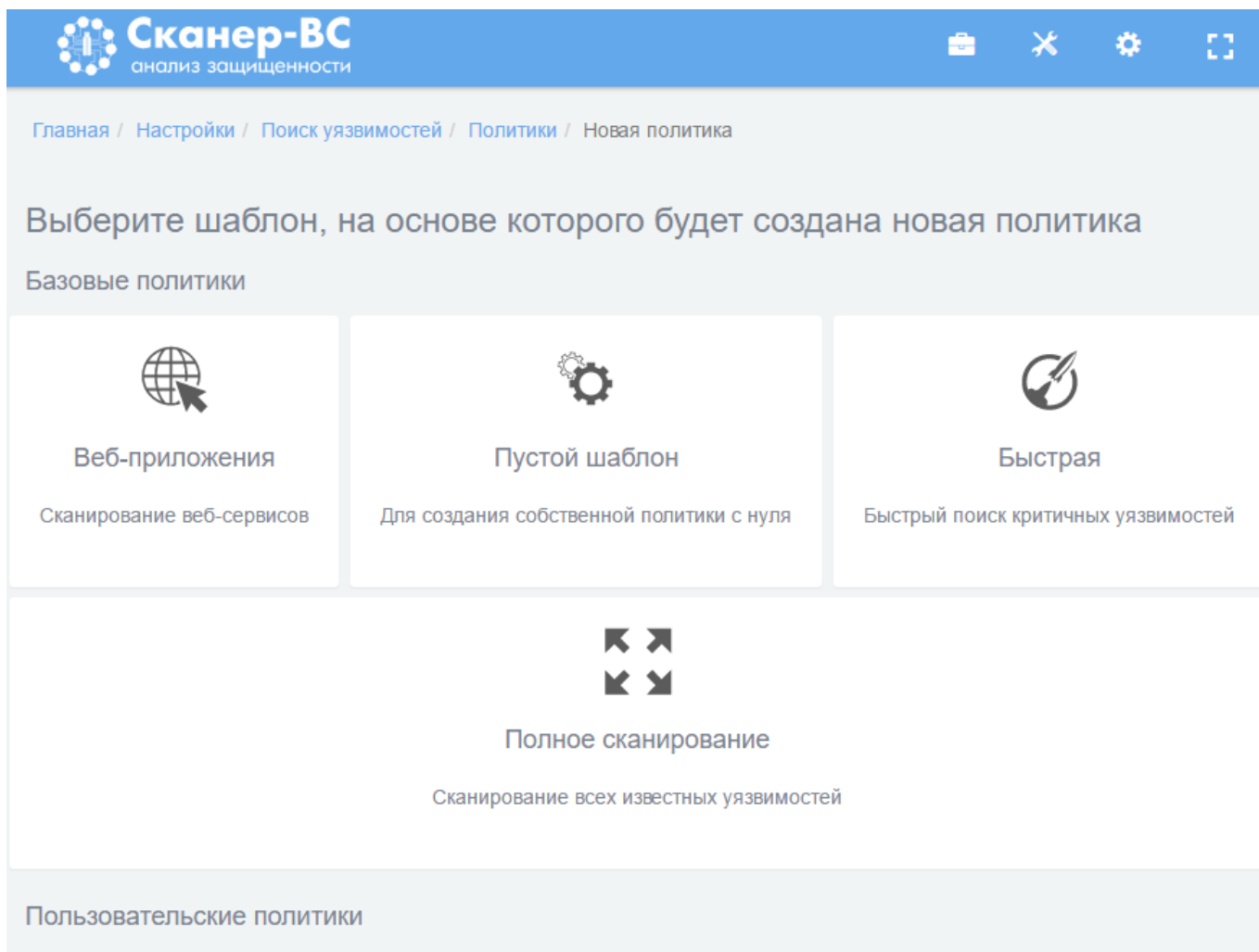


Рисунок 16 – Выбор шаблона политики

После выбора пустого шаблона откроется окно, в котором необходимо указать параметры сканирования (имя, описание, иконку, плагины) (Рисунок 17). После ввода необходимых параметров для создания политики нажмите кнопку **Создать**.

Примечание. В пустом шаблоне пользовательской политики включены плагины только необходимые для запуска сканирования.

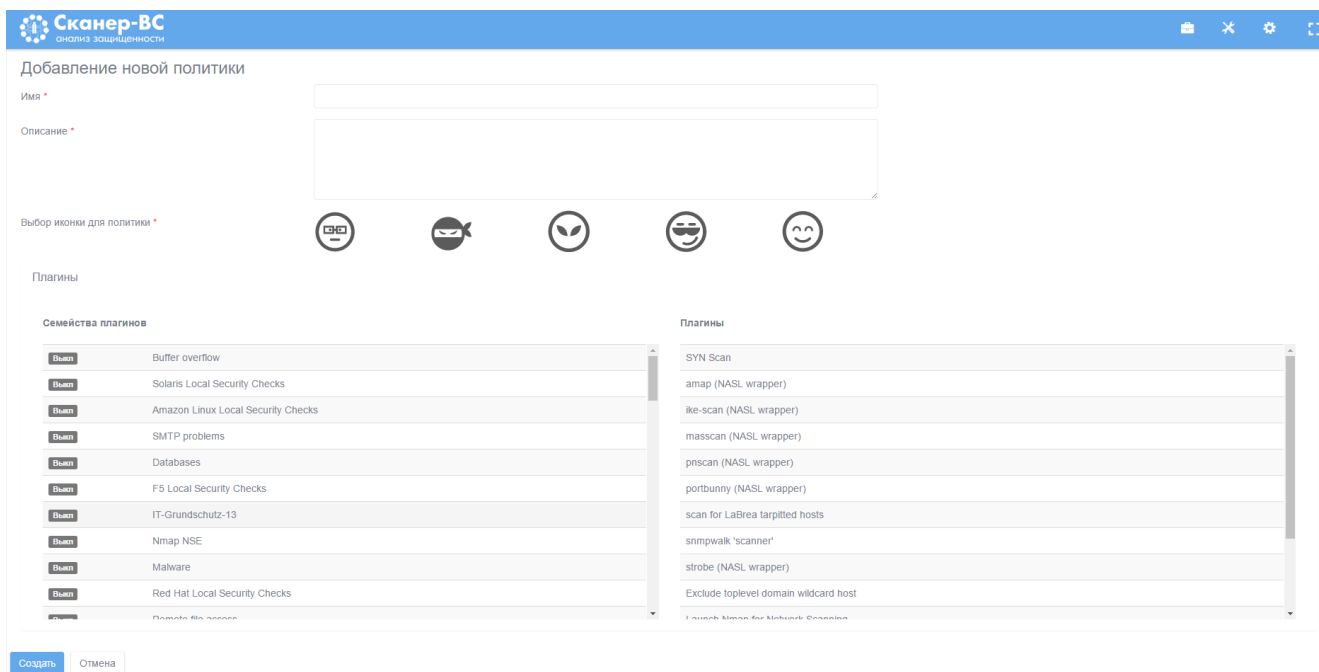


Рисунок 17 – Создание пользовательской политики

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 оператору необходимо 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 18).

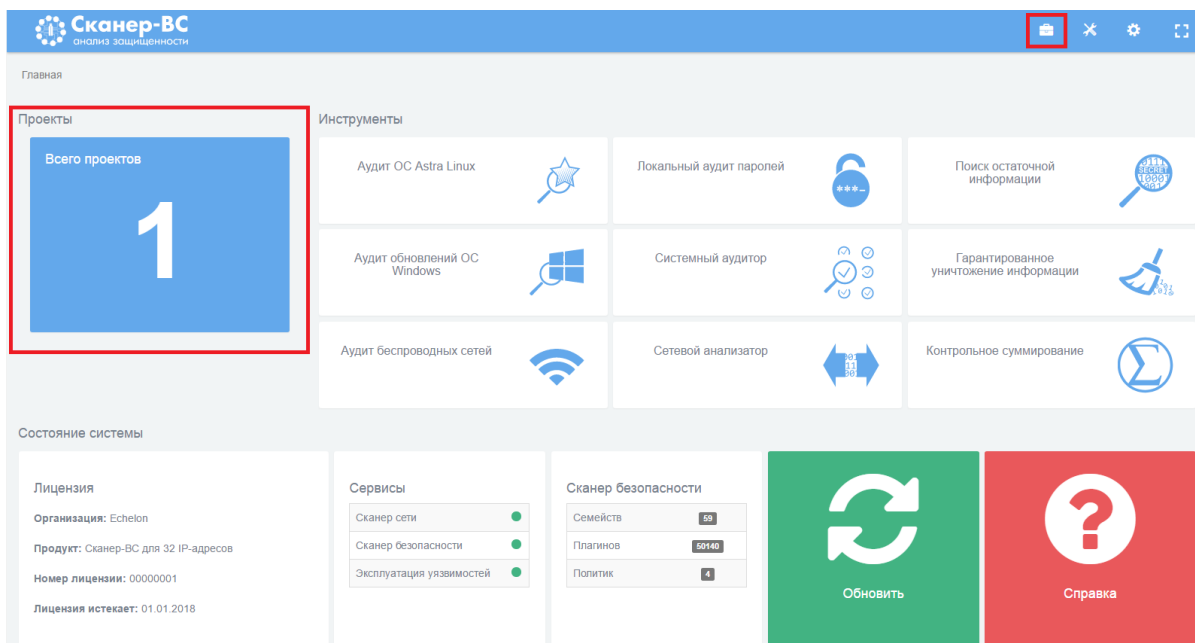


Рисунок 18 – Раздел «Проекты»

В открывшемся окне нажмите на кнопку **Новый проект** или выберите уже существующий проект из перечисленных в рабочей области (Рисунок 19).

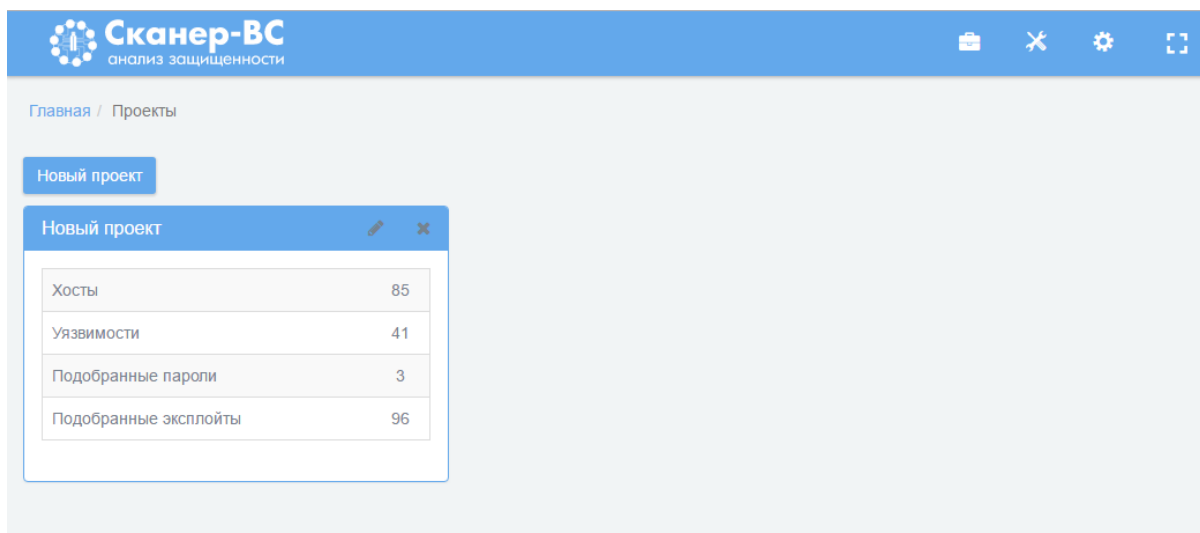


Рисунок 19– Создание проекта

При нажатии на кнопку **Новый проект** откроется окно представленное ниже (Рисунок 20).

Сканер-ВС
анализ защищенности

Главная / Проекты / Новый проект

Добавление нового проекта

Имя *

Описание *

Рисунок 20 – 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 21.

Сканер-ВС
анализ защищенности

Главная / Проекты / 2

Поиск целей

| | |
|----------------------|------------|
| Количество хостов | 0 |
| Операционные системы | Нет данных |

Поиск уязвимостей

| | |
|------------------------|---|
| Количество уязвимостей | 0 |
| Критичные | 0 |
| Средней критичности | 0 |
| Низкой критичности | 0 |
| Заметки | 0 |

Эксплуатация

| | |
|--|---|
| Количество подобранных учетных записей | 0 |
| Количество подобранных эксплойтов | 0 |

Задачи

| Задача | Всего | Активные | Завершенные | Ошибка |
|-----------------------|-------|----------|-------------|--------|
| Поиск целей | 0 | 0 | 0 | 0 |
| Поиск уязвимостей | 0 | 0 | 0 | 0 |
| Онлайн подбор паролей | 0 | 0 | 0 | 0 |
| Эксплуатации | 0 | 0 | 0 | 0 |

Отчет

| | |
|------------------|------|
| Название проекта | Тест |
|------------------|------|

Рисунок 21 – Вид рабочего пространства

Рабочее пространство разделено на сектора, каждый из которых соответствует определенной фазе тестирования.

3.3. Поиск целей

3.3.1. Краткое описание

В начале тестирования обязательным является *поиск целей* – обзор локальной сети, к которой подключен ПК «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 ПК «Сканер-ВС», в частности, невозможно производить поиск эксплойтов (подробнее см. п. 3.5. 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.

3.3.2. Запуск

Нажмите левой кнопкой мыши по сектору **Поиск целей** (Рисунок 22).

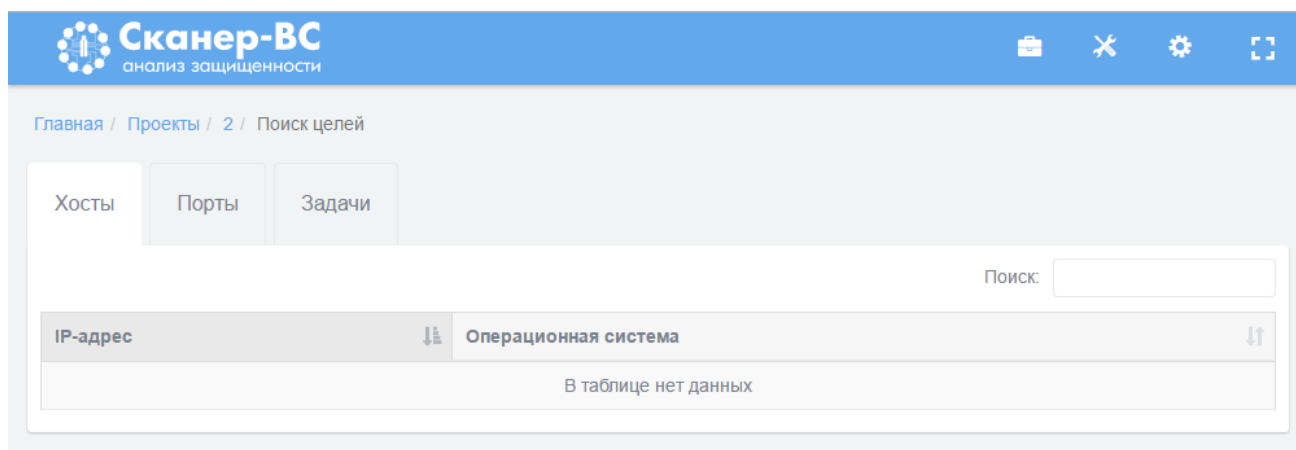


Рисунок 22 – Сектор «Поиск целей»

Перейдите на вкладку **Задачи** и нажмите на кнопку **Новое сканирование** (Рисунок 23).

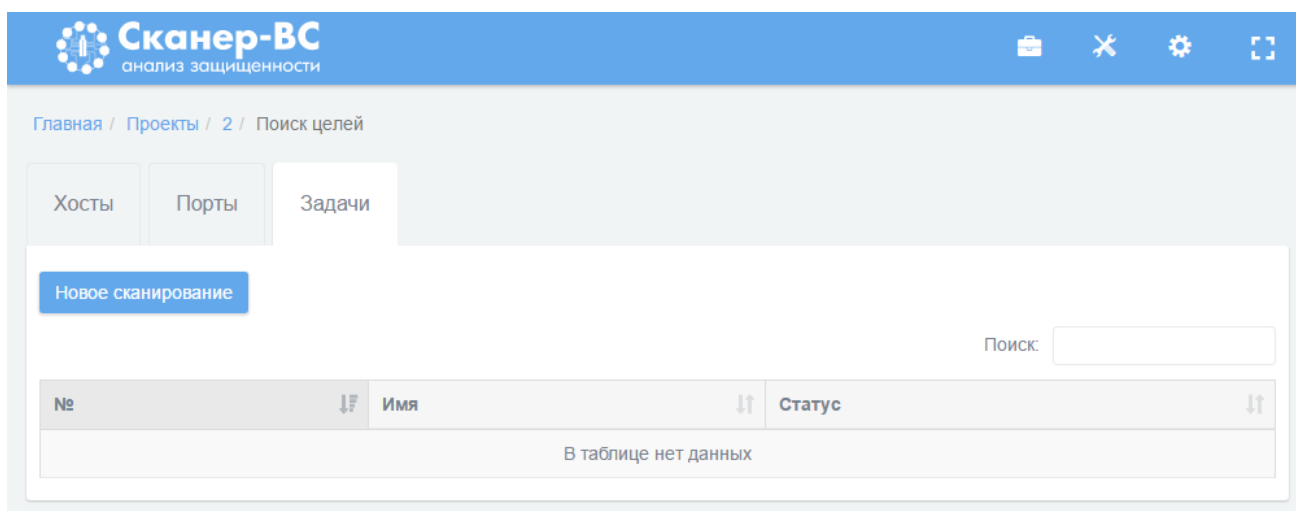


Рисунок 23 – Вкладка «Задачи»

3.3.3. Поиск целей

Настройки, необходимые для запуска сканирования сети, находятся на вкладке **Базовые** (Рисунок 24), где в поле **Цели** необходимо указать *цели сканирования*: конкретный IP-адрес, множество IP-адресов – сеть или подсеть.

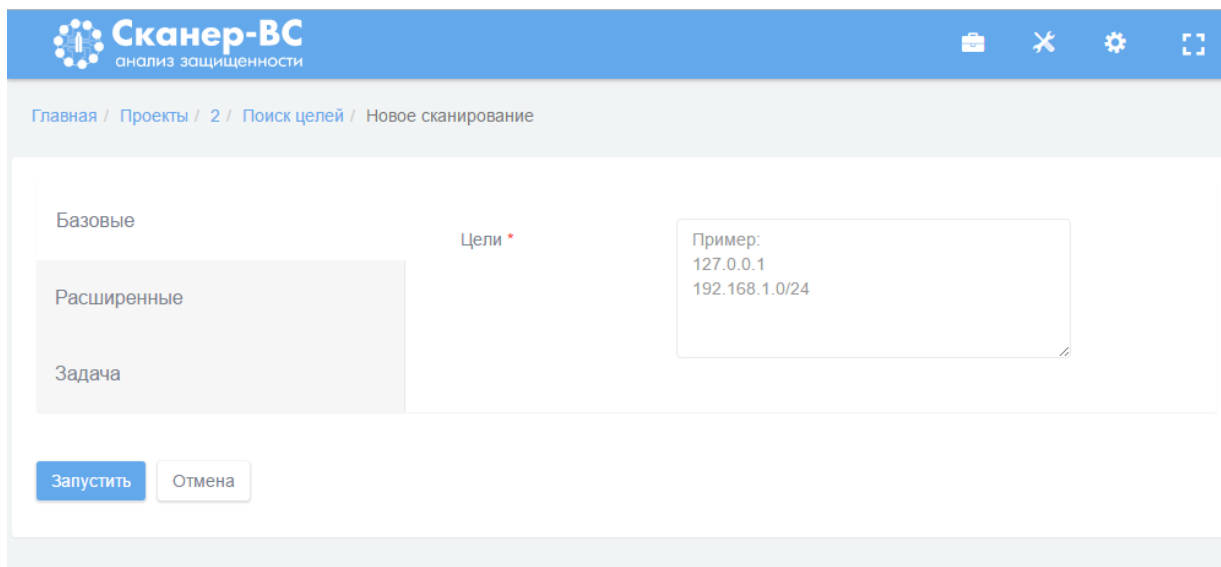


Рисунок 24 – Основные настройки сканирования

Дополнительные настройки сканирования сети расположены на вкладке **Расширенные** и используются при необходимости (Рисунок 25). Для сканирования конкретных портов TCP и UDP включите соответствующий тумблер и укажите порты. При необходимости укажите скорость сканирования: Paranoid или Sneaky для обхода системы обнаружения вторжений, Polite для снижения интенсивности сканирования, Aggressive для повышения интенсивности сканирования, Insane для очень быстрого сканирования. Для увеличения скорости сканирования можно включить тумблер **Не пытаться определять версию сервисов**. Укажите таймаут сканирования для прекращения сканирования медленных целей. Для обнаружения заданных хостов с помощью TCP SYN включите тумблер **Игнорировать результаты Ping**.

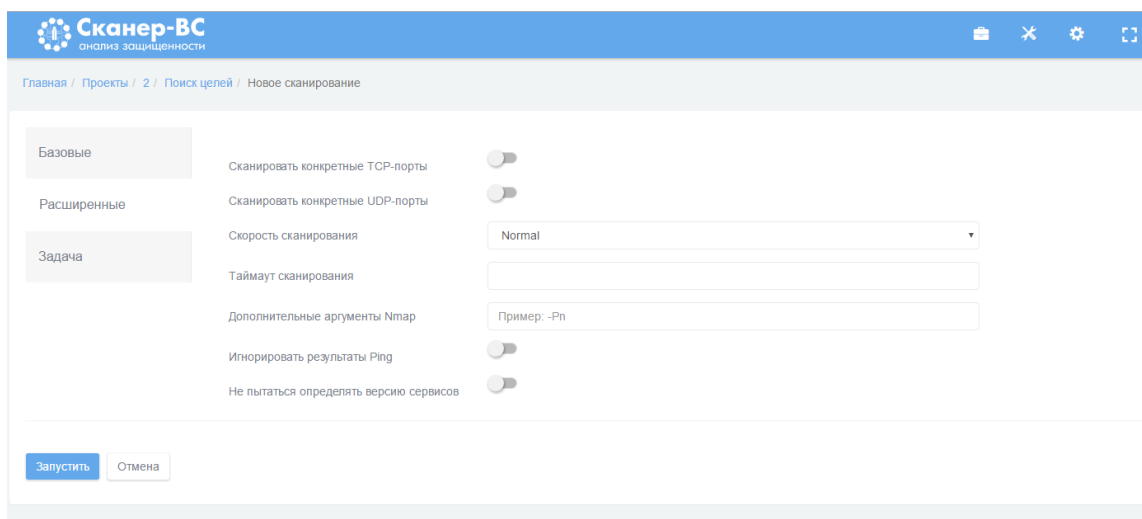


Рисунок 25 – Дополнительные настройки сканирования

На вкладке **Задача** необходимо задать имя и описание текущего сканирования в соответствующие пустые поля (Рисунок 26). Если поля оставить пустыми, они будут заполнены автоматически, исходя из установленных настроек сканирования.

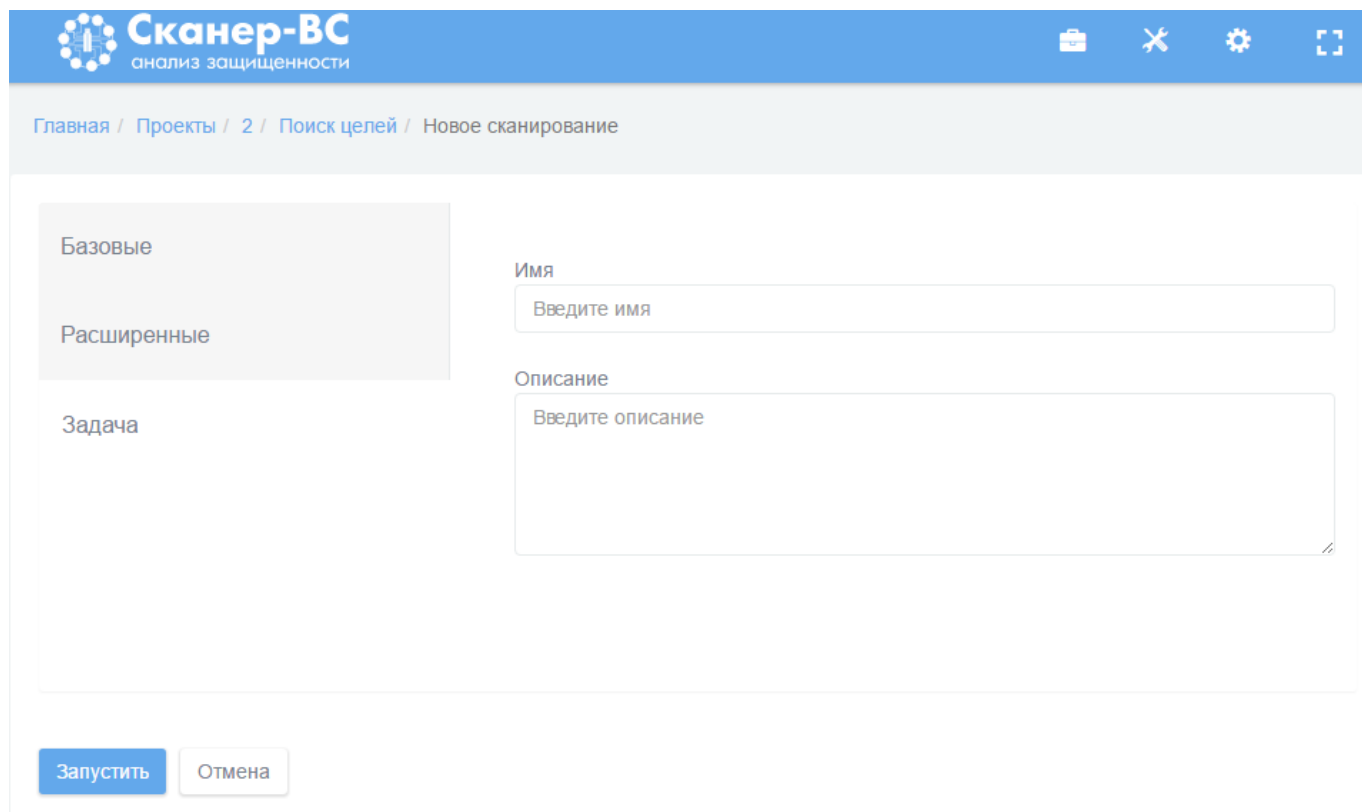
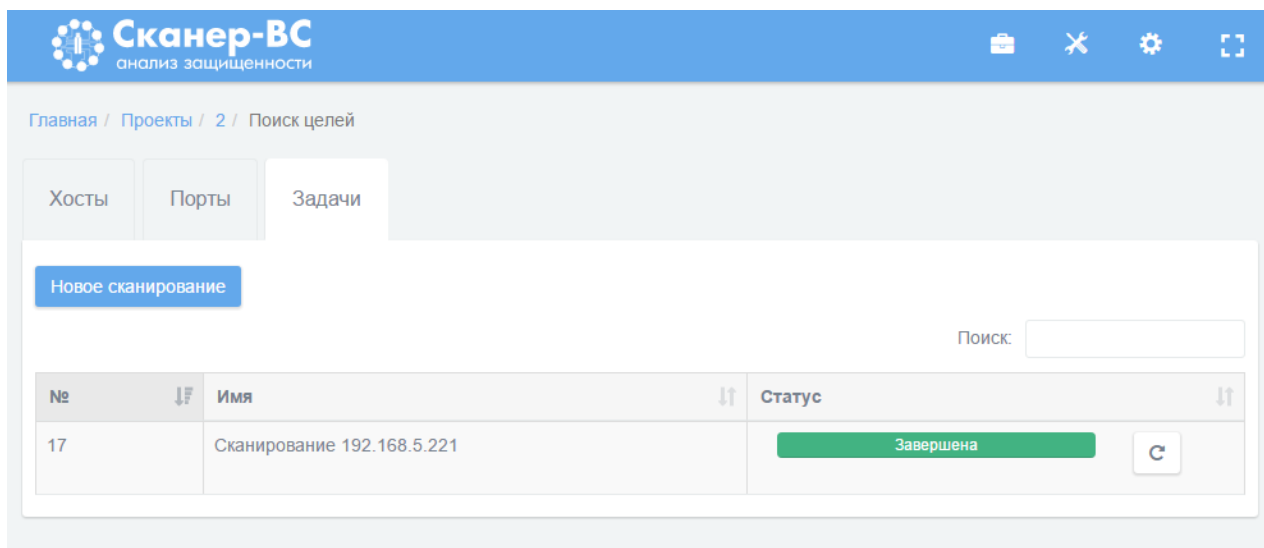


Рисунок 26– Имя и описание сканирования

Чтобы начать сканирование нажмите кнопку **Запустить** (Рисунок 26).

3.3.4. 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 27), красный – процесс сканирования завершен с ошибкой.

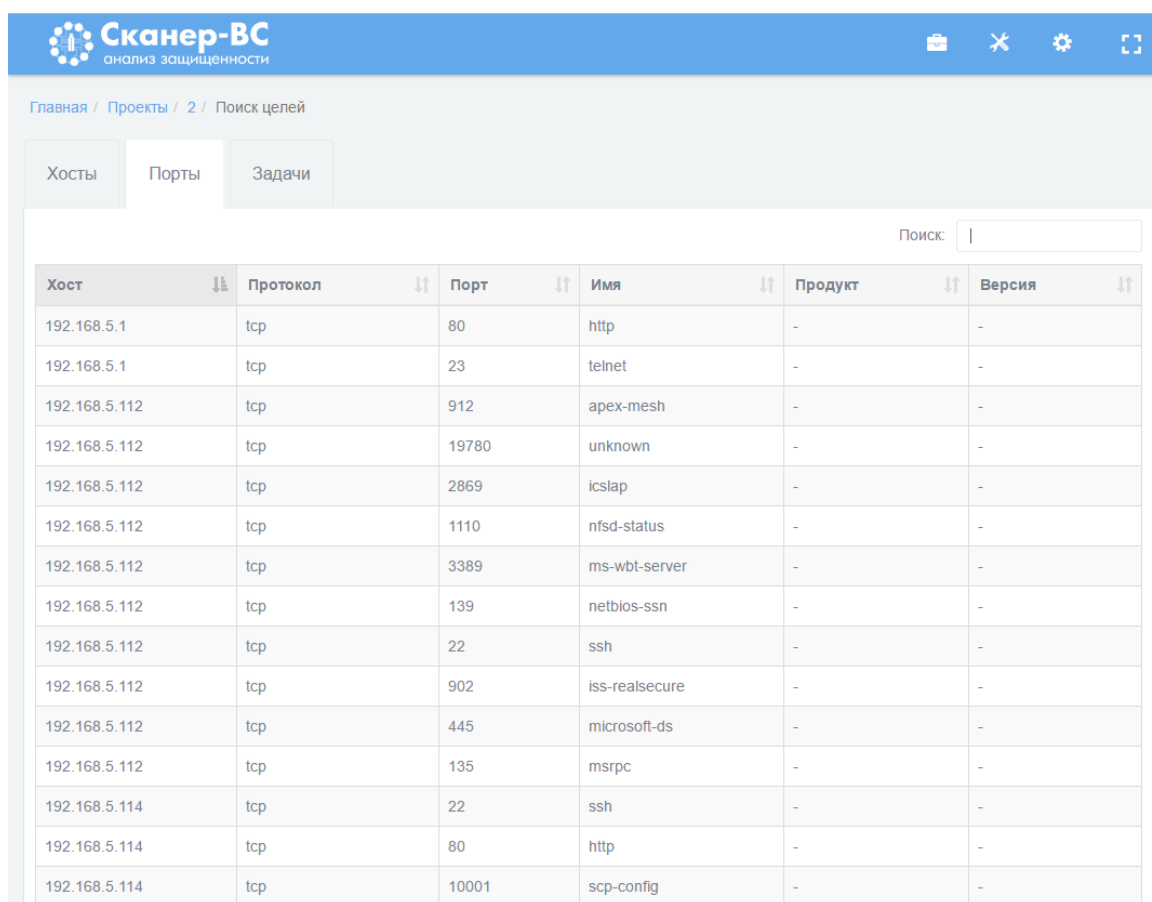


| № | Имя | Статус |
|----|----------------------------|-----------|
| 17 | Сканирование 192.168.5.221 | Завершена |

Рисунок 27 – Процесс сканирования

Независимо от результатов сканирования любую задачу можно перезапустить, нажав на кнопку **Повторить** (Рисунок 27), 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 28).



| 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 28 – Вкладка «Порты»

Во вкладке **Хосты** в таблице показаны IP-адреса и ОС, которые им соответствуют (Рисунок 29).

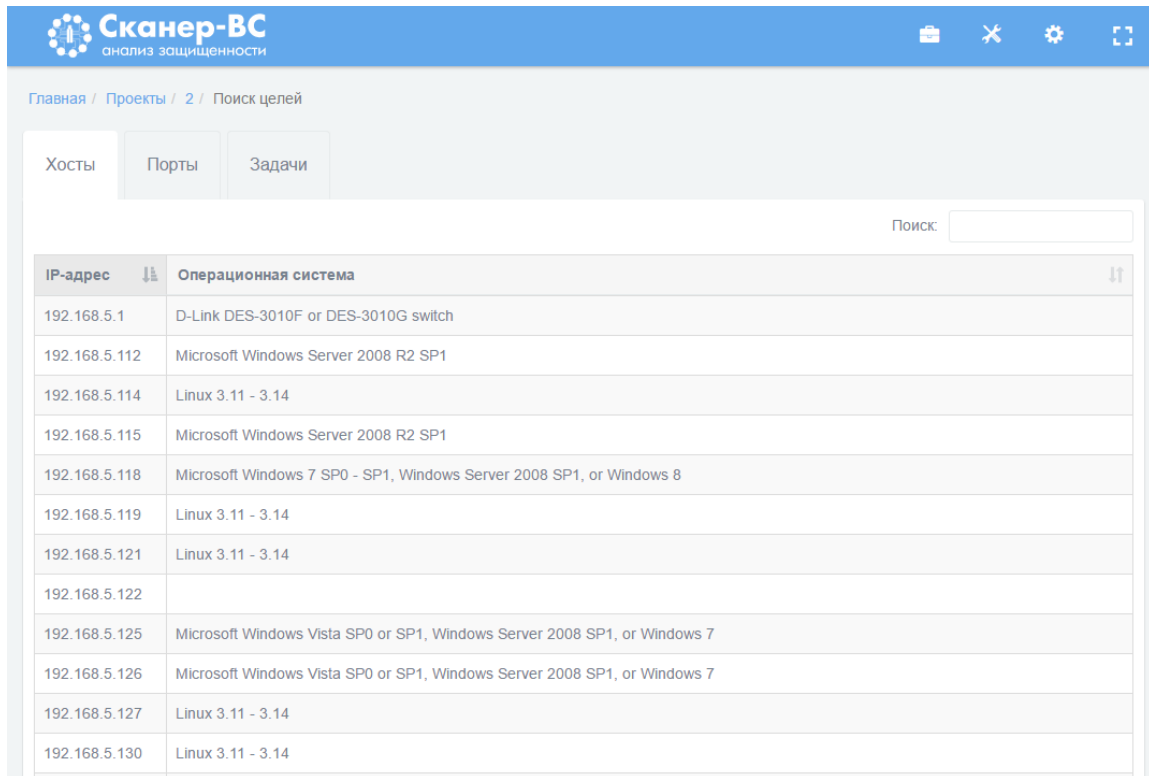


Рисунок 29 – Вкладка «Хосты»

3.4. Поиск уязвимостей

3.4.1. Краткое описание

Под уязвимостью ПО подразумевается дефект, 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.

3.4.2. 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 30).

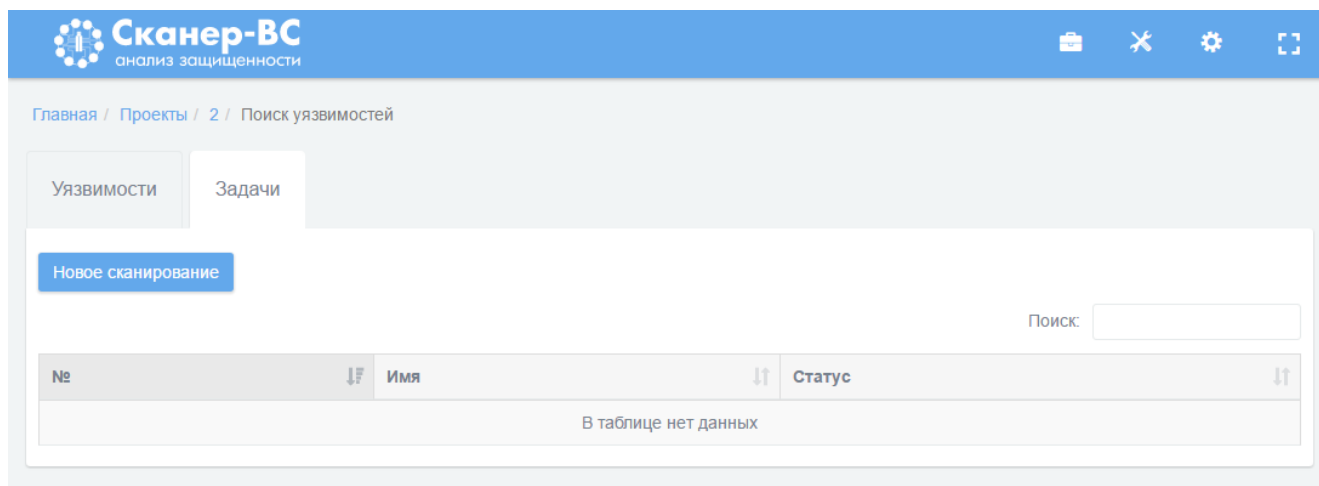


Рисунок 30 – Сектор «Поиск уязвимостей»

3.4.3. Поиск уязвимостей

Настройки, необходимые для запуска поиска уязвимостей, находятся на вкладке **Базовые** (Рисунок 31), где необходимо указать *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. 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. 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**.

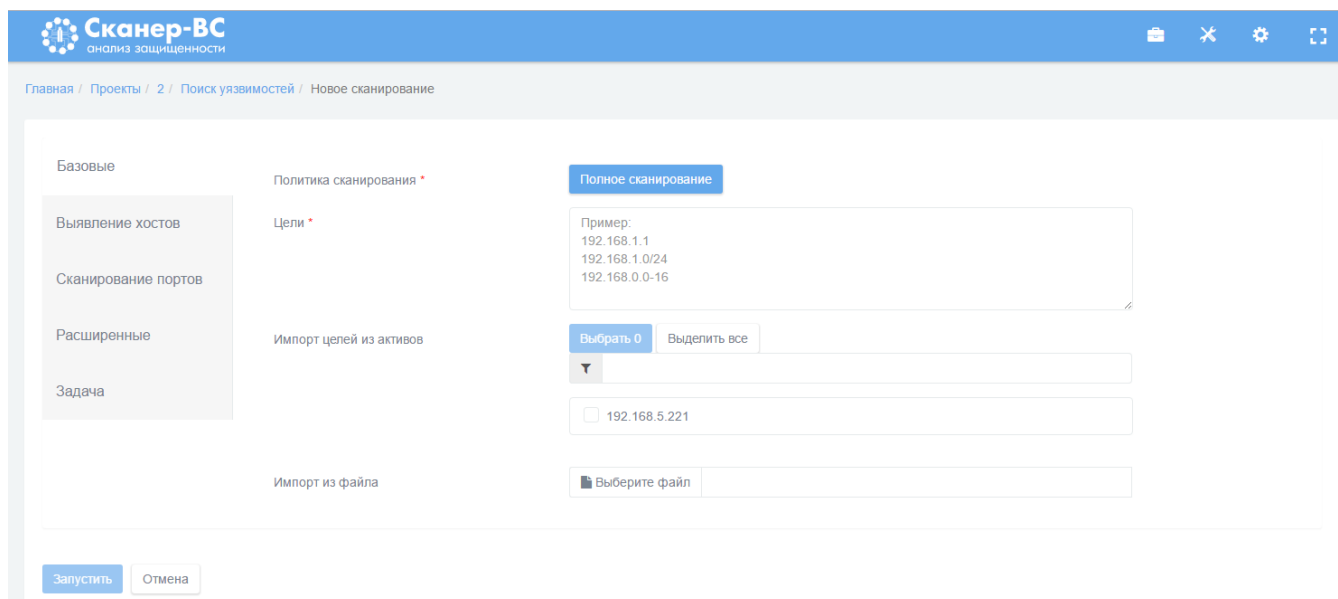


Рисунок 31 – Основные настройки сканирования

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 выберите пользовательскую, созданную ранее (Рисунок 32).

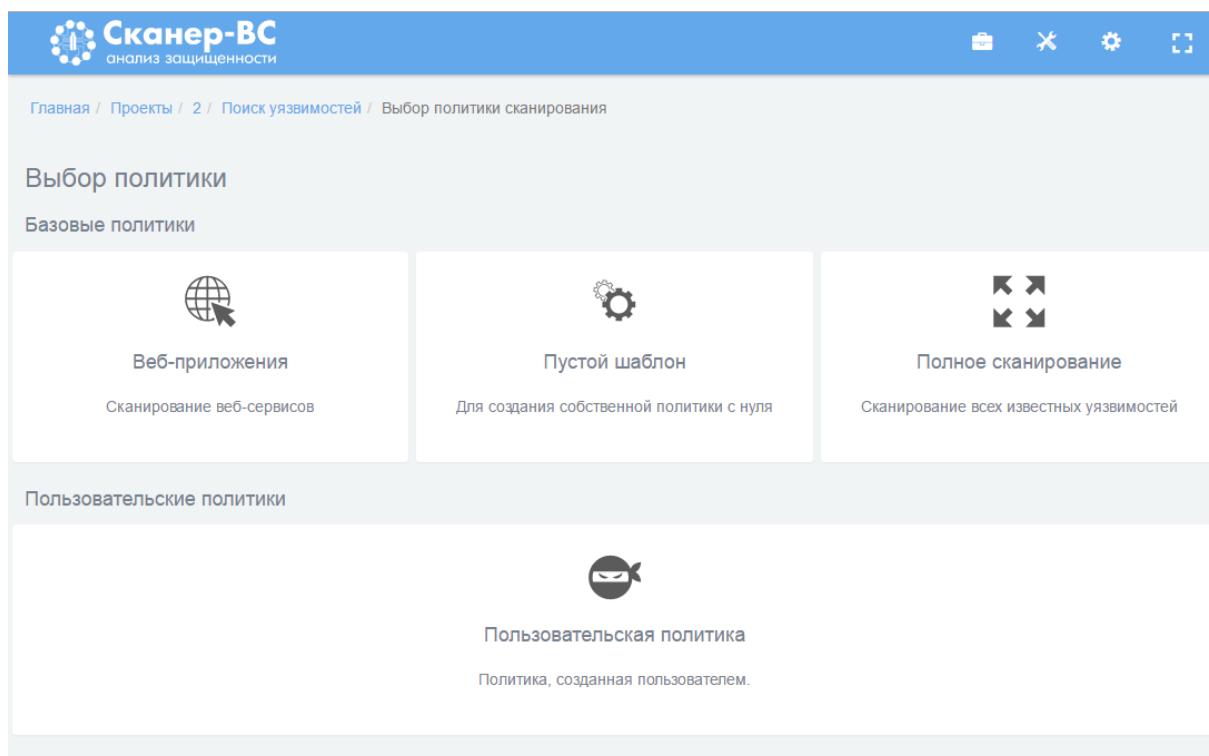


Рисунок 32 – Выбор политики сканирования

Дополнительные настройки сканирования расположены на вкладках **Выявление хостов**, **Сканирование портов**, **Расширенные** (Рисунок 33) и используются оператором при необходимости.

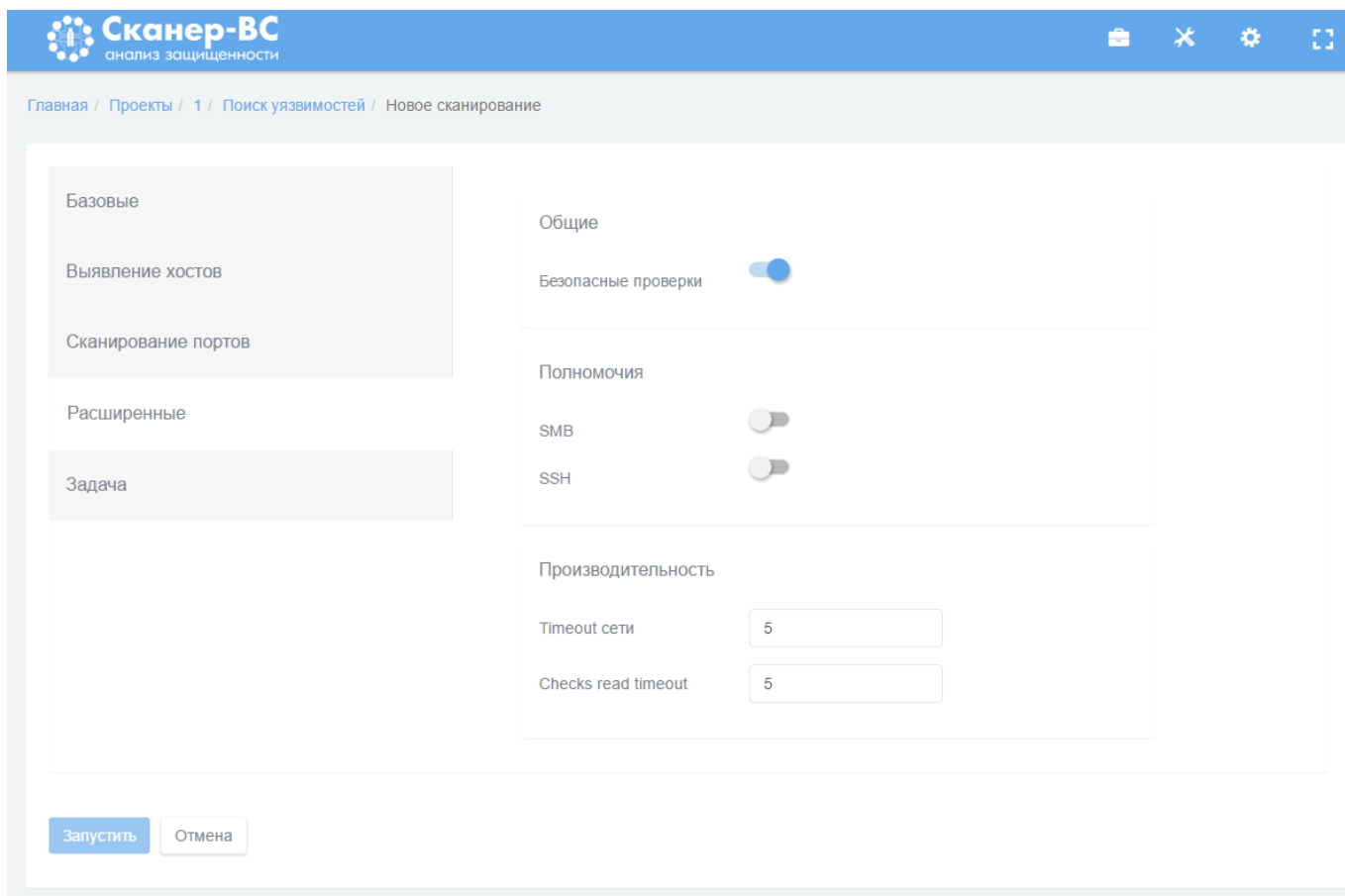
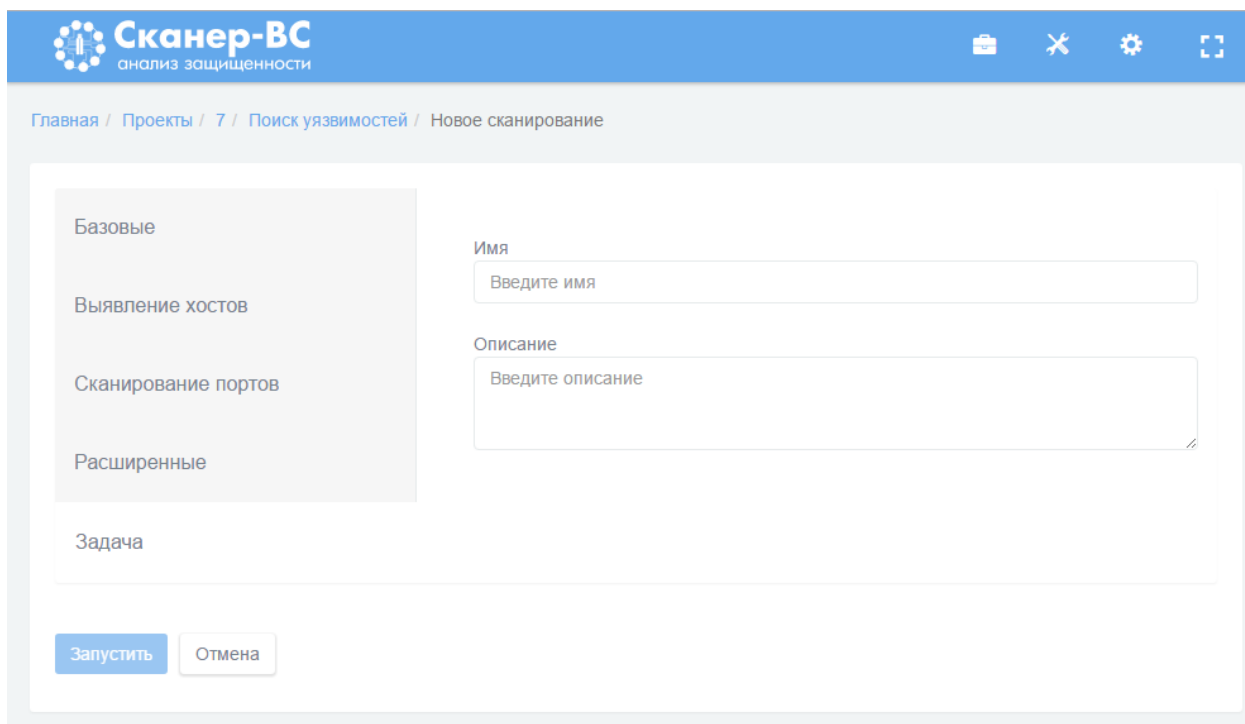


Рисунок 33 – Расширенные настройки

Включенный тумблер **Безопасные проверки** позволяет использовать при тестировании тесты, которые не приведут к нарушениям в работе сканируемых систем. Для проведения тестирования с полномочиями администратора включите тумблер **SMB** (для рабочей станции с ОС семейства Microsoft Windows), **SSH** (для рабочей станции с ОС семейства Linux) и введите логин и пароль администратора.

На вкладке **Задача** (Рисунок 34) необходимо указать имя и описание в соответствующие пустые поля. Если поля оставить пустыми, они будут заполнены автоматически, исходя из указанных настроек сканирования.



Сканер-ВС
анализ защищенности

Главная / Проекты / 7 / Поиск уязвимостей / Новое сканирование

Базовые

Выявление хостов

Сканирование портов

Расширенные

Имя

Введите имя

Описание

Введите описание

Задача

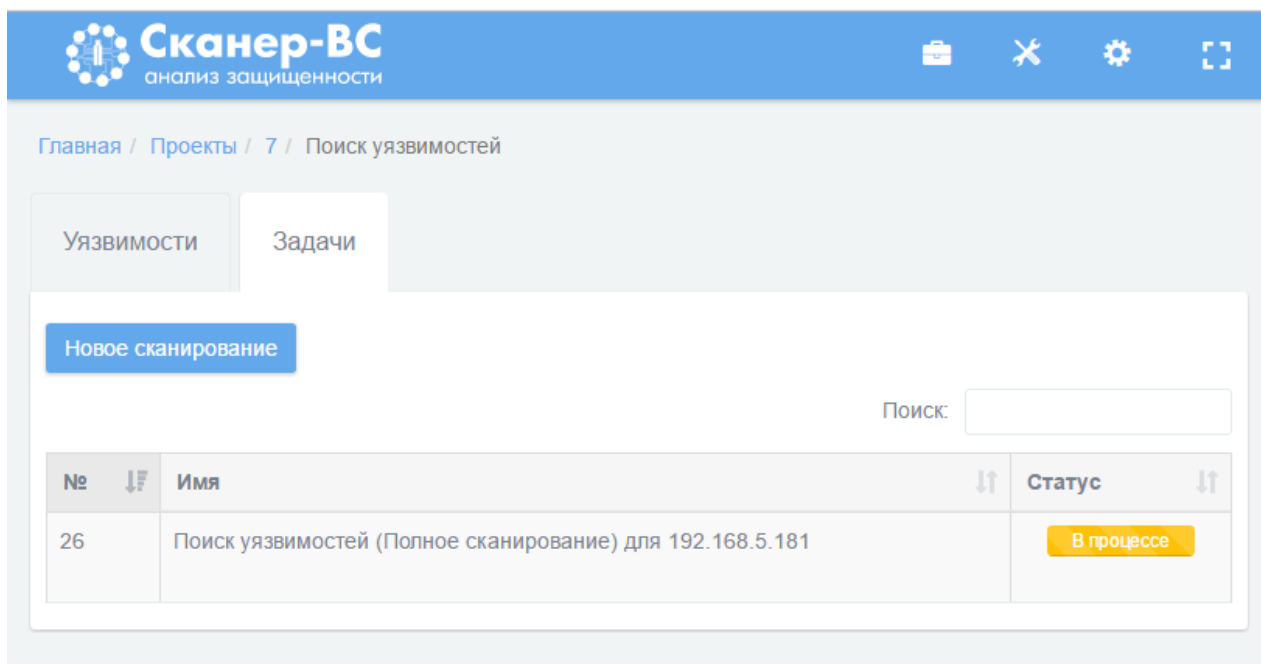
Запустить Отмена

Рисунок 34 – Имя и описание сканирования

Для начала процесса сканирования нажмите кнопку **Запустить** (Рисунок 34).

3.4.4. Завершение работы

После запуска сканирования в таблицу на вкладке **Задачи** будет добавлена строка, содержащая номер задачи, ее имя и индикатор статуса (Рисунок 35). Желтый цвет индикатора означает, что в текущий момент сканирование выполняется, зеленый - сканирование успешно завершено, красный - процесс сканирования завершен с ошибкой.



Сканер-ВС
анализ защищенности

Главная / Проекты / 7 / Поиск уязвимостей

Уязвимости Задачи

Новое сканирование

Поиск:

| № | Имя | Статус |
|----|---|------------|
| 26 | Поиск уязвимостей (Полное сканирование) для 192.168.5.181 | В процессе |

Рисунок 35 – Процесс сканирования

Независимо от результатов сканирования любую задачу можно перезапустить, нажав на кнопку **Повторить** (Рисунок 27), 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 36).

| 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 36 – Результаты поиска

3.5. Эксплуатация

3.5.1. Краткое описание

Фаза **Эксплуатация** объединяет две задачи: сетевой аудит паролей и поиск *эксплоитов* – 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 эксплоитов – тестирование компьютеров в проверяемой сети на возможность их использования описанными выше способами.

3.5.2. Запуск

Для запуска сетевого аудита паролей и поиска эксплойтов (Рисунок 37) нажмите левой кнопкой мыши по сектору **Эксплуатация**.

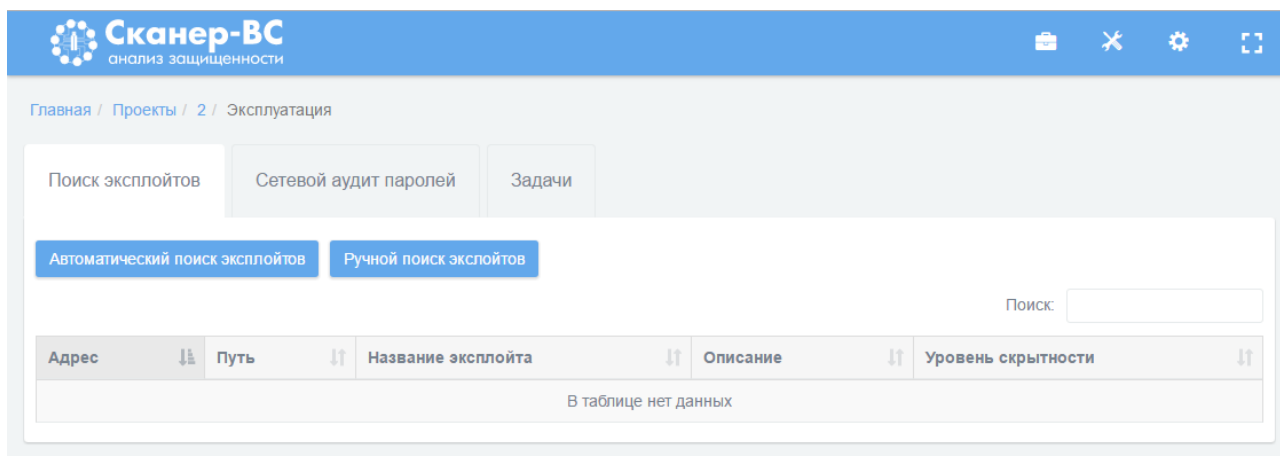


Рисунок 37 – Сектор «Эксплуатация»

3.5.3. 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 38).

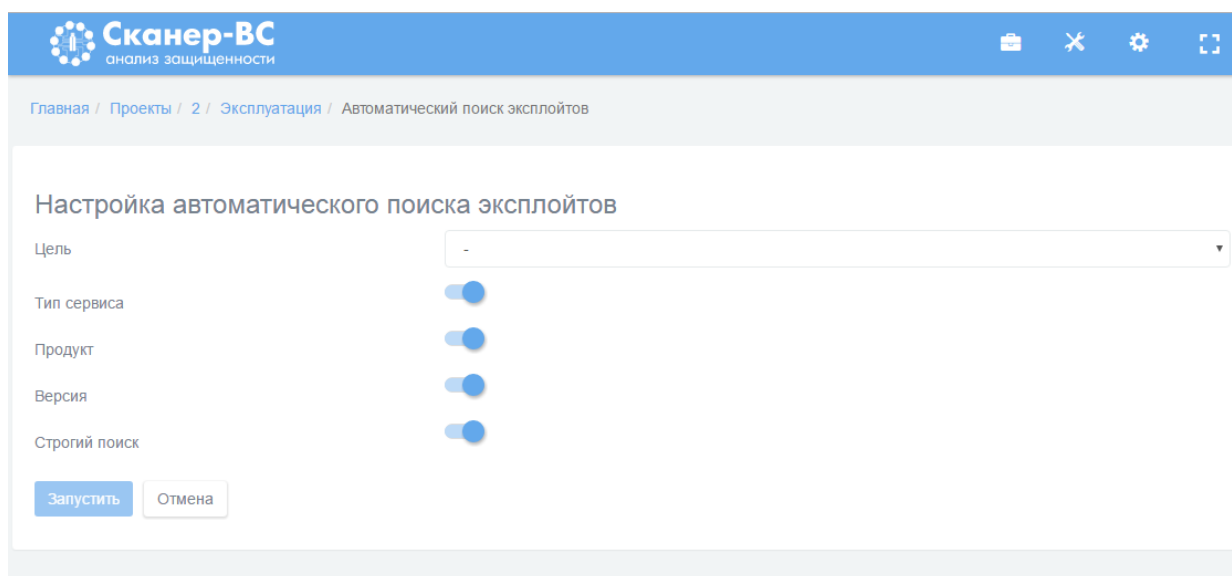


Рисунок 38 – Интерфейс настройки и запуска автоматического поиска эксплойтов

В поле **Цель** выберите IP-адрес. Запуск тестирования можно произвести только для одного IP-адреса. Далее укажите 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 39).

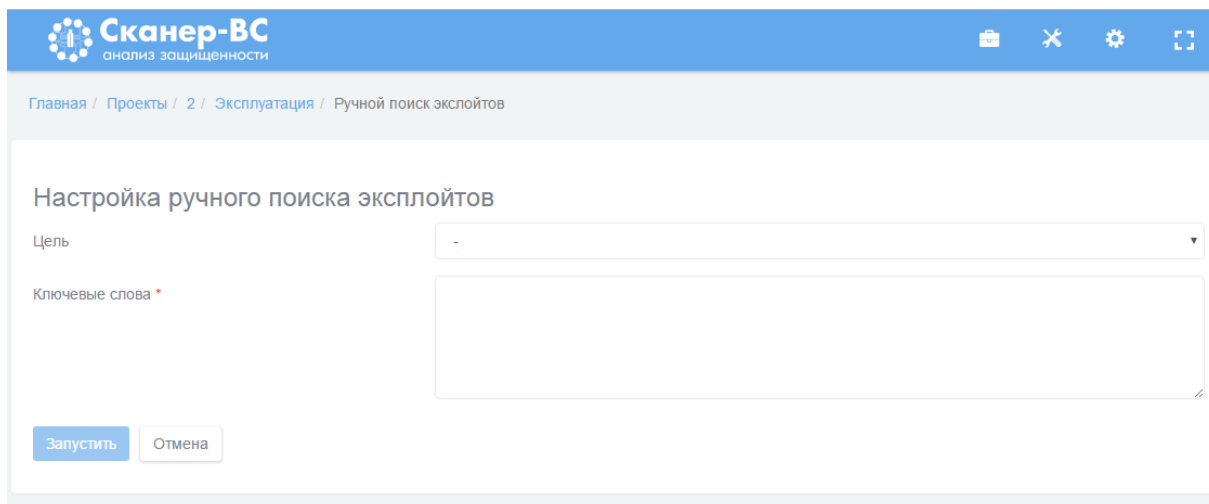


Рисунок 39 – Интерфейс настройки и запуска ручного поиска эксплойтов

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 кнопку **Запустить**. Поиск будет производиться аналогично строгому поиску.

3.5.4. Сетевой аудит паролей

Перейдите на вкладку **Сетевой аудит паролей** и нажмите на кнопку **Новый подбор паролей** (Рисунок 40).

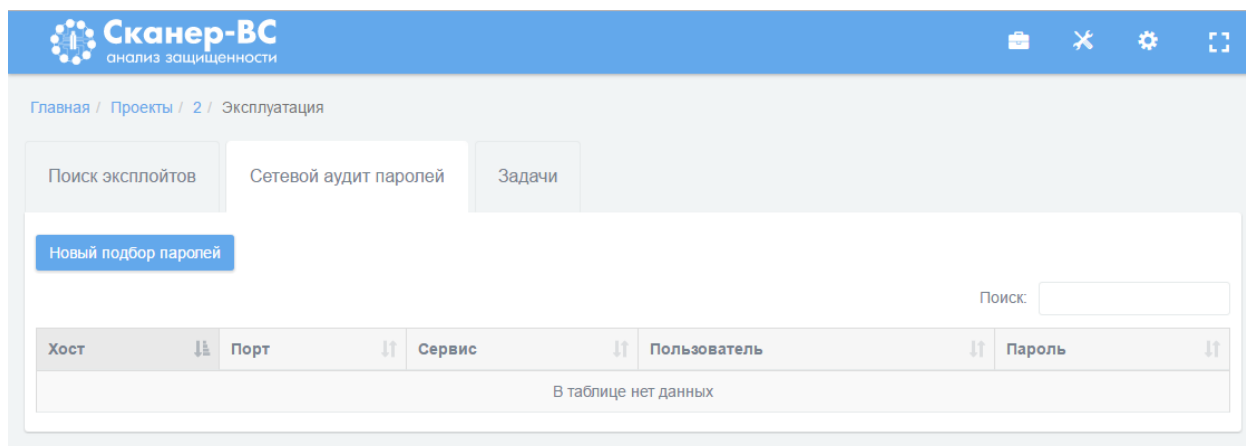


Рисунок 40 – Интерфейс запуска подбора паролей

На вкладке **Базовые** расположены базовые параметры сетевого аудита паролей, которые требуется задать (Рисунок 41): 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 ТХТ, где одна строка документа должна содержать только один IP-адрес. Затем нажмите кнопку **Выберите файл** и в открывшемся окне отметьте имя импортируемого списка. Нажмите кнопку **Открыть**. Перечень целей сканирования появится в поле **Цели**.

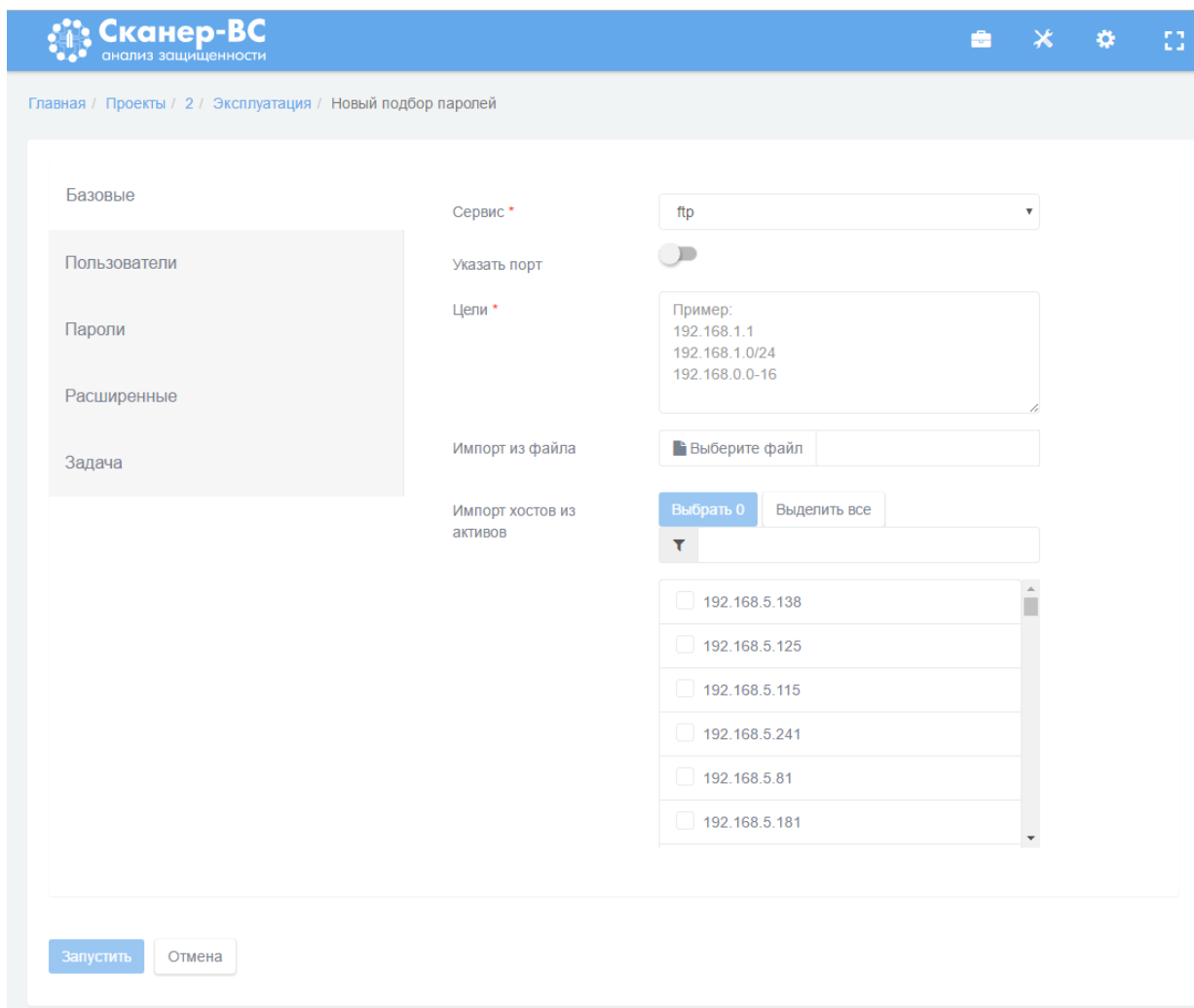


Рисунок 41 – Основные настройки подбора паролей

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

На вкладке **Пользователи** необходимо задать идентификаторы (имена, login) пользователей проверяемых рабочих станций (Рисунок 42). Задать их можно вручную в поле **Пользователи** или

импортировать из файла в формате ТХТ, где одна строка документа должна содержать только одно имя. Дополнительные настройки (**Списки по умолчанию, Найденные ранее пользователи**) используются оператором при необходимости.

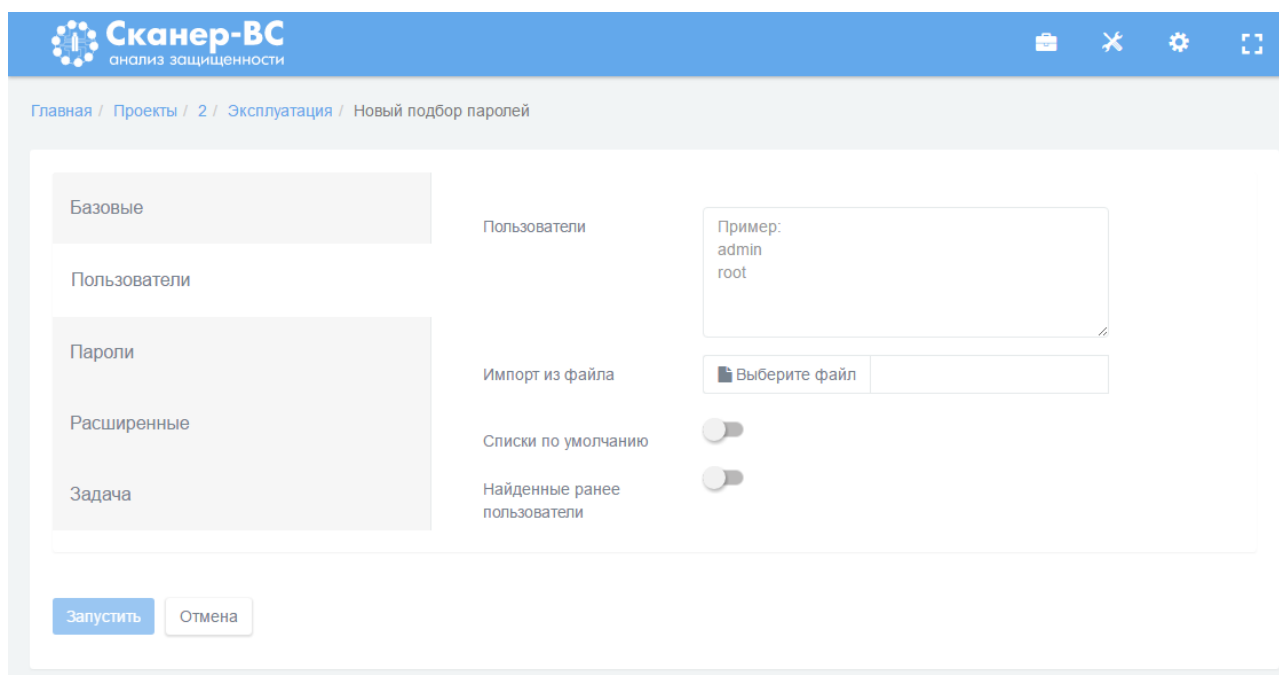


Рисунок 42 – Настройка подбора паролей, вкладка «Пользователи»

На вкладке **Пароли** в поле **Пароли** необходимо указать комбинации букв и цифр, которые будут использоваться в качестве аутентификационной информации (Рисунок 43). Каждая комбинация должна находиться на отдельной строке. Настройки программы поддерживают загрузку паролей из файла в формате ТХТ, где одна строка документа должна содержать только один пароль. Дополнительные настройки (**Пароли по умолчанию, Найденные ранее пароли** и другие) используются оператором при необходимости.

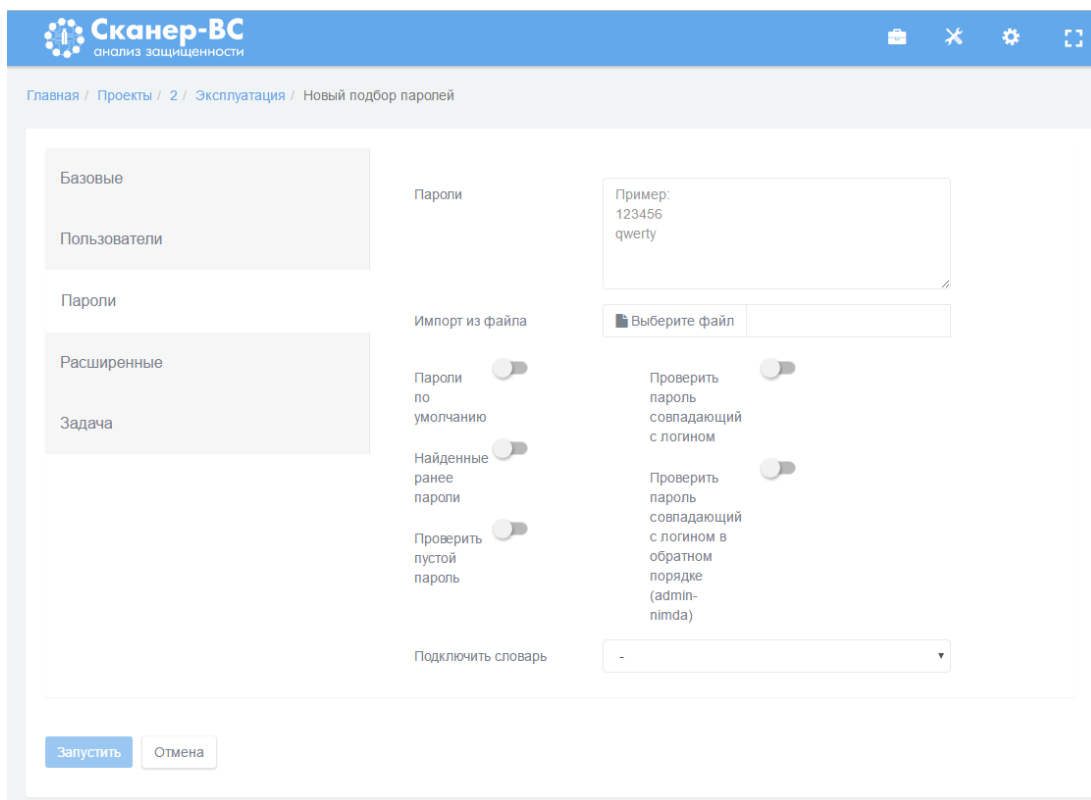


Рисунок 43 – Настройка подбора паролей

Для завершения подбора паролей при первой подобранной паре имя - пароль, перейдите на вкладку **Расширенные** и активируйте **Закончить подбор при первом положительном результате** (Рисунок 44).

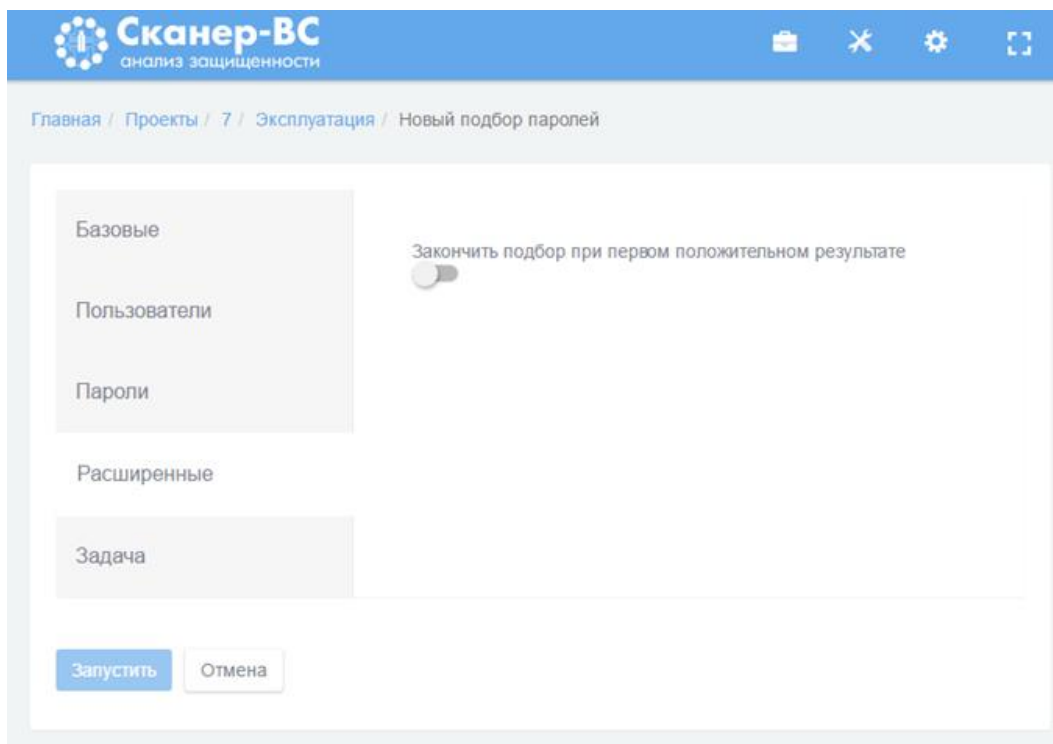


Рисунок 44 – Расширенные настройки подбора паролей

На вкладке **Задача** необходимо задать 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 44).

3.5.5. Завершение работы

После нажатия кнопки **Запустить** на вкладке **Задачи** в таблице появится номер задачи, имя и индикатор статуса (Рисунок 45). Желтый цвет индикатора означает процесс сканирования, зеленый - завершение сканирования, красный - процесс сканирования завершен с ошибкой.

| № | Имя | Статус |
|----|---|------------|
| 29 | Онлайн подбор для 192.168.5.181 | В процессе |
| 27 | Ручной поиск эксплойтов для 192.168.5.115 | Завершена |
| 26 | Автоматический поиск эксплойтов для 192.168.5.181 | Завершена |

Рисунок 45 – Таблица задач поиска эксплойтов

После завершения сканирования в разделе **Сетевой аудит паролей** появятся данные о подобранных паролях (Рисунок 46), а в разделе **Эксплойты** таблица с найденными эксплойтами (Рисунок 47).

| Хост | Порт | Сервис | Пользователь | Пароль |
|---------------|------|--------|--------------|----------|
| 192.168.5.122 | 21 | ftp | msfadmin | msfadmin |
| 192.168.5.122 | 21 | ftp | ftp | 000000 |

Рисунок 46 – Информация о подобранных паролях

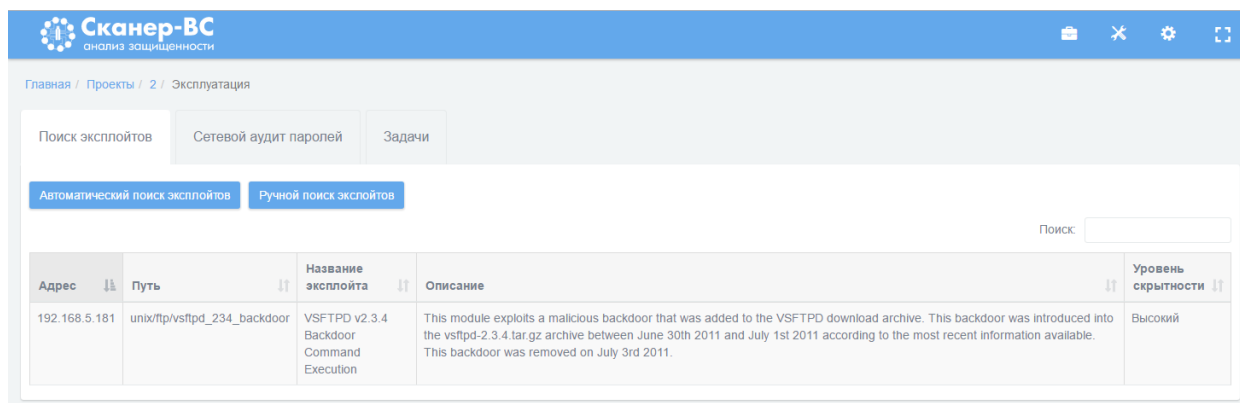


Рисунок 47 – Информация о найденных эксплоитах

3.6. Отчеты

3.6.1. Краткое описание

Документирование является неотъемлемой частью анализа защищенности информационной системы. Для объединения результатов всех этапов тестирования в ПК «Сканер-ВС» используется сектор **Отчет** (Рисунок 21), с помощью которого можно построить отчет с результатами тестирований.

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

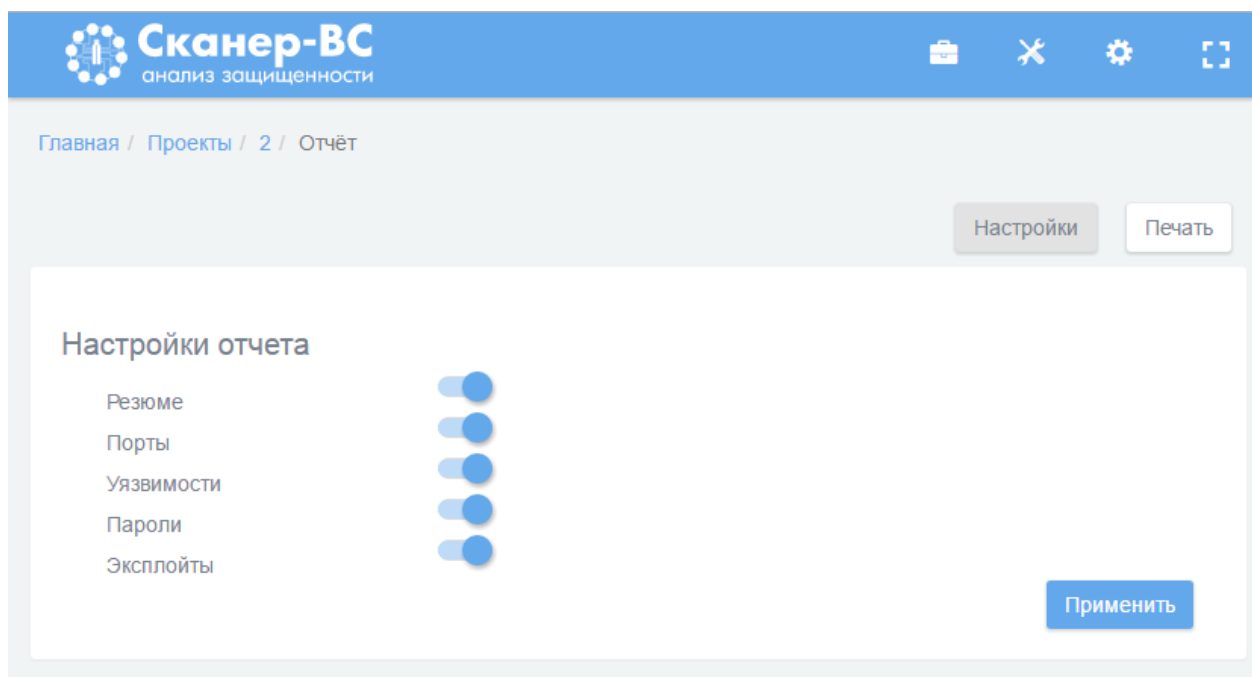


Рисунок 48 – Конструктор отчетов

Полный отчет состоит из следующих разделов: **Резюме, Порты, Уязвимости, Пароли и Эксплойты**. Раздел **Резюме** содержит краткую информацию по всем этапам тестирования в виде диаграмм и общей таблицы распределения уязвимостей по хостам (Рисунок 49).

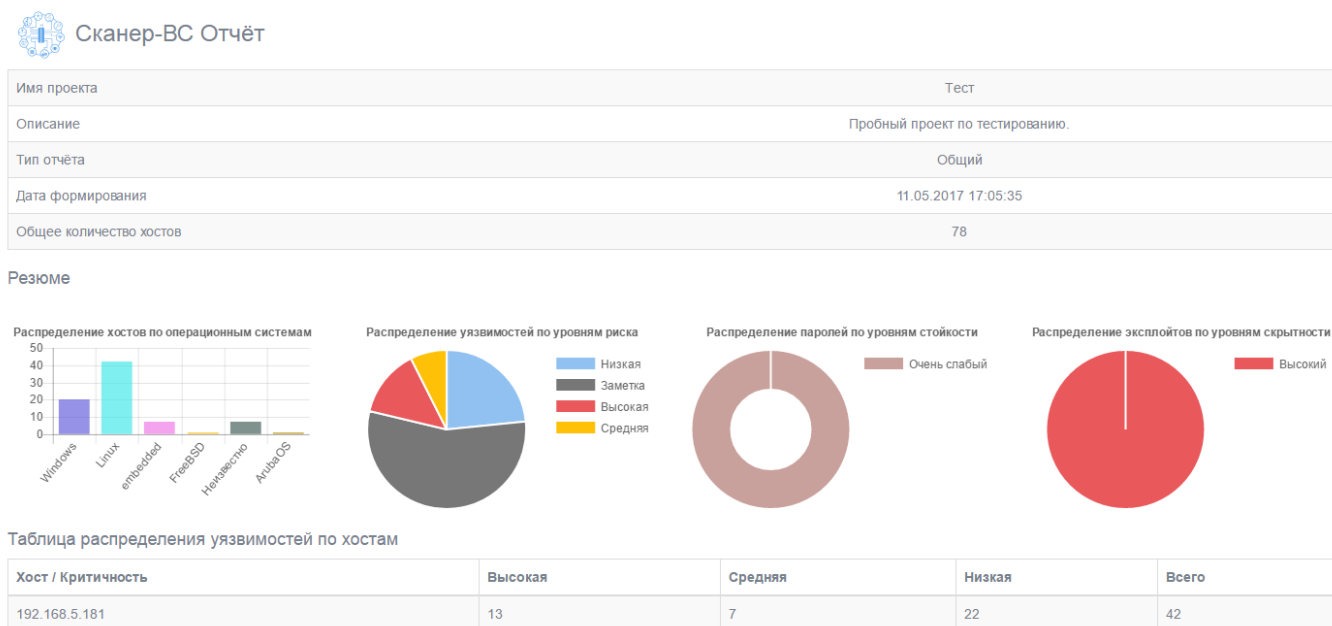


Рисунок 49 – Фрагмент отчета ПК «Сканер-ВС»

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.

3.7. Работа с инструментами

3.7.1. Средство аудита ОС Astra Linux

Средство аудита ОС Astra Linux предназначено для аудита настроек комплекса средств защиты ОС специального назначения «Astra Linux Serial Edition» по требованиям безопасности.

3.7.1.1. Запуск модуля

Модуль запускается из веб-интерфейса **Аудит ОС Astra Linux** или из подменю стартера приложений (red hat) → **Поиск уязвимостей** → **Аудит ОС Astra Linux**.

После запуска откроется окно терминала (Рисунок 50).

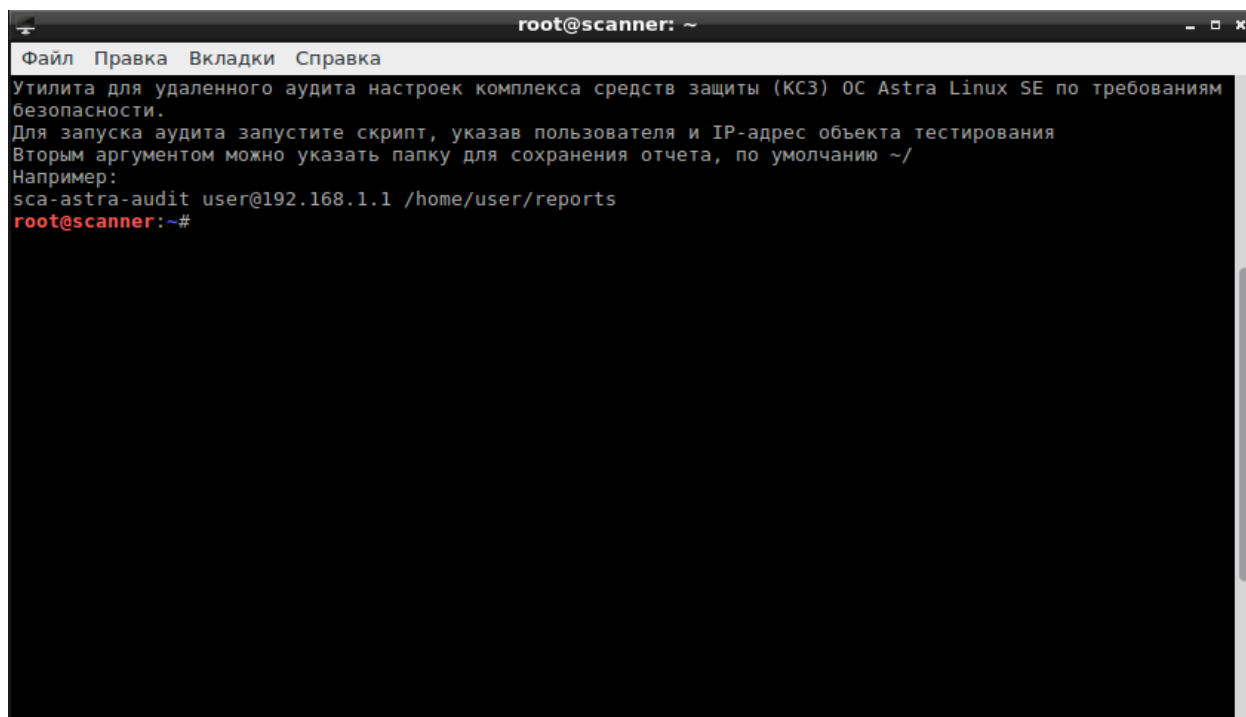


Рисунок 50 – Окно терминала

3.7.1.2. Работа с модулем

Для запуска процесса аудита, необходимо запустить скрипт на проверяемой рабочей станции. Для этого в терминале необходимо прописать команду, в которой указаны пользователь и IP-адрес тестируемой рабочей станции и нажать клавишу **Enter**. Дополнительно можно указать папку для сохранения отчета. На рисунке 51 показан пример команды запуска скрипта на рабочей станции с IP-адресом 192.168.1.57 под учетной записью пользователя root и указанной папкой root для сохранения отчета.

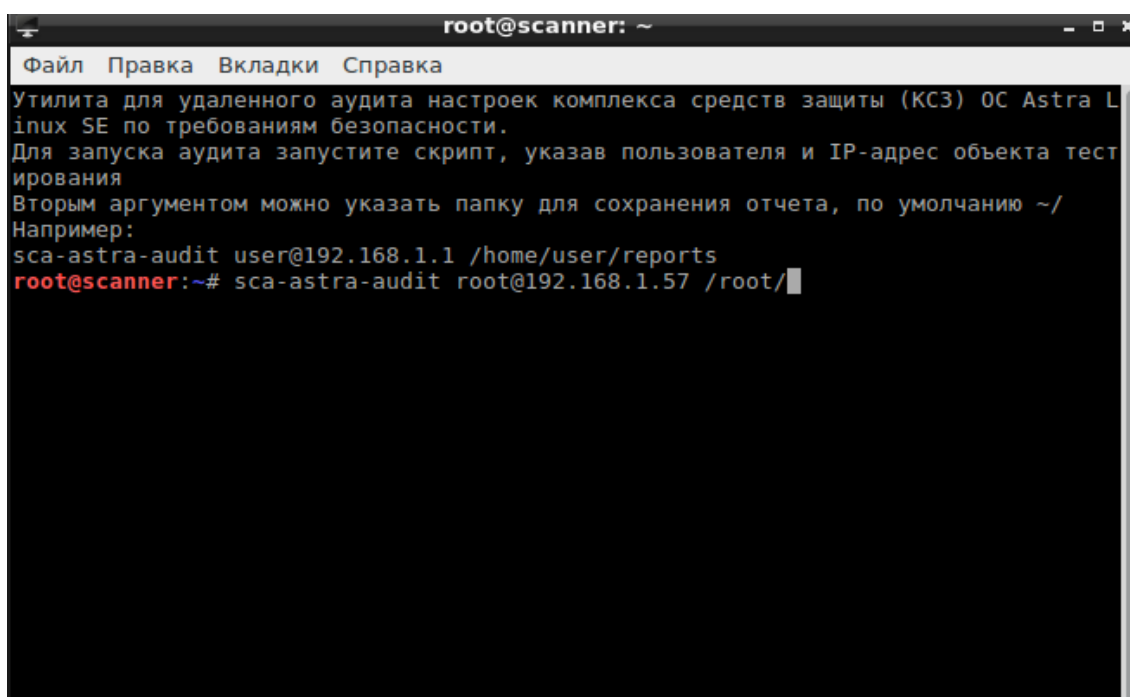
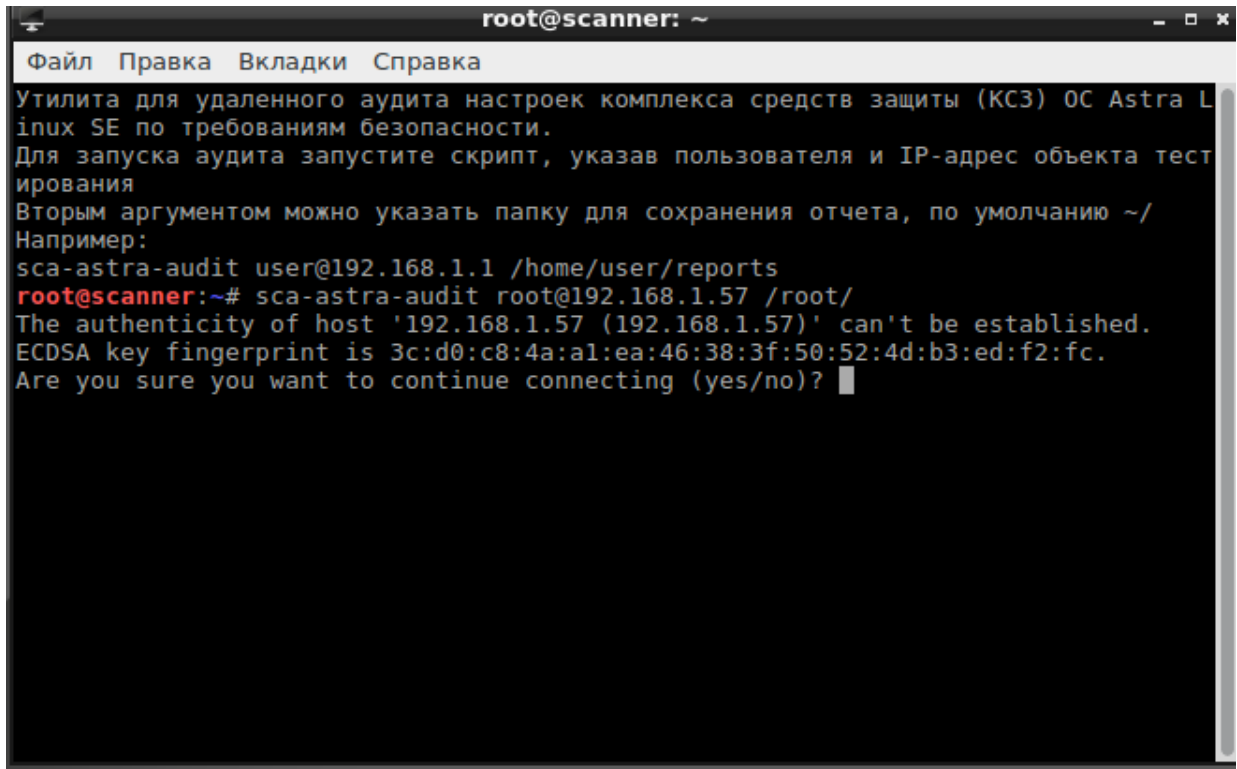


Рисунок 51 – Пример команды

В терминале будет отображено сообщение о подтверждении проведения аудита на рабочей станции, указанной в команде (Рисунок 52). Введите в терминале **yes** и нажмите клавишу **Enter**.



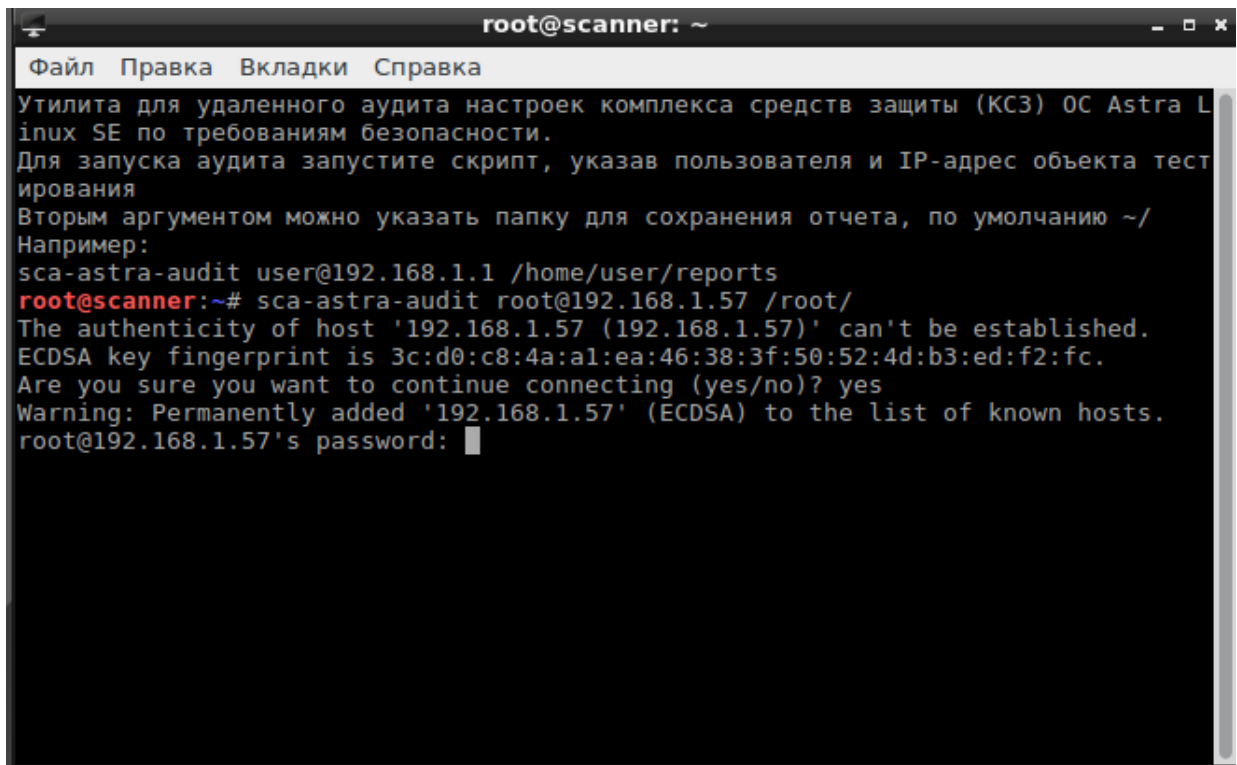
```

root@scanner: ~
Файл Правка Вкладки Справка
Утилита для удаленного аудита настроек комплекса средств защиты (КСЗ) ОС Astra Linux SE по требованиям безопасности.
Для запуска аудита запустите скрипт, указав пользователя и IP-адрес объекта тестирования
Вторым аргументом можно указать папку для сохранения отчета, по умолчанию ~/
Например:
sca-astra-audit user@192.168.1.1 /home/user/reports
root@scanner:~# sca-astra-audit root@192.168.1.57 /root/
The authenticity of host '192.168.1.57 (192.168.1.57)' can't be established.
ECDSA key fingerprint is 3c:d0:c8:4a:a1:ea:46:38:3f:50:52:4d:b3:ed:f2:fc.
Are you sure you want to continue connecting (yes/no)? █

```

Рисунок 52 – Сообщение о подтверждении

Для начала аудита необходимо указать пароль пользователя, указанного в команде (Рисунок 53). Если аудит ОС Astra Linux проводится на рабочей станции впервые, пароль будет запрошен дважды. Введите в терминале пароль и нажмите клавишу **Enter**.



```

root@scanner: ~
Файл Правка Вкладки Справка
Утилита для удаленного аудита настроек комплекса средств защиты (КСЗ) ОС Astra Linux SE по требованиям безопасности.
Для запуска аудита запустите скрипт, указав пользователя и IP-адрес объекта тестирования
Вторым аргументом можно указать папку для сохранения отчета, по умолчанию ~/
Например:
sca-astra-audit user@192.168.1.1 /home/user/reports
root@scanner:~# sca-astra-audit root@192.168.1.57 /root/
The authenticity of host '192.168.1.57 (192.168.1.57)' can't be established.
ECDSA key fingerprint is 3c:d0:c8:4a:a1:ea:46:38:3f:50:52:4d:b3:ed:f2:fc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.57' (ECDSA) to the list of known hosts.
root@192.168.1.57's password: █

```

Рисунок 53 – Сообщение о запросе пароля

В окне терминала будет показан процесс аудита (Рисунок 54).

```

root@scanner: ~
Файл  Правка  Вкладки  Справка

---[mem_test]: start test
Test PASS
---[mem_test]: stop test

---[fmac]: start test
Test PASS
---[fmac]: stop test

---[ipc_mac]: start test
Test PASS
---[ipc_mac]: stop test

---[tcpip_mac.sh]: start test
Test PASS
---[tcpip_mac.sh]: stop test

---[cap_mac]: start test
Test PASS
---[cap_mac]: stop test

The testing was succesfully completed
идет тестирование...

```

Рисунок 54 – Процесс аудита

О завершении процесса аудита в терминале будет выведено сообщение (Рисунок 55).

```

root@scanner: ~
Файл  Правка  Вкладки  Справка

Добавляется пользователь «test123» в группу «floppy» ...
Добавляется пользователь «test123» в группу «audio» ...
Добавляется пользователь «test123» в группу «video» ...
Добавляется пользователь «test123» в группу «plugdev» ...
Добавляется пользователь «test123» в группу «users» ...
Новый пароль : НЕУДАЧНЫЙ ПАРОЛЬ: основан на слове из словаря
Повторите ввод нового пароля : passwd: пароль успешно обновлён
Добавляется пользователь «test123» в группу «sudo» ...
Добавление пользователя test123 в группу sudo
Готово.
ln: не удалось создать символическую ссылку «./test.txt»: Отказано в доступе
sudo: нет tty и не указана программа askpass
tests/
tests/parsec_test.log
tests/all_errors.log
tests/postgresql.log
tests/chkconfig.log
tests/security_updates_1.5.log
tests/astra_test.sh
tests/other_tests.log
tests/netstat.log
test.tar          100% 110KB 110.0KB/s   00:01
done
root@scanner: ~#

```

Рисунок 55 – Завершение аудита

В папке, указанной для сохранения отчета, после завершения аудита будет расположен архив с файлами отчетов. Для разархивации введите в терминале команду, представленную на рисунке 56, и нажмите **Enter**.

```

root@scanner: ~
Файл Правка Вкладки Справка
Добавляется пользователь «test123» в группу «floppy» ...
Добавляется пользователь «test123» в группу «audio» ...
Добавляется пользователь «test123» в группу «video» ...
Добавляется пользователь «test123» в группу «plugdev» ...
Добавляется пользователь «test123» в группу «users» ...
Новый пароль : НЕУДАЧНЫЙ ПАРОЛЬ: основан на слове из словаря
Повторите ввод нового пароля : passwd: пароль успешно обновлён
Добавляется пользователь «test123» в группу «sudo» ...
Добавление пользователя test123 в группу sudo
Готово.
ln: не удалось создать символическую ссылку «./test.txt»: Отказано в доступе
sudo: нет tty и не указана программа askpass
tests/
tests/parsec_test.log
tests/all_errors.log
tests/postgresql.log
tests/chkconfig.log
tests/security_updates_1.5.log
tests/astra_test.sh
tests/other_tests.log
tests/netstat.log
test.tar                               100% 110KB 110.0KB/s   00:01
done
root@scanner:~# tar -xvf 192.168.1.57.tar

```

Рисунок 56 – Команда разархивации

В папке, указанной для сохранения отчета, после завершения процесса разархивации будут расположены файлы отчета (Рисунок 57).

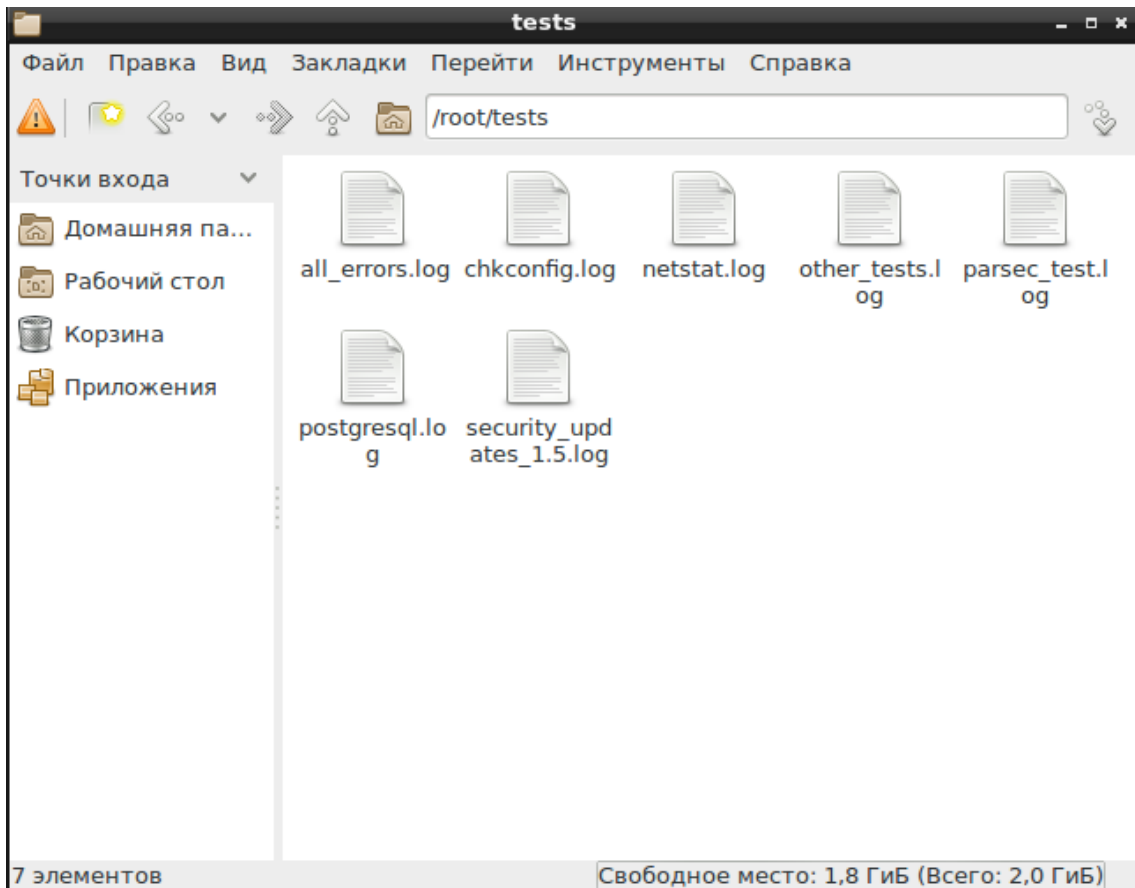


Рисунок 57 – Файлы отчетов

В файле «all_errors.log» содержится информация об обнаруженных ошибках (Рисунок 58).

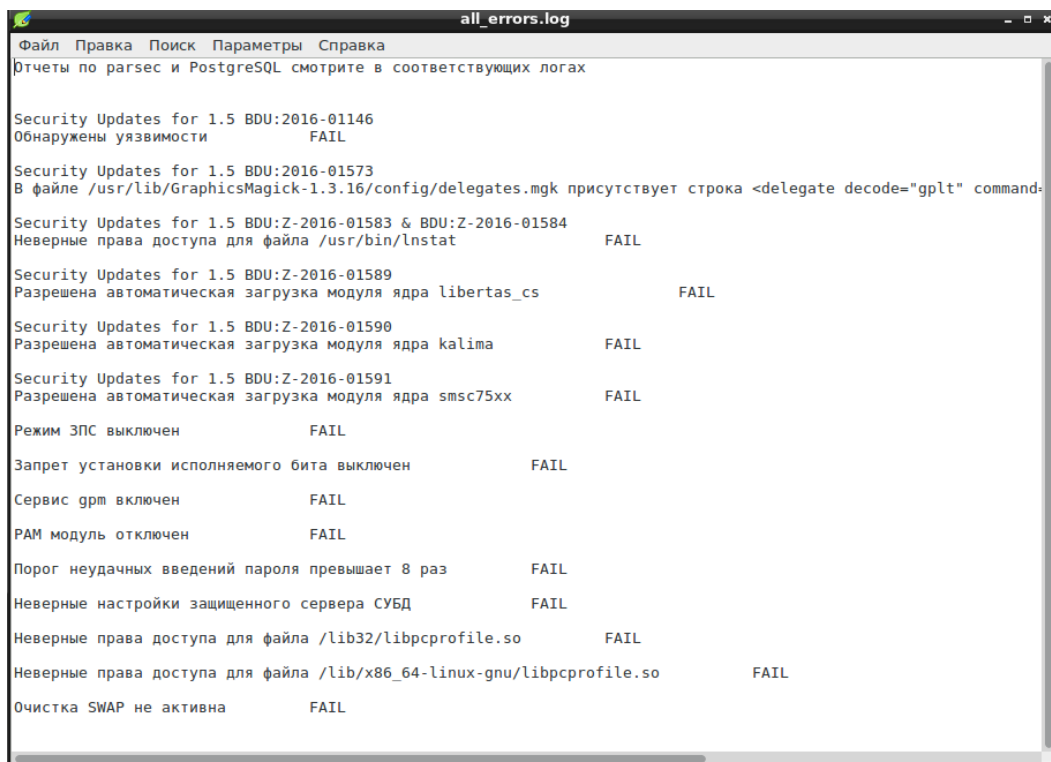


Рисунок 58 – Отчет об обнаруженных ошибках

В файле «chkconfig.log» содержится список системных служб и их состояния (Рисунок 59).

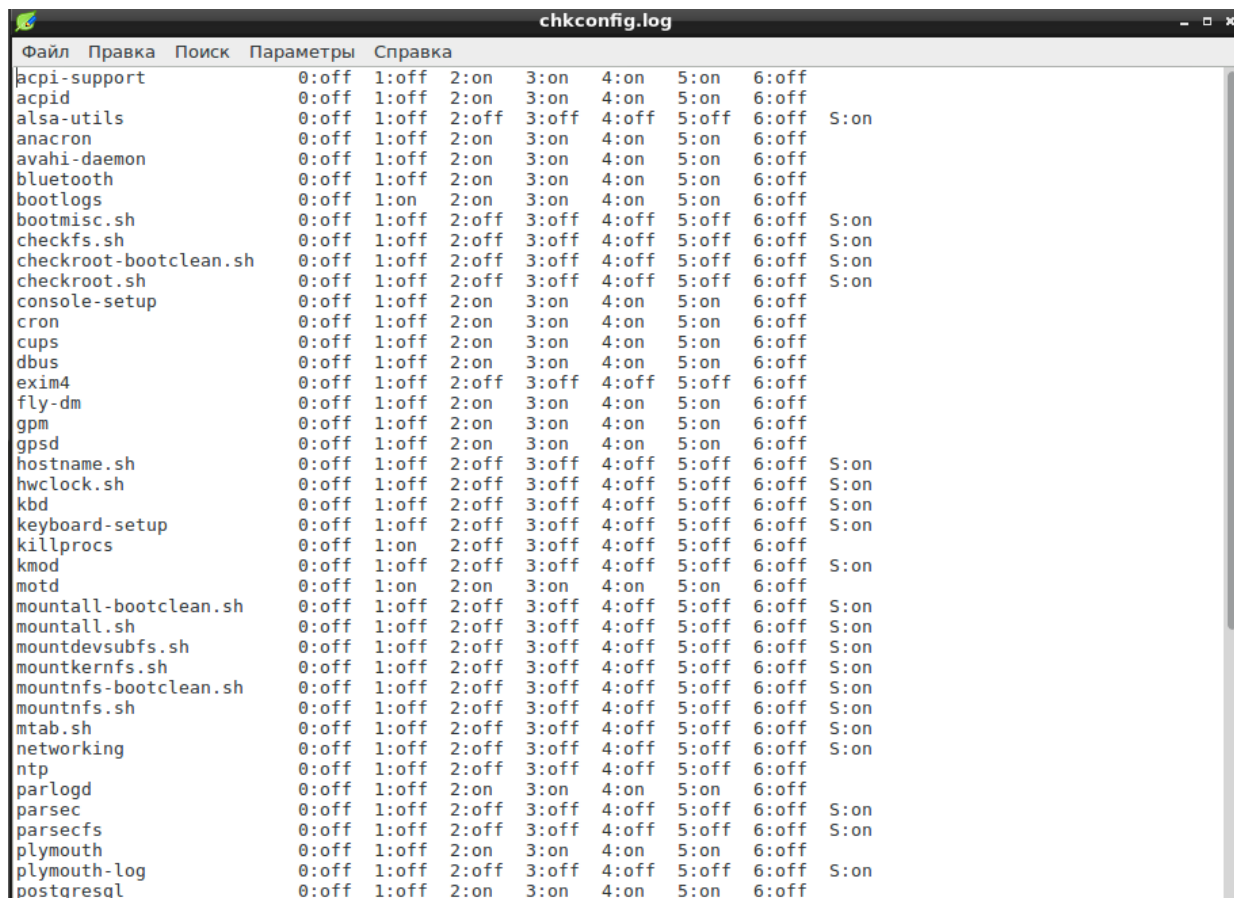
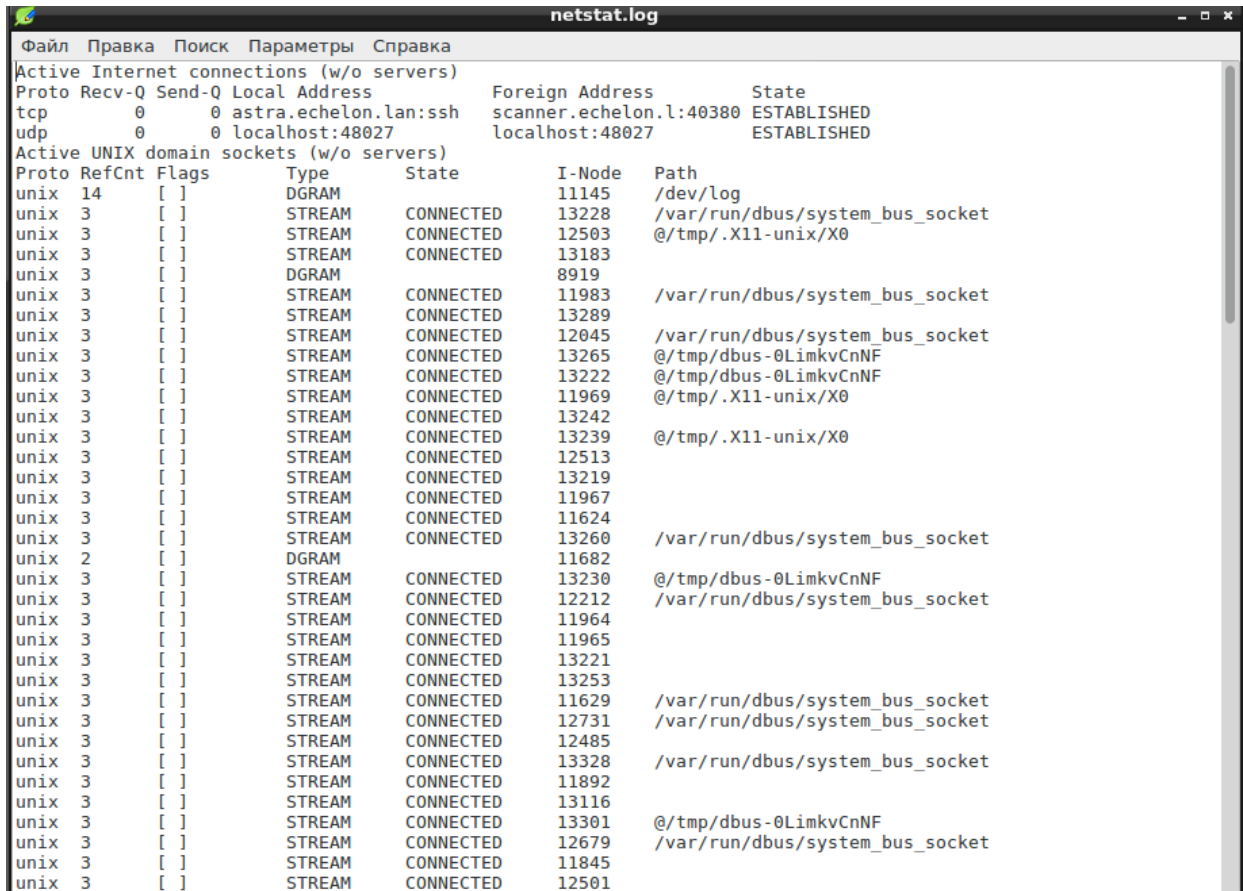


Рисунок 59 – Список системных служб

В файле «netstat.log» содержится список портов функционирующих на них процессах (Рисунок 60).



The screenshot shows a terminal window titled "netstat.log" with a menu bar (Файл, Правка, Поиск, Параметры, Справка). The content is divided into two sections: "Active Internet connections (w/o servers)" and "Active UNIX domain sockets (w/o servers)".

Active Internet connections (w/o servers)

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State |
|-------|--------|--------|-----------------------|-------------------------|-------------|
| tcp | 0 | 0 | astra.echelon.lan:ssh | scanner.echelon.l:40380 | ESTABLISHED |
| udp | 0 | 0 | localhost:48027 | localhost:48027 | ESTABLISHED |

Active UNIX domain sockets (w/o servers)

| Proto | RefCnt | Flags | Type | State | I-Node | Path |
|-------|--------|-------|--------|-----------|--------|---------------------------------|
| unix | 14 | [] | DGRAM | | 11145 | /dev/log |
| unix | 3 | [] | STREAM | CONNECTED | 13228 | /var/run/dbus/system_bus_socket |
| unix | 3 | [] | STREAM | CONNECTED | 12503 | @/tmp/.X11-unix/X0 |
| unix | 3 | [] | STREAM | CONNECTED | 13183 | |
| unix | 3 | [] | DGRAM | | 8919 | |
| unix | 3 | [] | STREAM | CONNECTED | 11983 | /var/run/dbus/system_bus_socket |
| unix | 3 | [] | STREAM | CONNECTED | 13289 | |
| unix | 3 | [] | STREAM | CONNECTED | 12045 | /var/run/dbus/system_bus_socket |
| unix | 3 | [] | STREAM | CONNECTED | 13265 | @/tmp/dbus-0LimkvCnNF |
| unix | 3 | [] | STREAM | CONNECTED | 13222 | @/tmp/dbus-0LimkvCnNF |
| unix | 3 | [] | STREAM | CONNECTED | 11969 | @/tmp/.X11-unix/X0 |
| unix | 3 | [] | STREAM | CONNECTED | 13242 | |
| unix | 3 | [] | STREAM | CONNECTED | 13239 | @/tmp/.X11-unix/X0 |
| unix | 3 | [] | STREAM | CONNECTED | 12513 | |
| unix | 3 | [] | STREAM | CONNECTED | 13219 | |
| unix | 3 | [] | STREAM | CONNECTED | 11967 | |
| unix | 3 | [] | STREAM | CONNECTED | 11624 | |
| unix | 3 | [] | STREAM | CONNECTED | 13260 | /var/run/dbus/system_bus_socket |
| unix | 2 | [] | DGRAM | | 11682 | |
| unix | 3 | [] | STREAM | CONNECTED | 13230 | @/tmp/dbus-0LimkvCnNF |
| unix | 3 | [] | STREAM | CONNECTED | 12212 | /var/run/dbus/system_bus_socket |
| unix | 3 | [] | STREAM | CONNECTED | 11964 | |
| unix | 3 | [] | STREAM | CONNECTED | 11965 | |
| unix | 3 | [] | STREAM | CONNECTED | 13221 | |
| unix | 3 | [] | STREAM | CONNECTED | 13253 | |
| unix | 3 | [] | STREAM | CONNECTED | 11629 | /var/run/dbus/system_bus_socket |
| unix | 3 | [] | STREAM | CONNECTED | 12731 | /var/run/dbus/system_bus_socket |
| unix | 3 | [] | STREAM | CONNECTED | 12485 | |
| unix | 3 | [] | STREAM | CONNECTED | 13328 | /var/run/dbus/system_bus_socket |
| unix | 3 | [] | STREAM | CONNECTED | 11892 | |
| unix | 3 | [] | STREAM | CONNECTED | 13116 | |
| unix | 3 | [] | STREAM | CONNECTED | 13301 | @/tmp/dbus-0LimkvCnNF |
| unix | 3 | [] | STREAM | CONNECTED | 12679 | /var/run/dbus/system_bus_socket |
| unix | 3 | [] | STREAM | CONNECTED | 11845 | |
| unix | 3 | [] | STREAM | CONNECTED | 12501 | |

Рисунок 60 – Список портов и процессов

В файле «other_tests.log» содержится информация о результатах прочих тестов аудита безопасности ОС Astra Linux (Рисунок 61).

```

other_tests.log
Файл Правка Поиск Параметры Справка
Версия ОС Astra Linux SE: SE 1.5 (smolensk), версия ядра: 4.2.0-23-generic

Версия ОС Astra Linux SE: SE 1.5 (smolensk), версия ядра: 4.2.0-23-generic

Аутентификация работает OK
Запрет на доступ работает OK
Создание символических ссылок запрещено OK
Режим ЗПС выключен FAIL
Запрет установки исполняемого бита выключен FAIL
Пароль на изменение настроек GRUB существует OK
Аутентификация сервера печати не отключена OK
Демон SSH включен
Удаленный вход по XDMCP разрешен
localhost #any host can get a login window
* CHOOSEER BROADCAST #any indirect host can get a chooser
Сервис grm включен FAIL
РАМ модуль отключен FAIL
Порог неудачных введений пароля превышает 8 раз FAIL
Неверные настройки защищенного сервера СУБД FAIL
Контроль целостности КСЗ активен OK
afick report_syslog выключен
Неверные права доступа для файла /lib32/libpcprofile.so FAIL
Неверные права доступа для файла /lib/x86_64-linux-gnu/libpcprofile.so FAIL
Очистка SWAP не активна FAIL
Аутентификация доступа не отключена OK
Отсутствует файл /etc/security/pam_mount.conf.xml

```

Рисунок 61 – Список портов и служб

В файле «parsec_test.log» содержится информация о результатах тестирования подсистемы безопасности PARSEC (Рисунок 62).

```

parsec_test.log
Файл Правка Поиск Параметры Справка

---[audit_file.sh]: start test
Запуск системы протоколирования УСПЕШНО
# Проверка системы протоколирования
Установка параметров флагов аудита для каталога /tmp/tmp/file-10369... УСПЕШНО
Установка флагов аудита для файла /tmp/file-10369... УСПЕШНО
Создание события аудита open /tmp/file-10369... УСПЕШНО
Создание события аудита chmod /tmp/file-10369... УСПЕШНО
Создание события аудита chown /tmp/file-10369... УСПЕШНО
Создание события аудита setfacl /tmp/file-10369... УСПЕШНО
Создание события аудита setfacl /tmp/file-10369... УСПЕШНО
Создание события аудита parsec_chmac /tmp/file-10369... УСПЕШНО
Создание события аудита exec /tmp/file-10369... УСПЕШНО
Создание события аудита unlink /tmp/file-10369... УСПЕШНО
Остановка службы протоколирования... УСПЕШНО
Удаление флагов аудита с каталога /tmp... УСПЕШНО
Поиск событий open в журнале...
УСПЕШНО
Поиск событий exec в журнале...
УСПЕШНО
Поиск событий unlink в журнале...
УСПЕШНО
Поиск событий chmod в журнале...
УСПЕШНО
Поиск событий chown в журнале...
УСПЕШНО
Поиск событий setfacl в журнале...
УСПЕШНО
Поиск событий audit в журнале...
УСПЕШНО
Поиск событий mac в журнале...
УСПЕШНО
Поиск событий create в журнале...
УСПЕШНО
Запуск системы протоколирования УСПЕШНО
Тест PASS
---[audit_file.sh]: stop test

---[audit_proc.sh]: start test
подготовка к тестам
добавление пользователя и выставление флагов аудита

```

Рисунок 62 – Результат аудита

В файле «postgresql.log» содержатся результаты тестирования комплекса средств защиты системы управления базами данных PostgreSQL (Рисунок 63).

```

postgresql.log
Файл  Правка  Поиск  Параметры  Справка
Подготовка к выполнению тестов СУБД PostgreSQL
Создание тестовых пользователей...
Создание пользователя u_0_00 с мандатной меткой {0,0}
минимальный уровень:    Уровень_0(0)
максимальный уровень:  Уровень_0(0)
минимальная категория: Нет(0)
максимальная категория: Нет(0)
Создание пользователя u2_0_00 с мандатной меткой {0,0}
минимальный уровень:    Уровень_0(0)
максимальный уровень:  Уровень_0(0)
минимальная категория: Нет(0)
максимальная категория: Нет(0)
Создание пользователя u_0_01 с мандатной меткой {0,1}
минимальный уровень:    Уровень_0(0)
максимальный уровень:  Уровень_0(0)
минимальная категория: Категория_1(1)
максимальная категория: Категория_1(1)
Создание пользователя u_1_01 с мандатной меткой {1,1}
минимальный уровень:    Уровень_1(1)
максимальный уровень:  Уровень_1(1)
минимальная категория: Категория_1(1)
максимальная категория: Категория_1(1)
Создание пользователя u_0_10 с мандатной меткой {0,2}
минимальный уровень:    Уровень_0(0)
максимальный уровень:  Уровень_0(0)
минимальная категория: Категория_2(2)
максимальная категория: Категория_2(2)
Создание пользователя u_1_10 с мандатной меткой {1,2}
минимальный уровень:    Уровень_1(1)
максимальный уровень:  Уровень_1(1)
минимальная категория: Категория_2(2)
максимальная категория: Категория_2(2)
Создание пользователя u_1_11 с мандатной меткой {1,3}
минимальный уровень:    Уровень_1(1)
максимальный уровень:  Уровень_1(1)
минимальная категория: Категория_1,Категория_2(3)
максимальная категория: Категория_1,Категория_2(3)
Создание пользователя u2_1_11 с мандатной меткой {1,3}
минимальный уровень:    Уровень_1(1)
максимальный уровень:  Уровень_1(1)
минимальная категория: Категория_1,Категория_2(3)

```

Рисунок 63 – Результаты тестирования

В файле «security_updates_1.5.log» содержится информация о результатах аудита по методическим указаниям по нейтрализации угроз эксплуатации уязвимостей ОС специального назначения «Astra Linux Special Edition» (версия 1.5) в информационных системах (Рисунок 64).


```

security_updates_1.5.log
Файл Правка Поиск Параметры Справка
Уязвимость BDU:2016-01146
Пакет imagemagick установлен
В файле /etc/ImageMagick/policy.xml отсутствует строка <policy domain="coder" rights="none" pattern="EPHEMERAL" />
В файле /etc/ImageMagick/policy.xml отсутствует строка <policy domain="coder" rights="none" pattern="HTTPS" />
В файле /etc/ImageMagick/policy.xml отсутствует строка <policy domain="coder" rights="none" pattern="MVG" />
В файле /etc/ImageMagick/policy.xml отсутствует строка <policy domain="coder" rights="none" pattern="MSL" />
В файле /etc/ImageMagick/policy.xml отсутствует строка <policy domain="coder" rights="none" pattern="FTP" />
Обнаружены уязвимости FAIL

Уязвимость BDU:2016-01573
В файле /usr/lib/GraphicsMagick-1.3.16/config/delegates.mgk присутствует строка <delegate decode="gplt" command-

Уязвимость BDU:Z-2016-01583 & BDU:Z-2016-01584
Неверные права доступа для файла /usr/bin/lnstat FAIL

Уязвимость BDU:Z-2016-01585
Пакет grpsd-clients установлен
Уязвимости не обнаружены OK

Уязвимость BDU:Z-2016-01586
Пакет sresch-tools установлен
Уязвимости не обнаружены OK

Уязвимость BDU:Z-2016-01587
Пакет texlive-binaries установлен
Уязвимости не обнаружены OK


Уязвимость BDU:Z-2016-01588
Пакет firebird2.5-classic-common установлен
Уязвимости не обнаружены OK

Уязвимость BDU:Z-2016-01589
Разрешена автоматическая загрузка модуля ядра libertas_cs FAIL

```

Рисунок 64 – Результаты аудита

3.7.1.3. Завершение работы с модулем

Для завершения работы нажмите  в верхнем правом углу терминала.

3.7.2. Средство локального аудита паролей

Средство локального аудита паролей предназначено для поиска и выявления на локальной рабочей станции неустойчивых к взлому паролей.

3.7.2.1. Запуск модуля

Модуль запускается из веб-интерфейса **Локальный аудит паролей** или из подменю стартера приложений (red hat) → **Атаки на пароли** → **Локальный аудит паролей**.

После запуска появится рабочее окно средства локального аудита паролей (Рисунок 65).

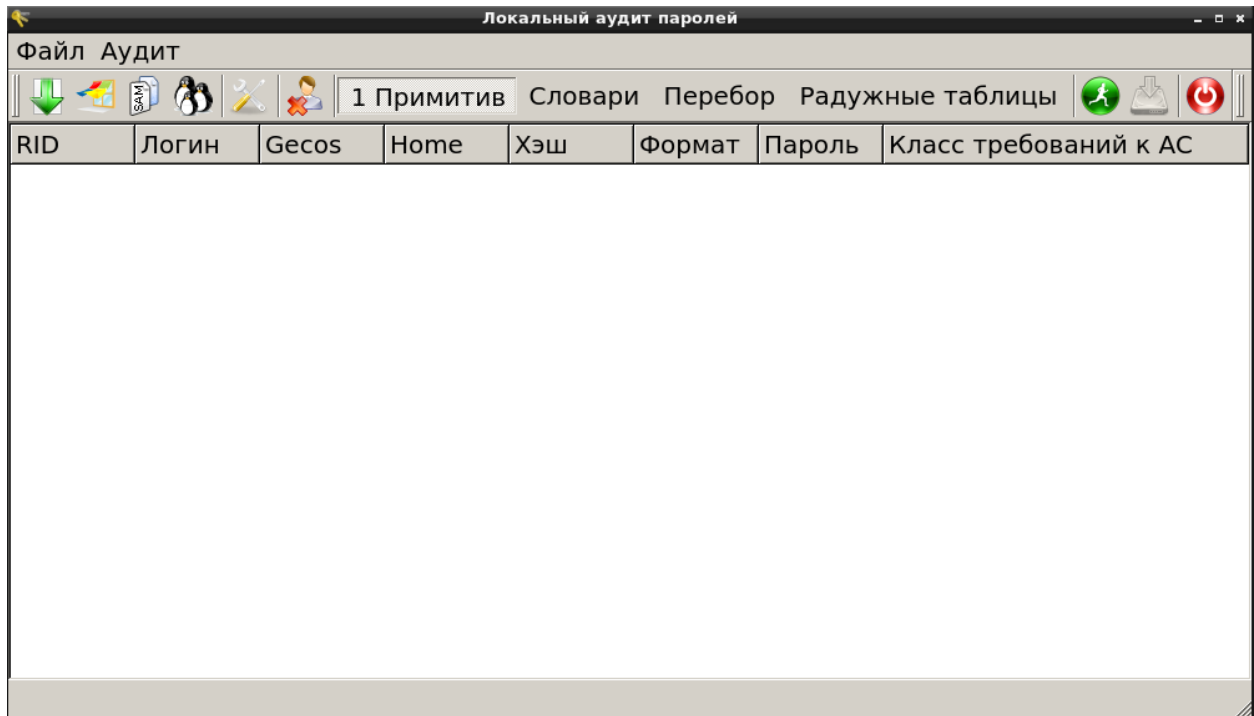


Рисунок 65 — Рабочее окно модуля

3.7.2.2. Работа с модулем

Для аудита необходимо импортировать файл с хешами паролей.

Для ОС семейства Microsoft Windows необходимо в подменю **Файл** → **Импорт из SAM** → **указать папку Windows** либо **указать непосредственно SAM файл**.

Для ОС семейства Linux необходимо в подменю **Файл** → **Импорт из shadow** – указать каталог **/etc/**.

Импорт файлов, находящихся вне директорий по умолчанию, настраивается из подменю **Файл** → **Импорт из файла** (Рисунок 66).

Примечание. Сопутствующие файлы SYSTEM (для ОС Windows), password (для ОС Linux) должны быть расположены в одном каталоге с файлами SAM и shadow соответственно.

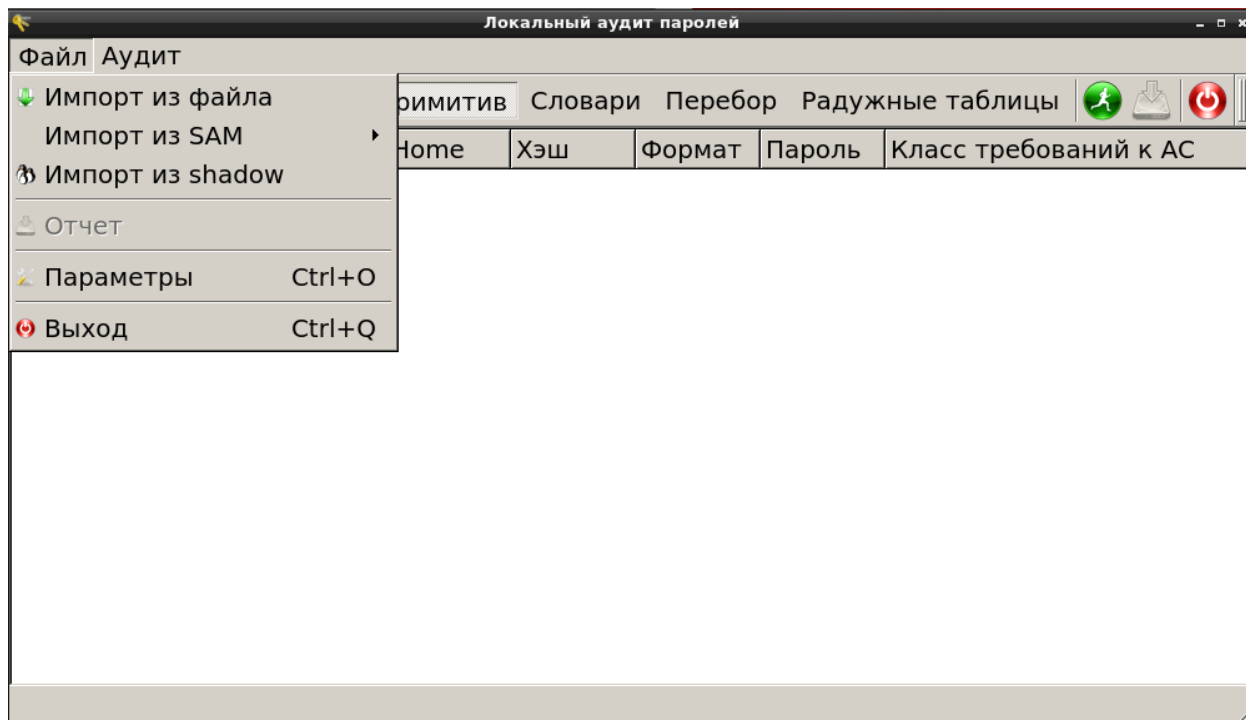


Рисунок 66 — Меню «Файл»

Импортировать файлы с хешами паролей можно при помощи кнопок, расположенных на панели инструментов модуля:



- импорт из файла,



- импорт из SAM с указанием папки Windows,



- импорт из SAM с непосредственным указанием файла,



- импорт из shadow.

Перед запуском процедуры аудита необходимо в подменю **Аудит** указать методы, с помощью которых будет осуществляться анализ (Рисунок 67). Эти методы можно выбрать и на панели инструментов модуля.

Метод аудита, основанный на поиске по примитивам, предполагает режим работы, при котором на предмет возможного пароля проверяется известная информация о пользователе. Например, идентификатор пользователя, логин, значения поля Gecos.

Поле Gecos (Рисунок 65) содержит вспомогательную информацию: номер телефона, адрес, полное имя пользователя и т.п.

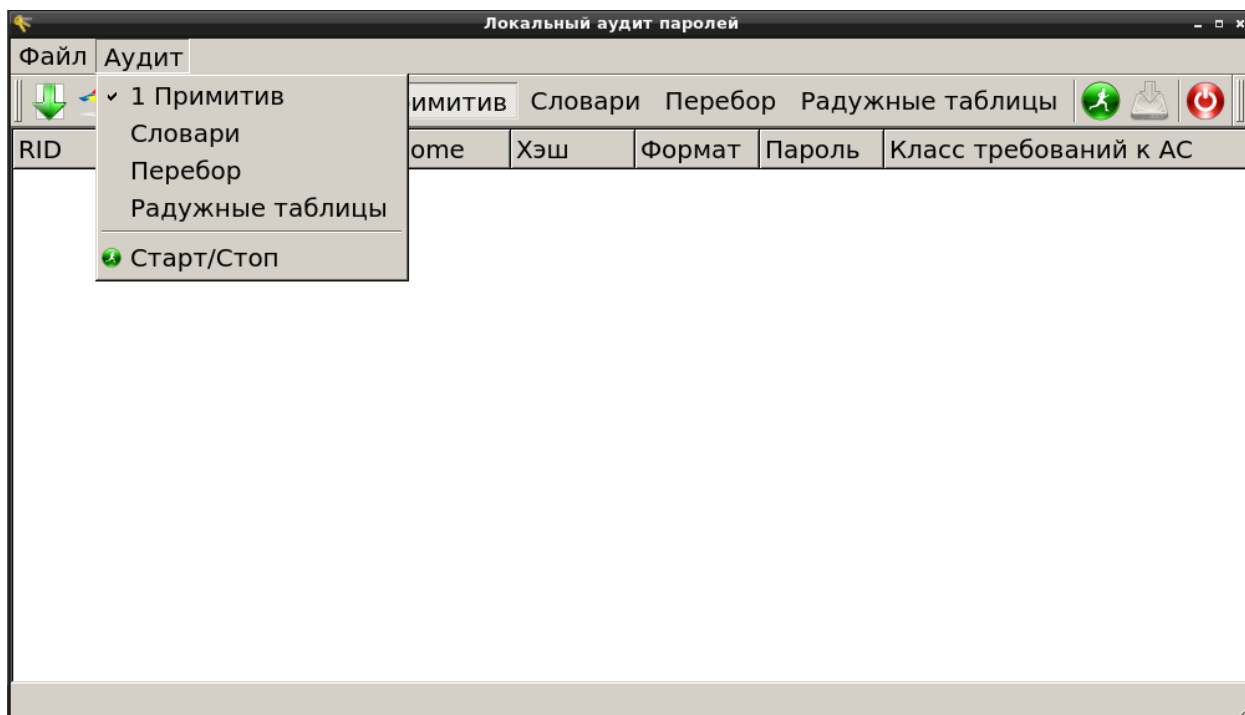


Рисунок 67 — Меню «Аудит»

Словари и наборы символов, которые будут использованы для последовательного перебора паролей, настраиваются в подменю **Файл** → **Параметры** (Рисунок 68). Окно **Параметры** можно

вызвать, нажав на кнопку  на панели инструментов модуля.

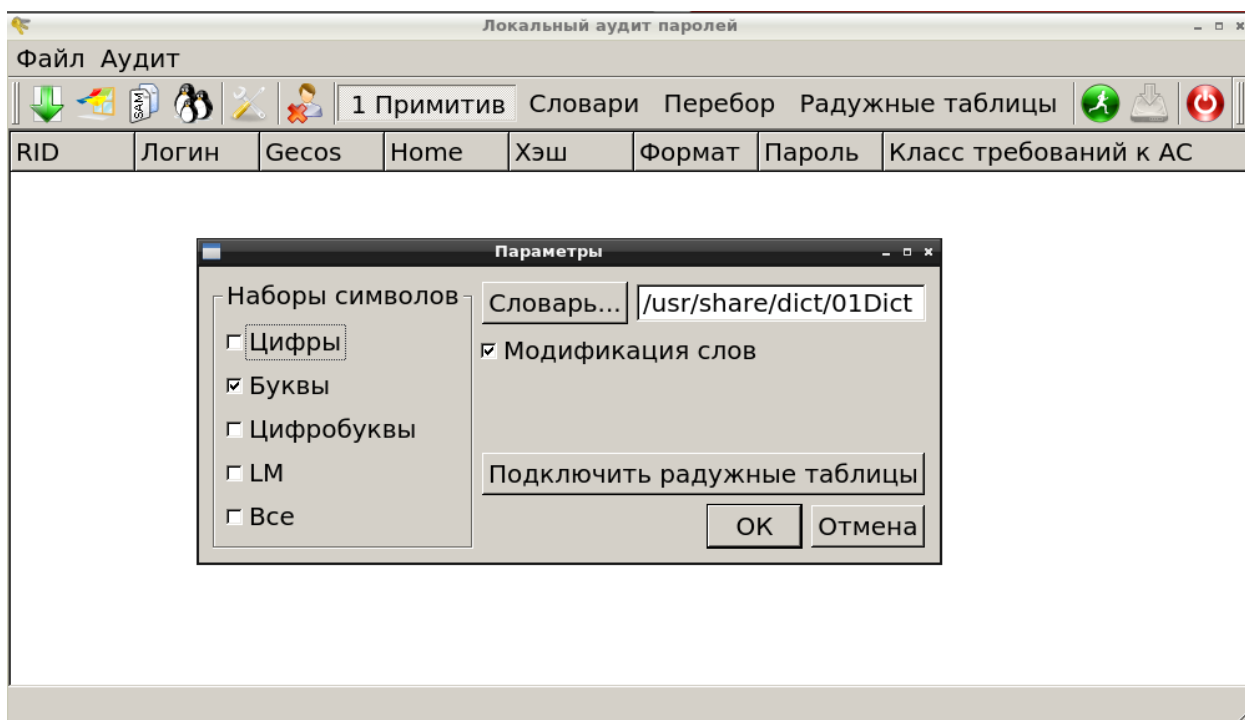




Рисунок 68 — Окно «Параметры»

Для запуска процедуры аудита необходимо нажать **Старт/Стоп** в меню **Аудит** (Рисунок 67) или воспользоваться кнопкой . Процесс анализа может быть остановлен в любой момент с помощью повторного нажатия **Аудит** → **Старт/Стоп**.

Результатом работы модуля является список с именами пользователей, не имеющих пароль, а также именами пользователей и паролей, являющихся неустойчивыми к взлому.

Для сохранения отчета нужно выбрать **Файл** → **Отчет** или нажать на кнопку  на панели инструментов модуля. В открывшемся окне необходимо выбрать путь для сохранения файла отчета (Рисунок 69).

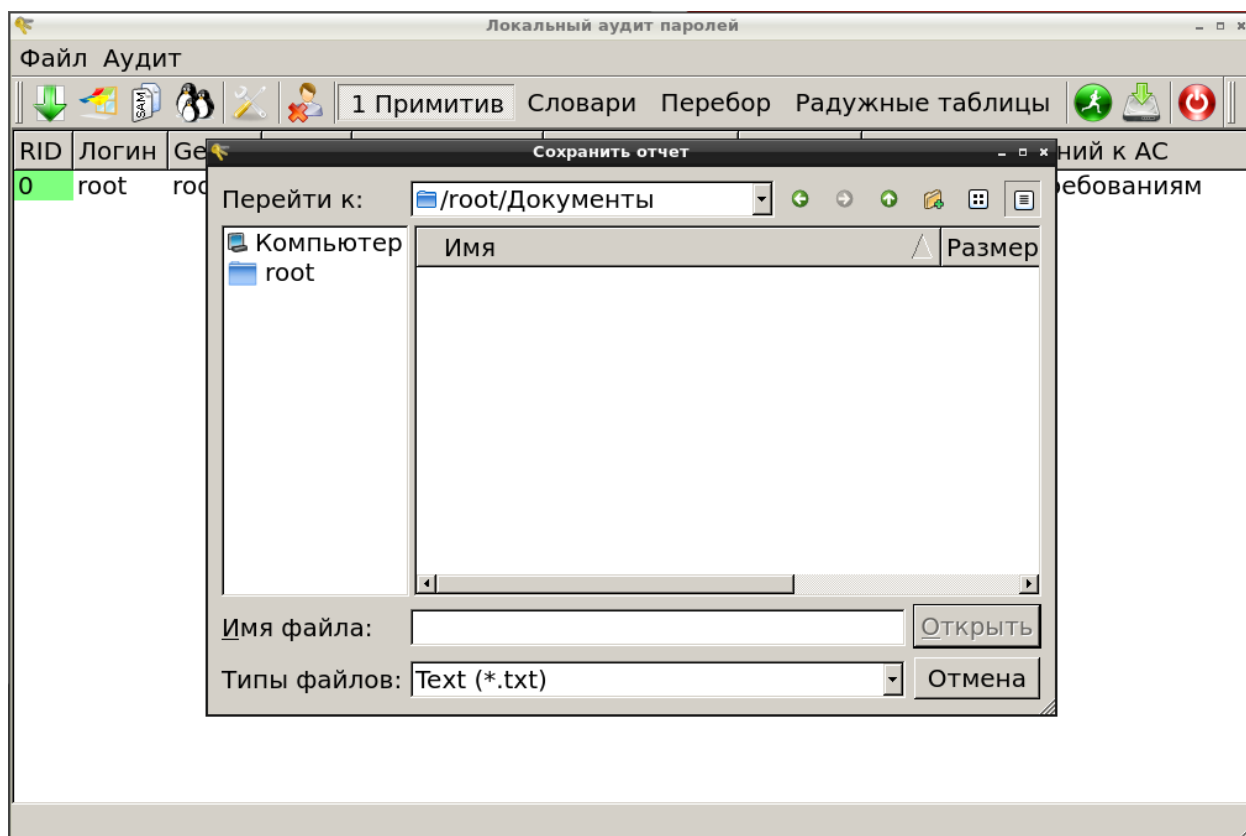



Рисунок 69 — Сохранение отчета

3.7.2.3. Завершение работы с модулем

Для выхода из модуля необходимо воспользоваться подменю **Файл** → **Выход** или нажать кнопку .

3.7.3. Средство поиска остаточной информации

Средство поиска остаточной информации предназначено для поиска по ключевым словам на запоминающем устройстве удаленных данных.

3.7.3.1. Запуск модуля

Модуль запускается из веб-интерфейса **Поиск остаточной информации** или из подменю стартера приложений (red hat) → **Остальные приложения** → **Прочие** → **Поиск остаточной информации**.

После запуска средства поиска остаточной информации откроется рабочее окно модуля (Рисунок 70).

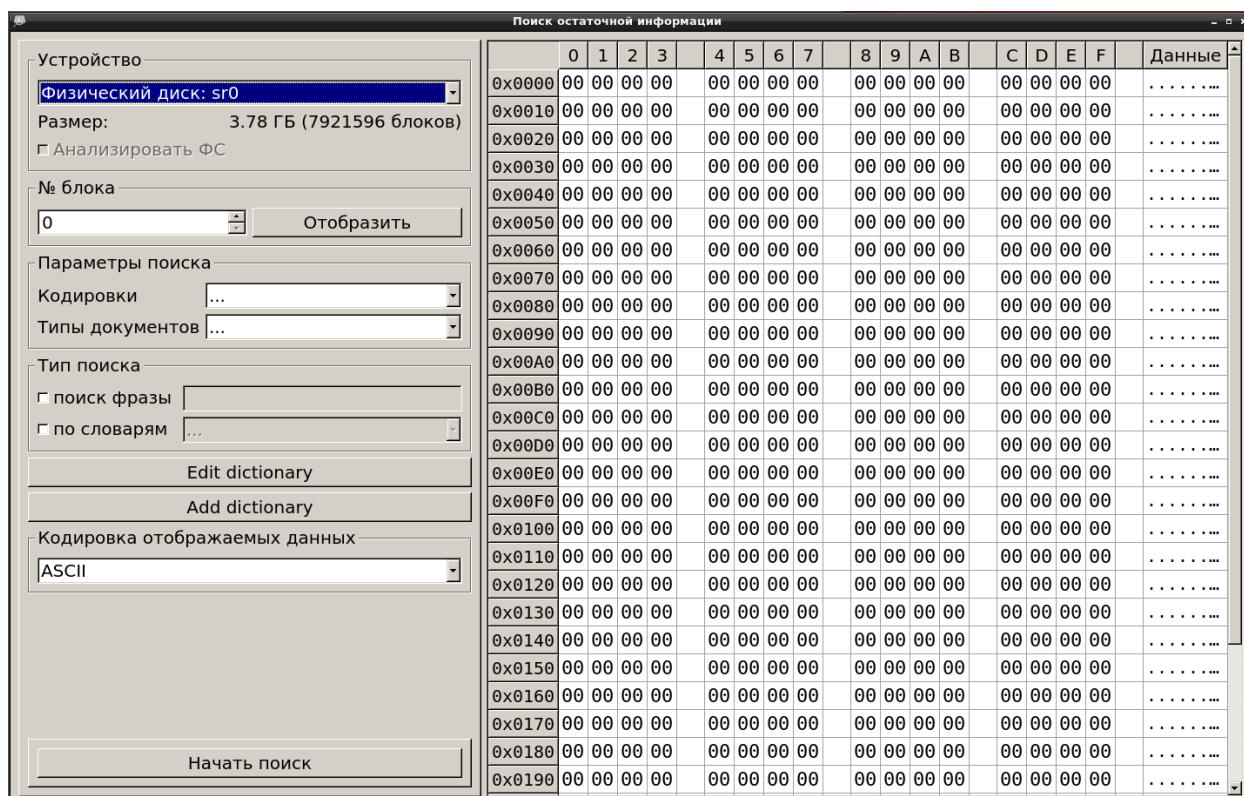


Рисунок 70 — Рабочее окно модуля

3.7.3.2. Работа с модулем

Для поиска остаточной информации необходимо в левой части рабочего окна модуля указать устройство, анализ которого будет производиться, фразу для поиска и при необходимости другие параметры.

Для запуска процесса поиска остаточной информации необходимо нажать **Начать поиск**. Процесс поиска может быть приостановлен нажатием на кнопку **Приостановить**.

Результаты поиска остаточной информации выводятся в виде списка, содержащего номер блока и величину смещения (Рисунок 71). Для просмотра найденной информации необходимо дважды нажать левой кнопкой мыши на интересующем секторе. При этом в рабочем окне модуля будет показана информация о выбранном секторе и выделено найденное слово (Рисунок 72).

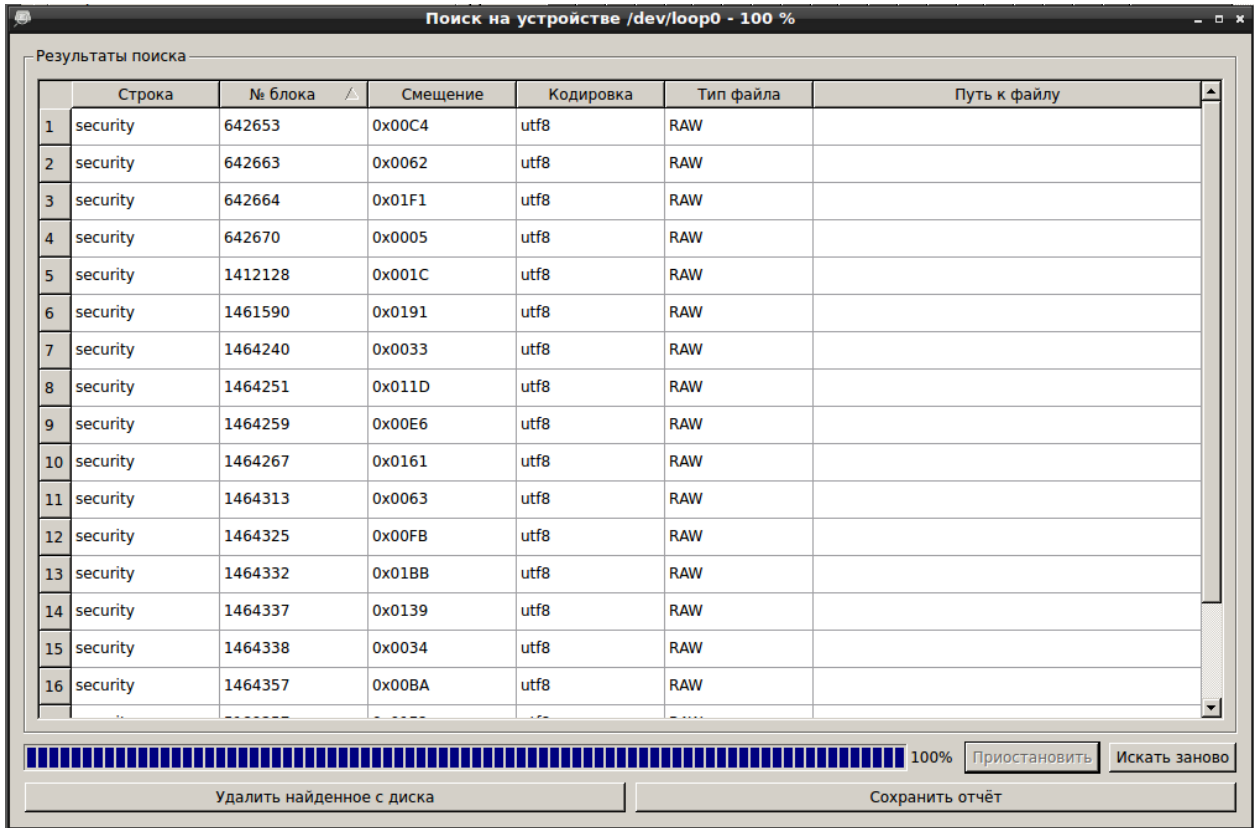


Рисунок 71 — Общие результаты поиска

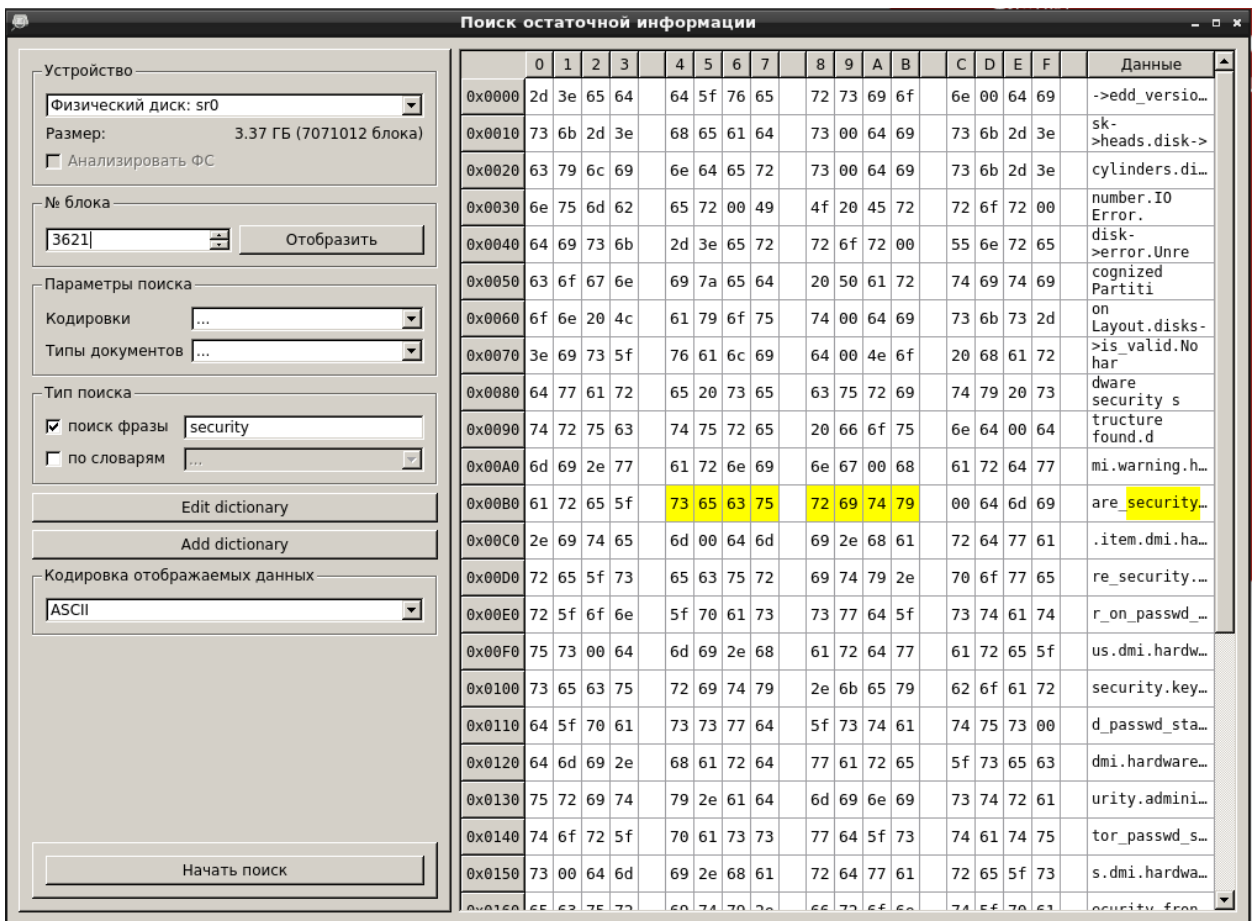


Рисунок 72 — Найденное слово в блоке № 3621

Примечание. В силу особенностей файловых систем возможно некорректное отображение информации, удовлетворяющей условиям поиска.

Оператор может сохранить полученный отчет, нажав на кнопку **Сохранить отчет** (Рисунок 71). В появившемся окне необходимо указать формат и директорию сохранения отчета (Рисунок 73).

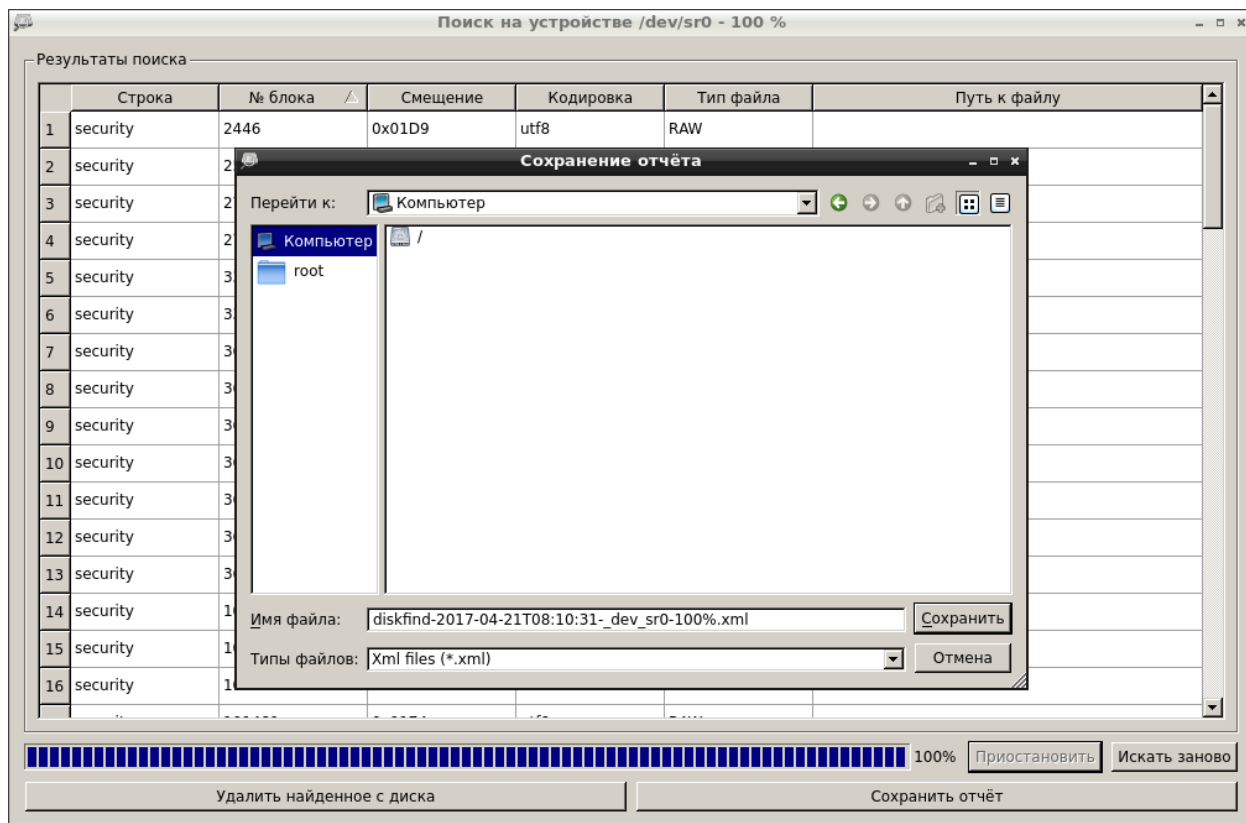


Рисунок 73 — Сохранение отчета

Для удаления найденной информации необходимо нажать **Удалить найденное с диска** (Рисунок 71). Перед удалением появится сообщение с предупреждением (Рисунок 74).

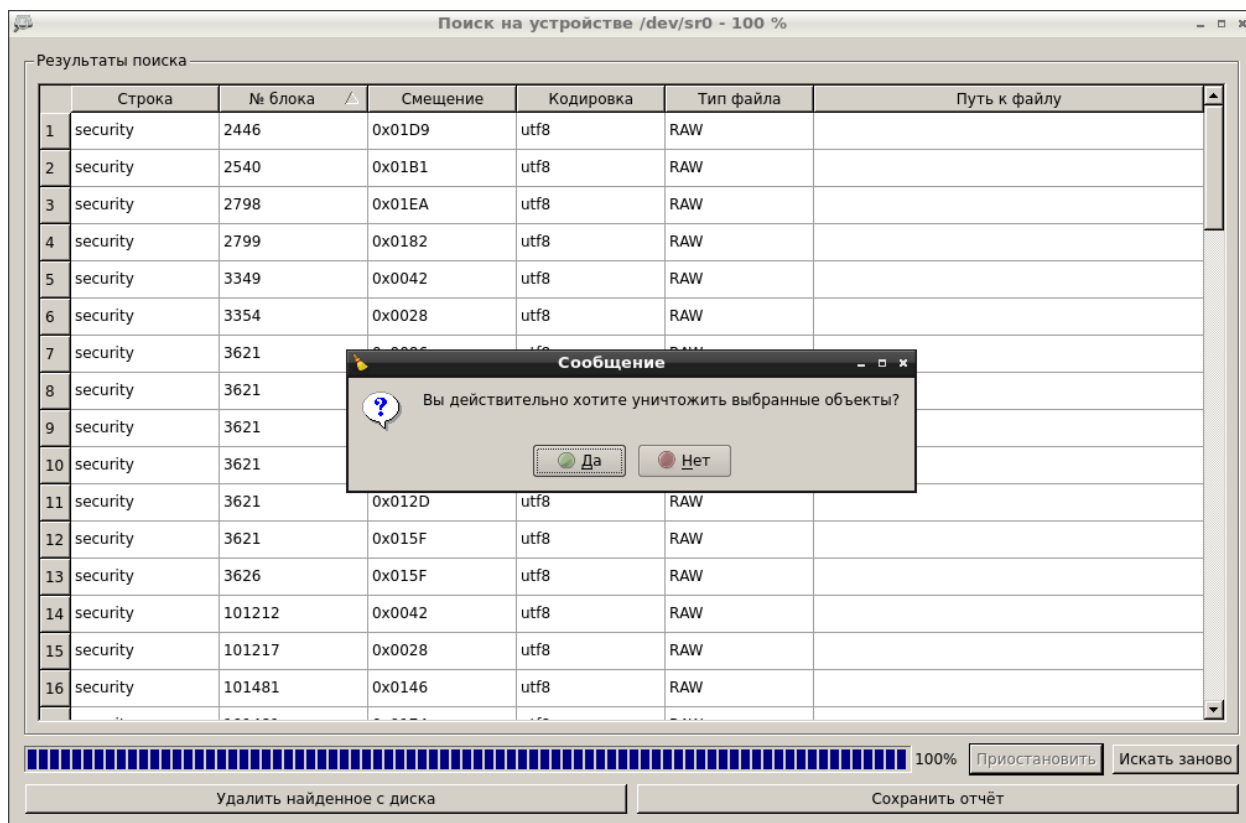


Рисунок 74 — Сообщение

3.7.3.3. Завершение работы с модулем

Для выхода из модуля необходимо нажать  в верхнем правом углу рабочего окна.

3.7.4. Средство аудита обновлений ОС Windows

3.7.4.1. Запуск модуля

Модуль запускается из веб-интерфейса **Аудит обновлений ОС Windows** или из подменю стартера приложений (red hat) → **Поиск уязвимостей** → **Аудит обновлений ОС Windows**.

После запуска средства аудита обновлений ОС Windows откроется рабочее окно модуля (Рисунок 75).

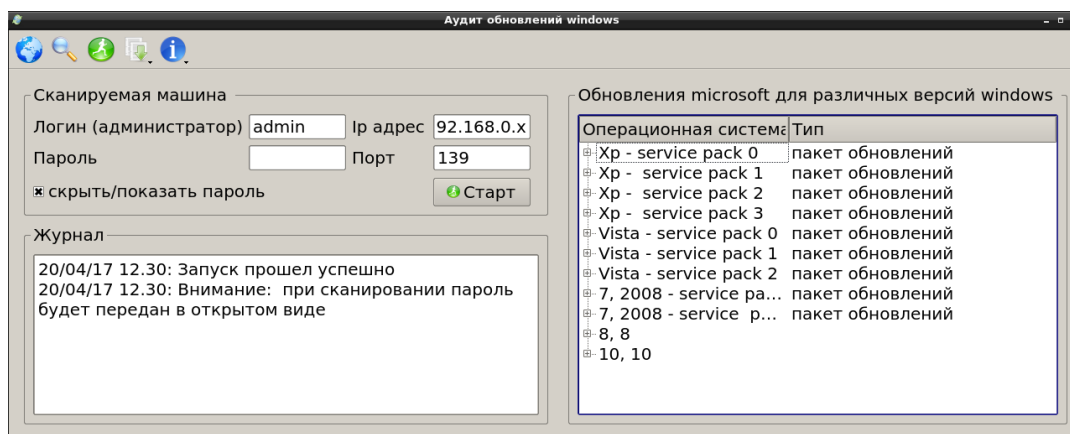


Рисунок 75 — Рабочее окно модуля

3.7.4.2. Работа с модулем

В рабочем окне модуля необходимо указать имя пользователя и пароль, порт и IP-адрес проверяемой машины.

Примечание. При наличии средств антивирусной защиты необходимо убедиться, что они не блокируют доступ по указанному порту.

Проверить состояние порта можно, например, в командной строке с помощью утилиты netstat: команда **netstat -a** (Рисунок 76).

```

Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

C:\Users\Jane>netstat -a

Активные подключения

Имя      Локальный адрес      Внешний адрес      Состояние
TCP      0.0.0.0:135          production:0      LISTENING
TCP      0.0.0.0:445          production:0      LISTENING
TCP      0.0.0.0:5357         production:0      LISTENING
TCP      0.0.0.0:8834         production:0      LISTENING
TCP      0.0.0.0:49152        production:0      LISTENING
TCP      0.0.0.0:49153        production:0      LISTENING
TCP      0.0.0.0:49154        production:0      LISTENING
TCP      0.0.0.0:49155        production:0      LISTENING
TCP      0.0.0.0:49156        production:0      LISTENING
TCP      0.0.0.0:49161        production:0      LISTENING
TCP      0.0.0.0:55126        production:0      LISTENING
TCP      127.0.0.1:1241       production:0      LISTENING
TCP      127.0.0.1:5939       production:0      LISTENING
TCP      127.0.0.1:49216     nair:49217       ESTABLISHED
TCP      127.0.0.1:49217     nair:49216       ESTABLISHED
TCP      127.0.0.1:49222     nair:49223       ESTABLISHED
TCP      127.0.0.1:17223     nair:17222       ESTABLISHED
TCP      192.168.5.89:139    production:0      LISTENING
TCP      192.168.5.89:55647  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55737  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55758  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55778  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55782  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55783  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55786  192.168.0.6:3128 TIME_WAIT
TCP      192.168.5.89:55789  192.168.0.6:3128 TIME_WAIT
TCP      192.168.5.89:55790  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55794  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55797  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55798  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55799  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55800  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55803  192.168.0.6:3128 TIME_WAIT
TCP      192.168.5.89:55804  192.168.0.6:3128 ESTABLISHED
TCP      192.168.5.89:55805  192.168.0.6:3128 ESTABLISHED
TCP      [::]:135            production:0      LISTENING
TCP      [::]:445            production:0      LISTENING

```


Рисунок 76 — Проверка состояния порта

Затем необходимо запустить сканирование с помощью кнопки **Старт** или из панели

инструментов с помощью кнопки  .

Процесс сканирования отображается в окне **Журнал** (Рисунок 77), список доступных обновлений — в окне **Обновления Microsoft для различных версий Windows**.

После завершения сканирования в окне **Журнал** появится список неустановленных обновлений (Рисунок 77).

Сохранить результаты можно с помощью кнопки  на панели инструментов. При нажатии на эту кнопку появится окно (Рисунок 78), в котором необходимо указать папку для сохранения отчета.

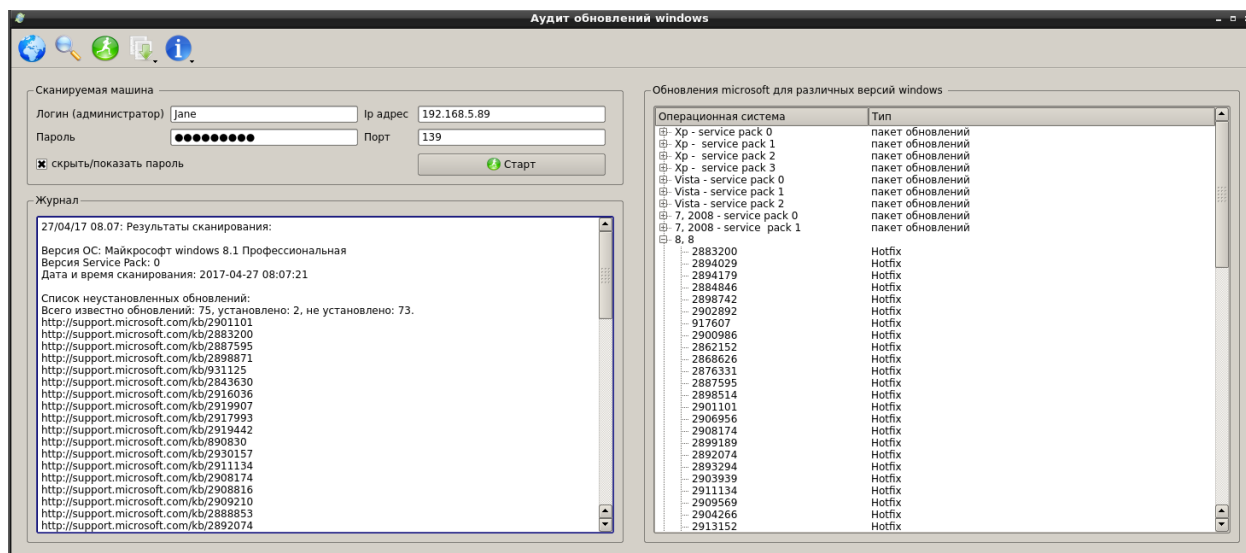


Рисунок 77 — Результат сканирования

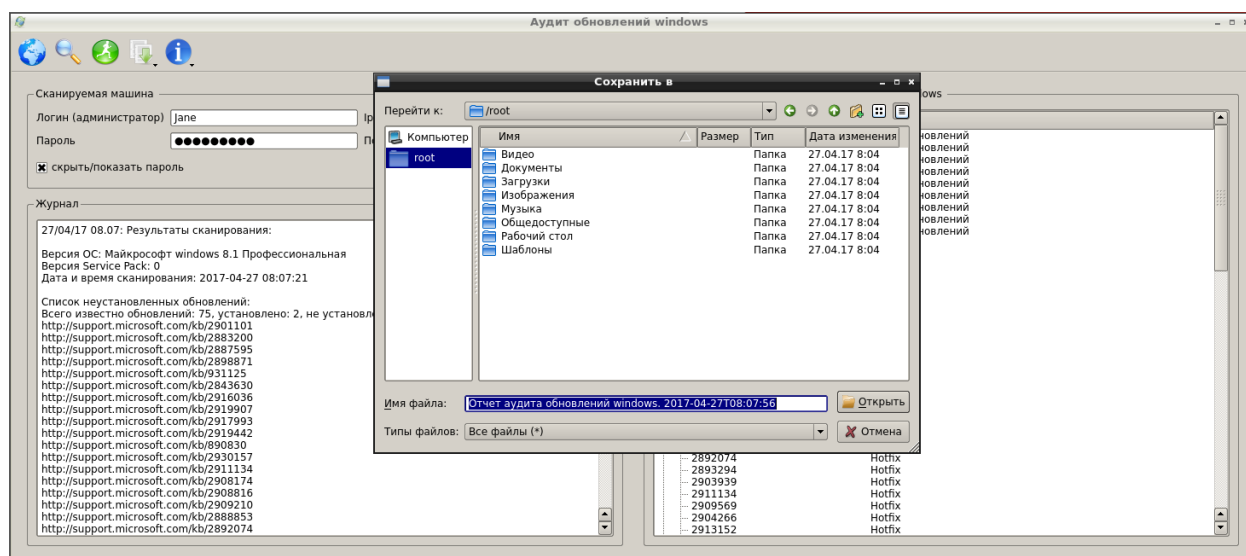


Рисунок 78 — Сохранение отчета

3.7.4.3. Завершение работы с модулем

Для выхода из модуля необходимо нажать  в верхнем правом углу рабочего окна.

3.7.5. Системный аудитор

Системный аудитор предназначен для инвентаризации программ и аппаратных средств локальной рабочей станции.

3.7.5.1. Запуск модуля

Модуль запускается из веб-интерфейса **Системный аудитор** или из подменю стартера приложений (red hat) → **Форензика** → **Системный аудитор**.

После запуска модуля откроется рабочее окно (Рисунок 79).

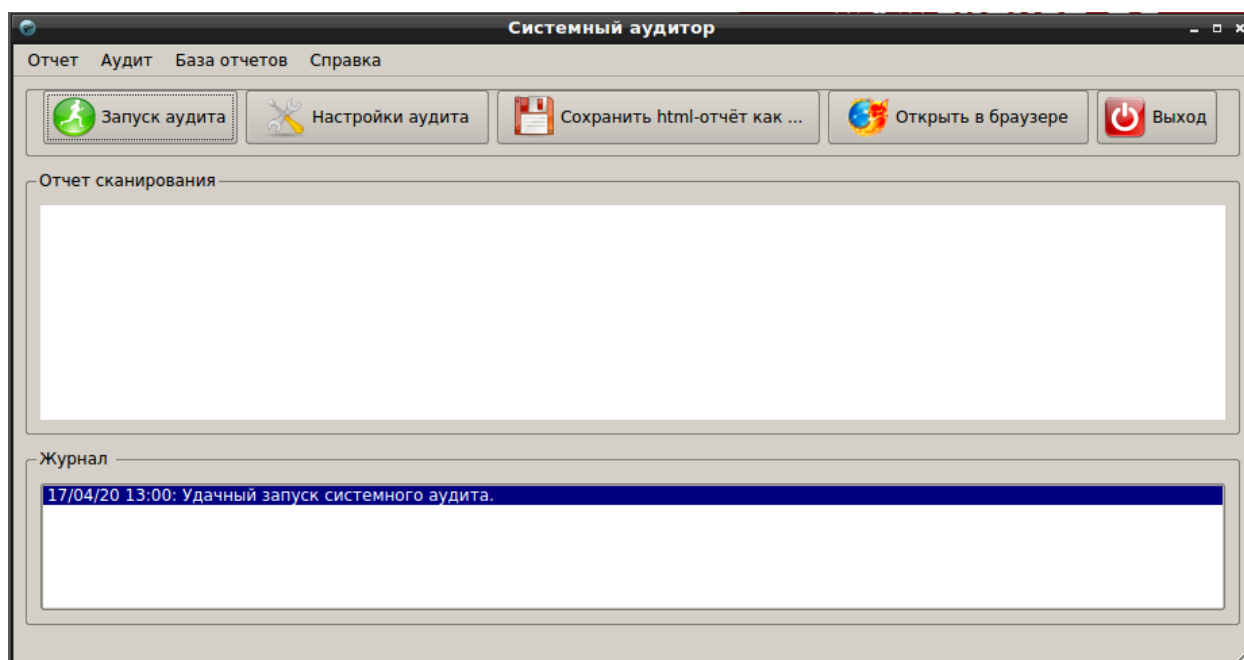


Рисунок 79 — Рабочее окно модуля

3.7.5.2. Работа с модулем

Для получения отчета об аппаратных комплектующих достаточно запустить сканирование, нажав на кнопку **Запуск аудита** или выбрать подменю **Аудит** → **Запуск аудита...**

Для получения в отчете дополнительной информации о системе необходимо нажать на кнопку **Настройки аудита** и в появившемся окне (Рисунок 80) отметить нужные пункты и нажать **Принять**.

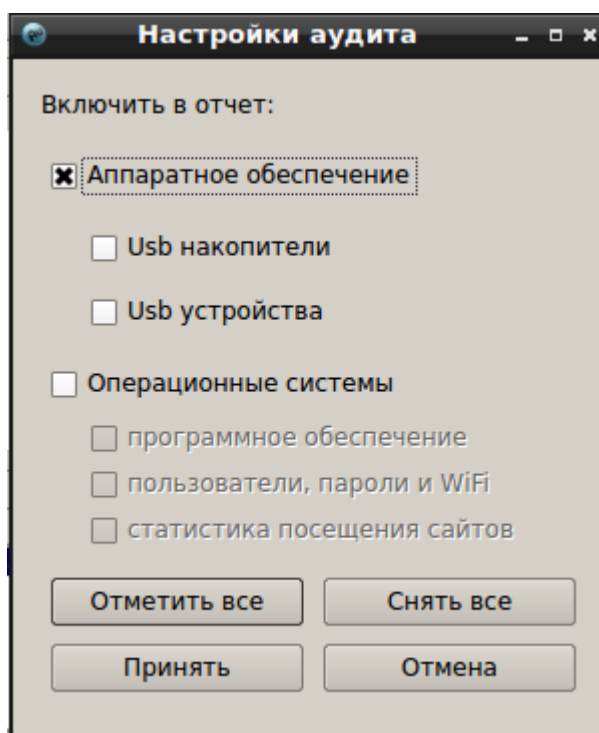


Рисунок 80 — Настройки аудита

Вызвать окно **Настройки аудита** можно альтернативным способом, выбрав в верхней части главного окна меню **Аудит** → **Настройки аудита...**

После выбора нужных настроек для анализа информации о системе необходимо нажать на кнопку **Запуск аудита**.

Результаты анализа представлены в тематических разделах: **Операционные системы**, **Система**, **Память**, **Хранилища**, **Периферия** и **Коммуникации** (Рисунок 81). Каждый раздел содержит подробную информацию о конкретных системах и устройствах.

В разделе **Операционные системы** представлено количество установленных операционных систем и их характеристики, а также информация об установленном программном обеспечении, пользователях и их паролях.

В разделе **Система** (Рисунок 81) представлены характеристики основных системных устройств, таких как центральный процессор, материнская плата, мост (вкладки **Центральный процессор**, **Материнская плата**, **Мост** соответственно).

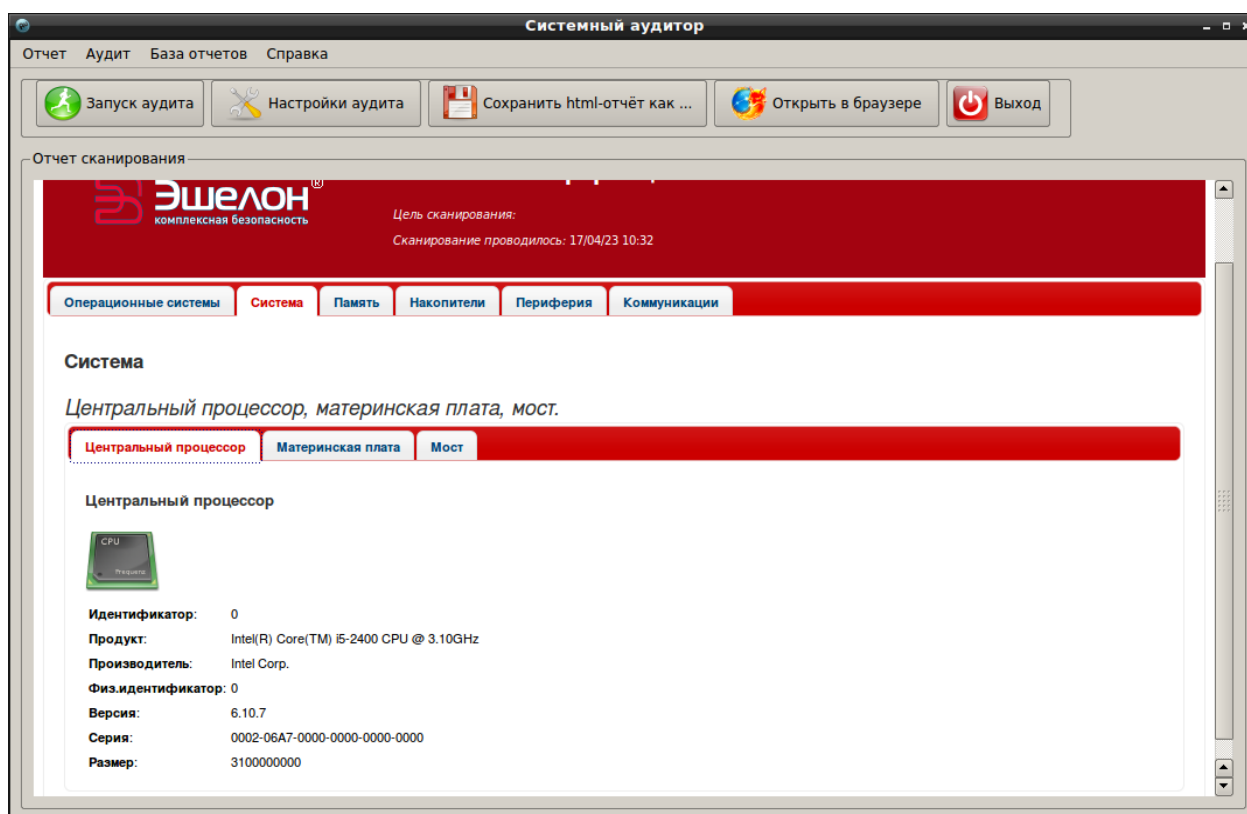


Рисунок 81 — Отчет сканирования системного аудита

Раздел **Память** содержит информацию о виде и объеме оперативной памяти.

Раздел **Накопители** (Рисунок 82) содержит информацию об основных устройствах хранения данных и их свойствах. Во вкладках **CD/DVD**, **USB**, **Жесткие диски**, **Тома** приводятся основные данные соответствующих носителей информации.

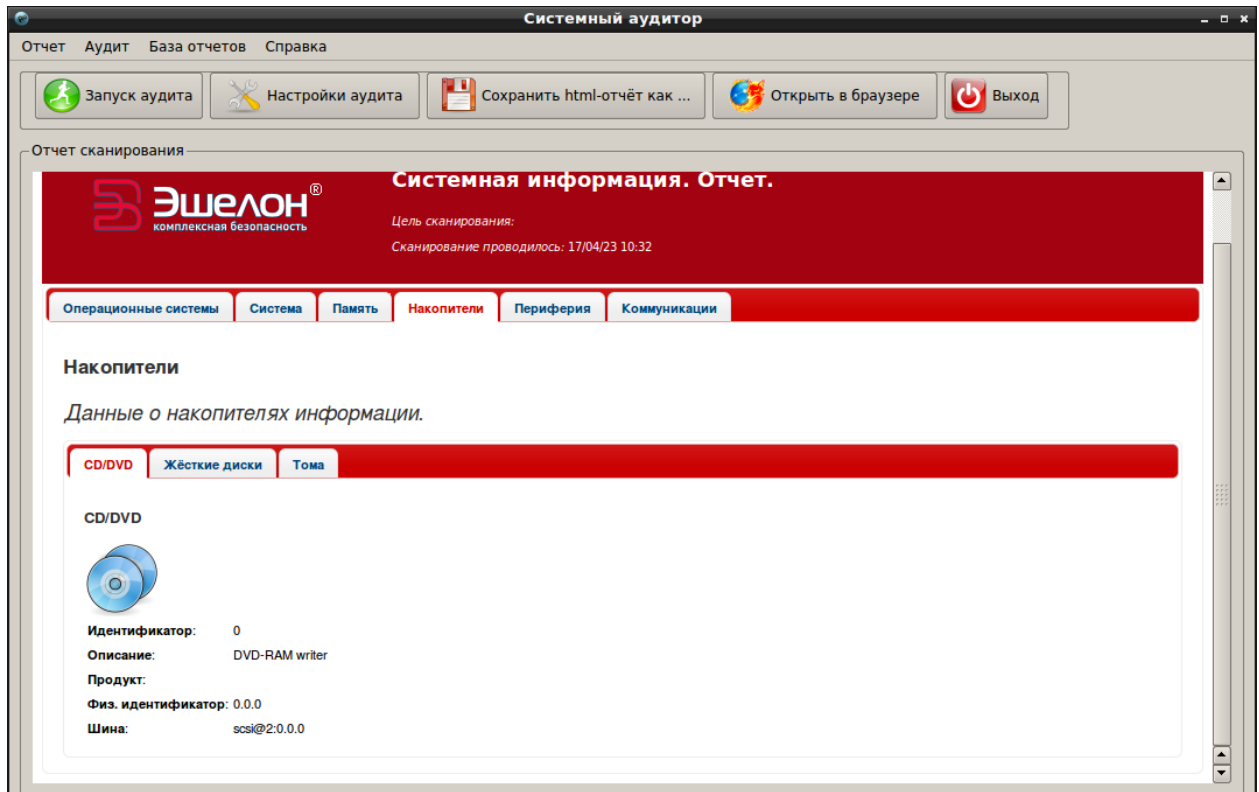


Рисунок 82 — Раздел «Накопители»

Информация о USB-подключениях предоставляется в виде таблицы с подробными данными об обнаруженных USB-устройствах (Рисунок 83).

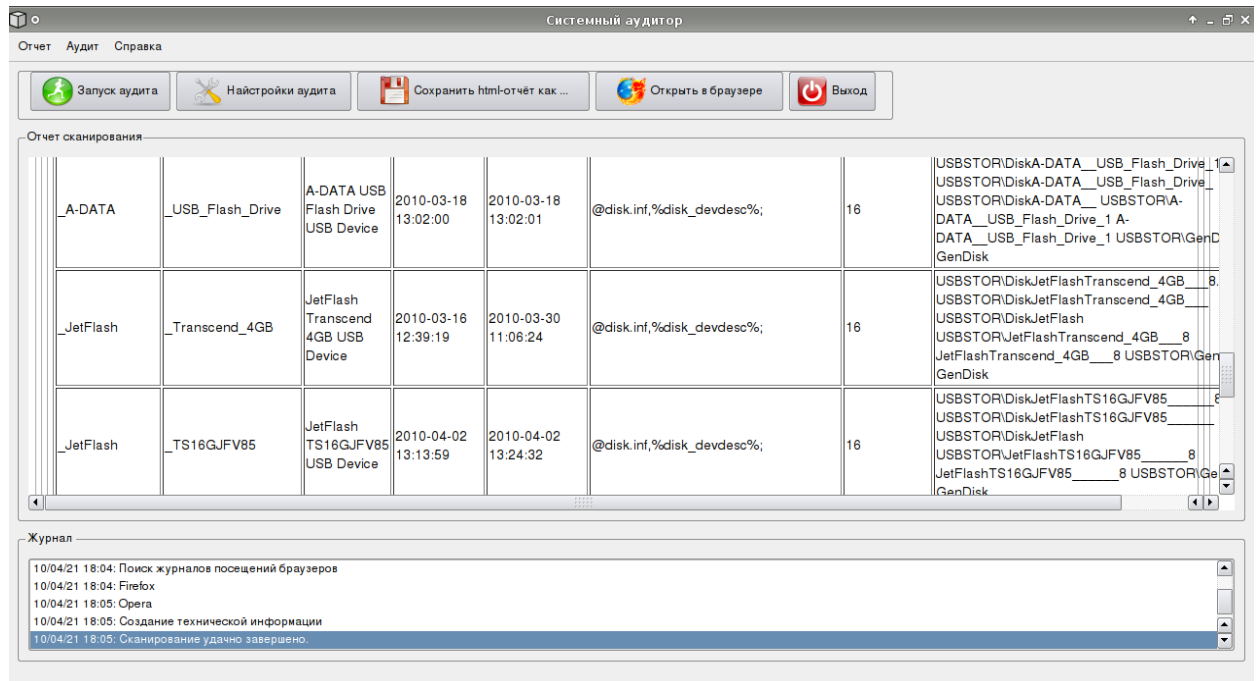


Рисунок 83 — Отчет об обнаруженных USB-устройствах

Раздел **Периферия** (Рисунок 84) содержит основную информацию о мультимедийных устройствах, видеокarte и USB-устройствах (вкладки **Мультимедия**, **Видео** и **USB** соответственно).

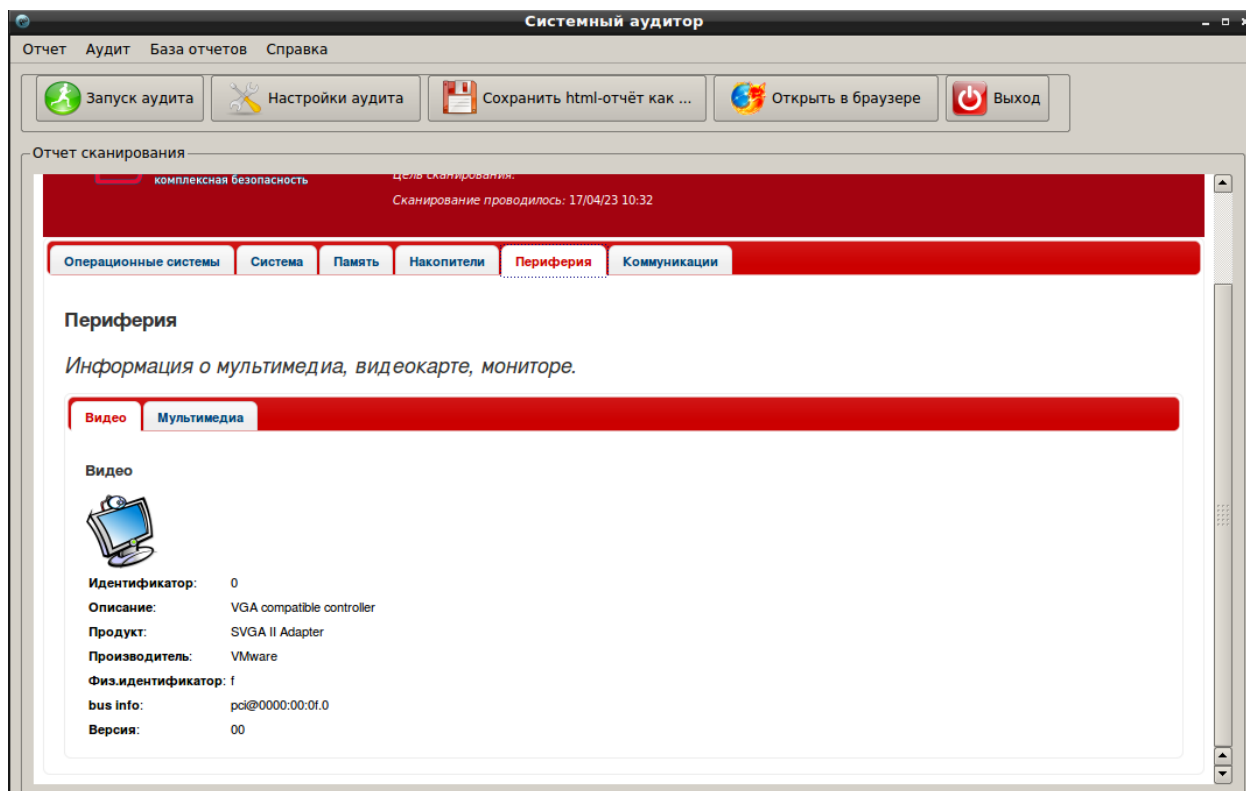


Рисунок 84 — Раздел «Периферия»

В разделе **Коммуникации** (Рисунок 85) приводятся данные о сетевых системных устройствах (беспроводных, Ethernet и т.д.).

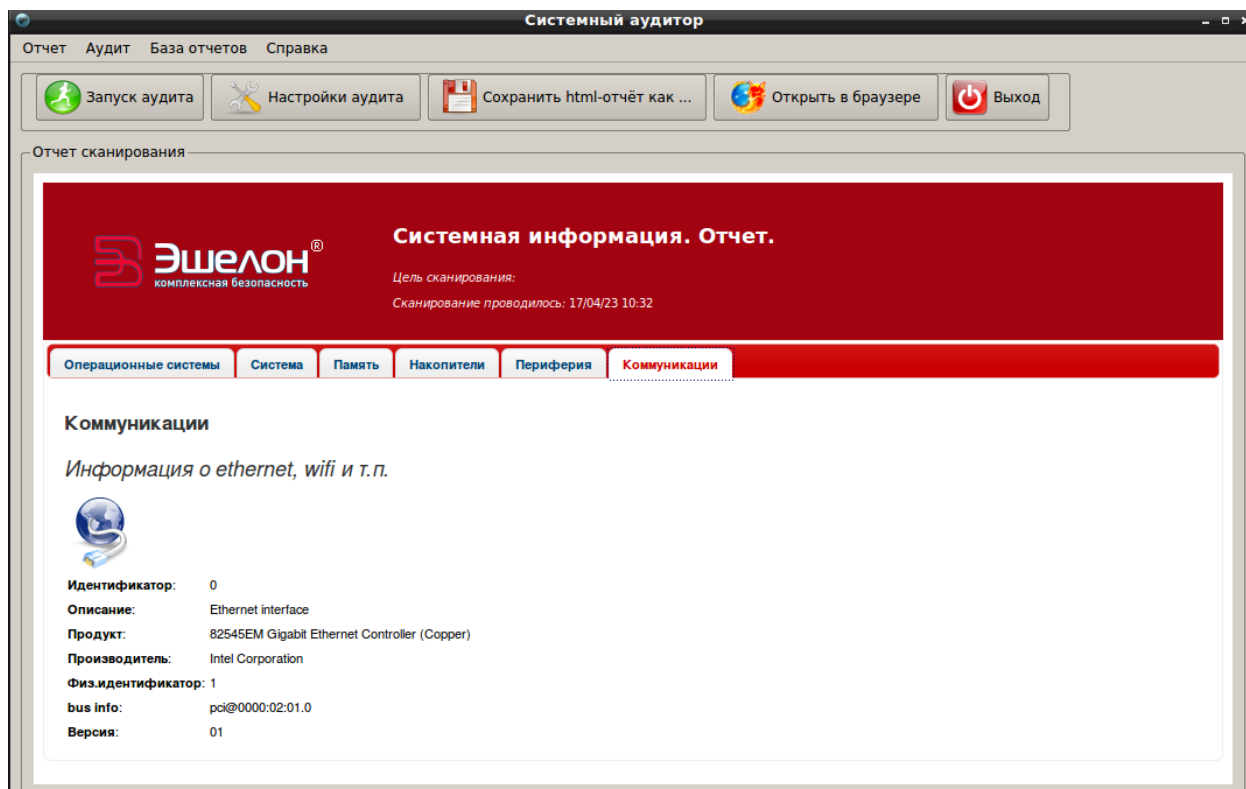


Рисунок 85 — Раздел «Коммуникации»

3.7.5.3. Работа с отчетами системного аудита

Полученный отчет системного аудита можно сохранить в форматах HTML, XML и PDF.

Для сохранения отчета в формате HTML необходимо нажать на кнопку в верхней панели главного окна **Сохранить html отчет как** или воспользоваться меню **Отчет → Сохранить html отчет...** и далее выбрать директорию сохранения отчета.

Чтобы сохранить отчет в формате XML, необходимо выбрать меню **Отчет → Сохранить xml отчет...**

Для сохранения отчета в формате PDF, необходимо выбрать меню **Отчет → Печатать html отчета в pdf...**

В модуле **Системный аудитор** реализована функция хранения и сравнения отчетов за различные периоды времени. Для этого необходимо задать месторасположение базы отчетов, выбрав подменю **База отчетов → Открыть базу** (Рисунок 81). В появившемся окне **База отчетов** (Рисунок 86) необходимо нажать **Задать базу** и указать месторасположение базы в заранее созданном каталоге. Отчеты сохраняются в базе в формате XML.

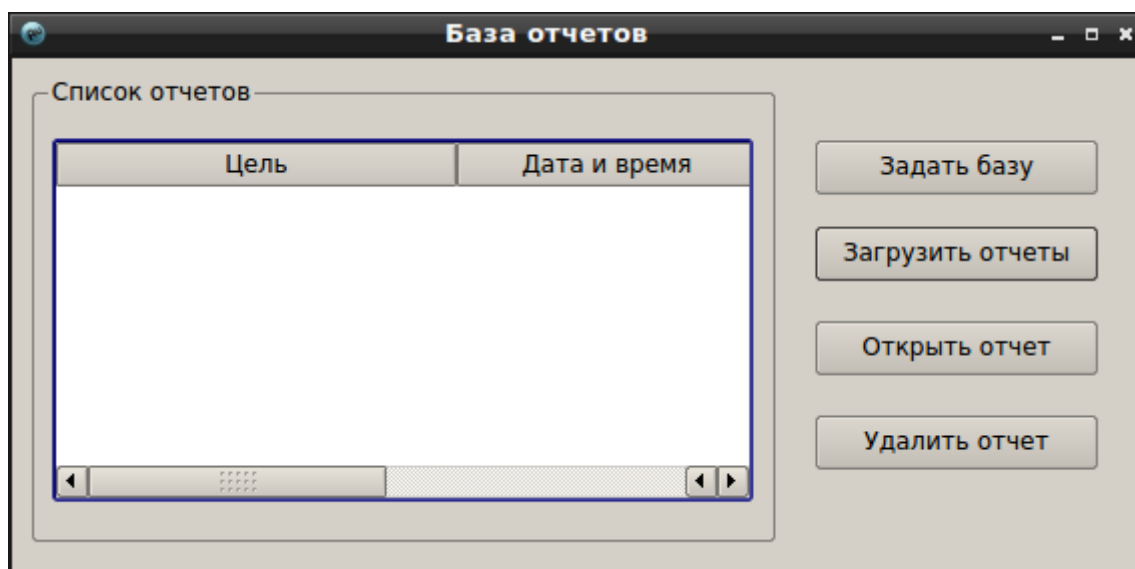


Рисунок 86 — База отчетов

После задания базы для добавления текущего отчета необходимо выбрать подменю **База отчетов → Добавить отчет** (Рисунок 81).

Для просмотра отчетов в указанной базе необходимо в окне **База отчетов** нажать **Загрузить отчеты** (Рисунок 87).

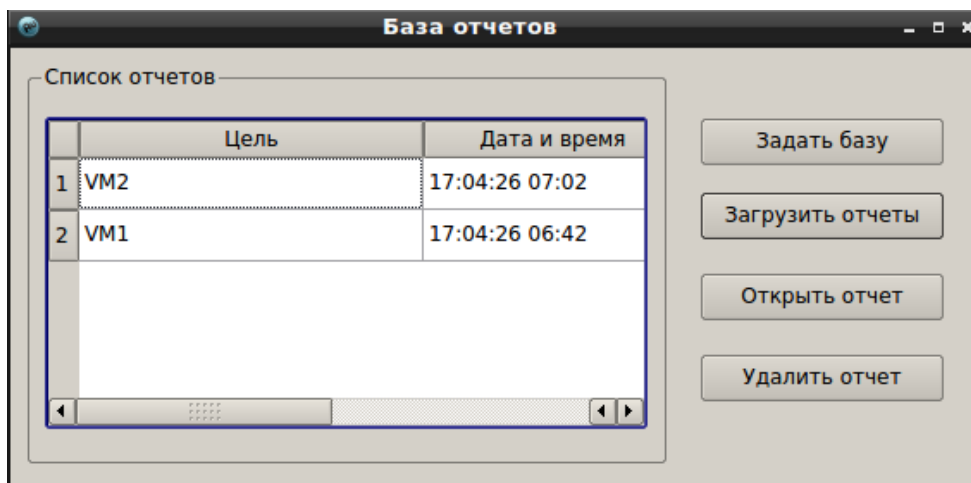


Рисунок 87 — Список загруженных отчетов

Для просмотра выделенного отчета необходимо в окне **База отчетов** нажать **Открыть отчет**. Отчет отображается в рабочем окне модуля.

Для удаления выделенного отчета необходимо в окне **База отчетов** нажать **Удалить отчет**.

Для сравнения отчетов в базе необходимо выбрать подменю **База отчетов** → **Сравнить отчеты**. Появляется окно **Сравнение отчетов** (Рисунок 88).

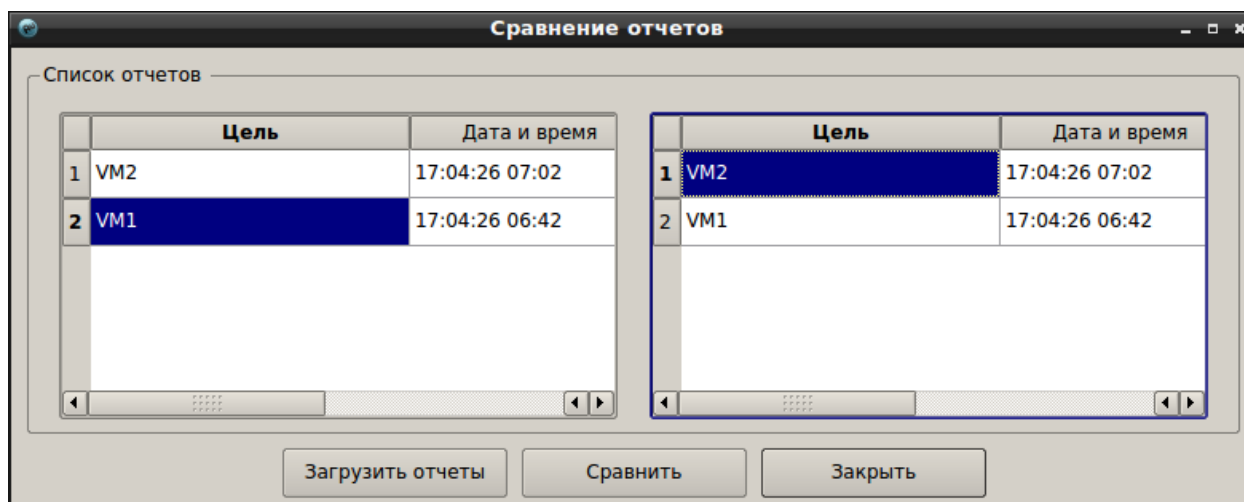


Рисунок 88 — Сравнение отчетов

В данном окне необходимо нажать **Загрузить отчеты**, выбрать отчеты и нажать **Сравнить**.

В рабочем окне модуля будет отображена информация о сравнении отчетов. Результаты сравнения располагаются в тематических разделах, среди которых **Операционные системы**, **Программное обеспечение**, **Пользователи**, **USB носители**, **USB устройства** (Рисунок 89).

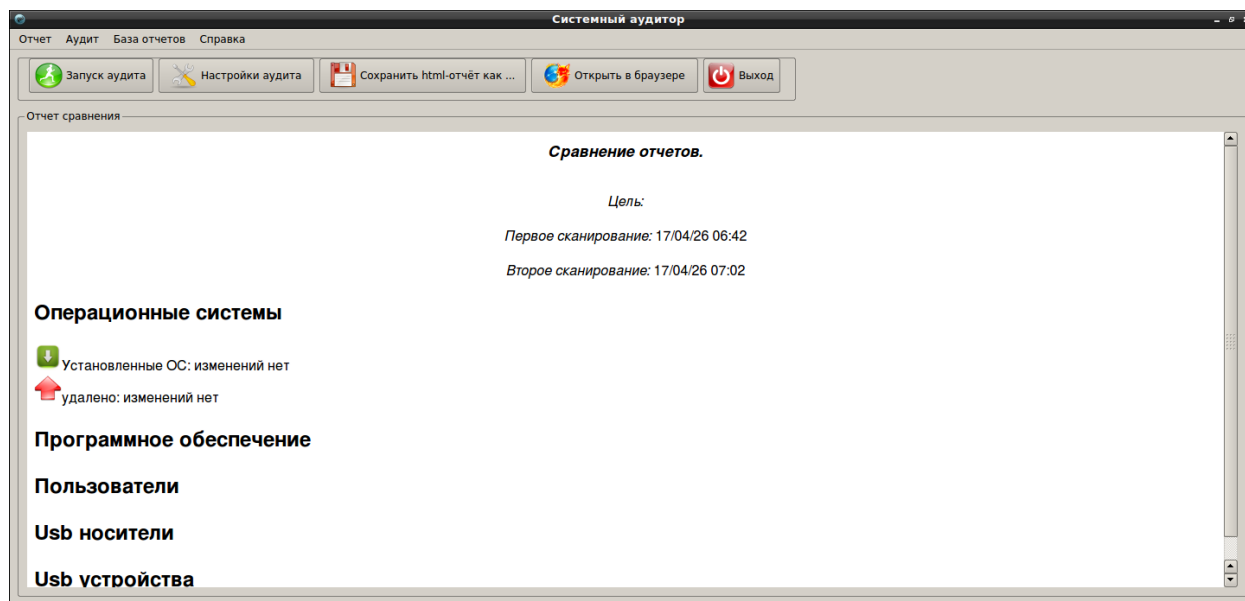



Рисунок 89 — Результаты сравнения

3.7.5.4. Завершение работы с модулем

Для выхода из модуля необходимо воспользоваться кнопкой **Выход**  на панели инструментов в главном окне модуля.

3.7.6. Средство гарантированного уничтожения информации

Средство гарантированного уничтожения информации предназначено для удаления информации путем затирания файла случайным набором символов для предотвращения восстановления данных.

3.7.6.1. Запуск модуля

Модуль запускается из веб-интерфейса **Гарантированное уничтожение информации** или из подменю стартера приложений (red hat) → **Остальные приложения** → **Прочее** → **Гарантированное уничтожение информации**.

После запуска средства появится рабочее окно модуля (Рисунок 90).

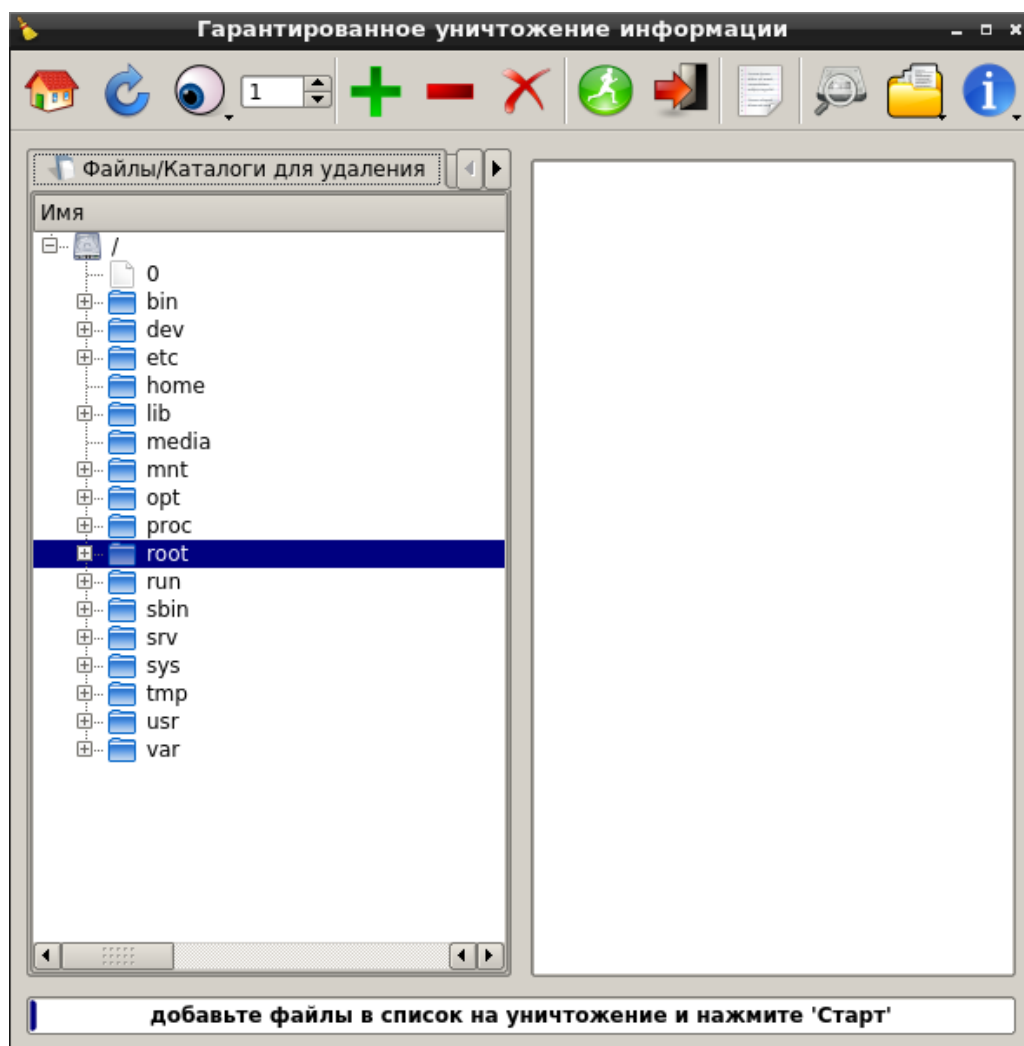





Рисунок 90 — Рабочее окно модуля

В верхней части рабочего окна находится панель инструментов. Кнопки, расположенные на панели инструментов, представлены в таблице ниже.

Таблица 2 – Описание кнопок модуля

| Пиктограмма | Название | Описание |
|---|--------------------|--|
|  | Домой | Программа возвращает пользователя в домашнюю директорию (домашнюю папку) |
|  | Обновить | При нажатии на кнопку обновляется список файлов |
|  | Отображение | Возможные варианты отображения: показать все, показать все, кроме скрытого и показать только папки |

| Пиктограмма | Название | Описание |
|---|-----------------------------|--|
|  | Количество затираний | Количество затираний файла случайным набором символов что предотвращает возможность восстановления файла |
|  | Добавить в список | Добавление выбранного файла в список на уничтожение |
|  | Удалить из списка | Удаление выбранного файла из списка на уничтожение |
|  | Очистить список | Очистка списка на уничтожение |
|  | Старт/Стоп | Запуск/остановка процесса уничтожения информации |
|  | Выход | Выход из модуля |
|  | Журнал | При нажатии на кнопку в блокноте открывается журнал, содержащий имена удаленных файлов и результаты выполнения операции удаления |
|  | Загрузка отчета | При нажатии на кнопку появится окно, в котором необходимо выбрать папку с отчетом средства поиска остаточной информации (Рисунок 91) |
|  | Отчет | При нажатии на кнопку предлагается выбор форматов отчетов для сохранения |
|  | Помощь | При нажатии на кнопку отображается окно с информацией о модуле и о горячих клавишах |

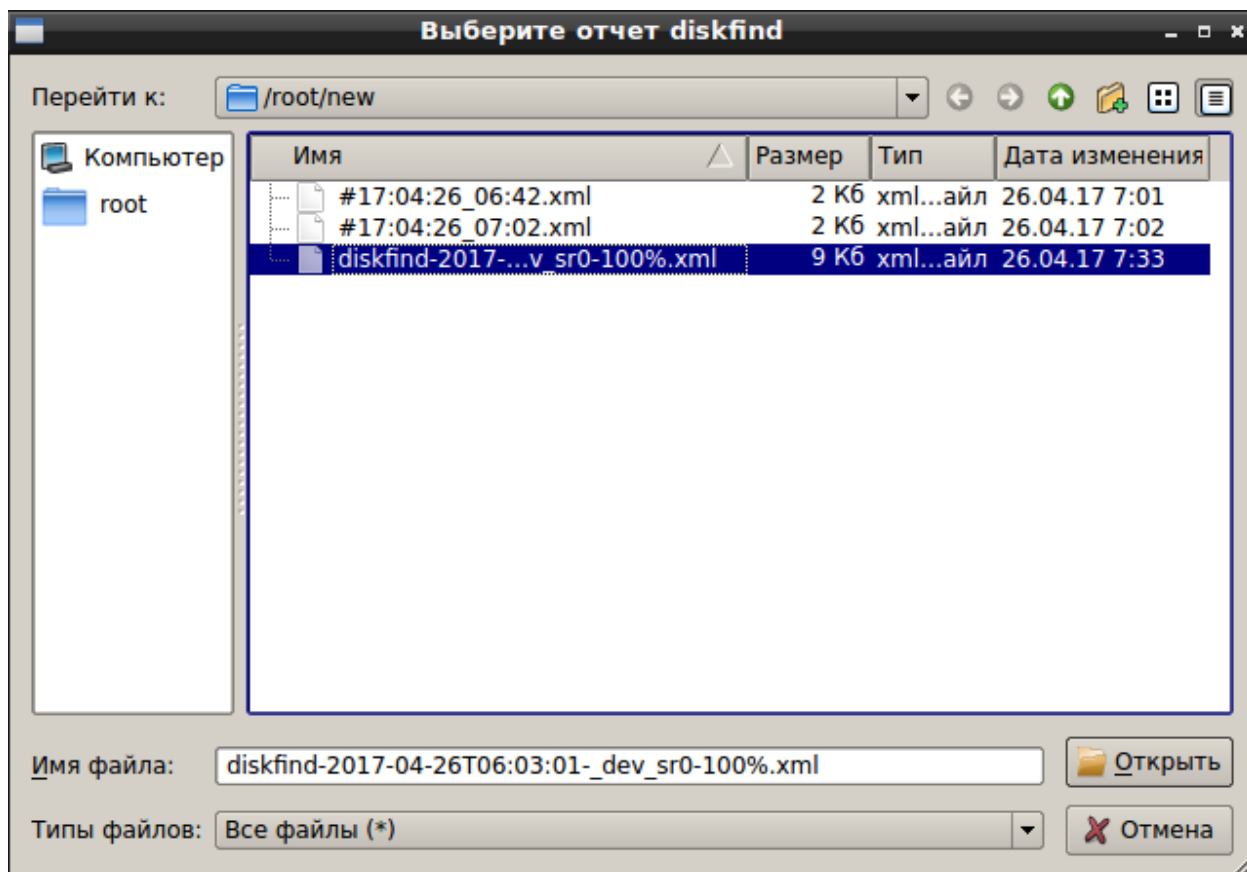



Рисунок 91 — Загрузка отчета

В нижней части рабочего окна находится строка состояния модуля. Если процесс уничтожения информации не запущен, то в строке отображается: «Добавьте файлы в список и нажмите 'Старт'».

Если процесс уничтожения информации запущен, то в строке отображается состояние выполнения процедуры уничтожения.

3.7.6.2. Работа с модулем

Чтобы запустить процесс уничтожения информации, необходимо выбрать файлы и добавить их в список с помощью значка **Добавить в список** . Удалить из списка или очистить список можно с помощью кнопок **Удалить из списка**  и **Очистить список** .

Список выбранных файлов на уничтожение отображается в правой части рабочего окна модуля. (Рисунок 92).

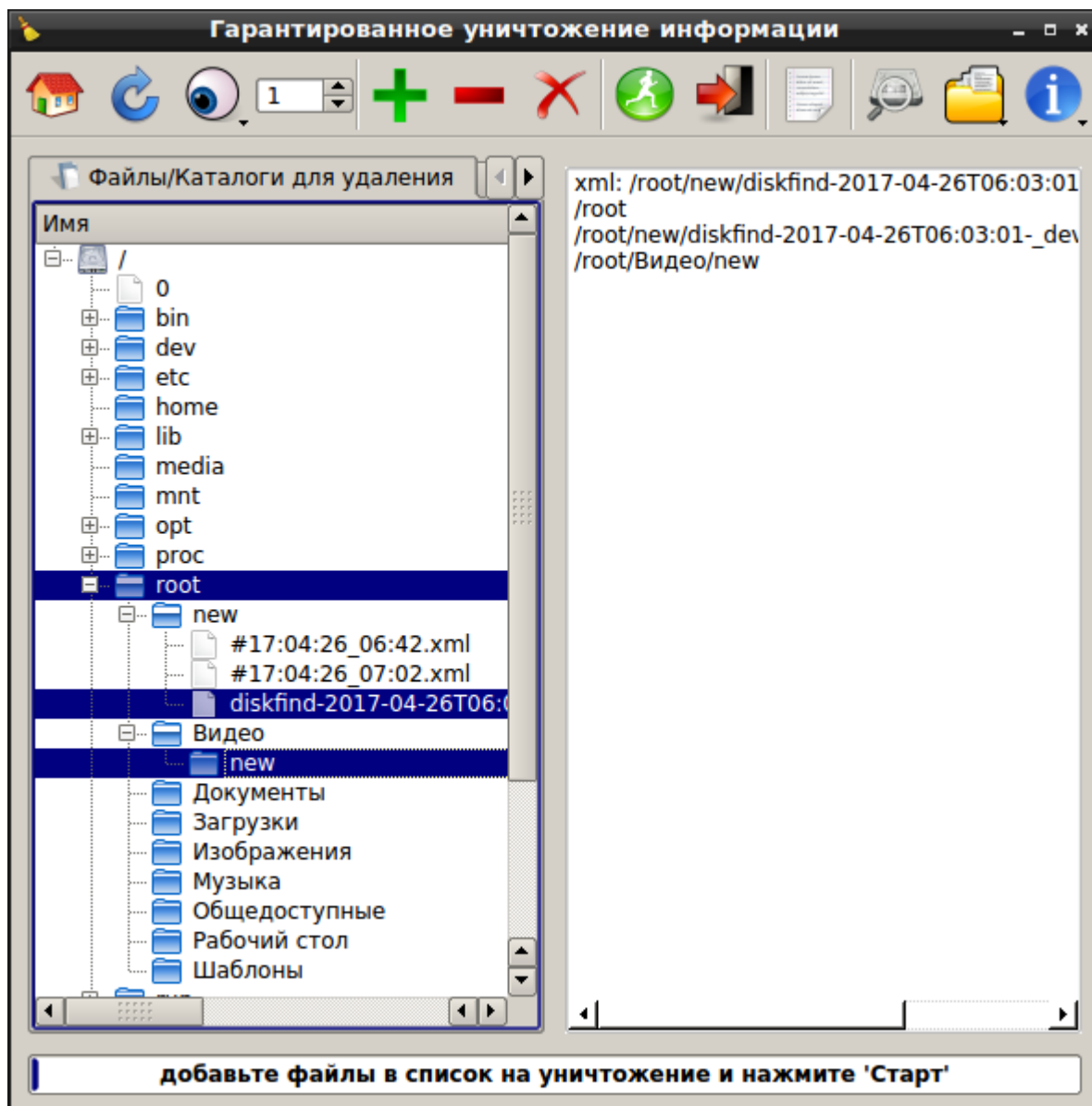



Рисунок 92 — Выбранные для уничтожения файлы

Затем необходимо указать количество затираний в поле **Количество затираний**.

Примечание. Максимальное количество затираний – 35.

Для запуска процедуры гарантированного уничтожения информации необходимо воспользоваться кнопкой **Старт/Стоп**  на панели инструментов модуля. Процесс уничтожения может быть остановлен в любой момент с помощью повторного нажатия на кнопку **Старт/Стоп**.

Перед началом процесса уничтожения появляется сообщение, требующее подтвердить удаление файлов (Рисунок 93).

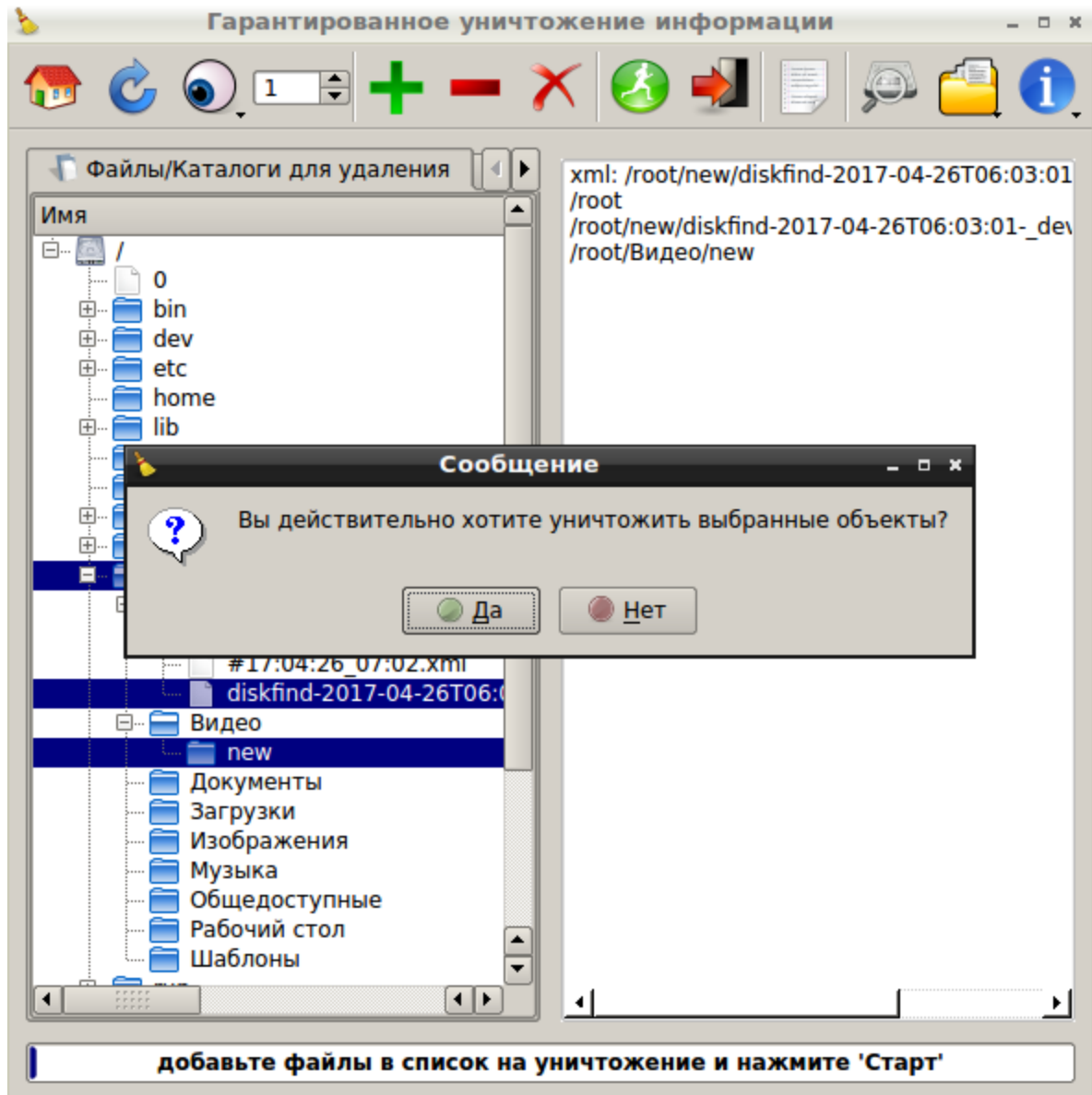


Рисунок 93 — Сообщение

Примечание. При попытке уничтожения системных файлов, появится предупреждение, показанное на рисунке 94.

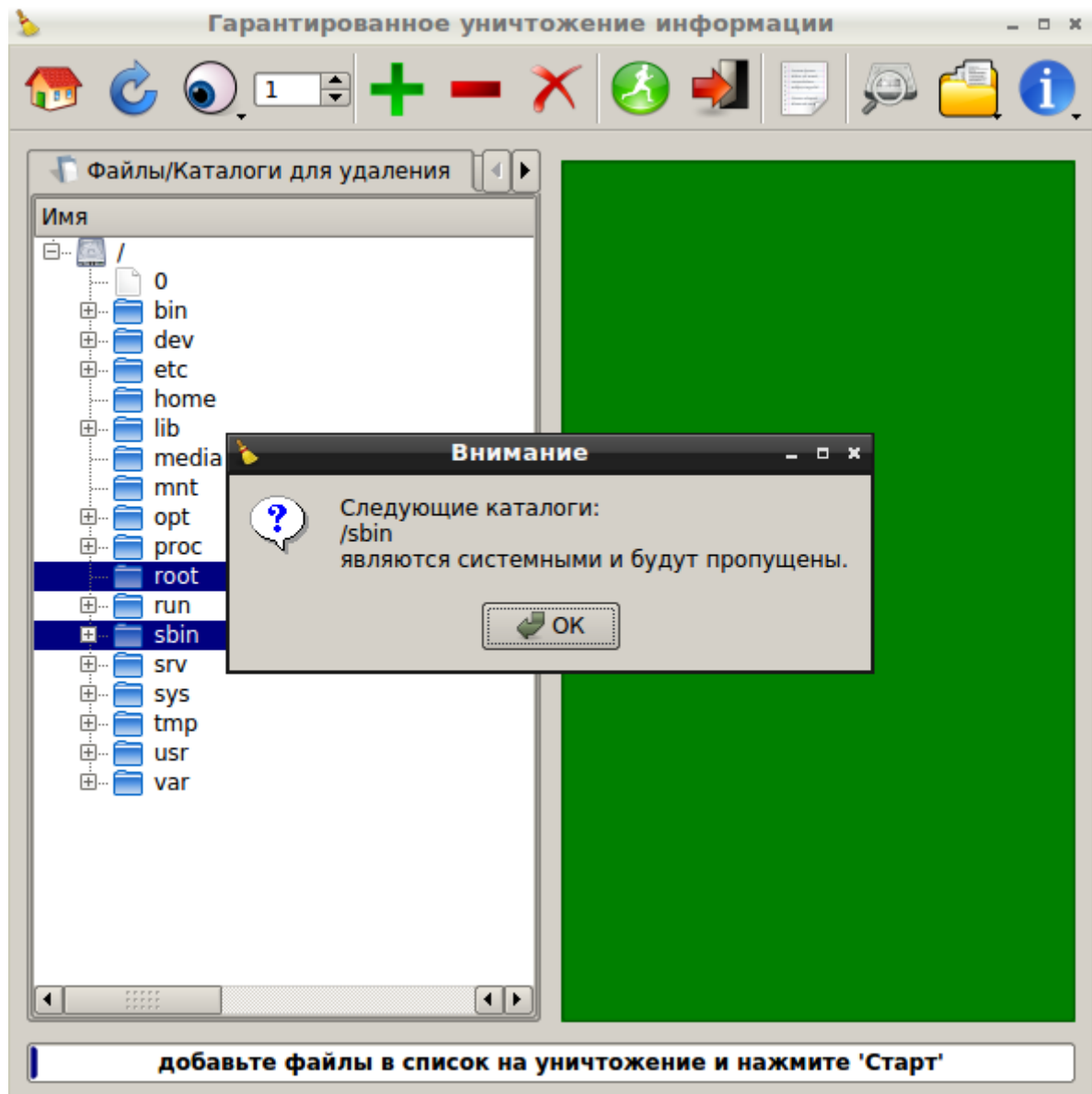



Рисунок 94 — Предупреждение

3.7.6.3. Завершение работы с модулем

Для выхода из модуля необходимо воспользоваться подменю **Файл** → **Выход** или нажать

кнопку **Выход**  на панели инструментов.

3.7.7. Средство аудита беспроводных сетей

Средство аудита беспроводных сетей предназначено для обнаружения, сканирования и проведения пассивных и активных атак на подбор паролей в беспроводных сетях с WEP, WPA, WPA-2 шифрованием.

3.7.7.1. Запуск средства аудита беспроводных сетей

Модуль запускается из веб-интерфейса **Аудит беспроводных сетей** или из подменю стартера приложений (red hat) → **Аудит беспроводных сетей** → **Аудит беспроводных сетей**.

После запуска появится рабочее окно модуля (Рисунок 95).

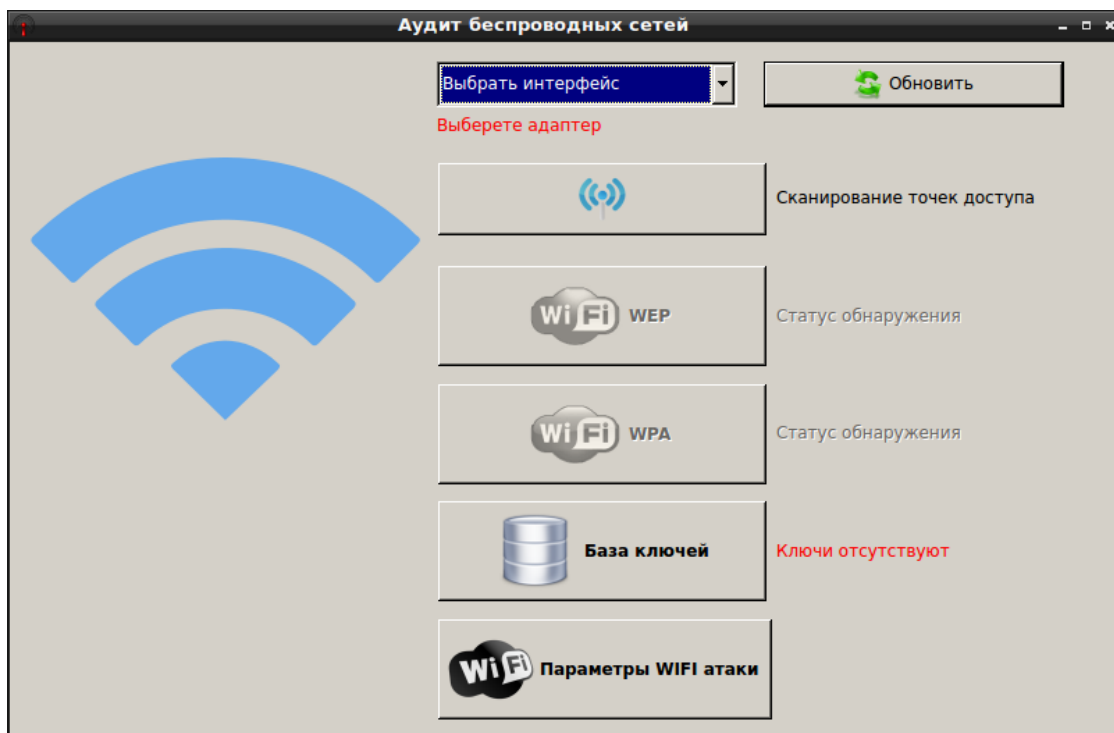


Рисунок 95 – Рабочее окно модуля

Примечание. Список поддерживаемых адаптеров приведен в таблице 1.1 приложения 1 к настоящему документу.

3.7.7.2. Прослушивание сети, использующей WEP шифрование

Для обнаружения точек доступа необходимо указать интерфейс в поле **Выбрать интерфейс** и нажать кнопку **Сканирование точек доступа**. После сканирования в рабочем окне модуля будет отражена информация о количестве найденных точек доступа (Рисунок 96).

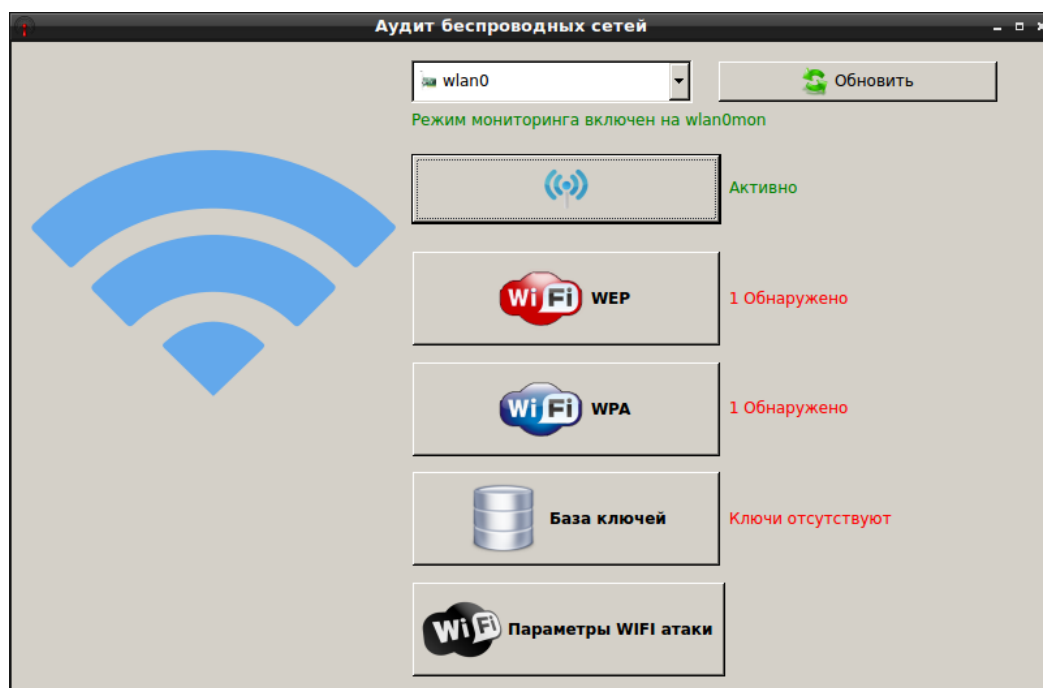


Рисунок 96 – Обнаруженные точки доступа

Для перехода к настройке атаки на точку доступа с WEP шифрованием нажмите кнопку **WEP**. В открывшемся окне укажите точку доступа и вид атаки.

Чтобы указать дополнительные настройки атаки в рабочем окне модуля нажмите кнопку **Параметры WiFi атаки**. В открывшемся окне укажите необходимые параметры (Рисунок 97).

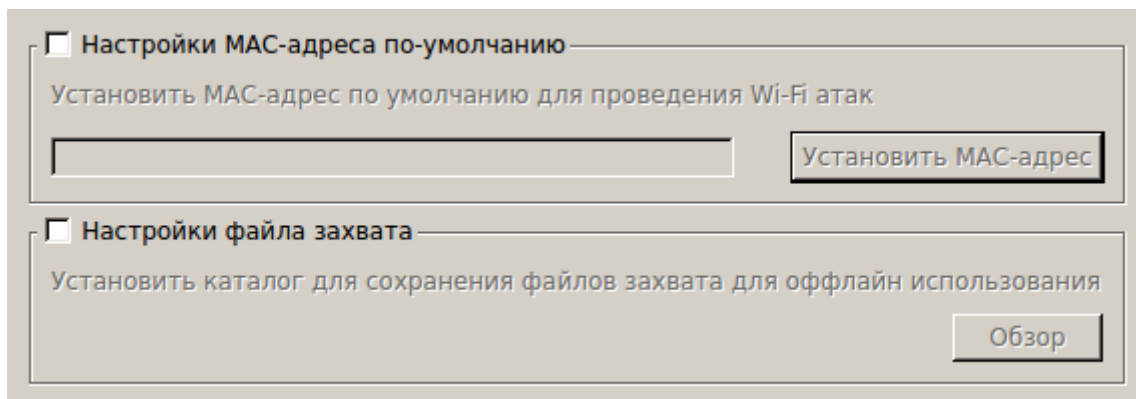


Рисунок 97 – Параметры атаки

Для начала или остановки атаки нажмите кнопку **Атака/Стоп**, расположенную справа от точек доступа (Рисунок 98).

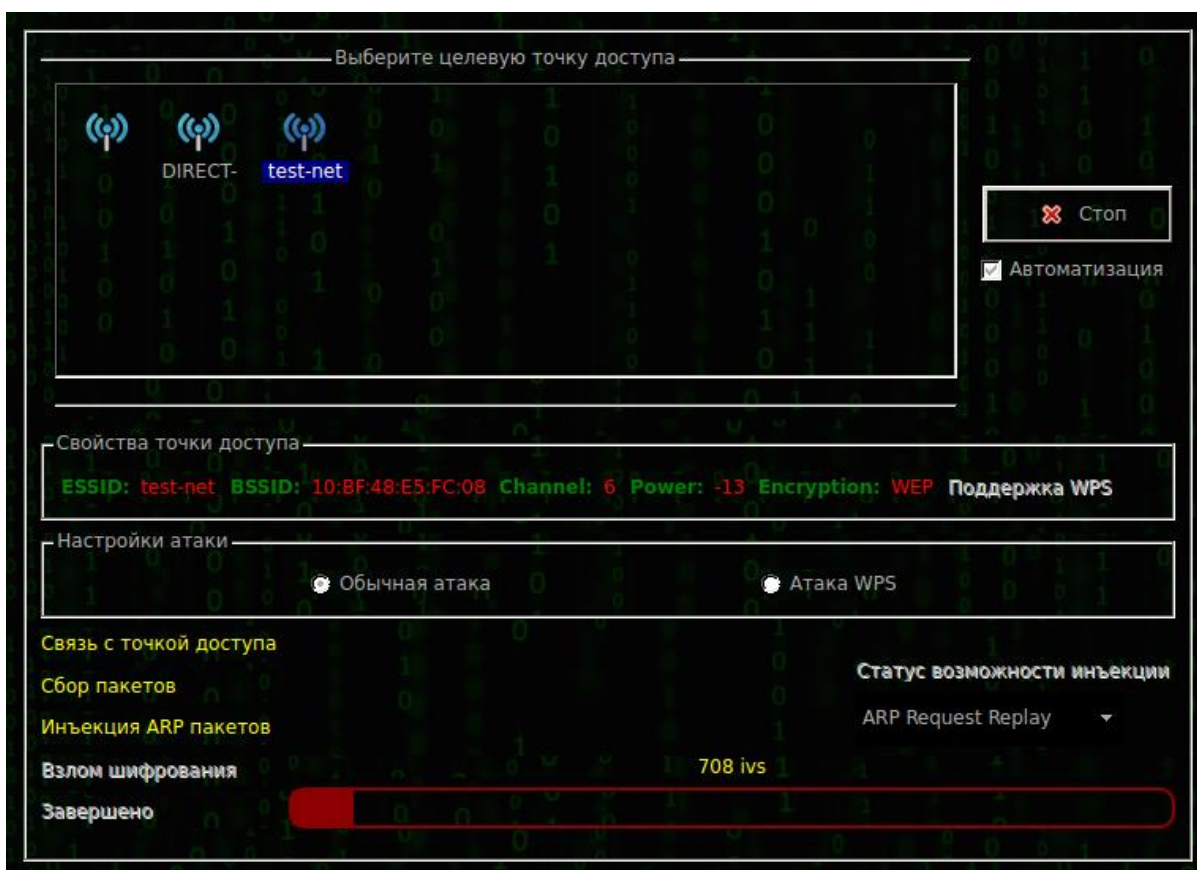


Рисунок 98 – Настройки атаки

После завершения атаки в нижней части окна настроек атаки будет отображен результат взлома (Рисунок 99).

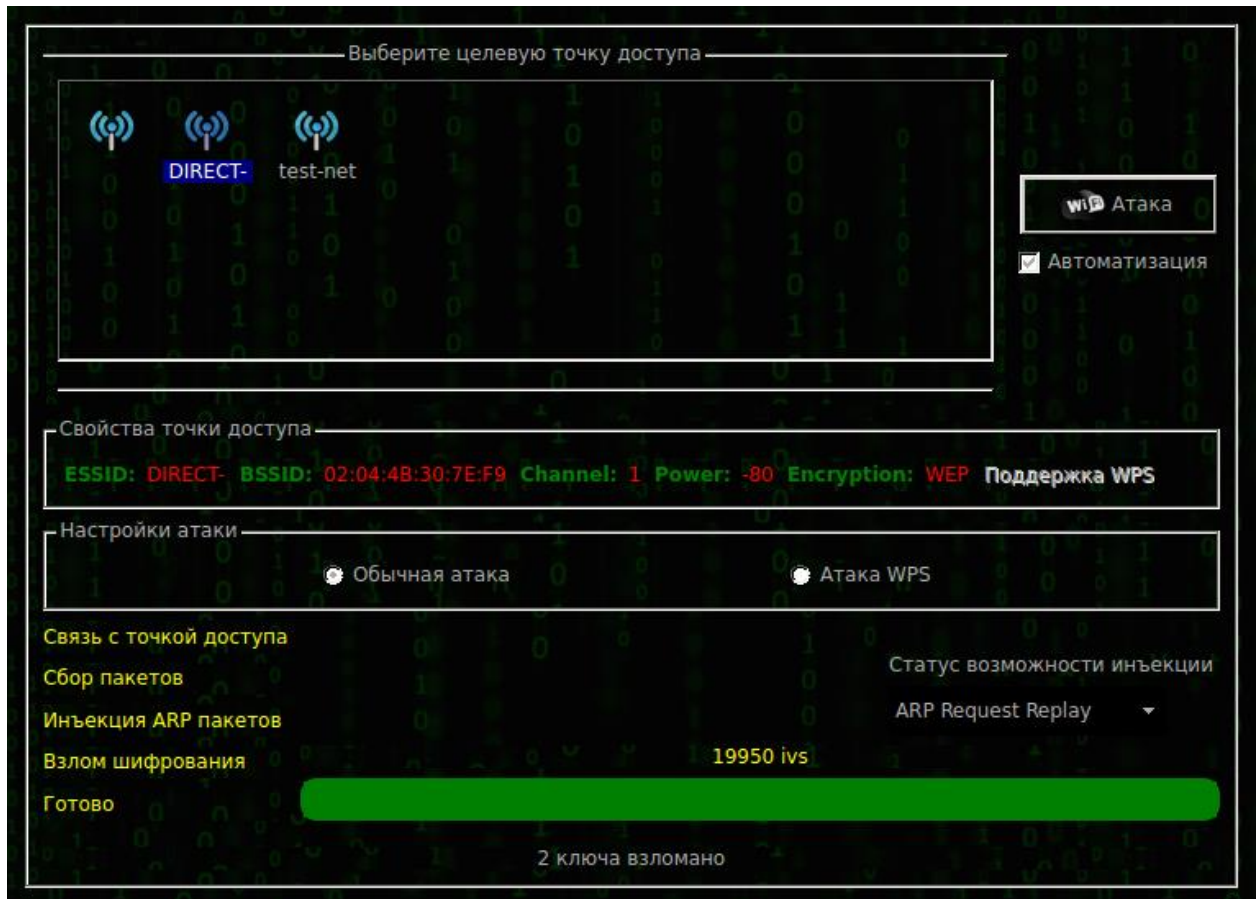


Рисунок 99 – Результат взлома

Для просмотра взломанных паролей в рабочем окне модуля (Рисунок 95) нажмите кнопку **База ключей**. В открывшемся окне отражена информация о найденных паролях в процессе аудита. Чтобы добавить новый ключ вручную, воспользуйтесь кнопкой **Добавить новый ключ** (Рисунок 100).

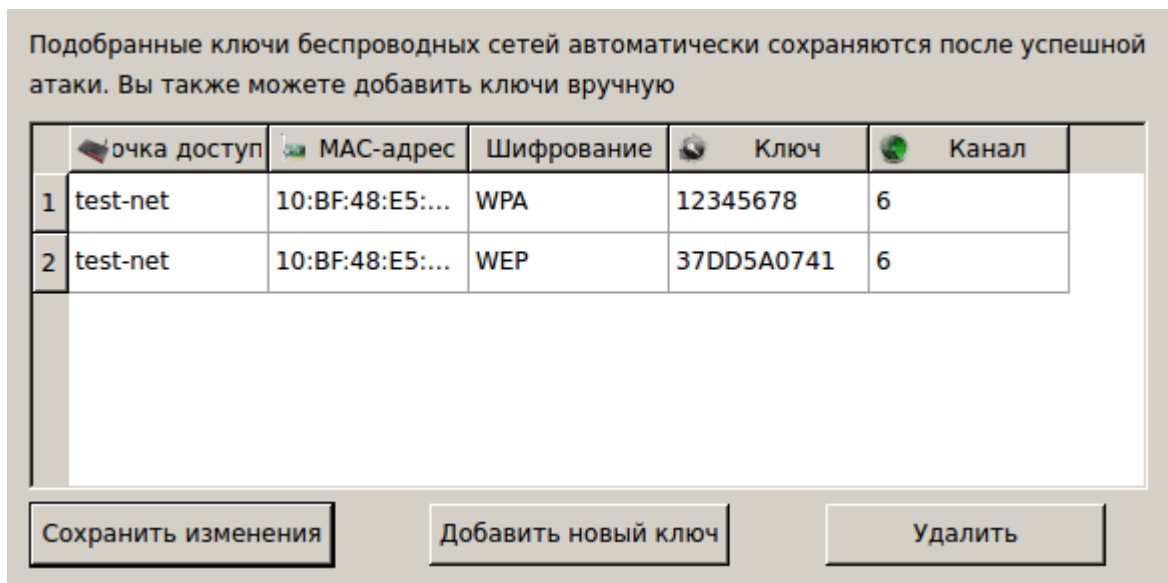


Рисунок 100 – База ключей

3.7.7.3. Прослушивание сети, использующей WPA шифрование

Для обнаружения точек доступа необходимо указать интерфейс в поле **Выбрать интерфейс** и нажать кнопку **Сканирование точек доступа**. После сканирования в рабочем окне модуля будет отражена информация о количестве найденных точек доступа (Рисунок 96).

Для перехода к настройке атаки на точку доступа с WPA шифрованием нажмите кнопку **WPA**. В открывшемся окне укажите точку доступа и вид атаки. Для осуществления атаки также необходимо загрузить файл с возможными комбинациями паролей. Для этого нажмите кнопку **Обзор** и выберите необходимый файл. Чтобы указать дополнительные настройки атаки в рабочем окне модуля нажмите кнопку **Параметры WiFi атаки**. В открывшемся окне укажите необходимые параметры (Рисунок 97).

Для начала или остановки атаки нажмите кнопку **Атака/Стоп**, расположенную справа от точек доступа (Рисунок 101).

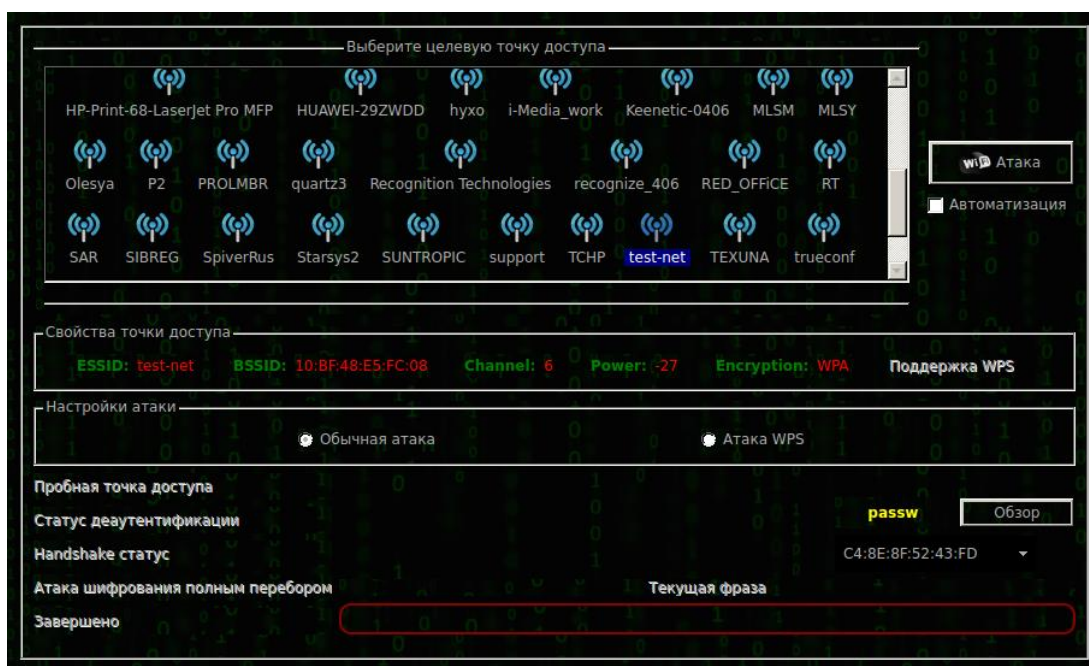


Рисунок 101 – Настройки атаки

После завершения атаки в нижней части окна настроек атаки будет отображен результат взлома (Рисунок 99).

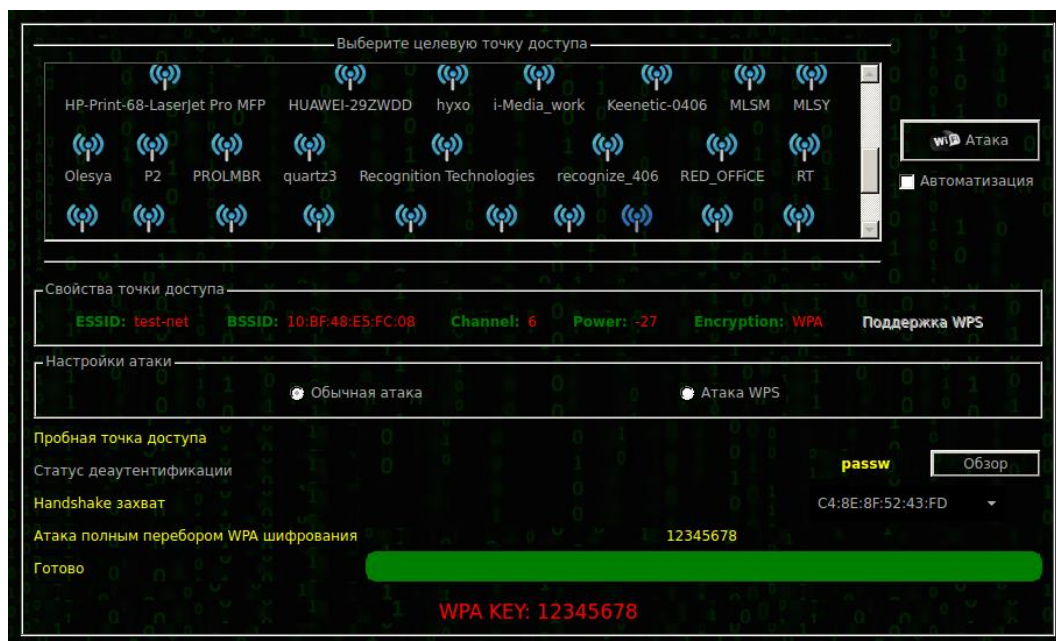



Рисунок 102 – Результат взлома

Для просмотра взломанных паролей в рабочем окне модуля (Рисунок 96) нажмите кнопку **База ключей**. В открывшемся окне отражена информация о найденных паролях в процессе аудита (Рисунок 100).

3.7.7.4. Выход из средства аудита беспроводных сетей

Для выхода из модуля необходимо нажать  в верхнем правом углу окна.

3.7.8. Сетевой анализатор

Модуль сетевого анализа предназначен для перехвата, анализа и фильтрации сетевого трафика.

3.7.8.1. Запуск модуля

Модуль запускается из веб-интерфейса **Сетевой анализатор** или из подменю стартера приложений (red hat) → **Сниффинг и спуфинг** → **Сетевой анализатор**.

После запуска модуля появляется рабочее окно модуля (Рисунок 103).

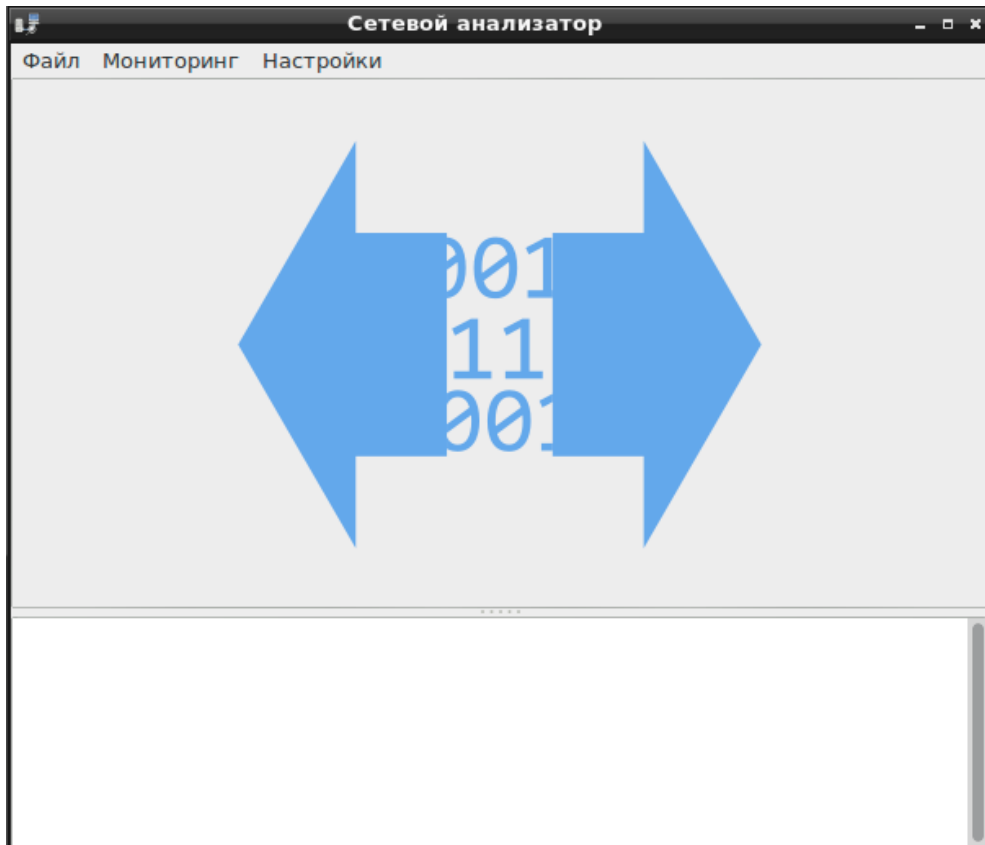


Рисунок 103 — Рабочее окно модуля

3.7.8.2. Начало работы с модулем

Для начала работы с модулем необходимо выбрать в пункте меню **Мониторинг** вид сети для анализа (Рисунок 104).

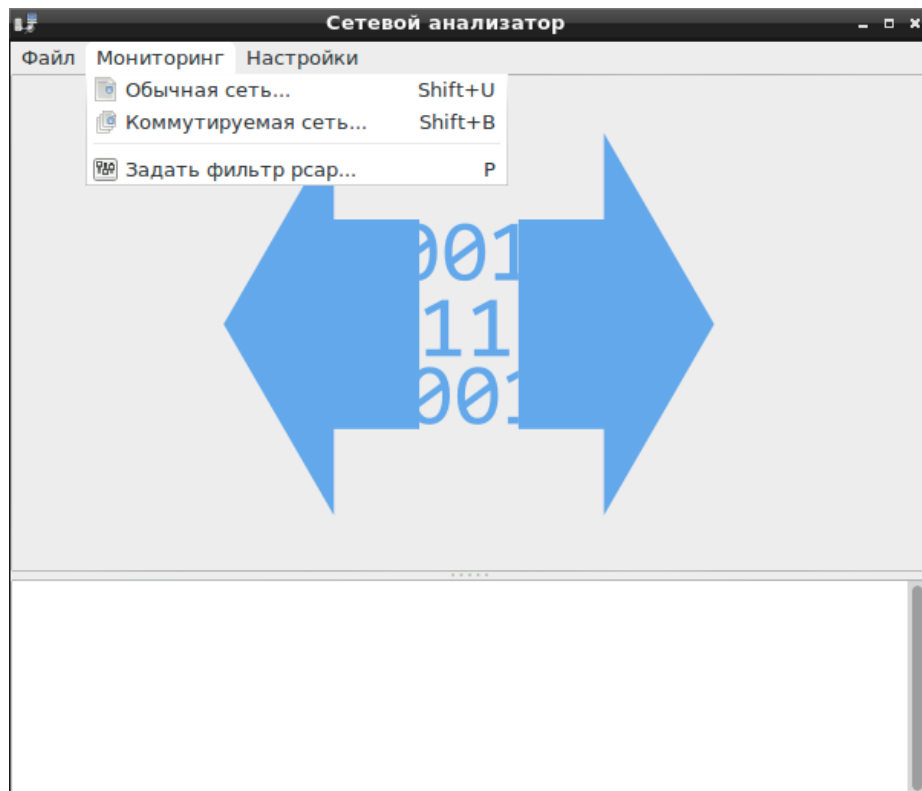


Рисунок 104 — Выбор сети для анализа

Для запуска процесса анализа сетевого трафика необходимо выбрать пункт меню **Начало** → **Начать мониторинг** (Рисунок 105).

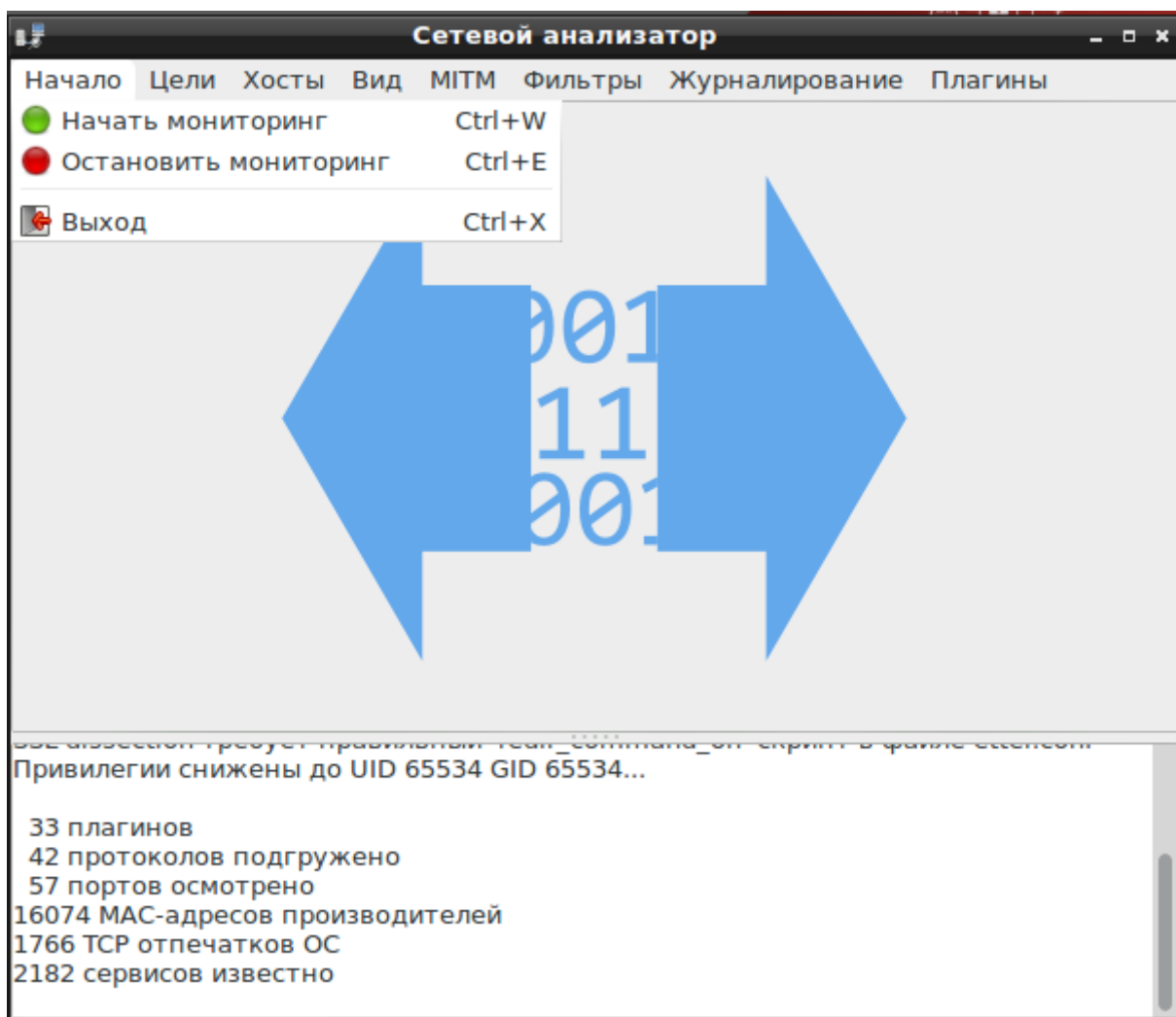


Рисунок 105 — Начало мониторинга

Для начала анализа необходимо определить IP-адреса хостов сети. Для этого необходимо выбрать подменю **Хосты** → **Сканирование хостов** (Рисунок 106). В подменю **Хосты** → **Список хостов** будет представлена информация о просканированных хостах сети (Рисунок 107).

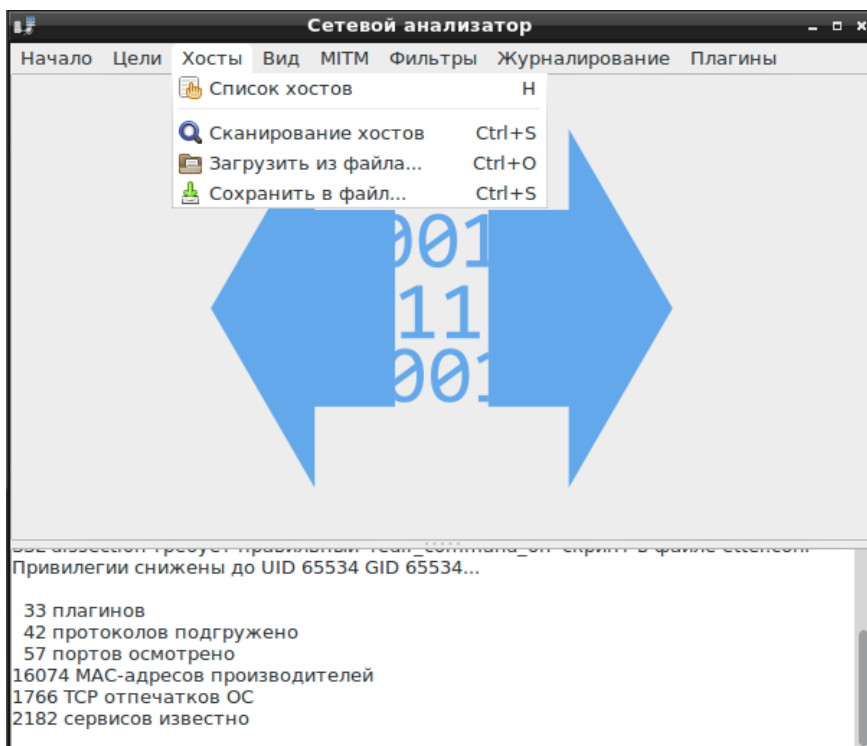


Рисунок 106 — Меню «Хосты»

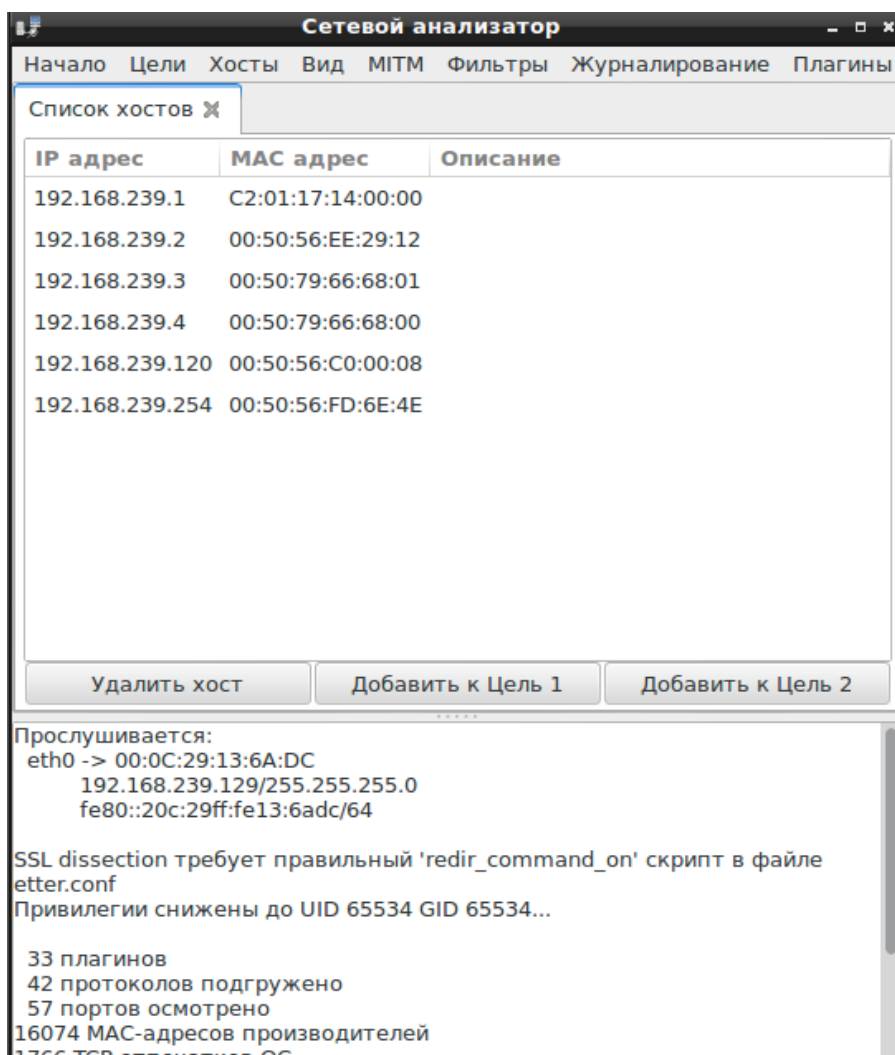


Рисунок 107 — Список хостов

В меню **Цели** необходимо указать адреса хостов, которые будут проанализированы. Для выбора нового хоста необходимо нажать **Выбор цели (целей)** (Рисунок 108), далее указать IP-адрес. Или из списка хостов выбрать IP-адрес и нажать **Добавить к цели 1** или **Добавить к цели 2** (Рисунок 107). Для просмотра и редактирования списка текущих целей необходимо выбрать подменю **Цели** → **Текущие цели** (Рисунок 109).

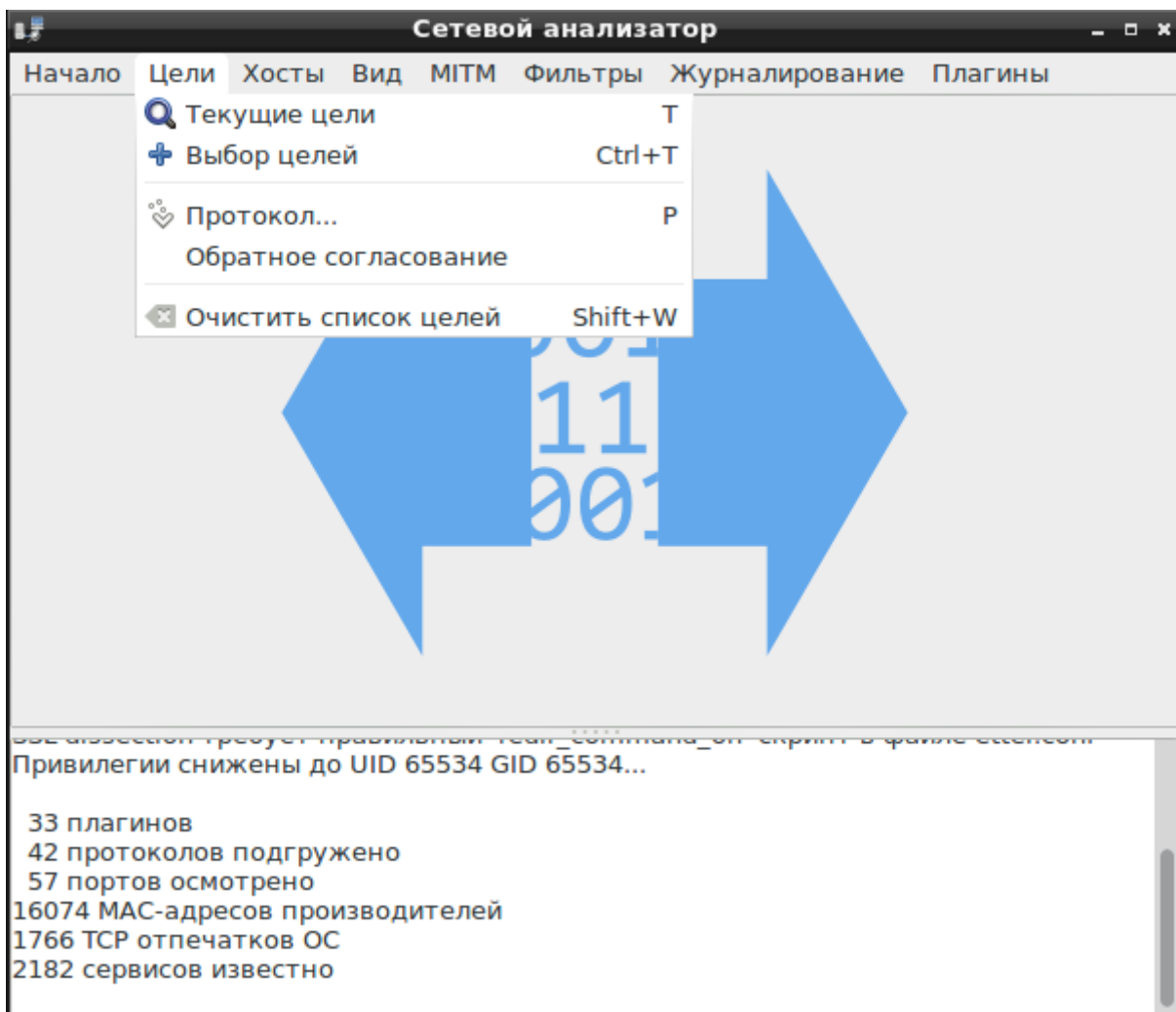


Рисунок 108 — Меню «Цели»

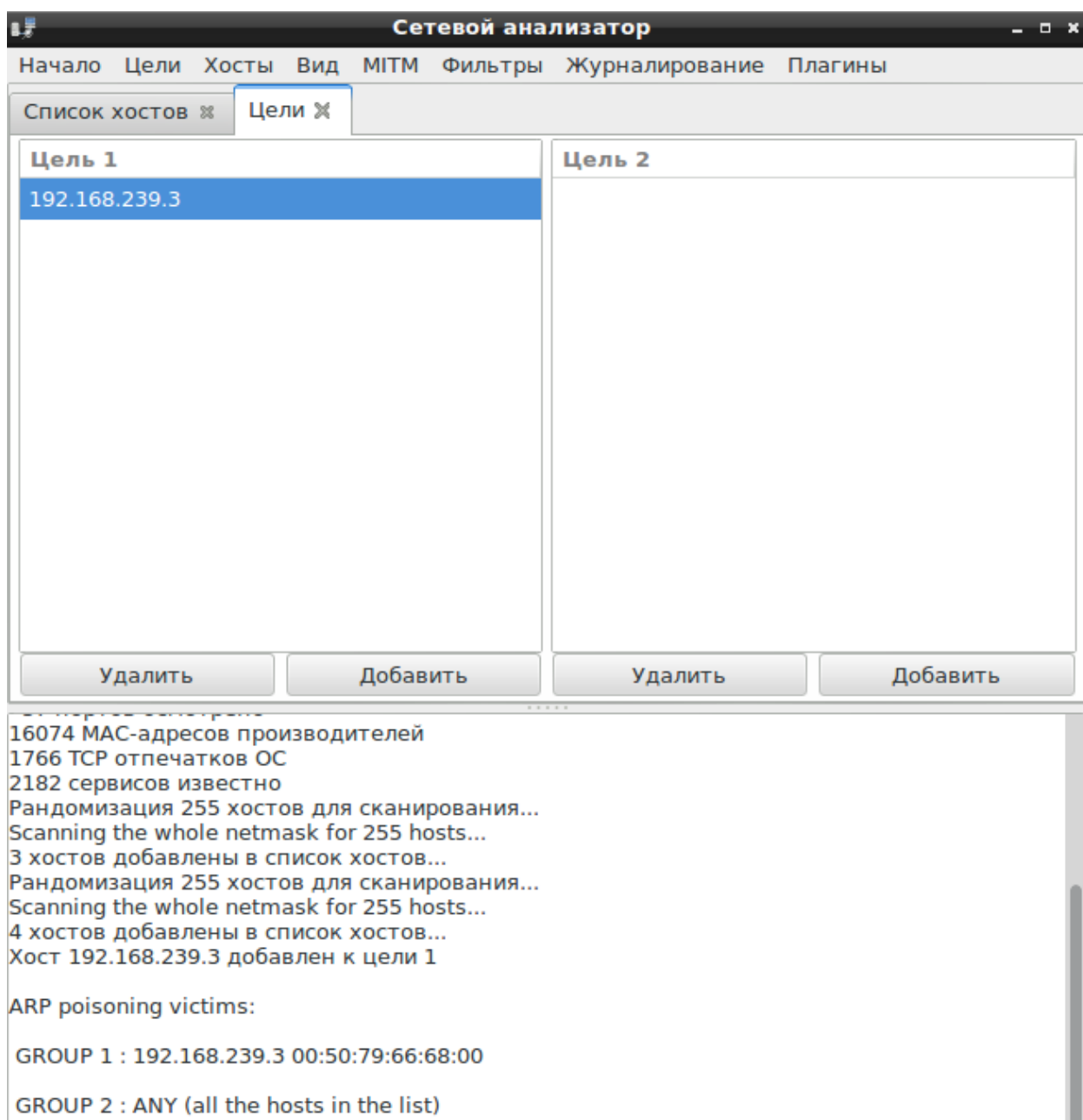


Рисунок 109 — Список текущих целей

Для определения протокола по которому будет производиться анализ выбранных целей, необходимо выбрать подменю Цели → **Протокол...** и в открывшемся окне (Рисунок 110) указать название протокола. Для использования всех протоколов необходимо вписать **all**.

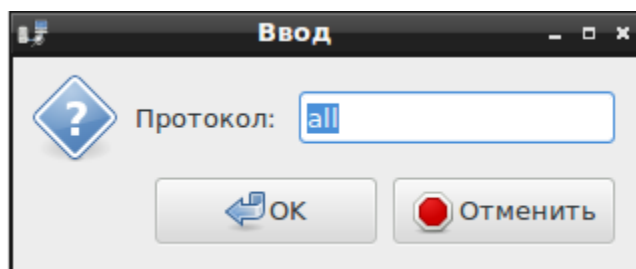


Рисунок 110 — Выбор используемых протоколов

Для просмотра информации о параметрах установленных соединений необходимо выбрать подменю **Вид** → **Соединения** (Рисунок 111, Рисунок 112).

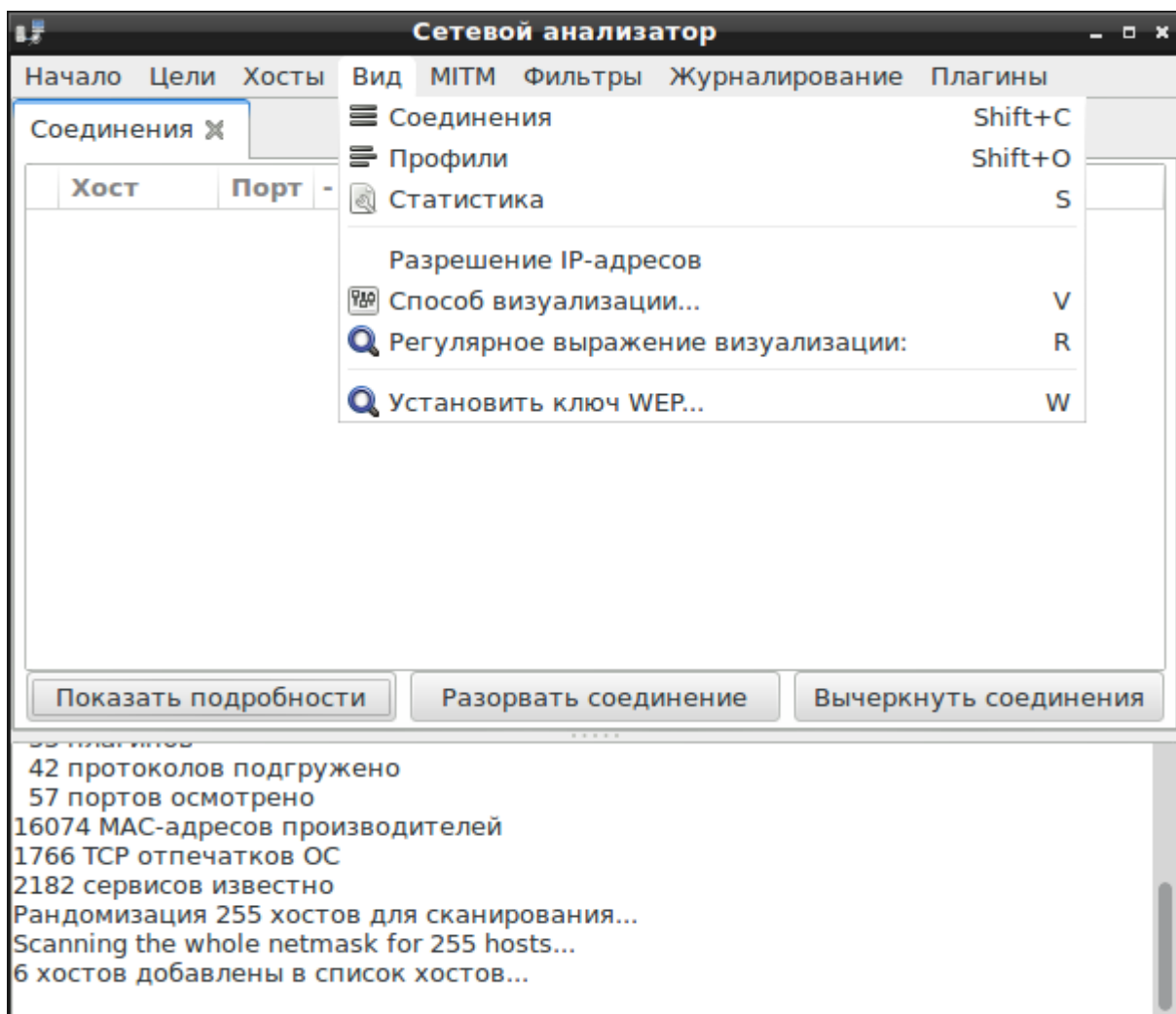


Рисунок 111 — Меню «Вид»

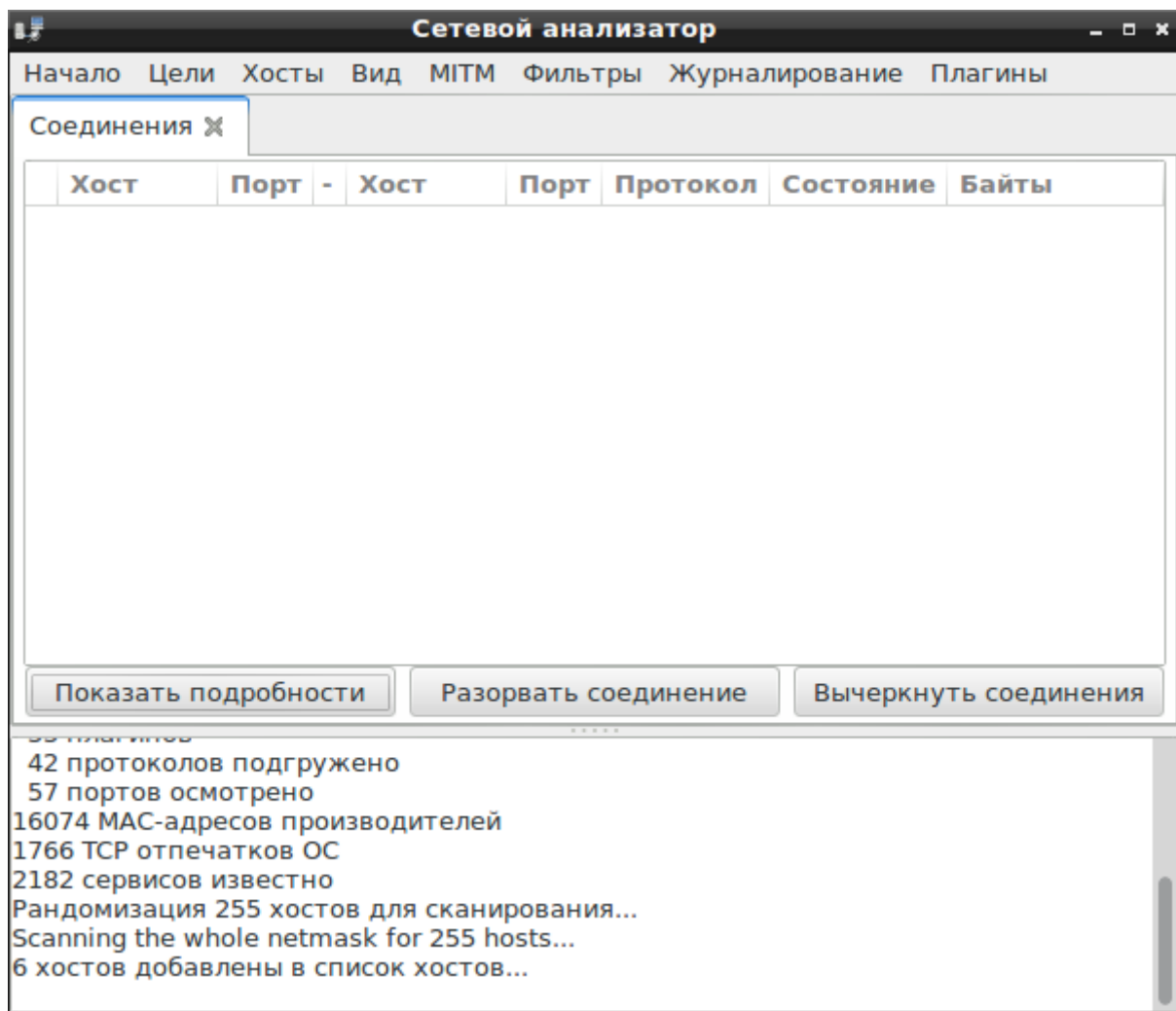


Рисунок 112 — Подменю «Соединения»

Подменю **Вид** → **Профили** содержит список IP-адресов анализируемой сети, который может быть преобразован в список хостов (Рисунок 113).

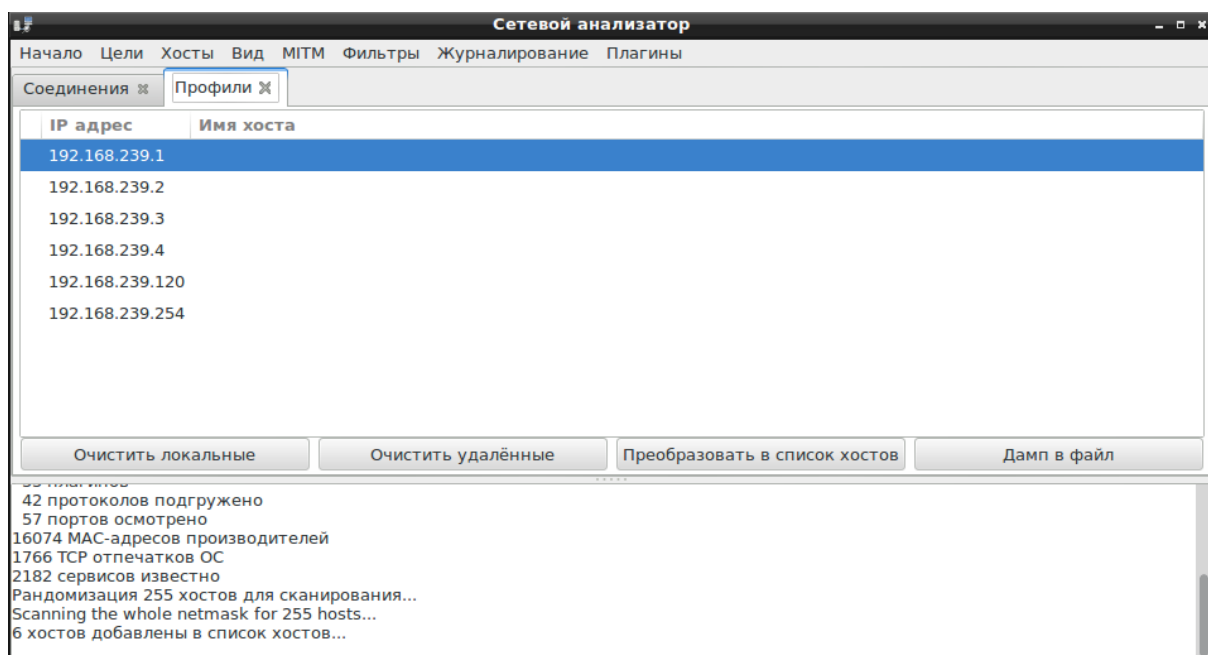


Рисунок 113 — Подменю «Профили»

В подменю **Вид** → **Статистика** отображена подробная информация о получении и передачи пакетов (Рисунок 114).

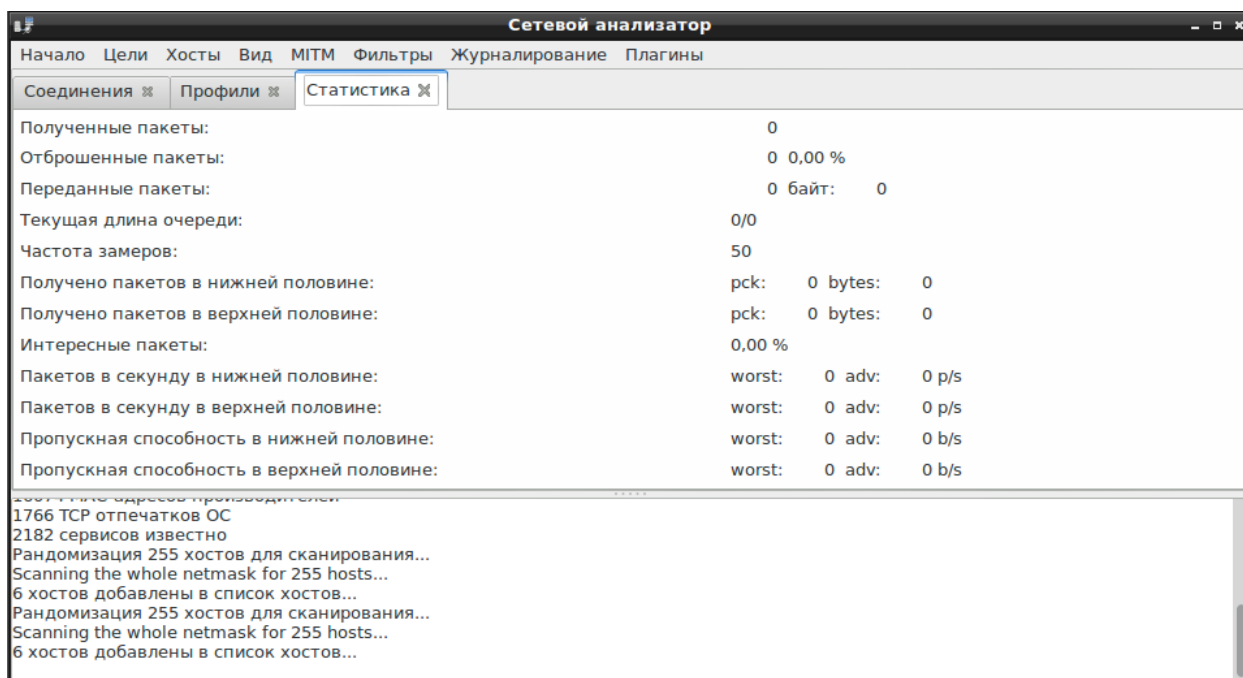


Рисунок 114 — Подменю «Статистика»

В подменю **Вид** → **Способ визуализации...** можно указать различные варианты отображения и форматирования пакетов и символов, а также установить кодировку, которую модуль сможет преобразовать в UTF8 (Рисунок 115).

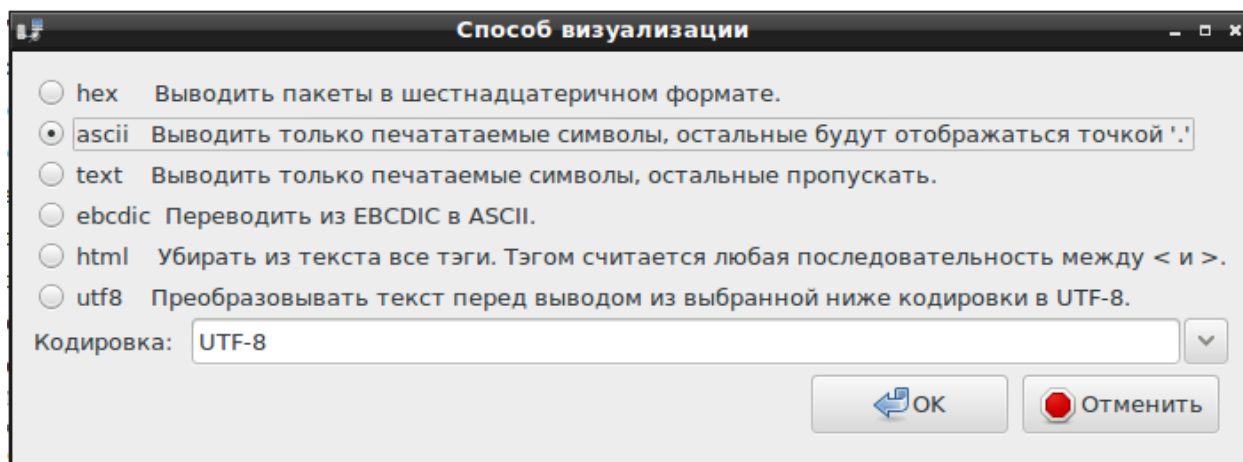


Рисунок 115 — Способы визуализации

В подменю **Вид** → **Регулярное выражение визуализации** можно задать выражение для визуализации (Рисунок 116).

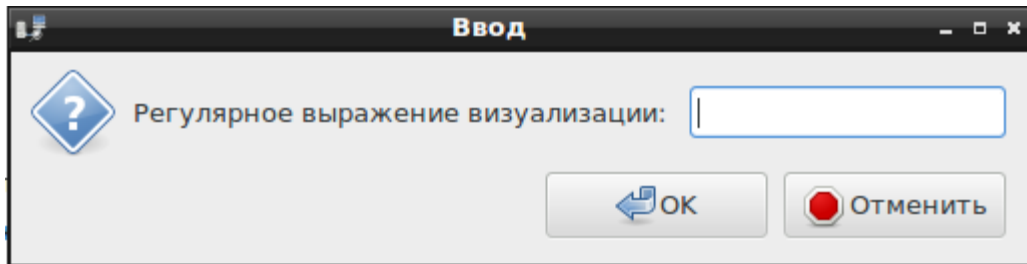


Рисунок 116 — Регулярное выражение визуализации

В подменю **Вид** → **Установить ключ WEP...** необходимо указать ключ WEP-шифрования, применяемый в анализируемой беспроводной сети (Рисунок 117).

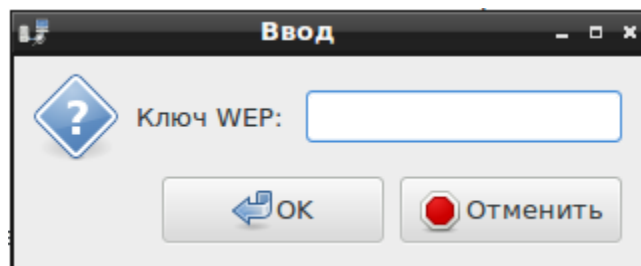


Рисунок 117 — Ввод ключа WEP

Для сортировки информации, полученной в ходе анализа необходимо выбрать подменю **Фильтры** → **Загрузить фильтр...** (Рисунок 118).

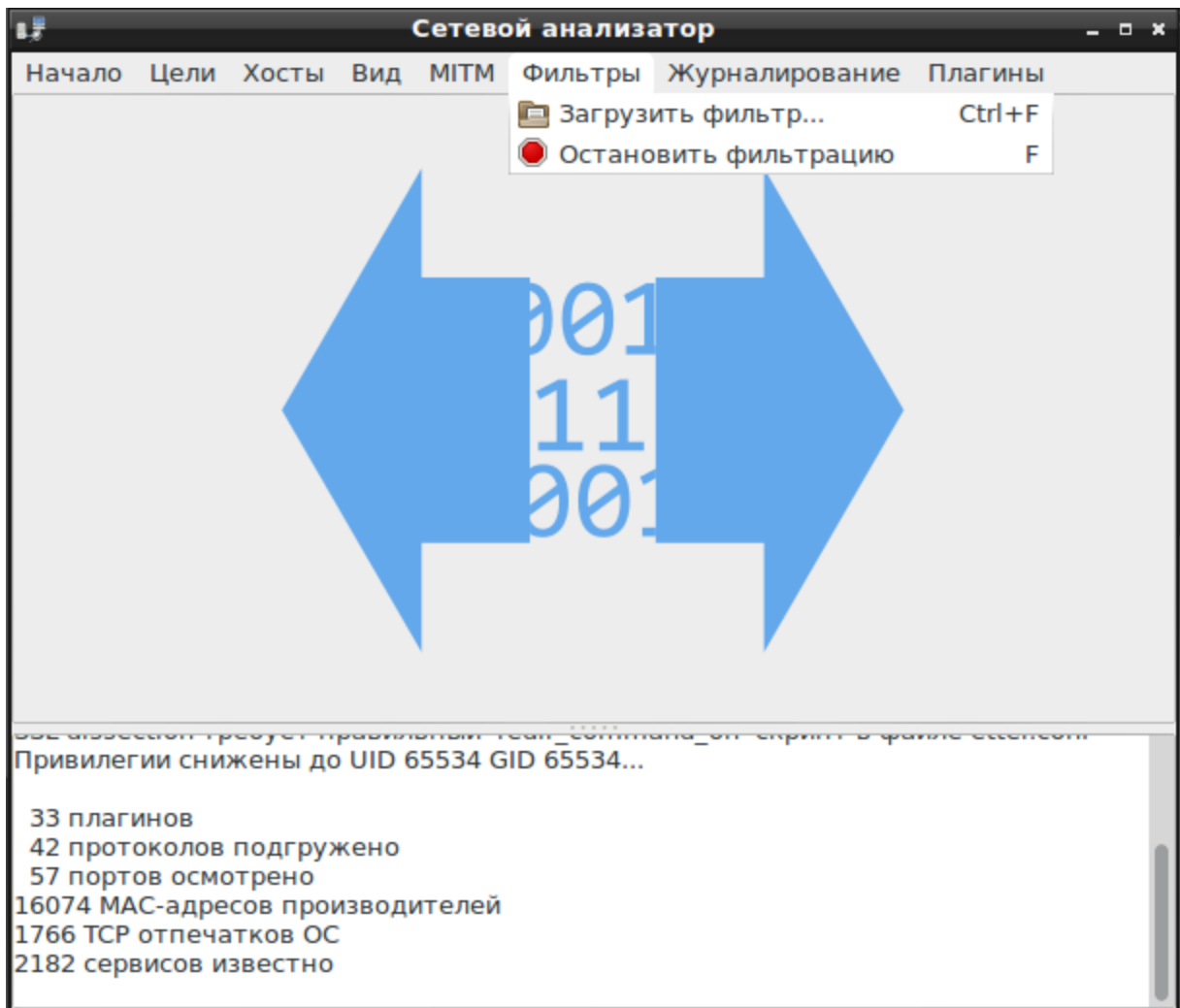


Рисунок 118 — Меню «Фильтры»

Оператор может вести журнал, в котором фиксируются запрашиваемые параметры. Для этого необходимо в меню **Журналирование** (Рисунок 119) указать тип журнала и его имя в открывшемся окне ввода файла журнала (Рисунок 120).

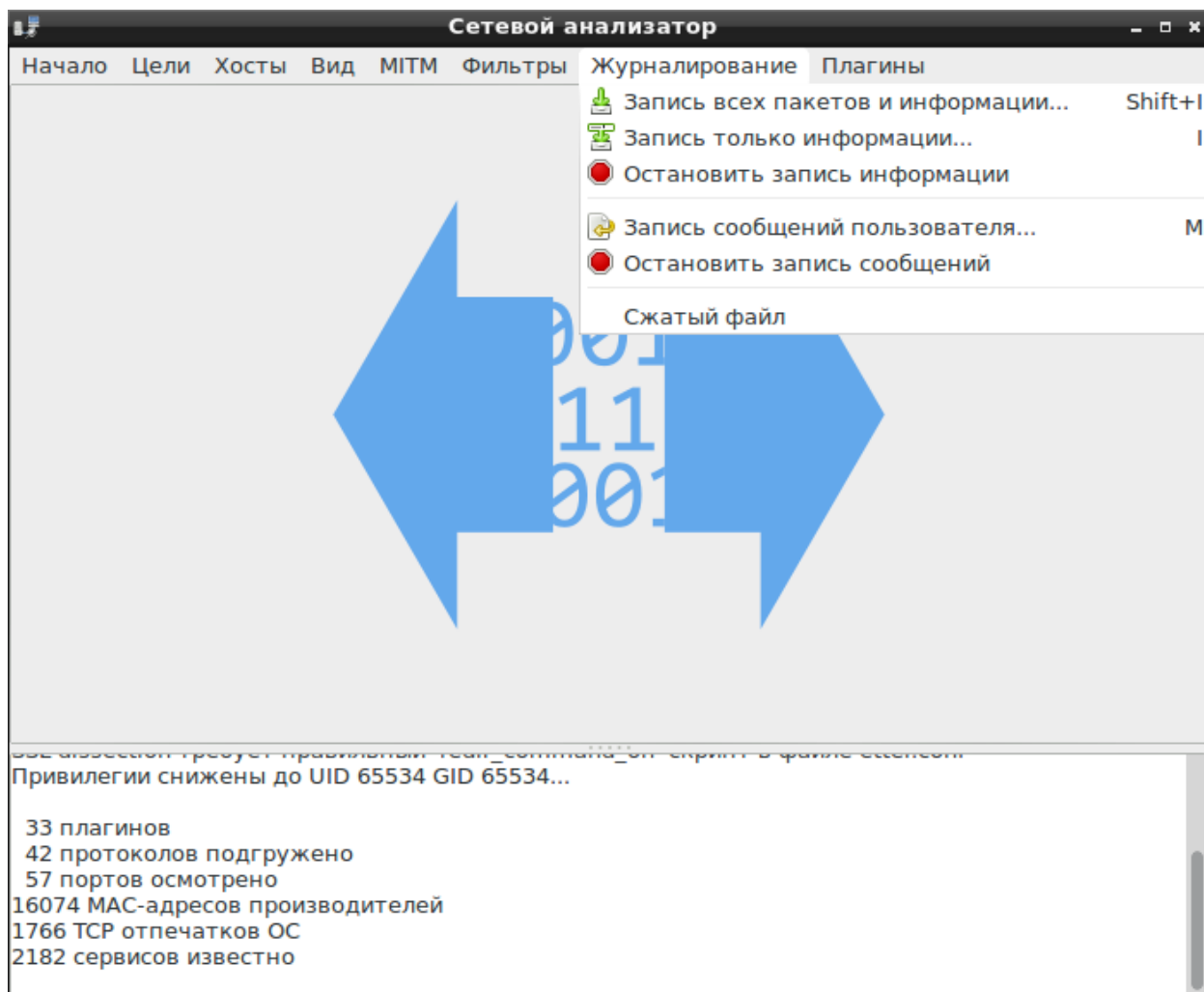


Рисунок 119 — Меню «Журналирование»

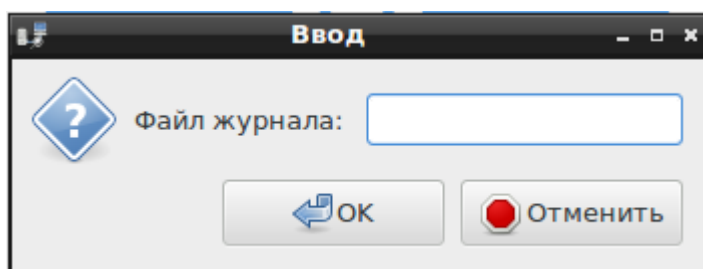


Рисунок 120 — Файл журнала

В модуле реализована функция использования различных плагинов для всестороннего анализа сети.

Для использования необходимого плагина следует загрузить его с помощью подменю **Плагины** → **Менеджер плагинов** (Рисунок 121).

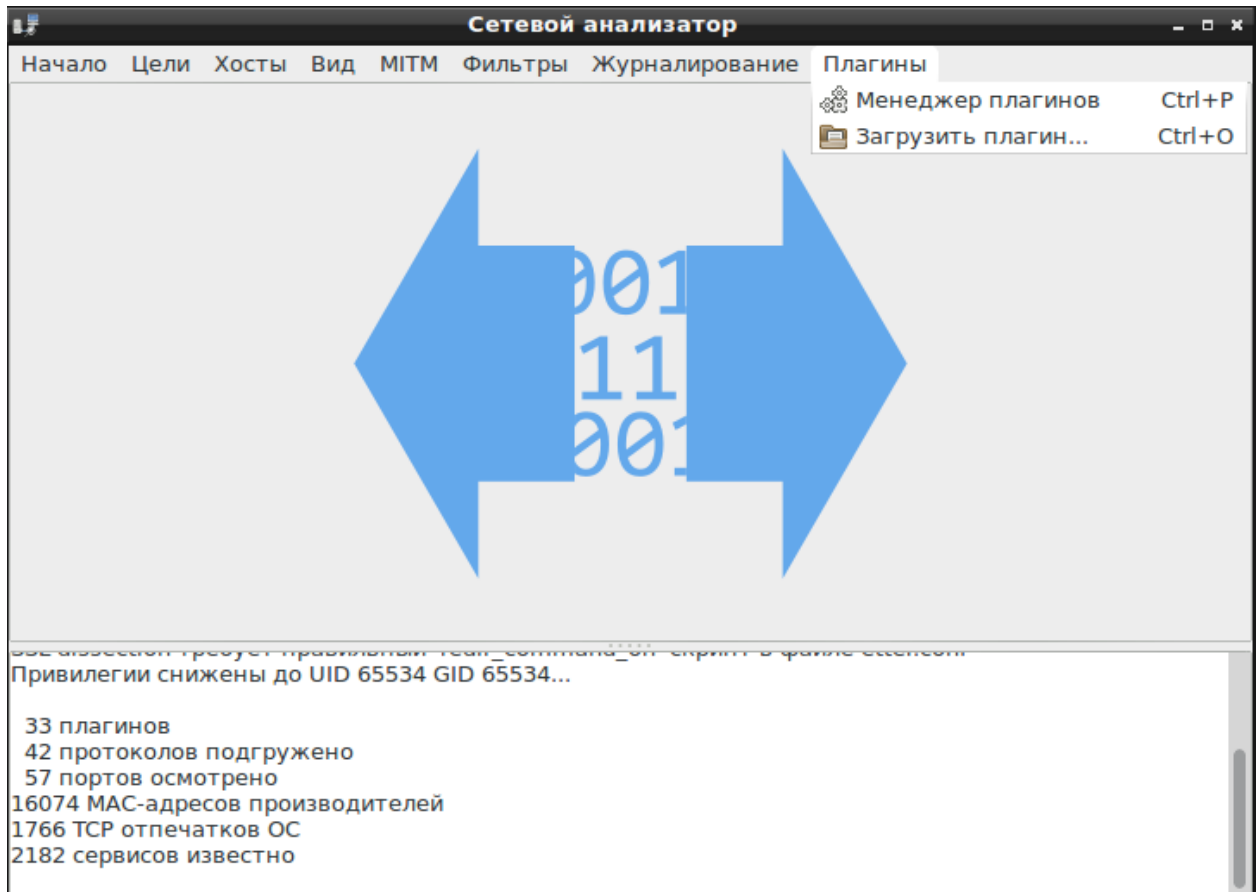


Рисунок 121 — Меню «Плагины»

В появившемся окне следует выбрать необходимые плагины из представленного списка с помощью двойного нажатия левой кнопки мыши на их именах (Рисунок 122).

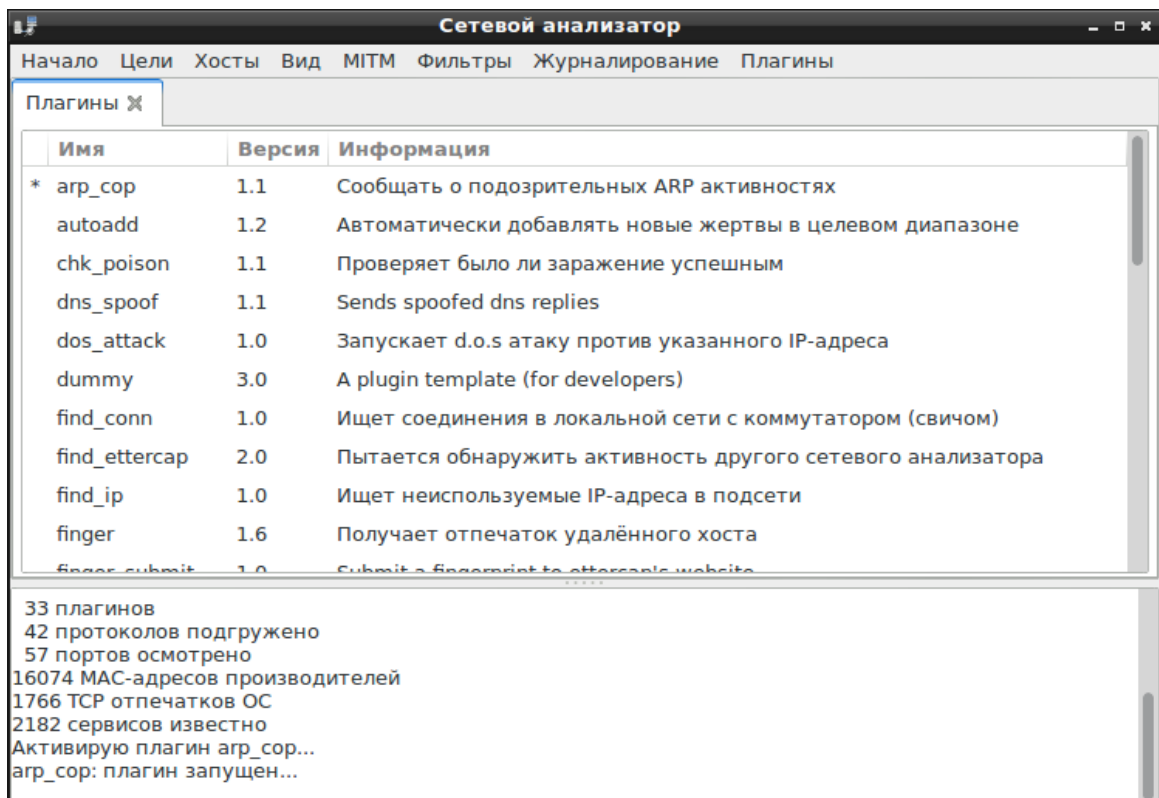


Рисунок 122 — Выбор плагина арр_сop

3.7.8.3. Работа с модулем в обычной сети

Для запуска процесса анализа локальной сети необходимо выбрать пункт меню **Мониторинг** → **Обычная сеть...** (Рисунок 104).

Далее в появившемся окне необходимо указать сетевой интерфейс и нажать **ОК** (Рисунок 123).

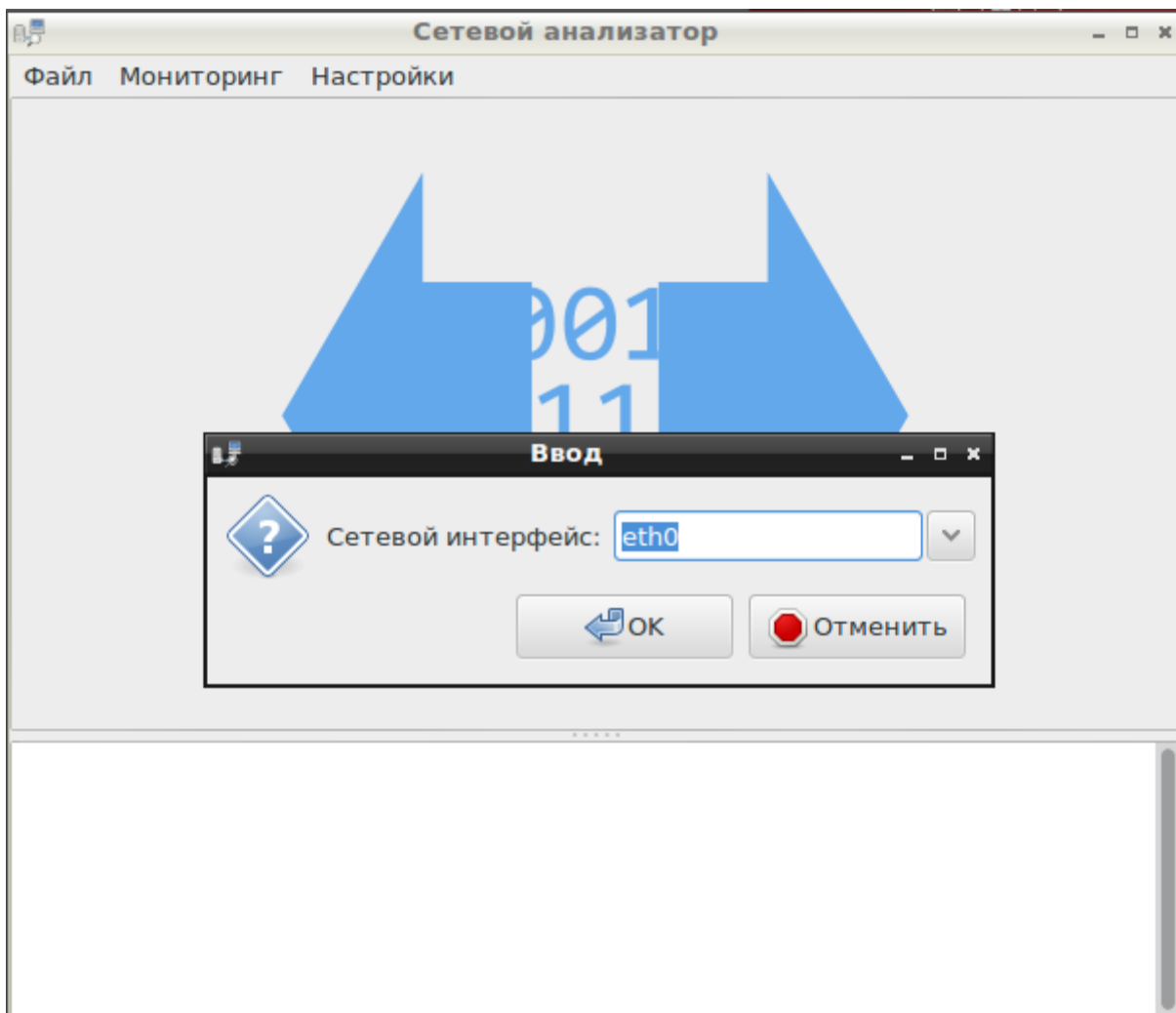


Рисунок 123 — Ввод сетевого интерфейса

Для запуска процесса анализа сетевого трафика необходимо выбрать пункт меню **Начало** → **Начать мониторинг** (Рисунок 105).

3.7.8.4. Атаки типа MITM

Для начала анализа необходимо определить IP-адреса хостов сети. Для этого необходимо выбрать подменю **Хосты** → **Сканирование хостов** (Рисунок 106). В подменю **Хосты** → **Список хостов** будет представлена информация о просканированных хостах сети (Рисунок 107).

В меню **Цели** необходимо указать адреса хостов, которые будут проанализированы (Рисунок 108).

Для осуществления атаки ARP-poisoning необходимо выбрать подменю **MITM** → **Атака "ARP poisoning"...** (Рисунок 124).

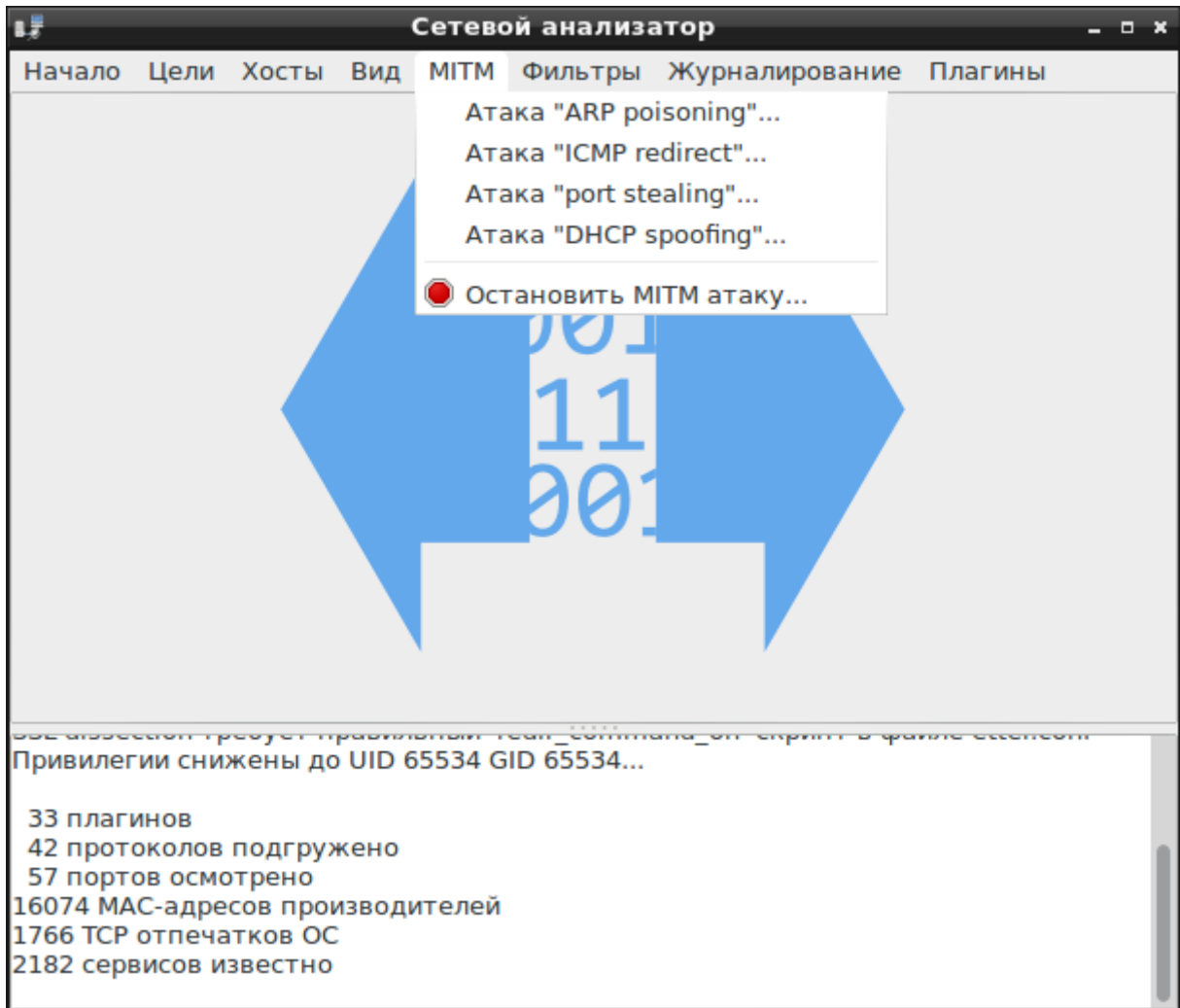


Рисунок 124 — Меню «MITM»

В результате атаки весь трафик от цели будет проходить через хост, на котором установлен ПК «Сканер-ВС» (Рисунок 125).

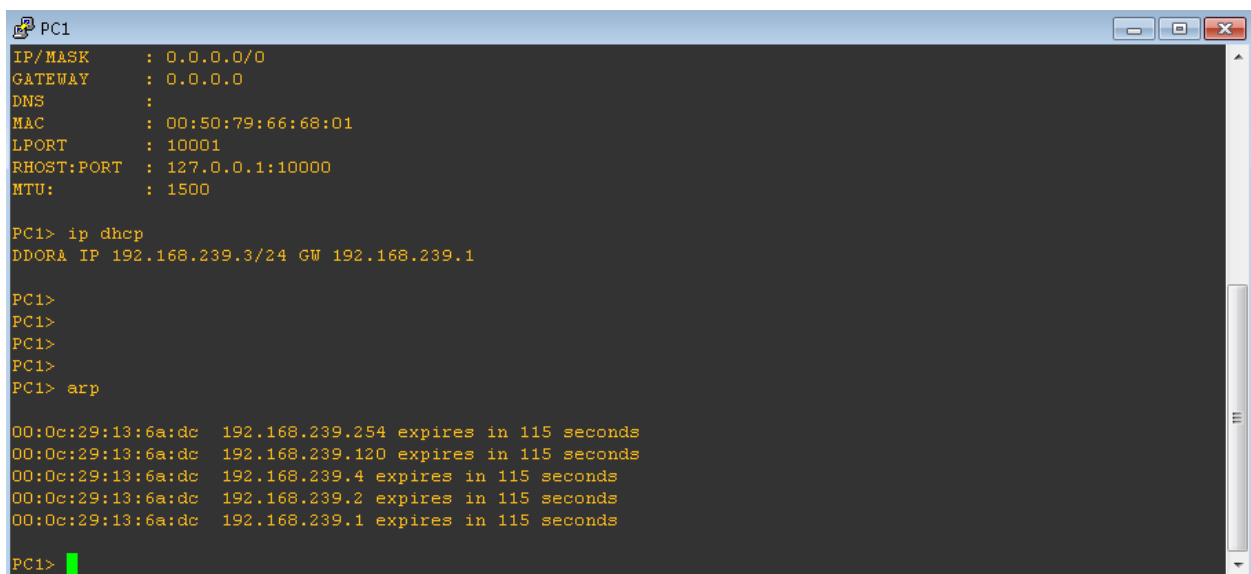


Рисунок 125 — Результат атаки

Чтобы остановить атаку необходимо выбрать подменю **MITM** → **Остановить MITM атаку** (Рисунок 124).

Для осуществления атаки ICMP redirect необходимо выбрать подменю **MITM** → **Атака "ICMP redirect"...** (Рисунок 124). В появившемся окне необходимо указать сведения о шлюзе сети (Рисунок 126).

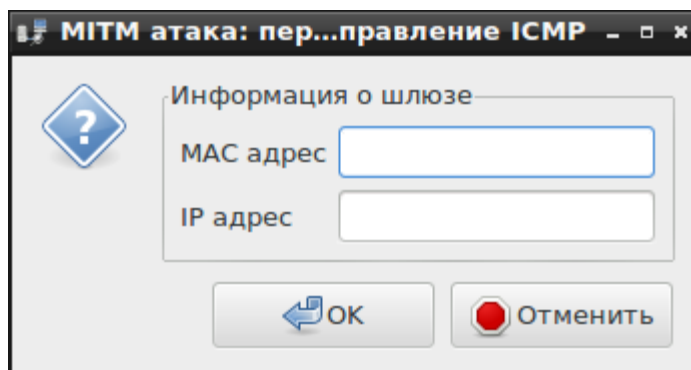


Рисунок 126 — Информация о шлюзе сети

В результате атаки ICMP пакеты будут перенаправлены от цели на хост ПК «Сканер-ВС». Чтобы остановить атаку необходимо выбрать подменю **MITM** → **Остановить MITM атаку** (Рисунок 124).

Для осуществления атаки port stealing необходимо выбрать подменю **MITM** → **Атака "port stealing"...** (Рисунок 124). В появившемся окне можно указать дополнительные параметры атаки (Рисунок 127).

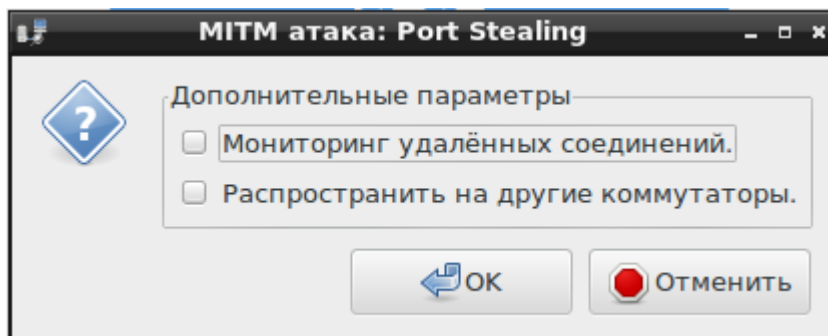


Рисунок 127 — Параметры атаки

Результатом атаки будет являться перенаправление трафика от цели к какому-либо порту на хост ПК «Сканер-ВС». Чтобы остановить атаку необходимо выбрать подменю **MITM** → **Остановить MITM атаку** (Рисунок 124).

Для осуществления атаки DHCP spoofing необходимо выбрать подменю **MITM** → **Атака "DHCP spoofing"...** (Рисунок 124). В появившемся окне необходимо указать информацию о сервере (Рисунок 128).

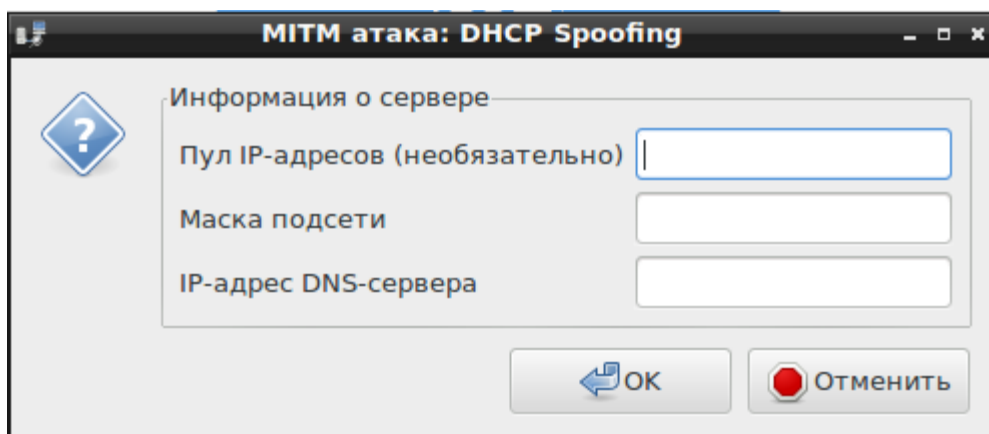


Рисунок 128 — Информация о сервере DHCP

В результате атаки хост ПК «Сканер-ВС» будет использоваться как DHCP-сервер сети по умолчанию. Чтобы остановить атаку необходимо выбрать подменю **MITM** → **Остановить MITM атаку** (Рисунок 124).

3.7.8.5. Работа с модулем в коммутируемой сети

Для работы модуля в коммутируемой сети необходимо выбрать пункт меню **Мониторинг** → **Коммутируемая сеть...** (Рисунок 104). Для корректной работы анализатора в коммутируемой сети необходимо указывать первый и второй сетевые интерфейсы (Рисунок 129).

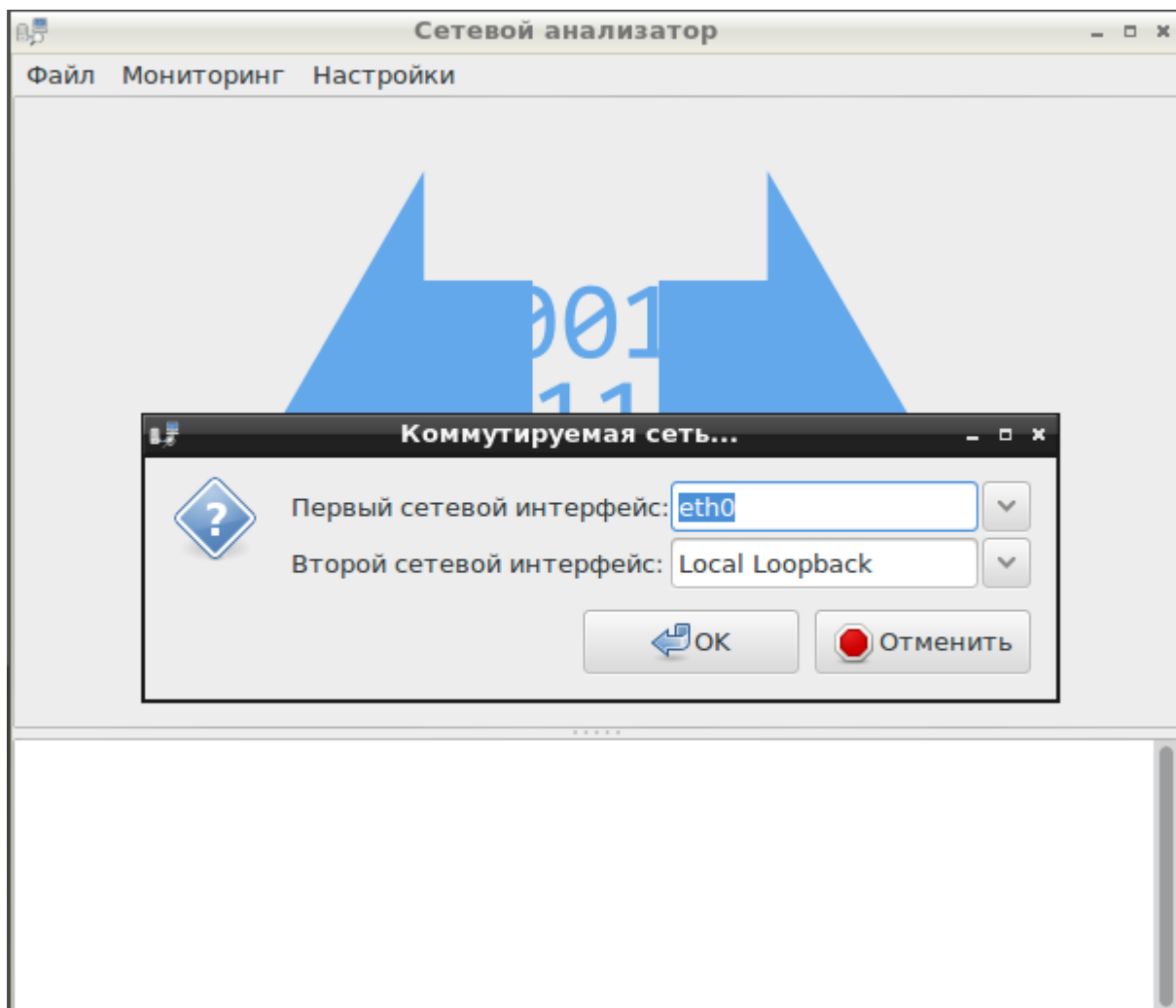




Рисунок 129 — Мониторинг коммутируемой сети

В рабочем окне модуля (Рисунок 103) необходимо задать цели, протокол и другие параметры анализа.

3.7.8.6. Завершение работы с модулем

Для выхода из модуля необходимо воспользоваться подменю  **Выход** меню **Начало** (Рисунок 105) или подменю  **Выход** меню **Файл**.

3.7.9. Средство контрольного суммирования

Средство контрольного суммирования предназначено для контроля целостности информации.

3.7.9.1. Запуск модуля

Модуль запускается из веб-интерфейса **Контрольное суммирование** или из подменю стартера приложений (red hat) → **Форензика** → **ПИК Эшелон**.

После запуска появится рабочее окно модуля (Рисунок 130).

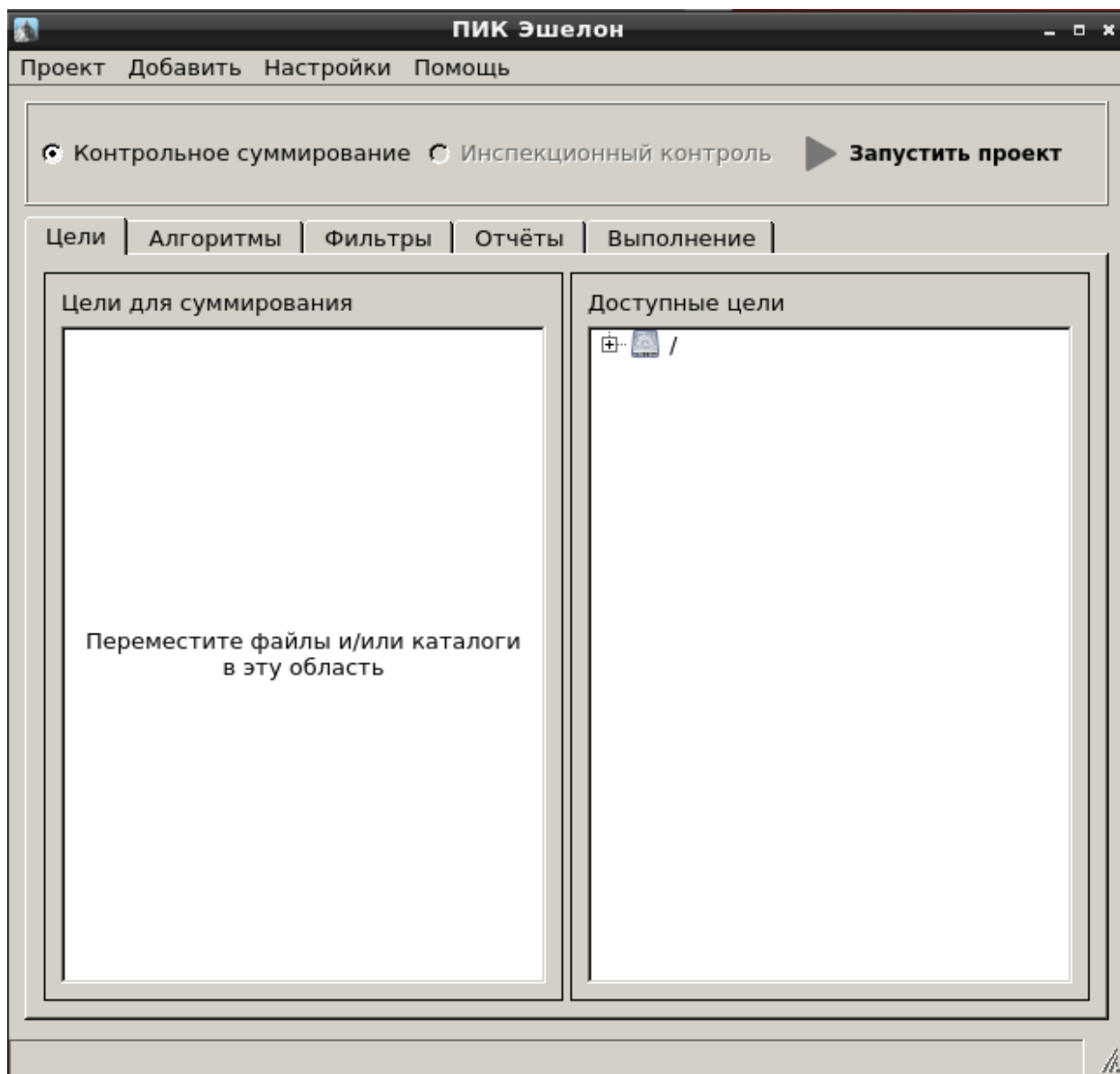


Рисунок 130 — Рабочее окно модуля

3.7.9.2. Работа с модулем

В модуле доступна только функция контрольного суммирования. Для использования функции инспекционного контроля программного обеспечения необходимо приобрести отдельный продукт АО «НПО Эшелон» «Программа инспекционного контроля «ПИК-Эшелон».

3.7.9.3. Контрольное суммирование

Рабочее окно средства контрольного суммирования содержит вкладки: **Цели**, **Алгоритмы**, **Фильтры**, **Отчеты**, **Выполнение**.

Вкладка **Цели** позволяет выбирать файлы для суммирования и содержит поля **Цели для суммирования** и **Доступные цели** (Рисунок 130).

В поле **Доступные цели** можно выбрать путь к диску, файлу или папке и переместить в поле **Цели для суммирования**.

В поле **Цели для суммирования** можно добавить или удалить диск, файл или папку, нажав правой кнопкой мыши и выбрав соответствующее действие.

Во вкладке **Алгоритмы** приведены краткие описания алгоритмов, используемых для проведения контроля (Рисунок 131). Выбрать алгоритмы суммирования можно вручную или воспользоваться кнопками **Выбрать стойкие** и **Выбрать все**. Для очистки списка выбранных алгоритмов можно воспользоваться кнопкой **Очистить всё**.

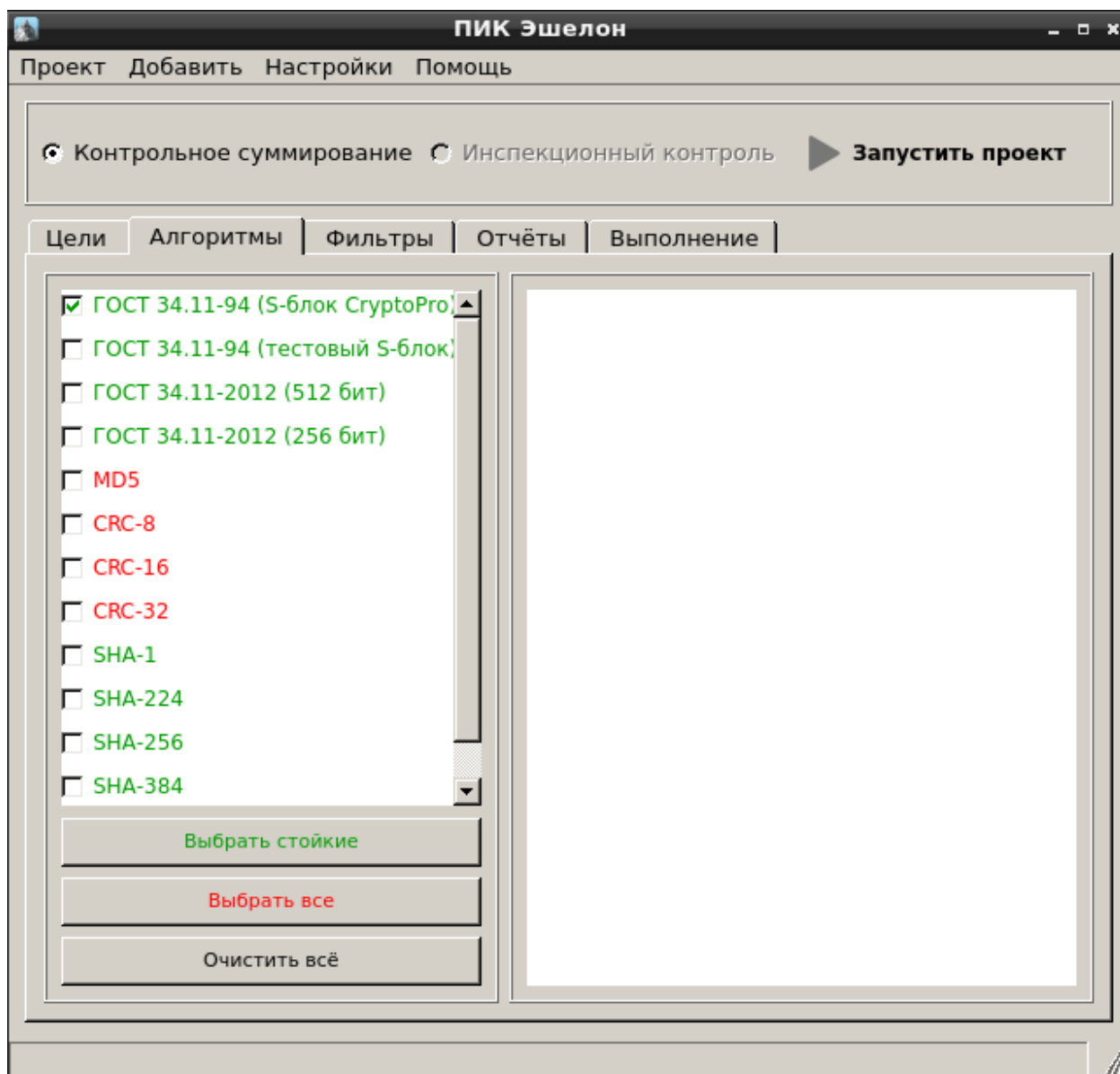


Рисунок 131 — Алгоритмы контрольного суммирования

В модуле реализована функция фильтрации по расширениям файлов. Во вкладке **Фильтры** указаны типовые расширения файлов (Рисунок 132).

По умолчанию в поле **Выбранные фильтры** указано «Все файлы». Чтобы ввести ограничение на расширения файлов для контрольного суммирования, необходимо перетащить название фильтра из поля **Доступные фильтры** в поле **Выбранные фильтры**.

При нажатии на правую кнопку мыши в поле **Доступные фильтры** появится меню (Рисунок 132), позволяющее удалить или изменить расширение из списка подменю (**Удалить** и **Изменить** соответственно). При выборе подменю **Загрузить стандартные расширения** будет восстановлен список по умолчанию.

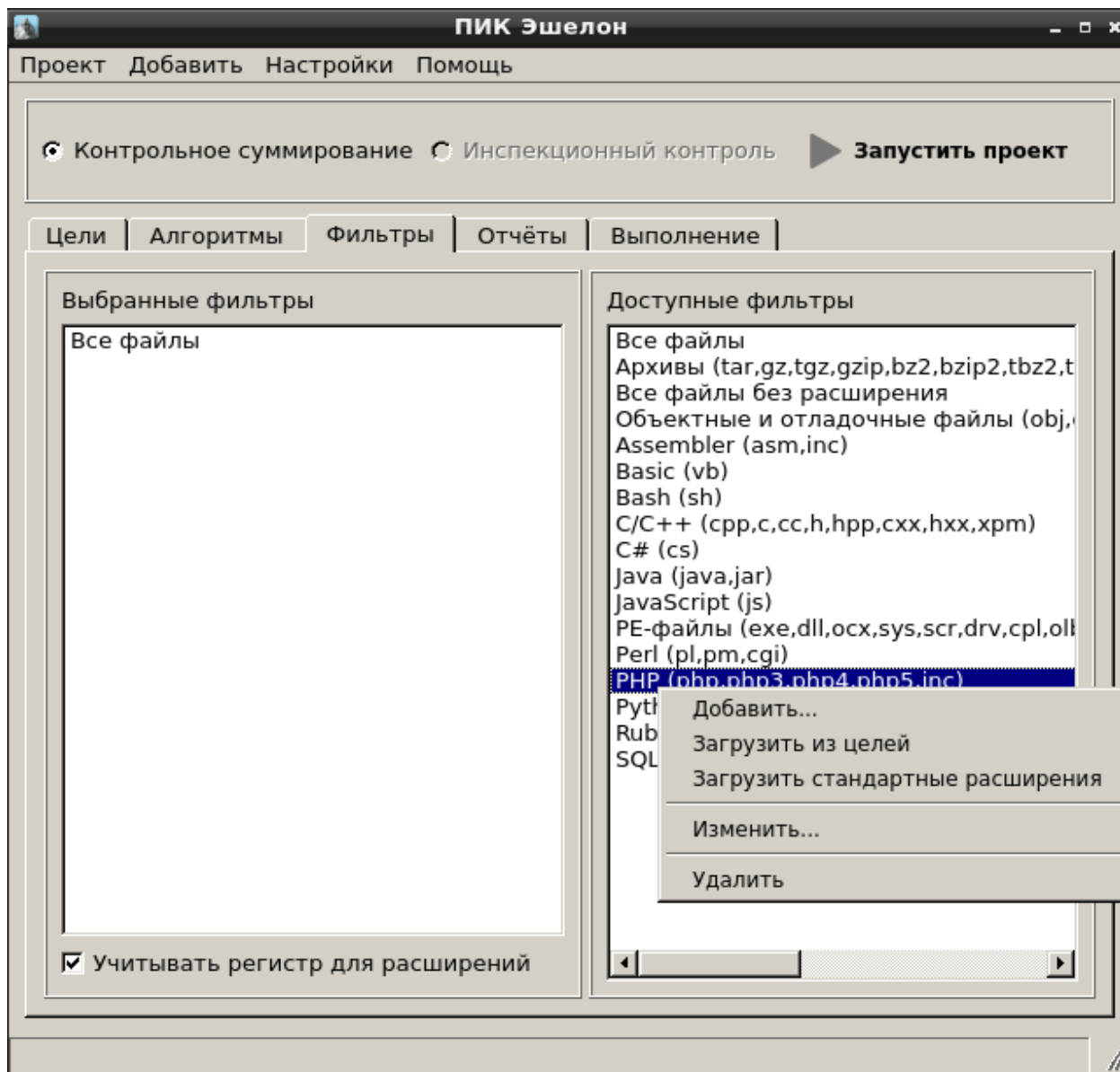


Рисунок 132 — Доступные фильтры

Чтобы вручную указать расширения, принимаемые на контроль необходимо выбрать подменю **Добавить**. С помощью подменю **Загрузить из целей** можно добавить фильтр из расширений файлов, выбранных для контрольного суммирования (Рисунок 132).

Во вкладке **Отчёты** можно указать директорию для сохранения отчетов (по умолчанию - Рабочий стол), ввести название папки для сохранения отчетов (по умолчанию - MyProject), выбрать вид отчетов и указать другие настройки (Рисунок 133).

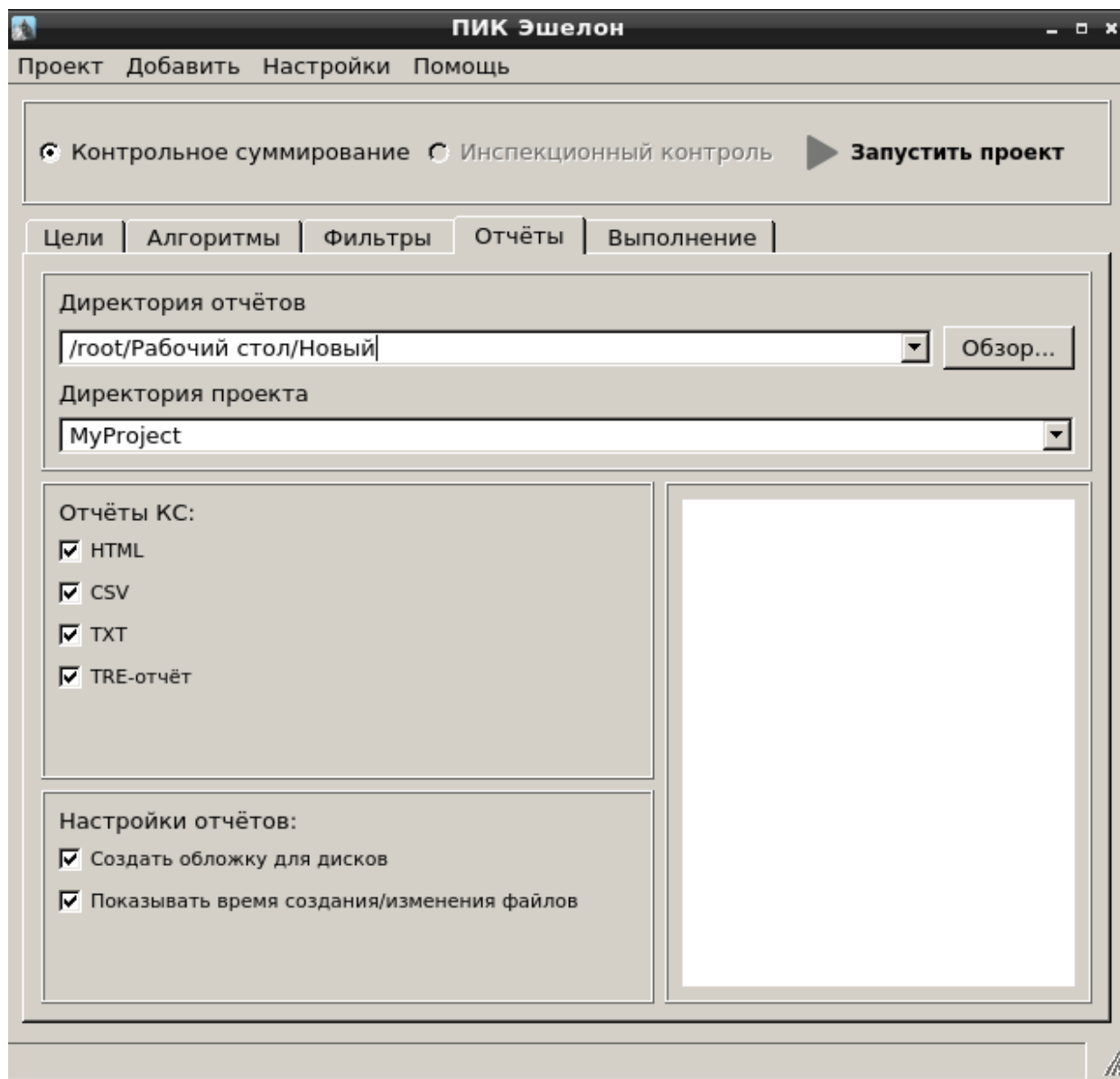


Рисунок 133 — Вкладка «Отчеты»

Для запуска процесса контрольного суммирования необходимо нажать **Запустить проект**. После запуска процесса во вкладке **Выполнение** будет отображаться процесс выполнения задачи. После завершения контрольного суммирования необходимо нажать на кнопку **Открыть директорию с отчётами** (Рисунок 134).

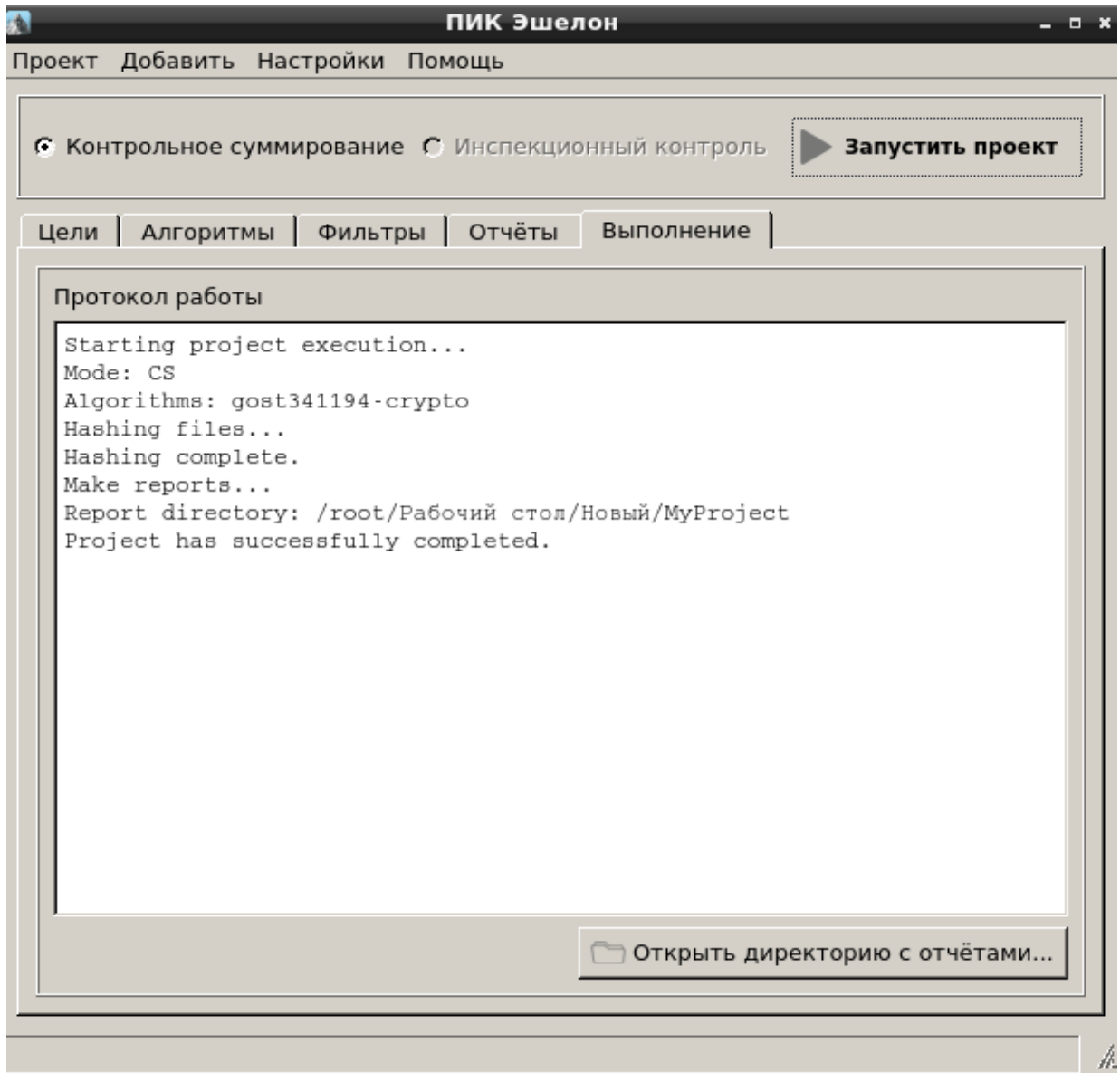


Рисунок 134 — Вкладка «Выполнение»


Отчет в формате HTML может содержать следующие вкладки: **Статистика проекта** (Рисунок 135), **Контрольные суммы** (Рисунок 136), **Дополнительные отчеты** (Рисунок 137).

Статистика проекта - отчёт по КС - Mozilla Firefox

Статистика проекта - ... x


file:///root/Рабочий стол/Новый/MyProject/cs_report-2017-04-21-: Поиск

Отчёт по контрольным суммам (КС) проекта "MyProject" от 21.04.2017


ППК Эшелон 1.0.06
 Владелец лицензии: "Демо-версия" № 1. Срок действия лицензии с 09.09.2016 по 09.09.2017.

Статистика проекта **Контрольные суммы** Дополнительные отчёты

| | |
|---|--|
| Локации | "/usr/games" |
| Файлов обработано | 0 |
| Директорий обработано | 1 |
| Размер | 0 байт |
| Время анализа | Начался: 21-04-2017 11:18:20 Закончился: 21-04-2017 11:18:20 |
| Повторяющиеся имена | 0 |
| Повторяющиеся КС | 0 |
| Количество расширений | 0 |
| Использованные фильтры | Все файлы |
| Контрольные суммы проекта | |
| ГОСТ 34.11-94 (S-блок CryptoPro) | 7cc8212687198c2f956d23b70fafa2d1513bf77f1dcbd7a35e2cdb6ecb20d6cd |
| Контрольные суммы локации "/usr/games" | |
| ГОСТ 34.11-94 (S-блок CryptoPro) | 981e5f3ca30c841487830f84fb433e13ac1101569b9c13584ac483234cd656c0 |


Эшелон
 комплексная безопасность

"ППК Эшелон" программное обеспечение © ЗАО "НПО "Эшелон" <http://cnpo.ru/>
 Контакты технической поддержки продукта: support.pik@cnpo.ru


Рисунок 135 — Статистика проекта

Контрольные суммы - отчёт по КС - Mozilla Firefox

Контрольные суммы - ... x

file:///root/Рабочий стол/Новый/MyProject/cs_report-2017-04-21-11-18-20-756/index.html#t Поиск


Отчёт по контрольным суммам (КС) проекта "MyProject" от 21.04.2017


ППК Эшелон 1.0.06
 Владелец лицензии: "Демо-версия" № 1. Срок действия лицензии с 09.09.2016 по 09.09.2017.

Статистика проекта **Контрольные суммы** Дополнительные отчёты

| Номер | Имя файла | Размер | Время создания | Время изменения | ГОСТ 34.11-94 (S-блок CryptoPro) |
|-------|------------|--------|---------------------|---------------------|--|
| | /usr/games | | 23-07-2015 07:00:44 | 23-07-2015 07:00:44 | 981e5f3ca30c841487830f84fb433e13ac1101569b9c13584ac483234cd656c0 |

+ Раскрыть все Столбцы


Эшелон
 комплексная безопасность

"ППК Эшелон" программное обеспечение © ЗАО "НПО "Эшелон" <http://cnpo.ru/>
 Контакты технической поддержки продукта: support.pik@cnpo.ru

Рисунок 136 — Контрольные суммы

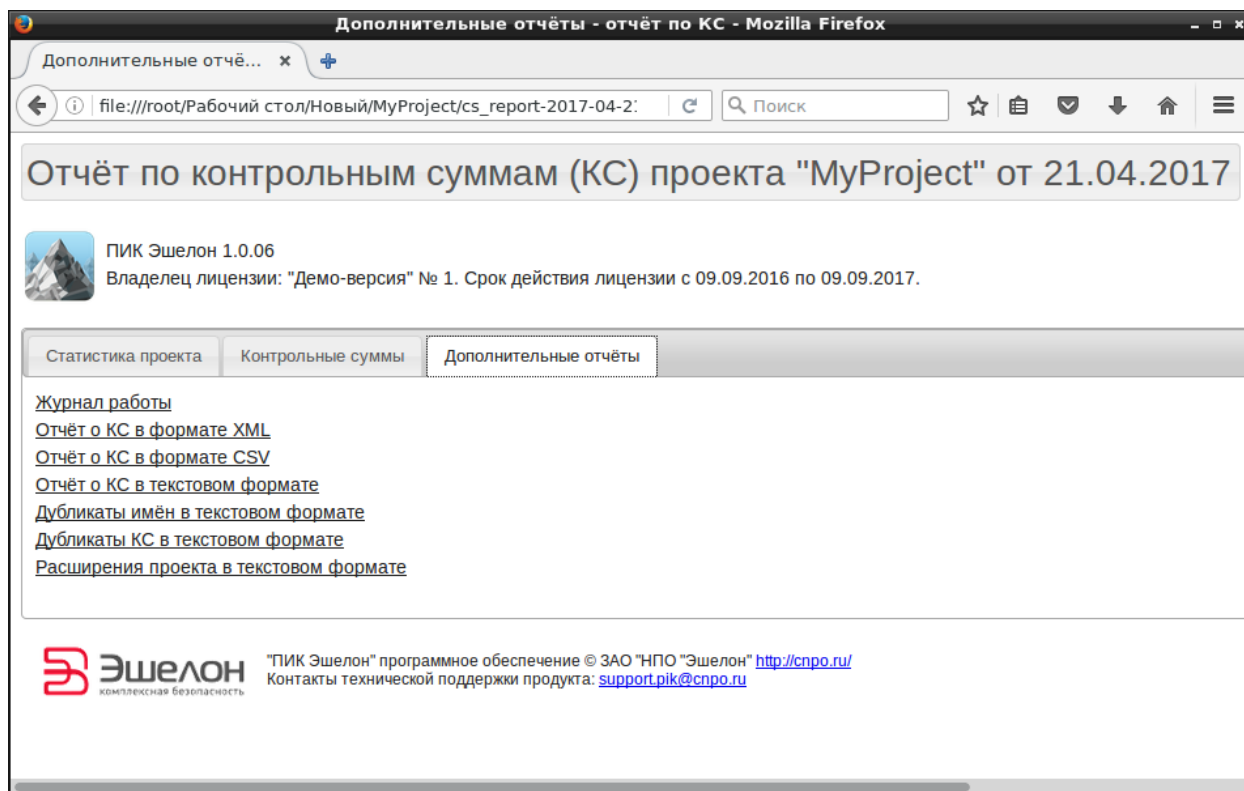


Рисунок 137 — Дополнительные отчеты

3.7.9.4. Завершение работы с модулем

Для выхода из модуля необходимо воспользоваться подменю **Проект** → **Выход** или нажать

 в верхнем правом углу окна.

3.8. Дополнительные модули

3.8.1. Менеджер сетевых подключений «Wicd Network Manager»

Сетевой менеджер представляет собой стандартное меню настроек беспроводных и проводных сетей.

Менеджер запускается из подменю стартера приложений (red hat) → **Остальные приложения** → **Интернет** → **Wicd Network Manager**.

После запуска откроется рабочее окно менеджера (Рисунок 138).

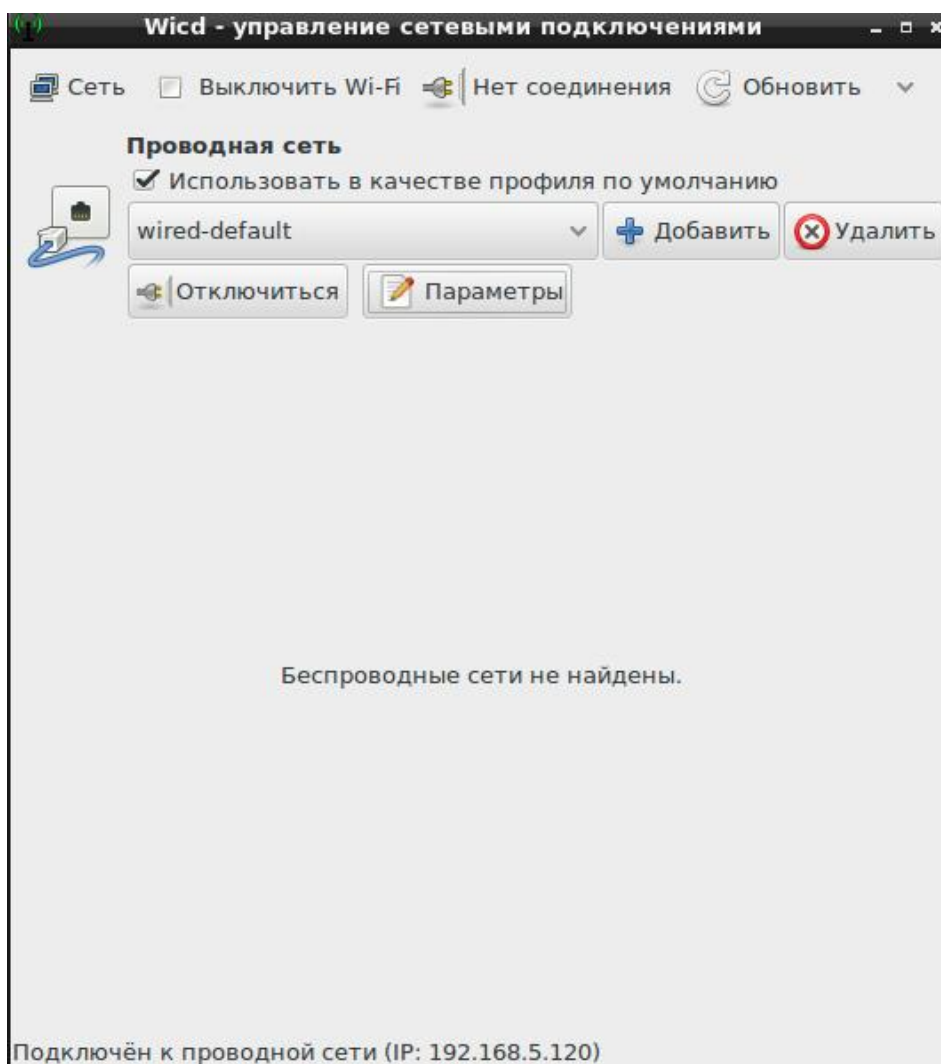


Рисунок 138 – Рабочее окно менеджера

Если в сети есть DHCP-сервер, то компьютер, на котором запущен ПК «Сканер-ВС», автоматически получит IP-адрес. Если DHCP-сервера в сети нет, то для взаимодействия с сетью его можно настроить вручную. Для этого необходимо нажать кнопку **Параметры** (Рисунок 138). Откроется диалоговое окно **Проводная сеть - Параметры** (Рисунок 139), в котором можно вручную задать параметры сети (Рисунок 140), поставив отметку напротив пункта **Использовать статические IP-адреса**.

Примечание. Аналогично производится настройка беспроводных сетей.

Проводная сеть - Параметры

Использовать статические IP

IP

Маска сети

Шлюз

Использовать статический DNS **Использовать глобальные серверы DNS**

Домен DNS

Домен поиска имён

DNS сервер: 1

DNS сервер: 2

DNS сервер: 3


DHCP Hostname

Использовать шифрование

802.1x

Идентификация

Пароль



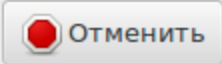

 

Рисунок 139 – Параметры сетевого подключения

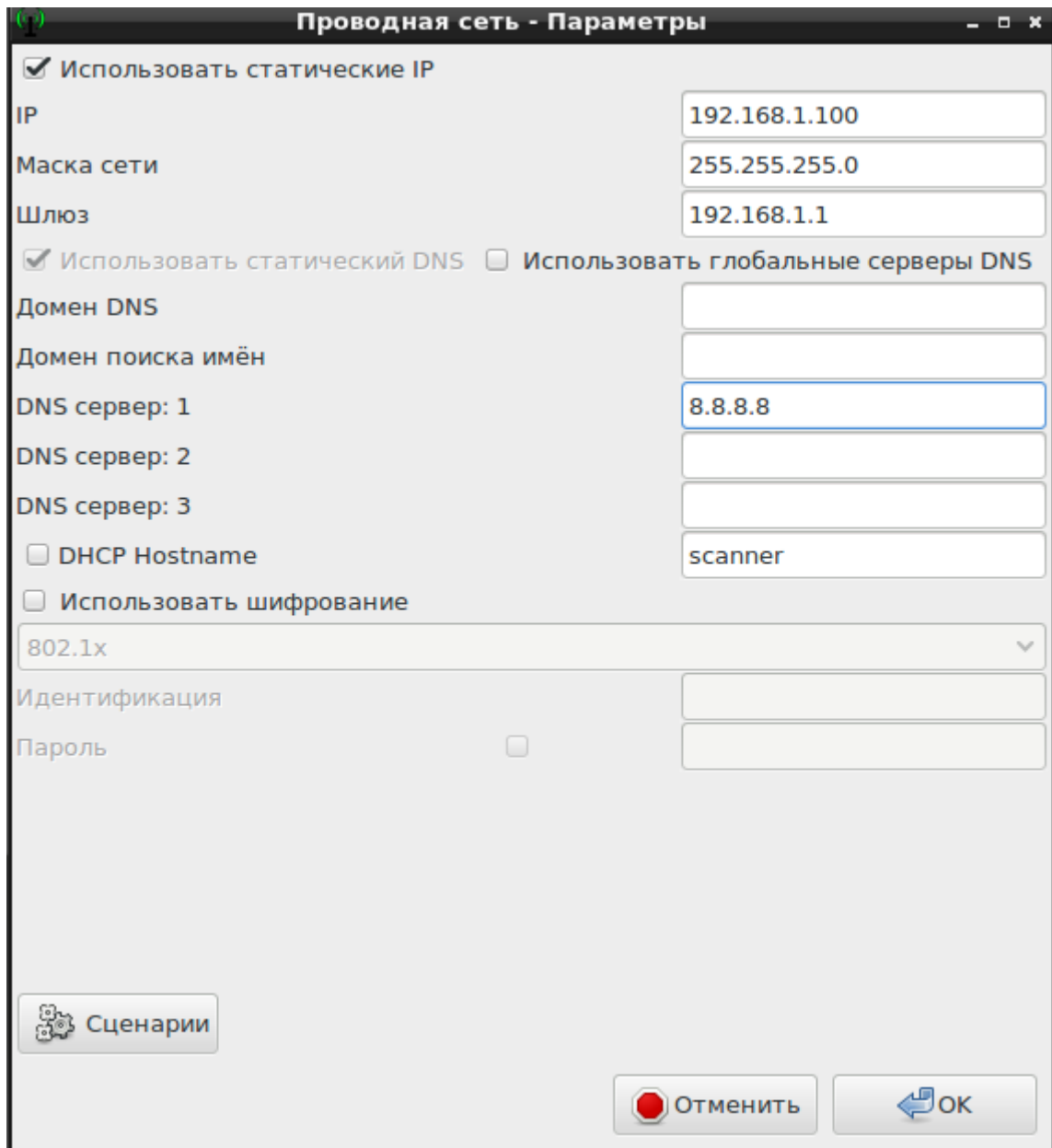


Рисунок 140 — Ручная настройка параметров сети

3.8.2. Менеджер обновлений

Менеджер обновлений предназначен для обновления ПО программного комплекса.

Менеджер обновлений запускается из веб-интерфейса **Обновить Сканер-ВС**.

После запуска откроется рабочее окно модуля (Рисунок 141).

Примечание. При первом запуске осуществляется поиск USB-накопителя с обновлениями.

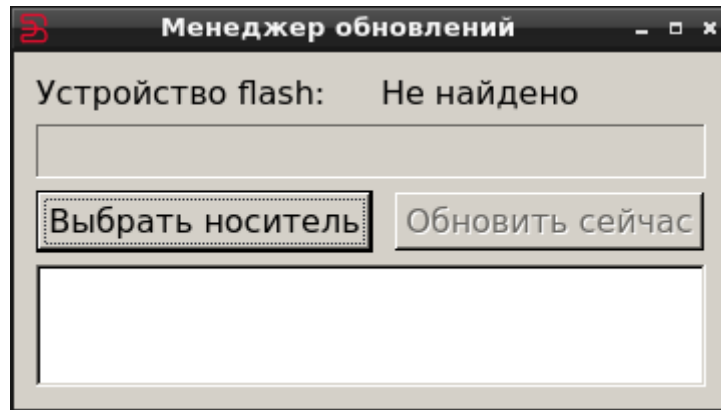


Рисунок 141 – Рабочее окно модуля

Подключите USB-накопитель с обновлениями, а затем выберите его из списка устройств с помощью кнопки **Выбрать носитель** и нажать **ОК** (Рисунок 142).

Примечание. В списке устройств содержатся только внешние устройства.

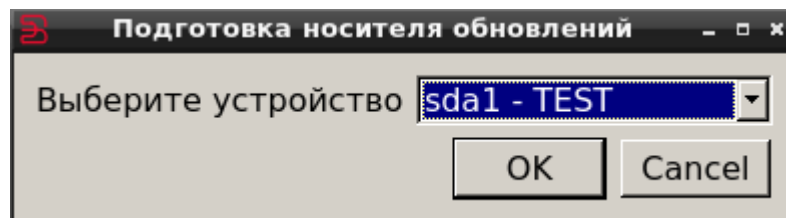


Рисунок 142 – Выбор USB-накопителя

При подключении подготовленного USB-накопителя автоматически откроется окно менеджера обновлений. Необходимо нажать **Обновить сейчас** для запуска процесса обновления (Рисунок 143).

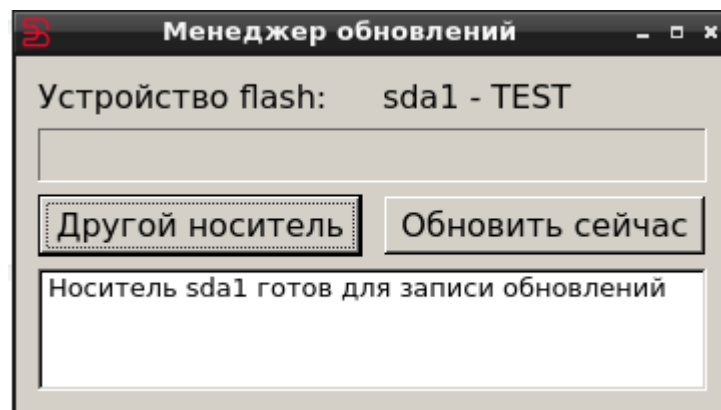


Рисунок 143 – Запуск процесса обновлений

Текущий статус процесса обновления отражается в строке над кнопками (Рисунок 144).

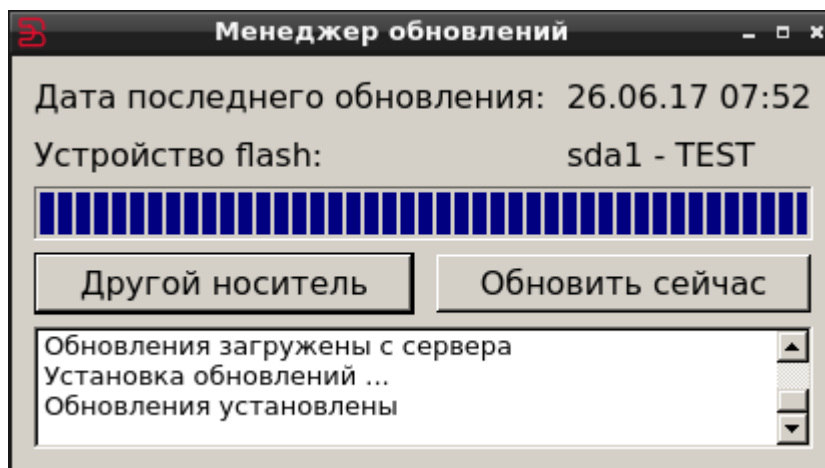


Рисунок 144 – Статус процесса обновления

3.9. Завершение работы с ПК «Сканер-ВС»

Для выхода из программного комплекса необходимо воспользоваться подменю стартера приложений (red hat) → **Выйти**.

Появится меню с вариантами завершения работы (Рисунок 145).



Рисунок 145 – Меню выхода

При выборе **Выйти** будет произведена перезагрузка программного комплекса, после которой можно будет сменить учетную запись.

При выборе **Перезагрузить** или **Выключить**, в зависимости от указанных параметров, будет загружена операционная система рабочей станции или новый сеанс работы с ПК «Сканер-ВС».

СПИСОК ПОДДЕРЖИВАЕМЫХ АДАПТЕРОВ

Список поддерживаемых адаптеров представлен в таблице 1.1.

Таблица 1.1 – Список поддерживаемых адаптеров

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|----------------|-------------|----------|-----------|
| 3Com | 3CRDAG675 | PCI | Atheros | Mad WiFi |
| 3Com | 3CRDAG675B | PCI | Atheros | Mad WiFi |
| 3Com | 3CRPAG175 | Cardbus | Atheros | Mad WiFi |
| 3Com | 3CRWE154A72 | Cardbus | Atheros | Mad WiFi |
| 3Com | 3CRXJK10075 | Cardbus | Atheros | Mad WiFi |
| 3Com | 3CRUSB10075 | USB | Zydas | ZD1211 |
| 3Com | 3CRUSB10075 | USB | Zydas | ZD1211 |
| Abit | AirPace WLP-01 | PCI-E | Atheros | Mad WiFi |
| Accton | WN 4402 | Mini-PCI | Atheros | Mad WiFi |
| Accton | WN 5301D | Cardbus | Atheros | Mad WiFi |
| Accton | WN 6301 | Cardbus | Atheros | Mad WiFi |
| Acer | built in | Mini-PCI | Broadcom | Bcm43xx |
| Actiontec | HWC05490-01 | Cardbus | Atheros | Mad WiFi |
| Airlink101 | AWLC-4030 | Cardbus | Atheros | Mad WiFi |
| Airlink101 | AWLH-4030 | PCI | Atheros | Mad WiFi |
| Airlink101 | AWLH-4130 | PCI | Atheros | Mad WiFi |
| Airlink101 | AWLC-3026 | Cardbus | Ralink | rt61 |
| Airlink101 | AWLL5088 | USB | RealTek | rtl8192cu |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|-----------------|-------------|----------|------------|
| Airlink101 | AWLL3025 | USB | Zydas | ZD1211 |
| Airlink101 | AWLL3025 v. 2 | USB | Zydas | ZD1211 |
| Airlink101 | AWLL3026 | USB | Zydas | ZD1211 |
| Airlink101 | AWLL3026 | USB | Zydas | ZD1211 |
| Airnet | AWN108 | Cardbus | Atheros | Mad WiFi |
| Airvast | XN-100 | Cardbus | Atheros | Mad WiFi |
| Airvast | XN-200 | Mini-PCI | Atheros | Mad WiFi |
| Alfa | GWPC005 | Cardbus | Atheros | Mad WiFi |
| Alfa | GWPC006G | Cardbus | Atheros | Mad WiFi |
| Alfa | GWPC007 | Cardbus | Atheros | Mad WiFi |
| Allnet | ALL0281 | PCI | Atheros | Mad WiFi |
| Alloy | WLF245401 | Cardbus | Broadcom | Bcm43xx |
| Alloy | WLF2454USB | USB | Broadcom | Bcm43xx |
| Alloy | WLF2454VP | PCI | Broadcom | Bcm43xx |
| Ambit | T60H906 | Mini-PCI | Broadcom | Bcm43xx |
| Aopen | AOI-811 | Cardbus | Atheros | Mad WiFi |
| Aopen | WL54 | USB | Zydas | ZD1211 |
| Apple | Airport extreme | Mini-PCI | Broadcom | Bcm43xx |
| Apple | Airport extreme | Mini-PCI | Broadcom | Bcm43xx |
| Apple | Airport extreme | Mini-PCI | Atheros | madwifi-ng |
| Approx | appPCI300 | PCI | Atheros | ath9k |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|------------------|-------------|----------|---------------------|
| Arcadyan | WN4401C1-ZZ | Mini-PCI | Atheros | Mad WiFi |
| Asante | AL 5402-XG | Cardbus | Broadcom | Bcm43xx |
| Askey | WLL220 | Mini-PCI | Atheros | ath5k |
| Askey | WLC3010 | Cardbus | Broadcom | Bcm43xx |
| Askey | WLH3010 | PCI | Broadcom | Bcm43xx |
| Askey | WLL3010 | Mini-PCI | Broadcom | Bcm43xx |
| Askey | WLL220 | Cardbus | Atheros | Mad WiFi |
| Askey | WLL3020 | Mini-PCI | Atheros | Mad WiFi |
| Askey | WLL4070-D50 | Mini-PCI | Atheros | Mad WiFi / ath5k |
| Asus | WL-100G | Cardbus | Broadcom | Bcm43xx |
| Asus | WL-100G | Cardbus | Broadcom | Bcm43xx |
| Asus | WL-103b | Cardbus | Broadcom | Bcm43xx |
| Asus | WL-138G v.2 | PCI | Broadcom | Bcm43xx |
| Asus | WL-200 | Cardbus | Atheros | Mad WiFi |
| Asus | PCI-G31 | PCI | Ralink | rt61 |
| Asus | WL-167G v.2 | USB | Ralink | rt73 |
| Ativa | AWGNA54 | Cardbus | Atheros | Mad WiFi |
| Ativa | AWGUA54 | USB | Zydas | ZD1211 |
| Atlantis | A02-PCI-W54 v1.3 | PCI | Ralink | rt61 |
| Azio | AWU254 | USB | Ralink | rt73 |
| Azurewave | AW-NE771 | Mini-PCIe | Atheros | ath9k |
| Belkin | F5D8011 v. 1000 | Cardbus | Atheros | ath9k |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|-----------------|-------------|----------|-----------|
| Belkin | F5D7000 | PCI | Broadcom | Bcm43xx |
| Belkin | F5D7001 | PCI | Broadcom | Bcm43xx |
| Belkin | F5D7010 | Cardbus | Broadcom | Bcm43xx |
| Belkin | F5D7011 | Cardbus | Broadcom | Bcm43xx |
| Belkin | F5D7051 | USB | Broadcom | Bcm43xx |
| Belkin | F5D7000 v.5000 | PCI | Atheros | Mad WiFi |
| Belkin | F5D7010 v.5100 | Cardbus | Atheros | Mad WiFi |
| Belkin | F5D7000 v.6000 | PCI | Ralink | rt61 |
| Belkin | F5D7050 v. 5000 | USB | RealTek | rtl8187 |
| Belkin | F9L1001 | USB | RealTek | RTL8188SU |
| Belkin | F9L1004 | USB | RealTek | RTL8192CU |
| Belkin | F5D7050 v. 4000 | USB | Zydas | ZD1211 |
| Blitz | BWI-715 rev.1 | PCI | Atheros | Mad WiFi |
| Bromax | WE602B | Cardbus | Broadcom | Bcm43xx |
| Buffalo | WLI-CB-G54 | Cardbus | Broadcom | Bcm43xx |
| Buffalo | WLI-PCI-G54 | PCI | Broadcom | Bcm43xx |
| Buffalo | WLI-USB-G54 | USB | Broadcom | Bcm43xx |
| Buffalo | WLI-U2-SG54HG | USB | Ralink | rt73 |
| Buffalo | WLI-U2-KG54L | USB | Zydas | ZD1211 |
| Canyon Tech | CN-WF518 | USB | Zydas | ZD1211 |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|------------------------|-----------------|-------------|----------|----------|
| CC&C | WL-2100 | Cardbus | Broadcom | Bcm43xx |
| CC&C | WL-2400 | Mini-PCI | Broadcom | Bcm43xx |
| Cisco | Air-CB21AG | Cardbus | Atheros | Mad WiFi |
| Cnet | CWP-903 | PCI | Ralink | rt61 |
| Compex | WLM200NX | Mini-PCI | Atheros | ath9k |
| Compex | WLU108g | USB | Atheros | Mad WiFi |
| CompuShack | CS-23-543-84 | Cardbus | Atheros | Mad WiFi |
| Conceptronic | C54C | Cardbus | Atheros | Mad WiFi |
| Conceptronic | C54I | PCI | Atheros | Mad WiFi |
| Conceptronic | C54WIFIU | USB | Zydas | ZD1211 |
| Contec Flexscan | FX-DS540-PCC | Cardbus | Atheros | Mad WiFi |
| Dell | TrueMobile 1180 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | TrueMobile 1300 | Cardbus | Broadcom | Bcm43xx |
| Dell | TrueMobile 1300 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | TrueMobile 1350 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | TrueMobile 1370 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | TrueMobile 1400 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | TrueMobile 1450 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | Wireless 1390 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | Wireless 1395 | Mini-PCI | Broadcom | Bcm43xx |
| Delta Networks | LM-WB521 | Cardbus | Atheros | Mad WiFi |
| Dick Smith Electronics | XH9946 | PCI | Atheros | Mad WiFi |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|-----------------|-----------------|-------------|---------|-------------|
| Digicom | 8E4213 | USB | Zydas | ZD1211 |
| Digitus Network | DN-7031 | Cardbus | Atheros | Mad WiFi |
| Digitus Network | DN-7036 | PCI | Atheros | Mad WiFi |
| Digitus Network | DN-7003GV | USB | Zydas | ZD1211 |
| D-Link | WNA-1330 | Cardbus | Atheros | ath5k |
| D-Link | DWA-547 | PCI | Atheros | ath5k/ath9k |
| D-Link | DWA-522 rev. A1 | PCI | Atheros | ath9k |
| D-Link | DWA-522 rev. A2 | PCI | Atheros | ath9k |
| D-Link | DWA-547 | PCI | Atheros | ath9k |
| D-Link | DWA-642 | Cardbus | Atheros | ath9k |
| D-Link | DWA-652 | Cardbus | Atheros | ath9k |
| D-Link | DWL-650+ | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-A520 | PCI | Atheros | Mad WiFi |
| D-Link | DWL-A650 | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-A650 | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-AB520 | PCI | Atheros | Mad WiFi |
| D-Link | DWL-AB650 | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-AG520 | PCI | Atheros | Mad WiFi |
| D-Link | DWL-AG650 | Cardbus | Atheros | Mad WiFi |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|--------------------|-------------|---------|---------------------|
| D-Link | DWL-AG660 (rev. 1) | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-G510 | PCI | Atheros | Mad WiFi |
| D-Link | DWL-G520 | PCI | Atheros | Mad WiFi |
| D-Link | DWL-G550 | PCI | Atheros | Mad WiFi |
| D-Link | DWL-G650 | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-G650M | Cardbus | Atheros | Mad WiFi |
| D-Link | WDA-1320 | PCI | Atheros | Mad WiFi |
| D-Link | WDA-2320 | PCI | Atheros | Mad WiFi |
| D-Link | DWA-520 | PCI | Atheros | Mad WiFi / ath5k |
| D-Link | DWL-G520M | PCI | Atheros | Mad WiFi / ath5k |
| D-Link | DWL-G630 (rev. C1) | Cardbus | Atheros | Mad WiFi / ath5k |
| D-Link | DWL-G630 (rev. D) | Cardbus | Atheros | Mad WiFi / ath5k |
| D-Link | WDA-2320 v. 1 | PCI | Atheros | Mad WiFi / ath5k |
| D-Link | WNA-2330 | Cardbus | Atheros | Mad WiFi / ath5k |
| D-Link | DWL-AG530 | PCI | Atheros | Madi WiFi |
| D-Link | DWA-525 | PCI | Ralink | rt2800pci |
| D-Link | DWA-525 rev. A2 | PCI | Ralink | rt2800pci |
| D-Link | DWA-125 rev. A2 | USB | Ralink | rt2800usb |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|--------------------|-------------|---------|------------|
| D-Link | DWA-130 rev. B | USB | Ralink | rt2800usb |
| D-Link | DWA-510 | PCI | Ralink | rt61 |
| D-Link | DWL-G510 rev. C2 | PCI | Ralink | rt61 |
| D-Link | DWL-G510 rev.C1 | PCI | Ralink | rt61 |
| D-Link | DWL-G520+A v.C1 | PCI | Ralink | rt61 |
| D-Link | DWL-G630 (rev. E1) | Cardbus | Ralink | RT61 |
| D-Link | DWL-G630 (rev. E2) | Cardbus | Ralink | rt61 |
| D-Link | DWA-110 | USB | Ralink | rt73 |
| D-Link | DWA-111 | USB | Ralink | rt73 |
| D-Link | WUA-1340 | USB | Ralink | rt73 |
| D-Link | DWA-121 rev. A | USB | RealTek | RTL8192CU |
| D-Link | DWA-120 | USB | Atheros | ar5523 |
| Edimax | EW-7325IG | PCI | Atheros | Mad WiFi |
| Edimax | EW-7108PCG | Cardbus | Ralink | rt61 |
| Edimax | EW-7318USg | USB | Ralink | rt73 |
| Edimax | EW-7318Ug | USB | Ralink | rt73 |
| Edimax | EW-7811Un | USB | RealTek | RTL8192CU |
| Edimax | EW-7317Ug | USB | Zydas | zd1211 |
| EDUP | EP-MS8511 | USB | RealTek | RTL8188CUS |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|-----------------|---------------|-------------|----------|------------------|
| Eminent | EM4056 v. 1.0 | Cardbus | Atheros | Mad WiFi / ath5k |
| Eminent | EM4454 | USB | Ralink | rt73 |
| Enterasys | RBTBG-AW | Cardbus | Atheros | Mad WiFi |
| Eusso | GL 2454-01 | Cardbus | Atheros | Mad WiFi |
| Eusso | GL 2454-01 | PCI | Atheros | Mad WiFi |
| Farallon | PN4030 | Cardbus | Atheros | Mad WiFi |
| Farallon | PN4032 | PCI | Atheros | Mad WiFi |
| Fujitsu-Siemens | E-5454 | Cardbus | Atheros | Mad WiFi |
| Gemtek | WL-352BW | Mini-PCI | Broadcom | Bcm43xx |
| Gemtek | WL-360G | PCI | Broadcom | Bcm43xx |
| Gemtek | WPI-100G | PCI | Broadcom | Bcm43xx |
| Gemtek | WL-511 | Cardbus | Atheros | Mad WiFi |
| Gemtek | WL-550 | Mini-PCI | Atheros | Mad WiFi |
| Gemtek | WL-571 | Cardbus | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WIAG01 | Mini-PCI | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WIAG02 | Mini-PCI | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WLMA101 | Cardbus | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WLMA102 | Cardbus | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WLMAG | Cardbus | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WMAG01 | Cardbus | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WP01GT | PCI | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WI01HT | Mini-PCI | Atheros | Mad WiFi / ath5k |
| Gigabyte Tech | GN-WPKG | PCI | Ralink | rt2500pci |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|----------------|----------------|-------------|----------|----------|
| Gigabyte Tech | GN-WI01GS | Mini-PCI | Ralink | rt61 |
| Gigabyte Tech | GN-WB01GS | USB | Ralink | rt73 |
| Gigafast | WF748-CUI | USB | Zydas | ZD1211 |
| GlobalSun Tech | GL 245401-OA | Cardbus | Atheros | Mad WiFi |
| GlobalSun Tech | GL 2454MP | Mini-PCI | Atheros | Mad WiFi |
| GlobalSun Tech | GL 505401 | Cardbus | Atheros | Mad WiFi |
| GlobalSun Tech | GL 505402 | Cardbus | Atheros | Mad WiFi |
| GlobalSun Tech | GL 5054MP | Mini-PCI | Atheros | Mad WiFi |
| GlobalSun Tech | GL 5054VP | PCI | Atheros | Mad WiFi |
| GlobalSun Tech | GL 5254MP | Mini-PCI | Atheros | Mad WiFi |
| Hama | 62764 | USB | Ralink | rt73 |
| Hama | 39741 | USB | Zydas | ZD1211 |
| Hamlet | HNWU254G | USB | Ralink | rt73 |
| Hawking Tech | HWUG1 | USB | Ralink | rt73 |
| Hawking Tech | HWU54G | USB | Zydas | ZD1211 |
| Hawking Tech | HWU8DD rev. B | USB | Zydas | ZD1211 |
| Hercules | HWGPCI-54 v. 2 | PCI | Ralink | rt61 |
| HP | AR242x | PCI-E | Atheros | ath5k |
| HP | Wireless | Mini-PCI | Broadcom | Bcm43xx |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|-----------------------|-------------|----------|------------------|
| HP | AR5007 | Mini-PCI | Atheros | Mad WiFi |
| IBM | 22P7501 | Cardbus | Atheros | Mad WiFi |
| ICIDU | Wireless 11G PCI Card | PCI | Atheros | Mad WiFi / ath5k |
| Icom | SL-5000 | Cardbus | Atheros | Mad WiFi |
| Icom | SR-21BB | Cardbus | Atheros | Mad WiFi |
| Inexq | UR055g | USB | Zydas | ZD1211 |
| Intel | 3160ac rev. 83 | Mini-PCIe | Intel | iwlwifi |
| Intel | 3160ac rev. 84 | Mini-PCIe | Intel | iwlwifi |
| Intel | 7260ac rev. 83 | Mini-PCIe | Intel | iwlwifi |
| Intel | 7260ac rev. 84 | Mini-PCIe | Intel | iwlwifi |
| Intel | N6200 | Mini-PCIe | Intel | iwlwifi |
| Intel | WCB5000 | Cardbus | Atheros | Mad WiFi |
| Intel | WPCI5000 | PCI | Atheros | Mad WiFi |
| I-O Data | WN-A54/PCM | Cardbus | Atheros | Mad WiFi |
| IOGear | GWU523 | USB | Zydas | ZD1211 |
| JAHT | WN-5054CB | Cardbus | Atheros? | Mad WiFi |
| Lancom | MC-54a/g | Cardbus | Atheros | Mad WiFi |
| Lancom | MC-54ab | Cardbus | Atheros | Mad WiFi |
| Lancom | MC-54g | Cardbus | Atheros | Mad WiFi |
| Lancom | PCI-54a | PCI | Atheros | Mad WiFi |
| Lancom | PCI-54a/g | PCI | Atheros | Mad WiFi |
| LevelOne | WNC-0300 | PCI | Atheros | Mad WiFi |
| LevelOne | WPC-0300 | Cardbus | Atheros | Mad WiFi |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|--------------|-------------|----------|----------|
| LevelOne | WNC-0301 v.3 | PCI | Ralink | rt61 |
| LevelOne | WNC-0301 v.3 | USB | Ralink | rt73 |
| Linksys | WPC300N v. 2 | Cardbus | Atheros | ath9k |
| Linksys | WEC600N | PCI-E | Broadcom | Bcm43xx |
| Linksys | WMP11 v. 2.7 | PCI | Broadcom | Bcm43xx |
| Linksys | WMP300N | PCI | Broadcom | Bcm43xx |
| Linksys | WMP300N v. 1 | PCI | Broadcom | Bcm43xx |
| Linksys | WMP54G | PCI | Broadcom | Bcm43xx |
| Linksys | WMP54G v. 3 | PCI | Broadcom | Bcm43xx |
| Linksys | WMP54G v.2 | PCI | Broadcom | Bcm43xx |
| Linksys | WPC300N v. 1 | Cardbus | Broadcom | Bcm43xx |
| Linksys | WPC54G v. 1 | Cardbus | Broadcom | Bcm43xx |
| Linksys | WPC54G v. 3 | Cardbus | Broadcom | Bcm43xx |
| Linksys | WPC54GS | Cardbus | Broadcom | Bcm43xx |
| Linksys | WPM54G v.2 | PCI | Broadcom | Bcm43xx |
| Linksys | WMP300N v. 2 | PCI | Atheros | Mad WiFi |
| Linksys | WMP55AG | PCI | Atheros | Mad WiFi |
| Linksys | WPC51AB | Cardbus | Atheros | Mad WiFi |
| Linksys | WPC54A | Cardbus | Atheros | Mad WiFi |
| Linksys | WPC55AG | Cardbus | Atheros | Mad WiFi |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|---------------|-------------|------------------|------------------|
| Linksys | WMP110 v.1 | PCI | Atheros | Mad WiFi / ath9k |
| Linksys | WPC11 v.3 | PCMCIA | Prism 1 | orinoco |
| Linksys | WUSB54AG | USB | Intersil/Frisbee | p54usb |
| Linksys | WUSB54G v. 1 | USB | Intersil/Frisbee | p54usb |
| Linksys | WUSB54G v. 2 | USB | Intersil/Frisbee | p54usb |
| Linksys | WUSB54GP v. 1 | USB | Intersil/Frisbee | p54usb |
| Linksys | WUSB54G v. 4 | USB | Ralink | rt2500usb |
| Linksys | WUSB54GP v. 4 | USB | Ralink | rt2500usb |
| Linksys | WMP54G v. 4.1 | PCI | Ralink | RT61 |
| Linksys | WUSB54GC | USB | Ralink | rt73 |
| Longshine | LCS8131G3 | USB | Zydas | ZD1211 |
| Macromate | MWN-754 | Cardbus | Atheros | Mad WiFi |
| Macsense | WPE-800 | Cardbus | Broadcom | Bcm43xx |
| Micradigital | F5D7000eaE | PCI | Atheros | Mad WiFi |
| Microsoft | MN-720 | Cardbus | Broadcom | Bcm43xx |
| Microsoft | MN-730 | PCI | Broadcom | Bcm43xx |
| Microtik | 5G/ABG | PCI | Atheros | Mad WiFi |
| Microtik | 5G/ABM | PCI | Atheros | Mad WiFi |
| Minitar | MN54GCB | Cardbus | Broadcom | Bcm43xx |
| Minitar | MN54GPC | PCI | Broadcom | Bcm43xx |
| Minitar | MWGUHA | USB | Zydas | ZD1211 |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|-----------------|-------------|----------|----------|
| Motorola | WN825Gv2 | Cardbus | Broadcom | b43 |
| Motorola | WN825G | Cardbus | Broadcom | Bcm43xx |
| Motorola | WPCI810G | PCI | Broadcom | Bcm43xx |
| MSI | UB11B | USB | Broadcom | Bcm43xx |
| MSI | US54SE II | USB | Ralink | rt73 |
| MSI | US54SE | USB | Zydas | ZD1211 |
| NDC | NWH1054 | Cardbus | Atheros | Mad WiFi |
| NEC | WL-54AC | Cardbus | Atheros | Mad WiFi |
| NEC | WL54AG | Cardbus | Atheros | Mad WiFi |
| Netegriti | EM-500AG | Mini-PCI | Atheros | Mad WiFi |
| Netgear | WPN511 (rev. 1) | Cardbus | Atheros | ath5k |
| Netgear | WNA-1100 | USB | atheros | ath9k |
| Netgear | WN511B | Cardbus | Broadcom | Bcm43xx |
| Netgear | HA 311 | PCI | Atheros | Mad WiFi |
| Netgear | HA 501 | Cardbus | Atheros | Mad WiFi |
| Netgear | WAB501 | Cardbus | Atheros | Mad WiFi |
| Netgear | WAG311 | PCI | Atheros | Mad WiFi |
| Netgear | WAG511 | Cardbus | Atheros | Mad WiFi |
| Netgear | WG 311 | PCI | Atheros | Mad WiFi |
| Netgear | WG 311T | PCI | Atheros | Mad WiFi |
| Netgear | WG111T | USB | Atheros | Mad WiFi |
| Netgear | WG511T | Cardbus | Atheros | Mad WiFi |
| Netgear | WG511U | Cardbus | Atheros | Mad WiFi |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|-------------------|-------------|-------------|------------------|---------------------|
| Netgear | WPN111 | USB | Atheros | Mad WiFi |
| Netgear | WPN311 | PCI | Atheros | Mad WiFi |
| Netgear | WG511 v. 3 | Cardbus | Intersil/Frisbee | p54pci |
| Netgear | WG111 v. 1 | USB | Intersil/Frisbee | p54usb |
| Netgear | WG111 v. 2 | USB | Realtek | rtl8187 |
| Netgear | WG111 v. 3 | USB | RealTek | rtl8187 |
| Nortel/E-mobility | 2201 | Cardbus | Atheros | Mad WiFi |
| Nortel/E-mobility | 2202 | Cardbus | Atheros | Mad WiFi |
| Ovislink | W542USB | USB | Ralink | rt73 |
| Ovislink | W54USB v. 2 | USB | Ralink | rt73 |
| Ovislink | WT-2000USB | USB | Ralink | rt73 |
| Passys | ipw4965 | PCI-E | ipw4965 | iwlwifi |
| Passys | ipw5100 | PCI-E | ipw5100 | iwlwifi |
| Passys | ipw5150 | PCI-E | ipw5100 | iwlwifi |
| Passys | ipw5300 | PCI-E | ipw5300 | iwlwifi |
| Passys | ipw5350 | PCI-E | ipw5300 | iwlwifi |
| Philips | PH 10819 | Cardbus | Atheros | Mad WiFi |
| Philips | PH 11107 | Mini-PCI | Atheros | Mad WiFi |
| Philips | PH 11840 | Mini-PCI | Atheros | Mad WiFi |
| Philips | SNN6500 | Cardbus | Atheros | Mad WiFi |
| Philips | PH 12127E | Mini-PCI | Atheros | Mad WiFi / ath5k |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|-------------------|--------------|-------------|----------|------------------|
| Philips | SNU5600 | USB | Zydas | ZD1211 |
| Phoebe | PHWL54 | Cardbus | Broadcom | Bcm43xx |
| Phoebe | PHWL54-PCI | PCI | Broadcom | Bcm43xx |
| Planet Technology | WL-3560 | Cardbus | Atheros | Mad WiFi |
| Planet Technology | WL-8310 | PCI | Atheros | Mad Wifi / ath5k |
| Planet Technology | WL-U356 | USB | Zydas | ZD1211 |
| Planex | GW-NS540a | Cardbus | Atheros | Mad WiFi |
| Pluscom | WP-AR2413 | PCI | Atheros | ath5k |
| Pluscom | WMP-RT2561ST | Mini-PCI | Ralink | rt61 |
| Pluscom | WP-RT2561T | PCI | Ralink | rt61 |
| Pluscom | WU-RT2571 | USB | Ralink | rt73 |
| Pluscom | WU-TR2571W | USB | Ralink | rt73 |
| Pluscom | WU-RTL8187 | USB | RealTek | rtl8187 |
| Pluscom | WU-ZD1211B | USB | Zydas | ZD1211 |
| Proxim | 8450 | Cardbus | Atheros | Mad WiFi |
| Proxim | 8451 | Cardbus | Atheros | Mad WiFi |
| Proxim | 846005 | Cardbus | Atheros | Mad WiFi |
| Proxim | 846105 | Cardbus | Atheros | Mad WiFi |
| Proxim | 8470 | Cardbus | Atheros | Mad WiFi |
| Proxim | 8470 WD | Cardbus | Atheros | Mad WiFi |
| Proxim | 8471 | Cardbus | Atheros | Mad WiFi |
| Proxim | 8480 | Cardbus | Atheros | Mad WiFi |
| Proxim | 8480 WD | Cardbus | Atheros | Mad WiFi |
| Proxim | 8481 | Cardbus | Atheros | Mad WiFi |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------------|----------------|-------------|----------|------------------|
| Proxim | 8482 | PCI | Atheros | Mad WiFi |
| Roper | RO80211GA-CB | Cardbus | Atheros | Mad WiFi |
| Rosewill | RNX-G300EX | PCI | Ralink | rt61 |
| Safecom | SWLU-5400 | USB | Zydas | ZD1211 |
| Sceptre | SC254g | Cardbus | Atheros | Mad WiFi |
| Senao/Engenius | 3054pcia | PCI | Atheros | Mad WiFi |
| Senao/Engenius | 5354cba | Cardbus | Atheros | Mad WiFi |
| Senao/Engenius | SL-3054CB | Cardbus | Atheros | Mad WiFi |
| Senao/Engenius | SL-3054MP | Mini-PCI | Atheros | Mad WiFi |
| Senao/Engenius | SL-5054CB | Cardbus | Atheros | Mad WiFi |
| Senao/Engenius | SL-5054CB Dual | Cardbus | Atheros | Mad WiFi |
| Senao/Engenius | SL-5354CB | Cardbus | Atheros | Mad WiFi |
| Senao/Engenius | SL-5354MP | Mini-PCI | Atheros | Mad WiFi |
| Senao/Engenius | SL-NMP 8602 | Mini-PCI | Atheros | Mad WiFi |
| Siemens Speedstream | 1024 ver.2 | PCI | Broadcom | Bcm43xx |
| Siemens-Gigaset | usb 108 | USB | Atheros | Mad WiFi / ath5k |
| Sitecom | WL-100b | Cardbus | Broadcom | Bcm43xx |
| Sitecom | WL-110b | PCI | Broadcom | Bcm43xx |
| Sitecom | WL-170 v. 1 | Cardbus | Ralink | rt61 |
| Sitecom | WL-171 | PCI | Ralink | rt61 |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|-----------------|-------------|----------|---------------------|
| Sitecom | WL-113 v. 1.002 | USB | Ralink | rt73 |
| Sitecom | WL-172 | USB | Ralink | rt73 |
| Sitecom | WL-113 | USB | Zydas | ZD1211 |
| SMC | 2335W | Cardbus | Atheros | Mad WiFi |
| SMC | 2336W-AG | Cardbus | Atheros | Mad WiFi |
| SMC | 2536W-AG | Cardbusp | Atheros | Mad WiFi |
| SMC | 2735W | Cardbus | Atheros | Mad WiFi |
| SMC | SMCWPCI-G | PCI | Atheros | Mad WiFi |
| SMC | SMCWPCIT-G EU | PCI | Atheros | Mad WiFi |
| SMC | SMCWBCT | Cardbus | Atheros | Mad WiFi / ath5k |
| SMC | SMCWUSB-G | USB | Zydas | ZD1211 |
| Sony | PCWA-C300S | Cardbus | Atheros | Mad WiFi |
| Sony | PCWA-C500 | Cardbus | Atheros | Mad WiFi |
| Sony | PCWAC700 | Cardbus | Atheros | Mad WiFi |
| Sony | IFU-WLM2 | USB | Zydas | ZD1211 |
| Sparklan | WL-352 | Mini-PCI | Broadcom | Bcm43xx |
| Sparklan | WL-660GT | PCI | Broadcom | Bcm43xx |
| Sparklan | WL-555 | Mini-PCI | Atheros | Mad WiFi |
| Sparklan | WL-558 | Mini-PCI | Atheros | Mad WiFi |
| Sweex | LW051 v. 1.0 | Cardbus | Atheros | Mad WiFi |
| Sweex | LW052 | PCI | Atheros | Mad WiFi |
| Sweex | LW053 | USB | Ralink | rt73 |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|------------------|-------------|----------|-------------|
| TDK | WN-5CB01 | Cardbus | Atheros | Mad WiFi |
| TDK | WN-5MP01 | Mini-PCI | Atheros | Mad WiFi |
| Tecom | WL5021 | Cardbus | Broadcom | Bcm43xx |
| Tellus | C6100 | Cardbus | Atheros | Mad WiFi |
| Tellus | M6100 | Mini-PCI | Atheros | Mad WiFi |
| Topcom | 4001g | USB | Ralink | rt73 |
| Toshiba | AR2413 | Mini-PCI | Atheros | ath5k |
| Toshiba | Atheros AR5001 | PCI | Atheros | ath5k/ath9k |
| Totolink | N200UP | USB | Ralink | rt2800usb |
| TP-Link | TL-WN350GD | PCI | Atheros | ath5k |
| TP-Link | TL-WN851ND | PCI | Atheros | ath9k |
| TP-Link | TL-WN861N v1.1 | Mini-PCI | Atheros | ath9k |
| TP-Link | TL-WN861N v2 | Mini-PCI | Atheros | ath9k |
| TP-Link | TL-WN881ND v.1.1 | PCI | Atheros | ath9k |
| TP-Link | WN721N | USB | Atheros | ath9k |
| TP-Link | WN751ND | PCI-E | Atheros | ath9k |
| TP-Link | WN781ND | PCI-E | Atheros | ath9k |
| TP-Link | WN951N | PCI | Atheros | ath9k |
| TP-Link | WN322G v. 3.0 | USB | Atheros | ath9k_htc |
| TP-Link | WN422G v. 2 | USB | Atheros | ath9k_htc |
| TP-Link | WN722N | USB | Atheros | ath9k_htc |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|------------------------|-------------|----------|---------------------|
| TP-Link | WN822N v.2 | USB | Atheros | ath9k_htc |
| TP-Link | WN550G | PCI | Atheros | Mad WiFi |
| TP-Link | WN551G | PCI | Atheros | Mad WiFi |
| TP-Link | WN560G | Mini-PCI | Atheros | Mad WiFi |
| TP-Link | WN610G | Cardbus | Atheros | Mad WiFi |
| TP-Link | WN620g | USB | Atheros | Mad WiFi |
| TP-Link | WN651G | PCI | Atheros | Mad WiFi |
| TP-Link | WN510G | Cardbus | Atheros | Mad WiFi / ath5k |
| TP-Link | TL-WDN3200 rev. 1.2 | USB | Ralink | rt2800usb |
| TP-Link | WN321G | USB | Ralink | rt73 |
| TP-Link | TL-WN8200ND | USB | RealTek | RTL8192CU |
| TP-Link | TL_WN823N | USB | RealTek | RTL8192CU |
| TP-Link | Tl-wn821 v.4 | USB | RealTek | RTL8192CU |
| TP-Link | WN322G | USB | Zydas | ZD1211 |
| TP-Link | WN422G v. 1 | USB | Zydas | ZD1211 |
| TP-Link | WN442G | USB | Zydas | ZD1211 |
| TRENDware | TEW-401PC | Cardbus | Broadcom | Bcm43xx |
| TRENDware | TEW-403PCI | PCI | Broadcom | Bcm43xx |
| TRENDware | TEW-441PC | Cardbus | Atheros | Mad WiFi |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|-----------------|-------------|----------|----------|
| TRENDware | TEW-443PI | PCI | Atheros | Mad WiFi |
| TRENDware | TEW-424UB v.1 | USB | Zydas | ZD1211 |
| Trust | 13645 | PCI | Atheros | Mad WiFi |
| Trust | 13647 | Cardbus | Atheros | Mad WiFi |
| TwinMOS | G240 | USB | Zydas | ZD1211 |
| Ubiquiti | RC-UBI-SRC | Cardbus | Atheros | Mad WiFi |
| US Robotics | USR5417A | PCI | Broadcom | Bcm43xx |
| US Robotics | USR5421 | USB | Broadcom | Bcm43xx |
| US Robotics | USR805423 | USB | Zydas | ZD1211 |
| USI | MP-G-BR-01(3A) | Mini-PCI | Broadcom | Bcm43xx |
| USI | CB-AG-AT-01 | Cardbus | Atheros | Mad WiFi |
| USI | MP-AG-AT-01(3B) | Mini-PCI | Atheros | Mad WiFi |
| Wistron | CB-300G | Cardbus | Broadcom | Bcm43xx |
| Wistron | EM-300G | Mini-PCI | Broadcom | Bcm43xx |
| Wistron | CB-100AB | Cardbus | Atheros | Mad WiFi |
| Wistron | CB-500AG | Cardbus | Atheros | Mad WiFi |
| Wistron | EM-500AG | Mini-PCI | Atheros | Mad WiFi |
| Wistron | EM9-AB(VM4) | Mini-PCI | Atheros | Mad WiFi |
| W-Link | WEN-2091 | PCI | Broadcom | Bcm43xx |
| W-Link | WEN-2200 | Mini-PCI | Broadcom | Bcm43xx |
| X-Micro | XWL-11GPAG | Cardbus | Atheros | Mad WiFi |
| X-Micro | XWL-11GUZX | USB | Zydas | zd1211 |
| Z-Com | AG-320 | Cardbus | Atheros | Mad WiFi |

Продолжение таблицы 1.1

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|-----------|-------------|---------|---------------------|
| Z-Com | XV5300 | Cardbus | Atheros | Mad WiFi |
| Z-Com | XV5350 | Cardbus | Atheros | Mad WiFi |
| Zonet | ZEW 1500S | Cardbus | Atheros | Mad WiFi |
| Zonet | ZEW 2501 | USB | Zydas | ZD1211 |
| Zyxel Zyair | G-102 | Cardbus | Atheros | Mad WiFi |
| Zyxel Zyair | M-102 | Cardbus | Atheros | Mad WiFi / ath5k |
| Zyxel Zyair | M-302 | PCI | Atheros | Mad WiFi / ath5k |
| Zyxel Zyair | G-220 | USB | Zydas | ZD1211 |
| Zyxel Zyair | ag-225h | USB | Zydas | ZD1211 |