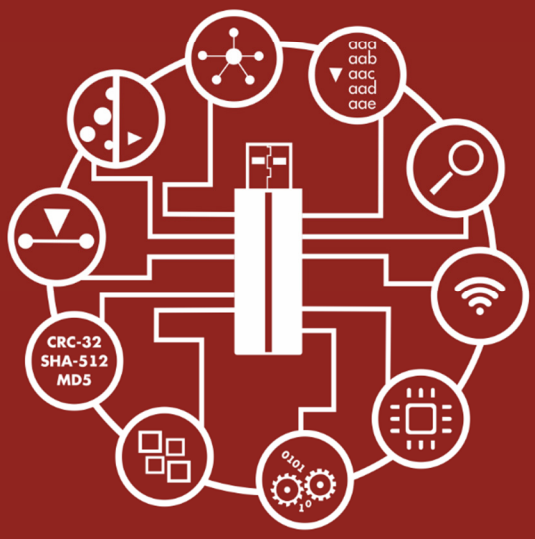
Эшелон
комплексная безопасность



Сканер-ВС

анализ защищенности

КРАТКОЕ РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

О КОМПАНИИ

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

Основными направлениями деятельности являются:

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

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

О РУКОВОДСТВЕ

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

СОДЕРЖАНИЕ

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

Программный комплекс (далее – ПК) 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» реализует следующие функции:

- выявление и анализ уязвимостей ИС;
- контроль установки обновлений операционных систем (далее – ОС) семейства Microsoft Windows;
- контроль параметров настройки комплекса средств защиты ОС специального назначения «Astra Linux Special Edition»;
- контроль ресурсов вычислительной сети, включая идентификацию узлов, построение топологии, определение сервисов, запущенных на узле, идентификацию ОС и приложений;
- контроль целостности программного обеспечения (далее – ПО), включая ПО средств защиты информации (далее – СЗИ);
- контроль уничтожения информации на машинных носителях;
- обеспечение поиска остаточной информации на машинных носителях;
- обеспечение контроля использования беспроводных сетей в ИС.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

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

- обеспечение сохранности оборудования и физической целостности системных блоков рабочих станций;
- обеспечение свободной от вирусов программной среды рабочей станции;
- обеспечение контроля изменения прикладной программной среды, исключение установки на рабочую станцию 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.

3 ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1 WEB-интерфейс ПК «Сканер-ВС»

3.1.1 Подключение к WEB-интерфейсу ПК «Сканер-ВС»

В строке браузера ввести IP-адрес ПК «Сканер-ВС».

Если все настройки выполнены корректно, в окне браузера отобразится окно авторизации ПК «Сканер-ВС», как это представлено на рисунке (рис. 1).

3.1.2 Общее описание web-интерфейса

После запуска ПК «Сканер-ВС» отобразится окно авторизации (рис. 1), где Оператор должен ввести логин и пароль.

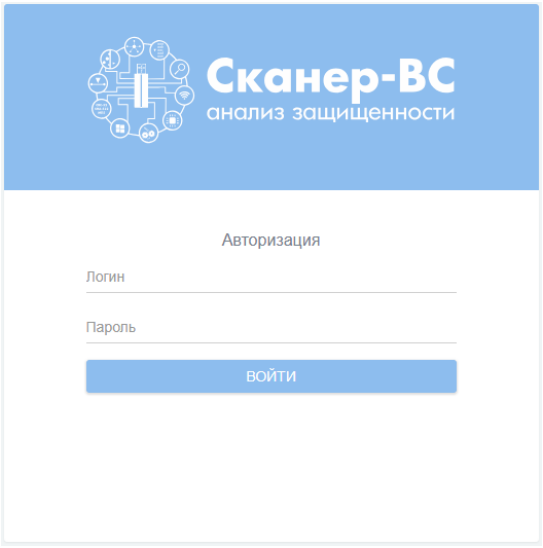


Рисунок 1 – Окно авторизации

Примечание. По умолчанию в ПК создана учетная запись «Администратор Сканер-ВС» с логином «admin» и паролем «admin». После первой авторизации рекомендуется сменить пароль на более надежный и обеспечить сохранность данного пароля. В целях безопасности пароль для учетной записи «Администратор Сканер-ВС» восстановить невозможно.

При успешной авторизации в WEB-интерфейсе будет отображено рабочее окно ПК «Сканер-ВС» (рис. 2).

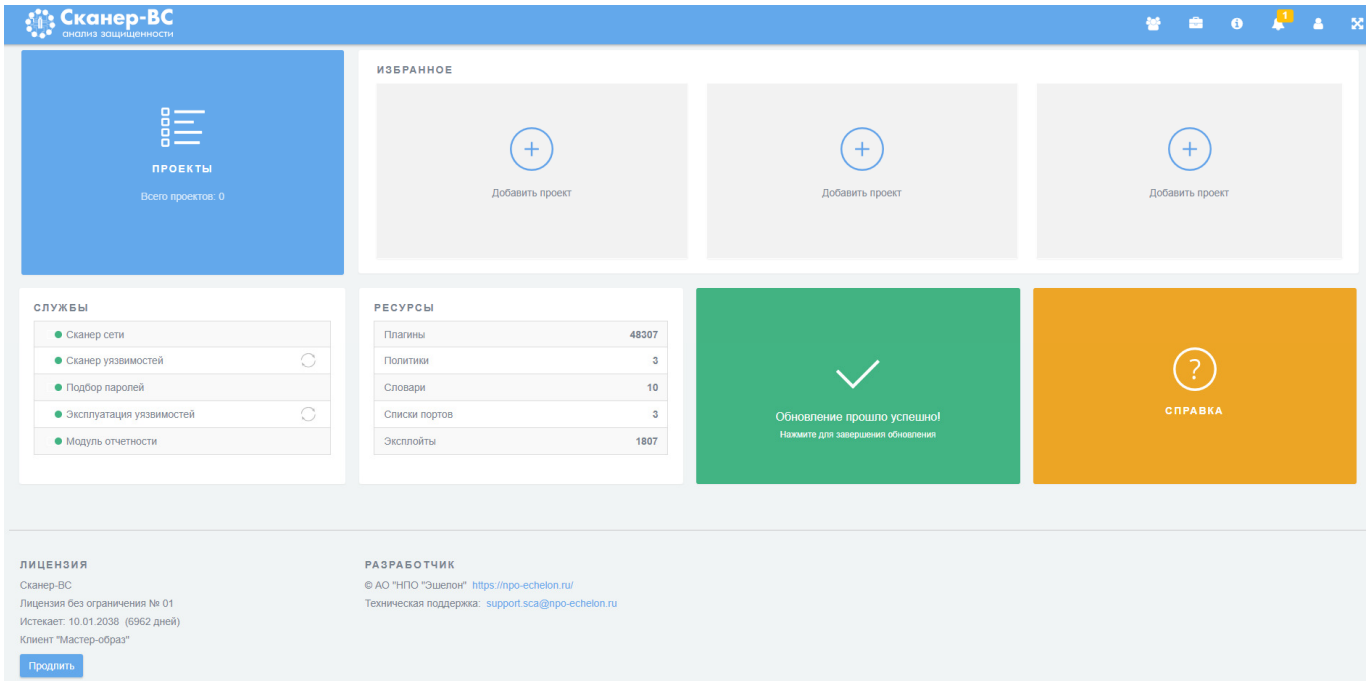


Рисунок 2 – Рабочее окно ПК «Сканер-ВС»

WEB-интерфейс ПК «Сканер-ВС» содержит два основных блока элементов:

– Панель навигации (рис. 3);

– Рабочее окно (рис. 4).

Блок «Панель навигации» всегда отображается в верхней части интерфейса ПК «Сканер-ВС» и используется для быстрого доступа к функциям ПК и навигации. Быстрый переход к функциям обеспечивают соответствующие пиктограммы:

– Администрирование;

– Проекты;

– Информация;

– Уведомления;

– Личная информация;

– Полноэкранный режим.

Рисунок 3 – Панель навигации

Описание пиктограмм блока «Панель навигации» представлено в таблице (см. Таблица 1).

Таблица 1 – Описание пиктограмм блока «Панель навигации»

Пиктограмма	Описание
	Пиктограмма «Администрирование» позволяет осуществить переход к интерфейсу, который выполняет управление пользователями, обеспечивает просмотр всех событий, происходящих в ПК «Сканер-ВС», а также выполнять настройку логотипа для отчета
	Пиктограмма «Проекты» позволяет выполнить быстрый доступ к интерфейсу управления проектами
	Пиктограмма «Информация» осуществляет доступ к интерфейсу, обеспечивающему просмотр информации о продукте
	Пиктограмма «Уведомления» при нажатии отображает все события, которые выполняются в ПК «Сканер-ВС»
	Пиктограмма «Личная информация» позволяет управлять профилем учетной записи, под которой вошел Оператор, осуществить выход из учетной записи или смену локали (языка)
	Пиктограмма «Полноэкранный режим» при нажатии позволяет перевести ПК «Сканер-ВС» в полноэкранный режим. Для выхода необходимо нажать клавишу «Esc»

Блок «Рабочее окно» (рис. 4) является основной рабочей областью интерфейса ПК «Сканер-ВС», в котором отображается информация о ходе выполнения задач.

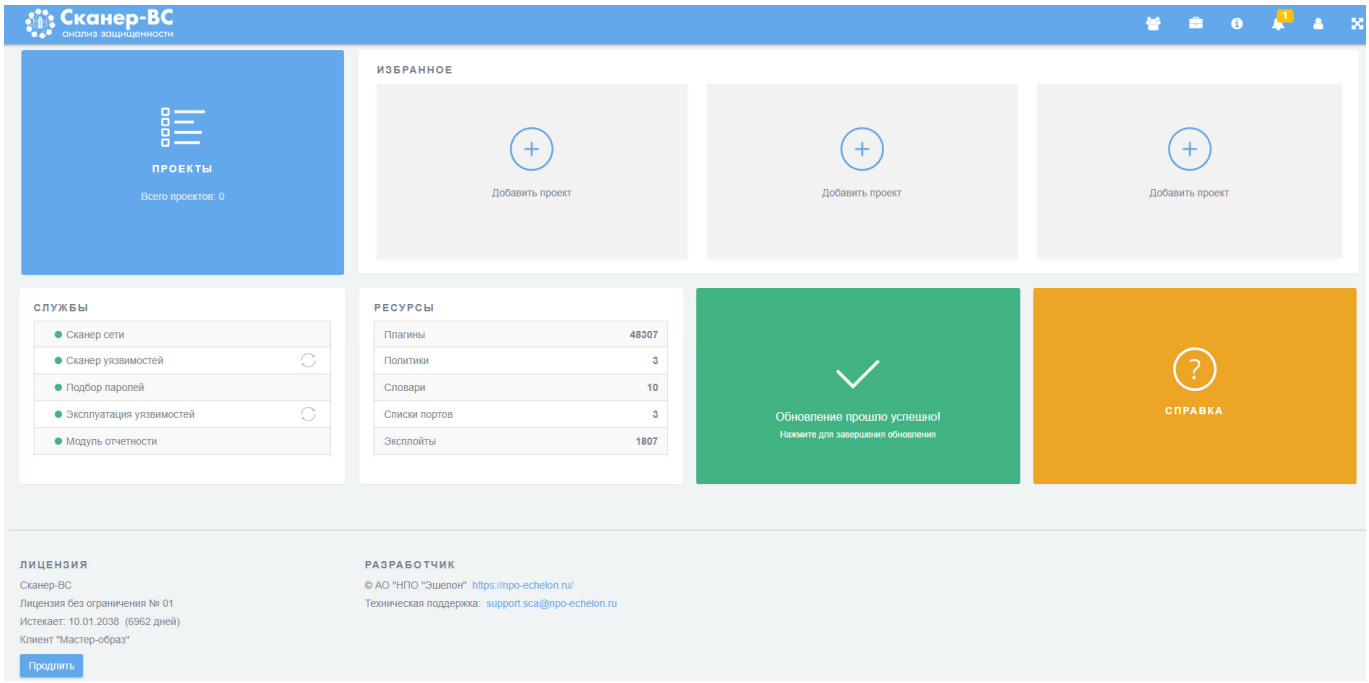


Рисунок 4 – Рабочее окно

Интерфейс ПК «Сканер-ВС» поддерживает унифицированный механизм отображения данных в табличном формате, при этом Оператору предоставляется возможность:

– управлять данными таблицы;

– экспортировать данные из таблицы.

Для удобства управления таблицами предусмотрены общие элементы управления (рис. 5):

– пиктограмма экспорта данных из таблицы « »;

– пиктограмма фильтра элементов таблицы « »;

– пиктограмма отображения элементов таблицы (рис. 7).

Рисунок 5 – Пиктограммы экспорта и фильтра таблицы

3.1.2.1 Пиктограмма экспорта данных из таблицы

Пиктограмма экспорта данных из таблицы предназначена для скачивания данных из таблицы в формате CSV.

При нажатии на данную пиктограмму появляется всплывающий список с выбором типа данных для скачивания. Доступны следующие данные:

– видимые данные;

– все данные.

После выбора данных откроется окно с параметрами скачиваемых данных (рис. 6).

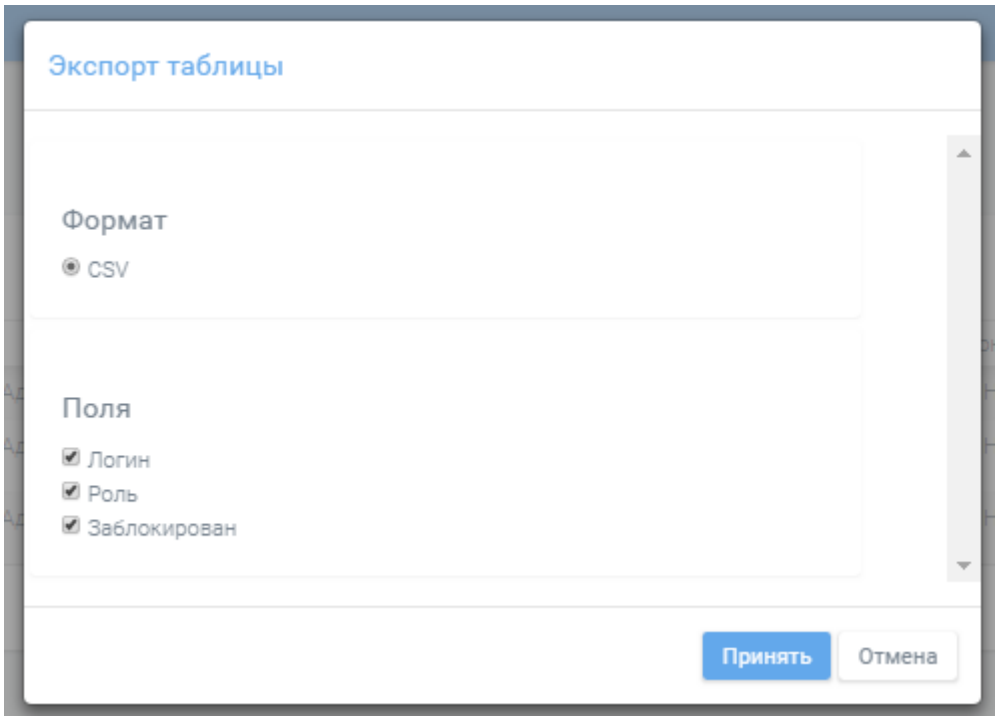


Рисунок 6 - Окно параметров скачиваемых данных

В окне «Экспорт таблицы» указан формат (CSV), в котором будут данные после скачивания, а также представлен выбор полей, которые можно скачать из таблицы.

Установленная галочка у поля с именем столбца означает, что в скачанных данных будут содержаться данные из этого столбца.

После установки галочек у необходимых полей, нажмите кнопку «Принять» для экспорта данных в формате CSV или кнопку «Отмена» для возврата в предыдущее меню.

3.1.2.2 Пиктограмма фильтра элементов таблицы

Пиктограмма фильтра элементов таблицы предназначена для настройки отображения данных, содержащихся в таблице.

При нажатии на пиктограмму фильтра появятся строки для поиска данных в каждом столбце таблицы.

Для завершения использования пиктограммы фильтра элементов таблицы, необходимо нажать повторно на пиктограмму фильтра.

3.1.2.3 Пиктограмма отображения элементов таблицы

Пиктограмма отображения элементов таблицы предназначена для выбора отображения количества строк таблицы, умещающихся на одной странице, и обеспечивает переключение между страницами.

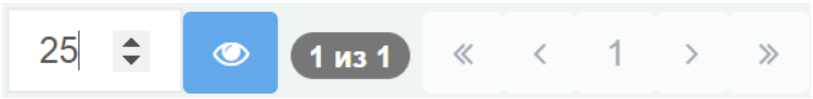


Рисунок 7 – Пиктограмма отображения элементов таблицы

Вводить количество строк можно с помощью клавиш или стрелочек, которые появляются после наведения курсора на окно. Введя необходимое число, следует нажать на пиктограмму «  », после чего таблица обновится и будет иметь требуемое количество строк.

Справа от пиктограммы отображается количество страниц в таблице и стрелочки для переключения между ними. Одна стрелочка означает перелистывание на одну страницу, две стрелочки означают перелистывание на первую или последнюю страницу.

3.1.1 Справка

Для получения справки по управлению ПК «Сканер-ВС», необходимо нажать на раздел «Справка» (рис. 8), после чего откроется новое окно с краткой документацией.

Рисунок 8 – Раздел справка на главном интерфейсе

3.1.1 Обновление комплекса

Для обновления ПО программного комплекса предназначен «Менеджер обновлений».

«Менеджер обновлений» запускается нажатием на раздел обновления ПК «Сканер-ВС» (рис. 9).

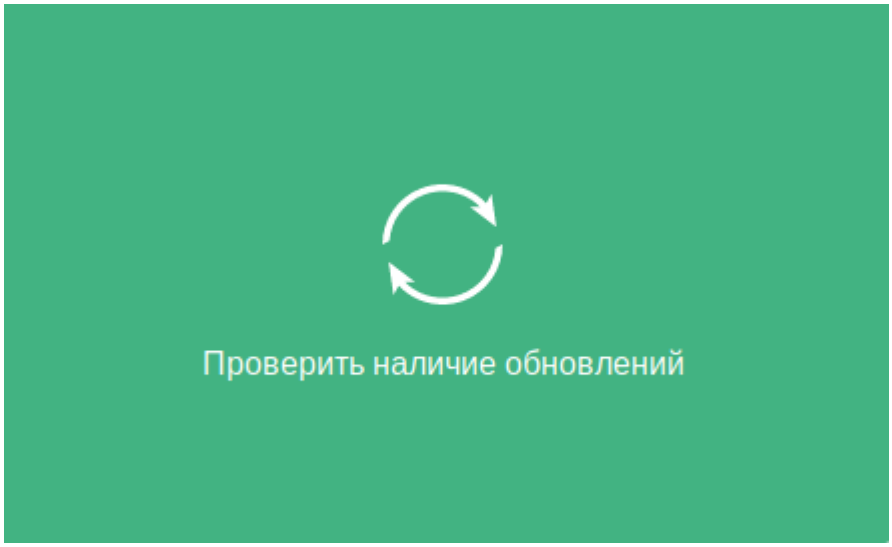


Рисунок 9 – Раздел обновления ПК «Сканер-ВС»

После проверки на сервере «Менеджер обновлений» выдаст данные о наличии обновлений (рис. 10).

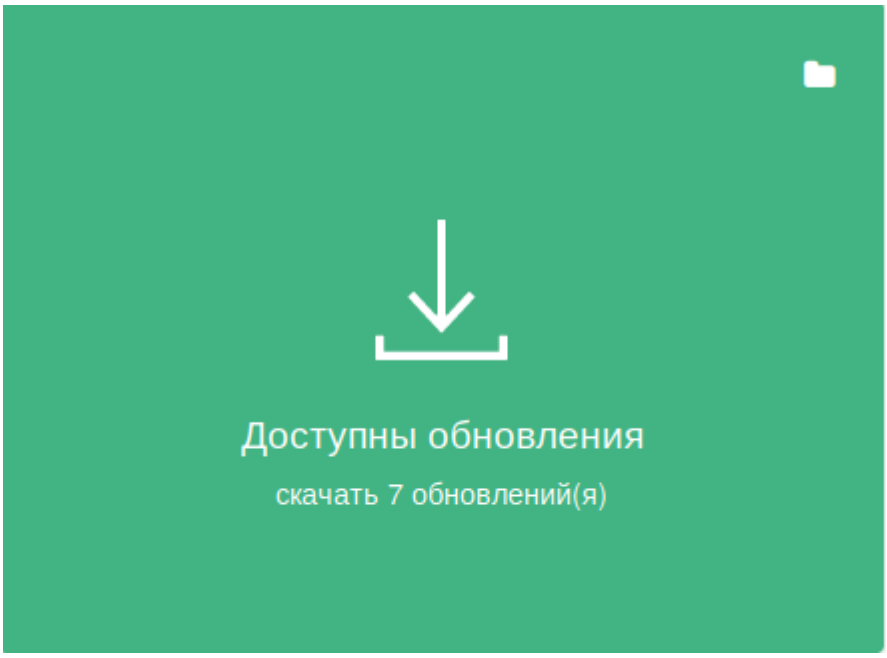


Рисунок 10 – Данные о наличии обновлений

Для скачивания обновлений необходимо нажать на раздел (рис. 10) и дождаться окончания загрузки обновлений (рис. 11).

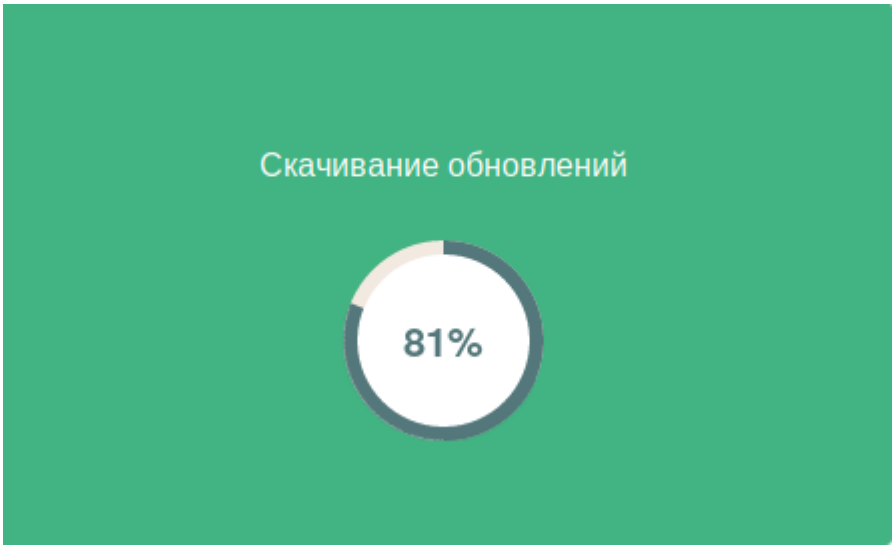


Рисунок 11 – Загрузка обновлений

После окончания загрузки раздел обновится. Для установки скачанных обновлений необходимо нажать на раздел обновления ПК «Сканер-ВС», изображенный на рисунке (рис. 12).

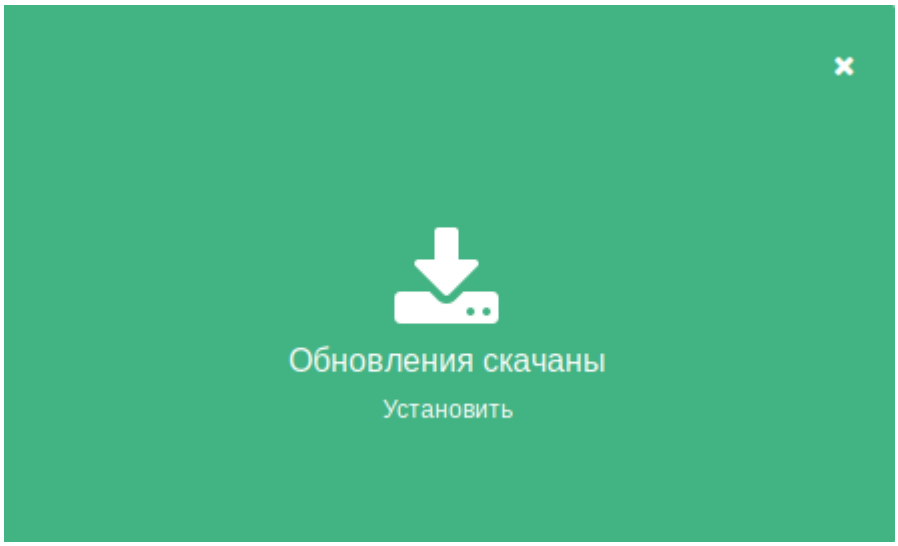


Рисунок 12 – Раздел обновления ПК «Сканер-ВС»

Далее начнется процесс установки обновлений (рис. 13).

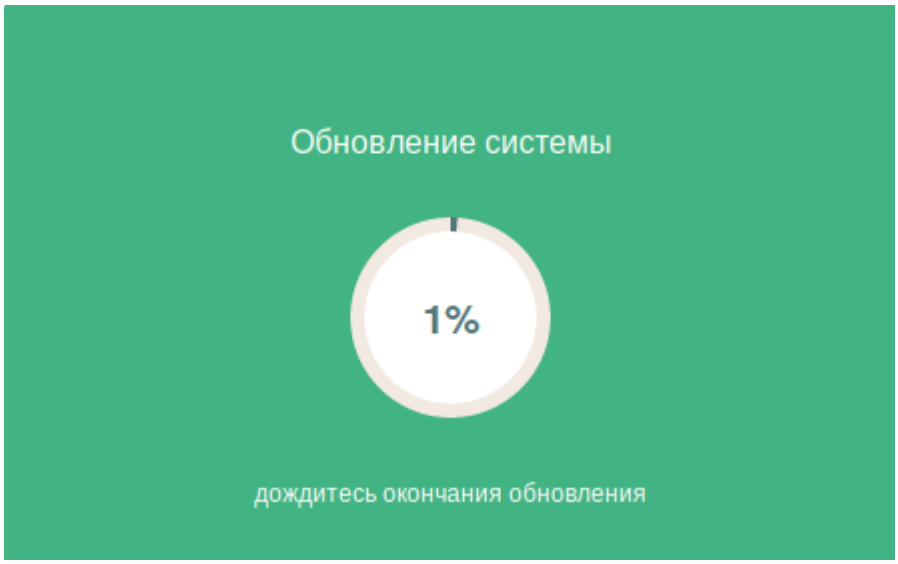


Рисунок 13 – Процесс установки обновлений

После окончания установки обновлений в разделе появится соответствующее сообщение. Для завершения обновления необходимо снова нажать на раздел (рис. 14).

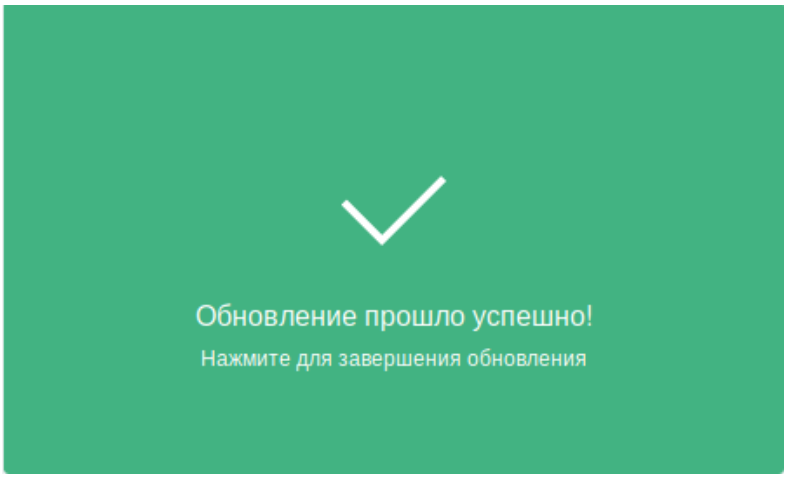


Рисунок 14 – Завершение обновления

В ПИ «Сканер-ВС» предусмотрена возможность скачивания обновлений на внешний накопитель. Для этого необходимо выполнить следующую последовательность:

– на этапе скачивания обновлений (рис. 12) нажать на иконку папки в верхнем правом углу. Откроется диалоговое окно как на рисунке (рис. 15);

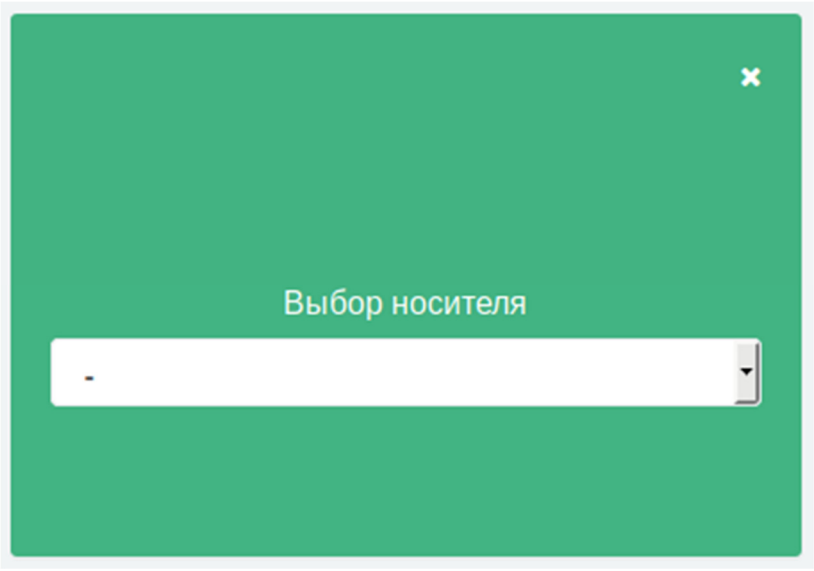


Рисунок 15 – Выбор носителя

– в выпадающем списке выберете необходимый USB-накопитель и нажмите на иконку стрелки (рис. 16);

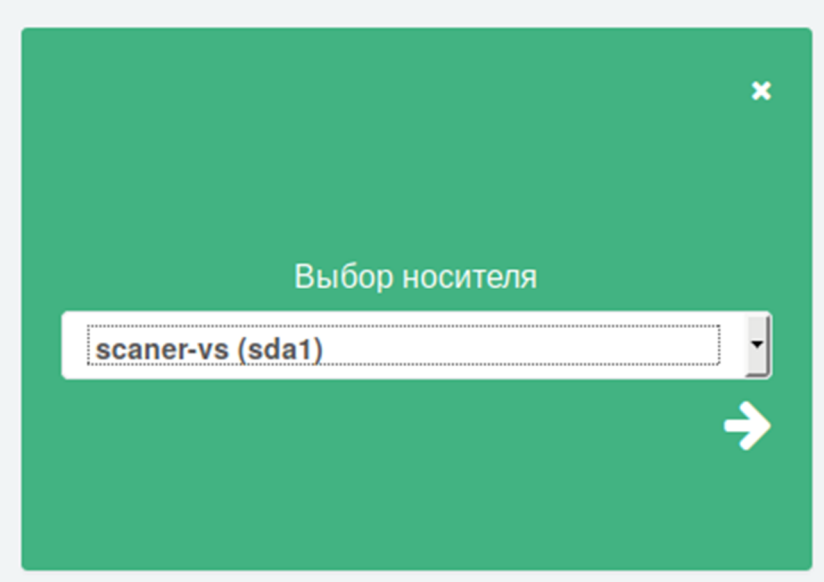


Рисунок 16 – Выпадающее меню выбора носителя

Обновления будут успешно скачаны на USB-накопитель в папку:
`/update/sca5/*`

С помощью USB-накопителя с обновлениями можно обновить Сканер-ВС, не имеющий доступа к внешней сети Интернет.

3.1.2 Управление лицензией

Для управления лицензией ПК «Сканер-ВС» предназначен специальный интерфейс «Лицензия». Интерфейс находится на главной панели ПК «Сканер-ВС» в нижней части.

Интерфейс управления лицензией представлен на рисунке (рис. 17).

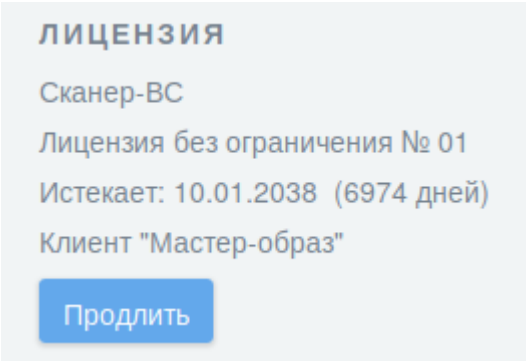


Рисунок 17 – Интерфейс управления лицензией

В разделе «Лицензия» содержатся следующие данные:

– информация о наименовании продукта;

– информация о типе лицензии и ее номер;

– информация о сроке действия лицензии;

– информация о владельце лицензии.

– кнопка продления лицензии.

За 30 дней до окончания срока действия лицензии ПК «Сканер-ВС» напоминает пользователю о необходимости продлить срок лицензии. Срок действия лицензии начинает подсвечиваться желтым цветом (рис. 18).

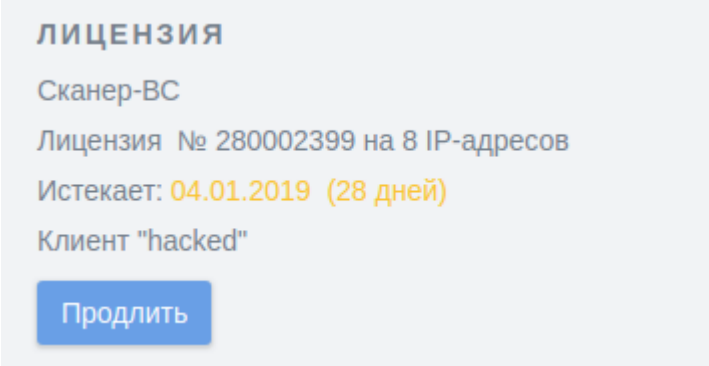


Рисунок 18 – Заканчивается срок действия лицензии

По истечению срока действия лицензии ПК «Сканер-ВС» сообщит пользователю с помощью красного текста (рис. 19). По истечению срока действия лицензии ПК «Сканер-ВС» пользователю становится недоступна функция обновления комплекса и функция экспорта отчетов.

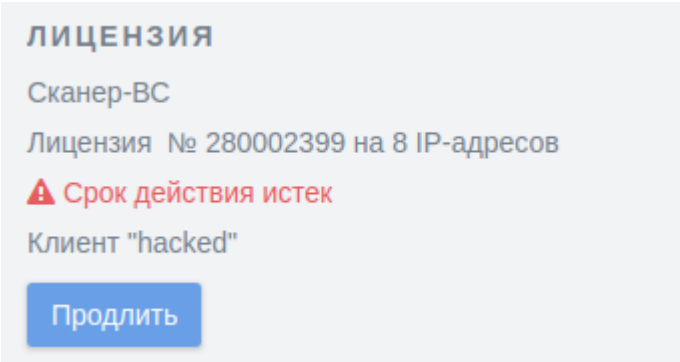


Рисунок 19 – Срок действия лицензии истек

Чтобы продлить лицензию ПК «Сканер-ВС», необходимо нажать на кнопку «Продлить». Откроется диалоговое окно «Обновление лицензии» (рис. 20).

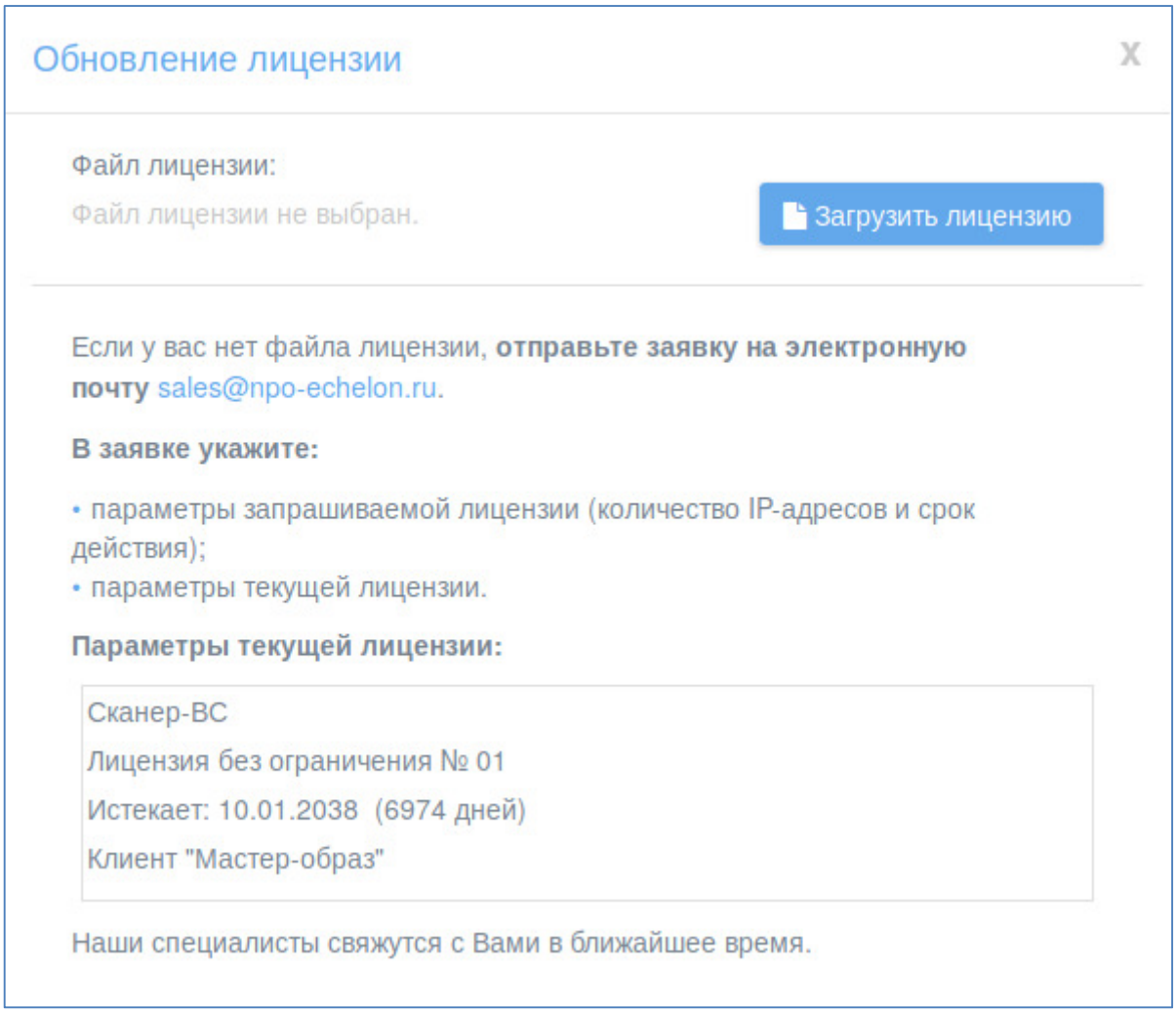


Рисунок 20 – Диалоговое окно «Обновление лицензии»

Чтобы загрузить новый файл лицензии нажмите на кнопку «Загрузить лицензию» и выберите файл лицензии формата *.lic. Диалоговое окно изменится (рис. 21).

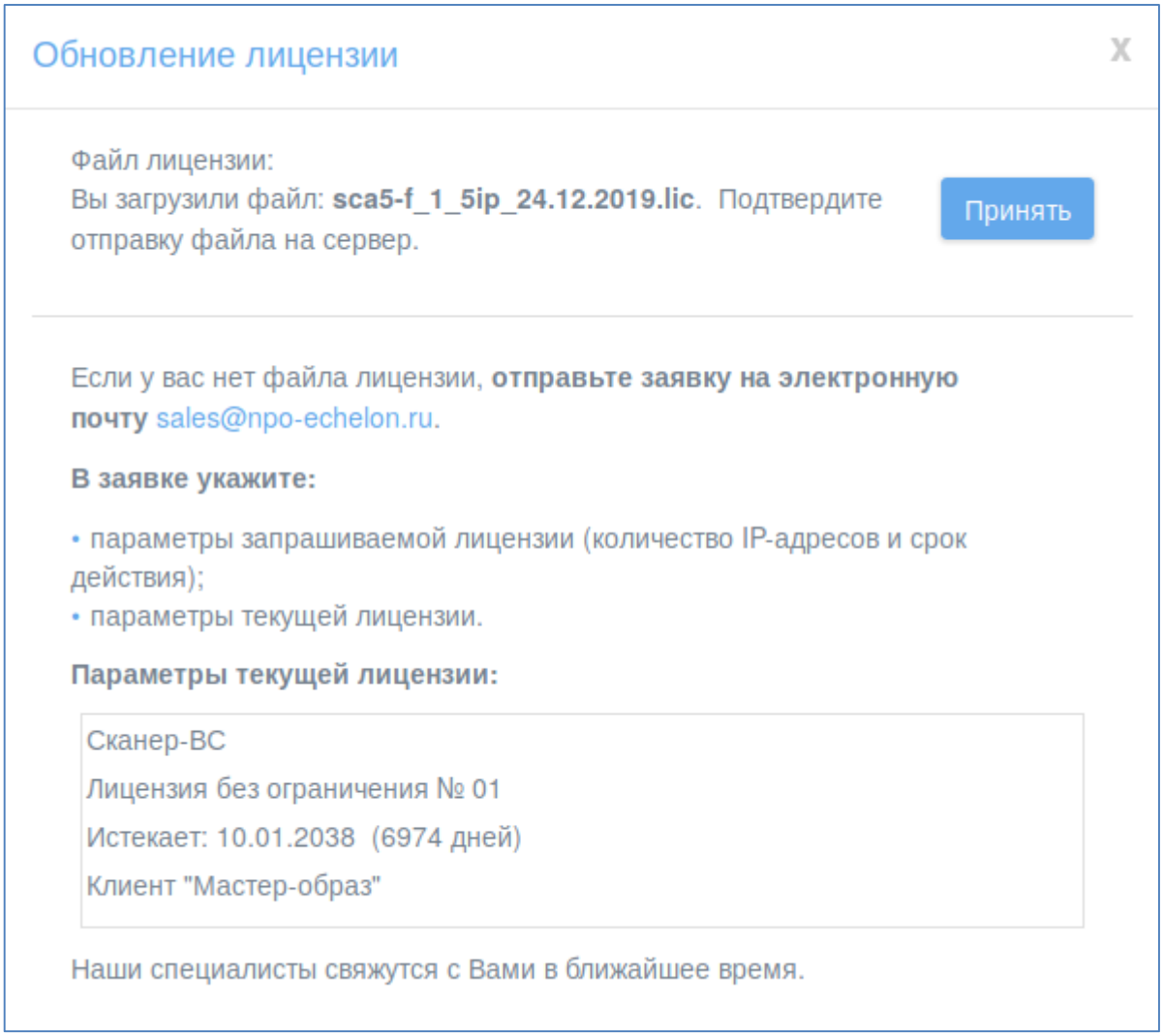


Рисунок 21 – Загрузка файла лицензии

Далее нажмите кнопку «Принять».

Если вы загрузили файл лицензии с некорректным расширением появится сообщение: «Файл с данным расширением не поддерживается.».

Если загрузка произошла успешно появится сообщение (рис. 22). Нажмите на крестик, чтобы завершить процесс обновления.

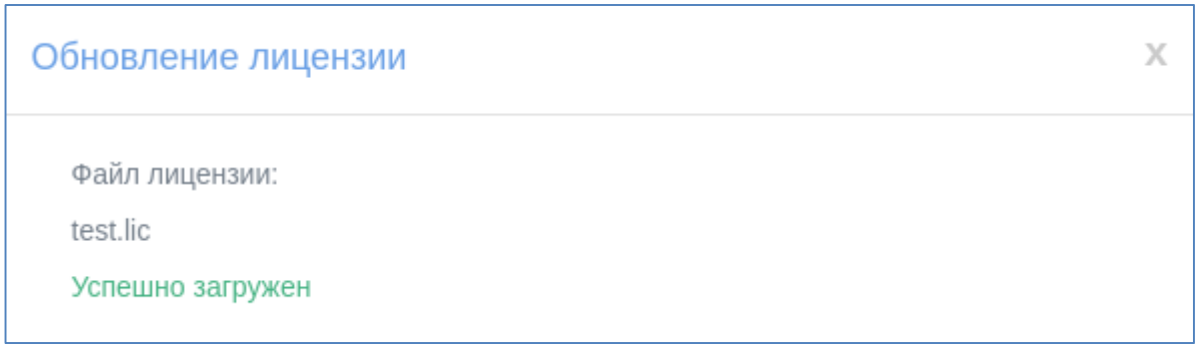


Рисунок 22 – Успешная загрузка файла лицензии

Если при загрузке файла произошла ошибка, появится сообщение: «При загрузке файла произошла ошибка. Пожалуйста, попробуйте еще раз.». Рекомендуется повторно произвести попытку загрузки файла лицензии, при повторной неудаче, рекомендуется обратиться в техническую поддержку.

3.1.3 Информация о продукте

Для ознакомления с информацией о продукте ПК «Сканер-ВС» предназначен специальный интерфейс, переход к которому осуществляется нажатием на пиктограмму «Информация» на панели навигации.

Интерфейс ознакомления с информацией о продукте представлен на рисунке (рис. 23).

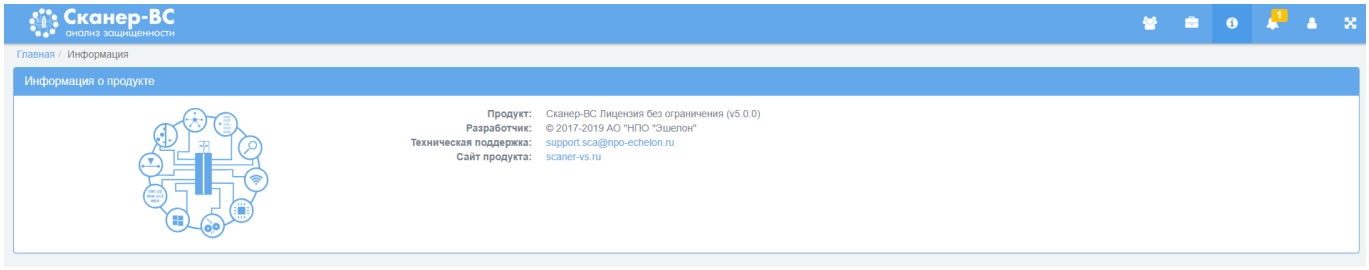


Рисунок 23 – Информация о продукте

В разделе «Информация о продукте» содержатся следующие данные:

– информация о продукте;

– разработчик продукта;

– электронный адрес технической поддержки;

– сайт продукта.

3.2 Администрирование

3.2.1 Общее описание

Доступность функции управления (администрирования) ПК «Сканер-ВС», определяется правами (ролью) назначенными Оператору. Ролевая модель управления доступом Оператора к функциям ПК «Сканер-ВС», предусматривает следующие роли:

– Пользователь;

– Администратор;

– Суперпользователь (только для учетной записи «Администратор Сканер-ВС»).

Роль «Пользователь» позволяет Оператору работать только со своими проектами. К проектам других пользователей у Оператора с ролью «Пользователь» доступа нет. Роль «Пользователь» позволяет Оператору, использовать следующие функции управления ПК «Сканер-ВС»:

– управление проектами;

– управление ресурсами;

– управление службами;

– обновление комплекса;

– управление лицензией.

Роль «Администратор» позволяет Оператору, помимо функций пользователя, использовать функцию управления пользователями ПК «Сканер-ВС», а также их проектами.

Роль «Суперпользователь» по умолчанию назначена только учетной записи «Администратор Сканер-ВС». Данные учетной записи: логин admin, пароль admin. Данная учетная запись является уникальной, обладает правами администратора, ей невозможно сменить роль, нельзя удалить и заблокировать. Рекомендуется немедленно после первой авторизации сменить пароль «Суперпользователю» ПК «Сканер-ВС» на надежный, и сохранить данный пароль, так как для данного пользователя в целях безопасности пароль восстановить невозможно.

3.2.2 Управление учетными записями пользователей

3.2.2.1 Общее описание

В процессе администрирования ПК «Сканер-ВС», Оператор выполняет задачи по управлению пользователями. Функционал ПК «Сканер-ВС», реализующий возможность управления пользователями, доступен Операторам, которым назначена роль «Администратор» или «Суперпользователь».

В рамках задач по управление пользователями Оператор может выполнить:

– создание учетной записи (пп. 3.2.2.2);

– управление правами пользователя (пп. 3.2.2.3);

– сброс пароля учетной записи (пп. 3.2.2.4);

– блокировку учетной записи (пп. 3.2.2.5);

– удаление учетной записи (пп. 3.2.2.6).

Для управления учетными записями пользователей ПК «Сканер-ВС» предназначен специальный интерфейс «Администрирование» (вкладка «Пользователи»), доступ к которому осуществляется нажатие на пиктограмму «Администрирование» в панели навигации.

Вид интерфейса «Администрирование» (вкладка «Пользователи») представлен на рисунке (рис. 24).

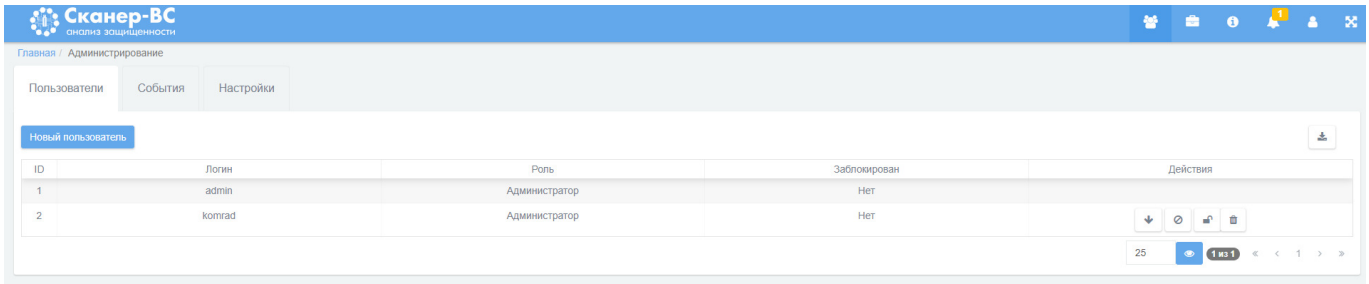


Рисунок 24 – Интерфейс «Администрирование» (вкладка «Пользователи»)

Интерфейс «Администрирование» вкладка «Пользователи» содержит следующие элементы:

– кнопка «Новый пользователь», предназначена для перехода к интерфейсу «Создание учетной записи пользователя» (пп. 3.2.2.2);

– список учетных записей зарегистрированных пользователей ПК «Сканер-ВС» в табличном формате.

Для каждой учетной записи пользователя ПК «Сканер-ВС» в таблице отображаются:

– ID - сведения об идентификационном номере пользователя;

– логин - сведения об имени учетной записи пользователя;

– роль - роль, назначенная Оператору;

– заблокирован – сведения о состоянии учетной записи пользователя. «Да» отображается в случае, если учетная запись заблокирована, «Нет» для активных учетных записей;

– действия – набор пиктограмм, отображающих управляющие действия, которые можно выполнить с данной учетной записью.

С существующей учетной записью могут быть выполнены следующие действия:

– смена роли пользователя (пп. 3.2.2.3);

– сброс пароля (пп. 3.2.2.4);

– блокировка / разблокировка (пп. 3.2.2.5);

– удаление (пп. 3.2.2.6).

3.2.2.2 Создание учетной записи пользователя

Создание учетной записи пользователя выполняется через специализированный интерфейс, (интерфейс запускается на панели инструментов ПК «Сканер-ВС» следующим образом:

– войти в интерфейс «Администрирование»;

– открыть вкладку «Пользователи»;

– нажать кнопку «Новый пользователь».

Вид интерфейса «Новый пользователь» представлен на рисунке (рис. 25).

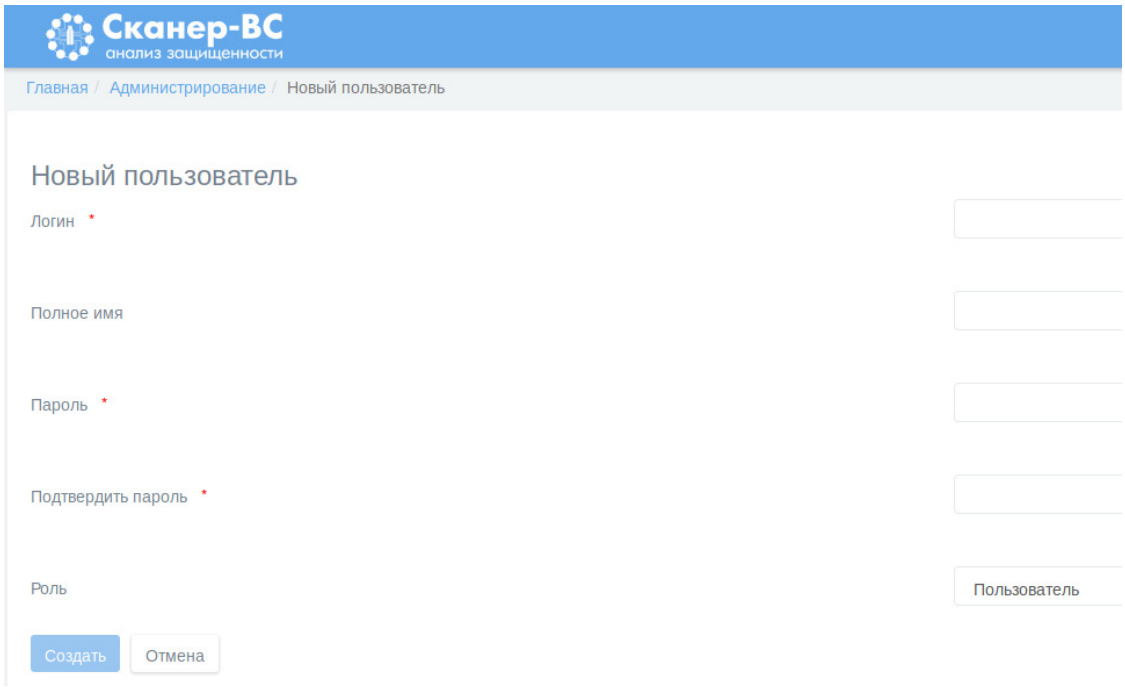


Рисунок 25 – Интерфейс «Новый пользователь»

Интерфейс «Новый пользователь» содержит следующие элементы:

– поле ввода «Логин»;

– поле ввода «Полное имя»;

– поле ввода «Пароль»;

– поле ввода «Подтвердить пароль»;

– выпадающий список «Роль»;

– кнопка «Создать»;

– кнопка «Отмена».

Поля ввода: «Логин», «Пароль», «Подтвердите пароль» являются обязательными к заполнению и отмечены знаком «*» (звездочка).

Поле «Логин» предназначено для ввода имени учетной записи, которое будет использоваться пользователем для доступа к ПК «Сканер-ВС». К логину предъявляются следующие требования:

– должен состоять только из одного слова;

– должен состоять только из строчных и прописных (заглавных) букв (A-z), цифр (0-9) и специальных символов (.-);

– максимальная длина – 20 символов;

– не должен повторяться с логинами других пользователей.

В случае ввода значения, не отвечающего предъявляемым требованиям, появится соответствующее сообщение об ошибке:

– «Логин должен состоять из строчных и прописных (заглавных) букв (A-z), цифр (0-9) и специальных символов (.-)»;

– «Превышена допустимая длина логина. Максимальная длина 20»;

– «Такой пользователь уже существует»;

– «Обязательное поле».

Поле «Полное имя» предназначено для ввода Имени, Фамилии и Отчества (при наличии) пользователя.

К формату записи ФИО предъявляется следующее требование: длина введенного значения не должна превышать 100 символов.

В случае ввода значения, не отвечающего предъявляемым требованиям, появится соответствующее сообщение об ошибке: «Количество введенных символов превышает допустимое значение (100)».

В поле «Пароль» необходимо ввести пароль для учетной записи нового пользователя. К паролю предъявляются следующие требования:

– минимальная длина – 8 символов;

– максимальная длина – 255 символов;

– должен состоять только из одного слова (не содержать символ «пробел»);

– должен содержать не менее одной буквы (a-z, A-Z), цифры (0-9) и специального символа (.?$#_-@:&%*!)».

В случае ввода значения, не отвечающего предъявляемым требованиям, появится соответствующее сообщение об ошибке:

– «Длина пароля должна быть не менее 8 символов»;

– «Превышена допустимая длина пароля. Максимальная длина 255»;

– «Пароль должен содержать не менее одной буквы (a-z, A-Z), цифры (0-9) и специального символа (.?$#_-@:&%*!)»;

– «Введенные пароли не совпадают».

В поле «Подтвердить пароль» необходимо повторно ввести пароль пользователя, совпадающий с указанным в поле «Пароль».

В поле «Роль» необходимо указать роль пользователя, путем выбора соответствующего значения («Пользователь» или «Администратор») из выпадающего списка, по умолчанию выбрано значение «Пользователь».

После заполнения всех обязательных полей без ошибок, станет доступна кнопка «Создать». При нажатии на нее в таблице вкладки «Пользователи» появится новая учетная запись пользователя. Если нового пользователя создавать не нужно, то необходимо нажать кнопку «Отмена».

3.2.2.3 Управление правами пользователя

Управление правами пользователя осуществляется через специальную пиктограмму, которая может находиться в двух состояниях в зависимости от того, какая роль у пользователя (пиктограмма расположена в таблице, в столбце «Действия»).

В таблицу можно попасть, выполнив следующие действия:

– открыть раздел «Администрирование»;

– зайти во вкладку «Пользователи».

Пиктограмма управления правами пользователей в двух состояниях представлена на рисунке (рис. 26).

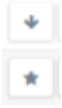


Рисунок 26 – Пиктограмма управления правами пользователей в двух состояниях

Пиктограмма управления пользователями может находиться в двух состояниях и в зависимости от этого может выполнять следующие действия с учетной записью пользователя, находящегося с ней в одной строке.

На рисунке (рис. 26) пиктограмма находится в следующих состояниях (сверху вниз):

– пиктограмма управления правами пользователя в данном состоянии предназначена для понижения роли администратора до пользователя;

– пиктограмма управления правами пользователя в данном состоянии предназначена для повышения роли пользователя до администратора.

3.2.2.4 Сброс пароля учетной записи

Сброс пароля учетной записи пользователя осуществляется через специальную пиктограмму (пиктограмма расположена в таблице, в столбце «Действия».

В таблицу можно попасть, выполнив следующие действия:

– открыть Раздел «Администрирование»;

– войти во вкладку «Пользователи».

Для сброса пароля учетной записи пользователя используется пиктограмма, изображенная на рисунке (рис. 27).

Рисунок 27 – Пиктограмма сброса пароля

При нажатии на пиктограмму сбрасывается текущий пароль учетной записи пользователя, находящегося в одной строке с пиктограммой, и появляется окно с новым сгенерированным и назначенным паролем для данной учетной записи (рис. 28).

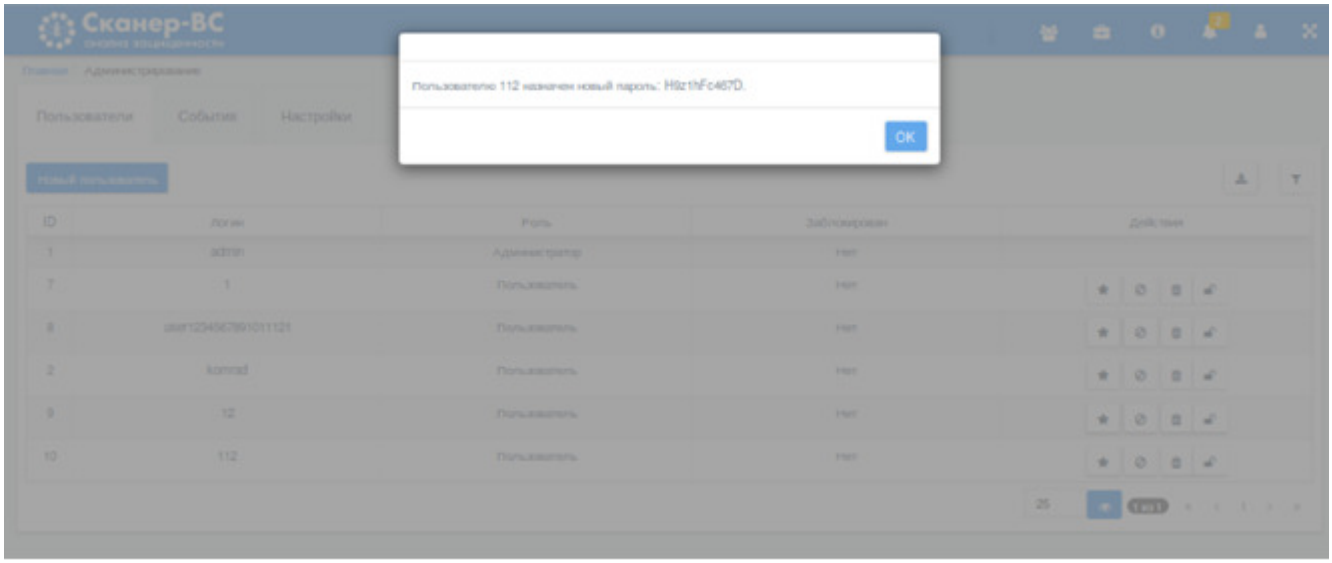


Рисунок 28 – Окно с новым паролем

3.2.2.5 Блокировка учетной записи

Блокировка и разблокировка учетной записи пользователя осуществляется через специальную пиктограмму, которая может находиться в двух состояниях в зависимости от того, заблокирован пользователь или нет (пиктограмма расположена в таблице, в столбце «Действия».

В таблицу можно попасть, выполнив следующие действия:

– открыть Раздел «Администрирование»;

– войти во вкладку «Пользователи».

Пиктограмма блокировки учетной записи может находиться в двух состояниях и в зависимости от этого может выполнять разные действия с учетной записью пользователя, находящегося с ней в одной строке (рис. 29).

Рисунок 29 – Пиктограмма блокировки в двух состояниях

На рисунке (рис. 29) пиктограмма находится в следующих состояниях (сверху вниз):

– пиктограмма блокировки в данном состоянии предназначена для блокировки учетной записи пользователя;

– пиктограмма блокировки в данном состоянии предназначена для разблокировки учетной записи пользователя.

3.2.2.6 Удаление учетной записи пользователя

Удаление учетной записи пользователя осуществляется через специальную пиктограмму (пиктограмма расположена в таблице, в столбце «Действия».

В таблицу можно попасть, выполнив следующие действия:

– открыть Раздел «Администрирование»;

– войти во вкладку «Пользователи».

Для удаления учетной записи пользователя используется пиктограмма, изображенная на рисунке (рис. 30). При нажатии на пиктограмму удаляется учетная запись пользователя,

находящегося в одной строке с пиктограммой. При удалении учетной записи пользователя, все проекты, созданные данным пользователем, будут удалены без возможности восстановления.

Рисунок 30 – Пиктограмма удаления пользователя

3.3 Проекты

3.3.1 Общее описание

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 фазе «Отчетность» в виде сгенерированных отчетов. Для проведения тестирования пользователь может создать новый проект или, в случае продолжения, начатого ранее и сохраненного тестирования, использовать его.

В процессе администрирования ПК «Сканер-ВС», Оператор выполняет задачи по управлению проектами. Функционал ПК «Сканер-ВС», реализующий возможность управления проектами, доступен Операторам, которым назначена роль «Пользователь», «Администратор» или «Суперпользователь».

В рамках задач по управлению проектами Оператор может выполнить:

– создание проекта (п. 3.3.2);

– настройку проекта (п. 3.3.3);

– удаление проекта (п. 3.3.4).

3.3.2 Создание проекта

Для создания проекта в левой части главной страницы ПК «Сканер-ВС» необходимо нажать левой кнопкой мыши по разделу «Проекты» (рис. 31) или на пиктограмму «Проекты» на панели навигации (рис. 32).

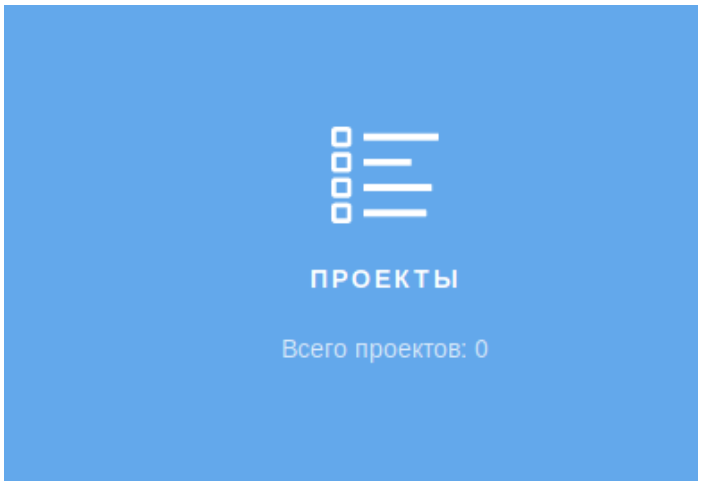


Рисунок 31 – Раздел «Проекты»

В открывшемся интерфейсе необходимо нажать кнопку «Новый проект» или выбрать уже существующий проект из перечисленных в рабочей области элемента «Проекты» (рис. 32).

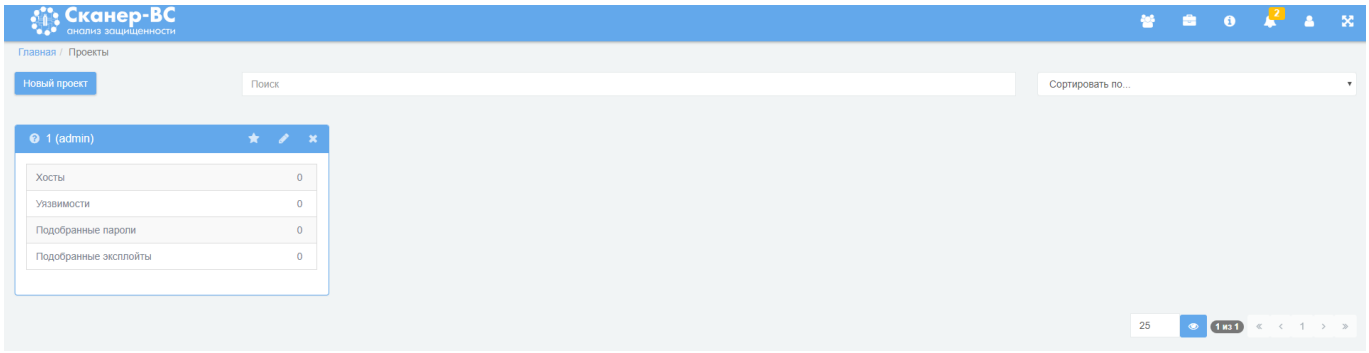


Рисунок 32 – Рабочая область элемента «Проекты»

При нажатии кнопки «Новый проект» откроется интерфейс «Добавление нового проекта» (рис. 33).

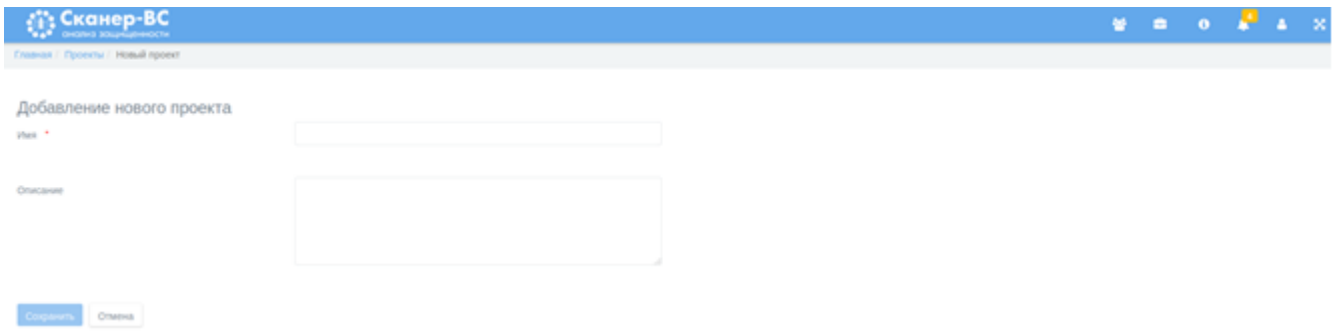


Рисунок 33 – Интерфейс «Добавление нового проекта»

Интерфейс «Добавление нового проекта» содержит следующие элементы:

– поле ввода «Имя»;

– поле ввода «Описание».

Поле ввода «Имя» является обязательным к заполнению и отмечено знаком «*» (звездочка).

Поле ввода «Имя» предназначено для ввода имени проекта, которое будет использоваться пользователем для поиска необходимого проекта. К имени проекта предъявляются следующие требования:

– максимальная длина – 80 символов;

– не должно повторяться с именами других проектов, если проект создан тем же пользователем.

В случае ввода значения, не отвечающего предъявляемым требованиям, появится соответствующее сообщение об ошибке:

– «Имя обязательное поле»;

– «Количество введенных символов превышает допустимое значение (80)»;

– «Проект с таким именем уже существует».

Поле ввода «Описание» предназначено для ввода описания проекта. К формату записи описания предъявляется следующее требование: длина введенного значения не должна превышать 250 символов.

В случае ввода значения, не отвечающего предъявляемым требованиям, появится соответствующее сообщение об ошибке: «Количество введенных символов превышает допустимое значение (250)».

После заполнения полей ввода, для сохранения введенной информации о новом проекте необходимо нажать кнопку «Сохранить», если же по каким-либо причинам проект создавать не требуется, нужно нажать кнопку «Отмена».

После нажатия кнопки «Сохранить» или после выбора ранее сохраненного проекта открывается интерфейс проекта (рис. 34).

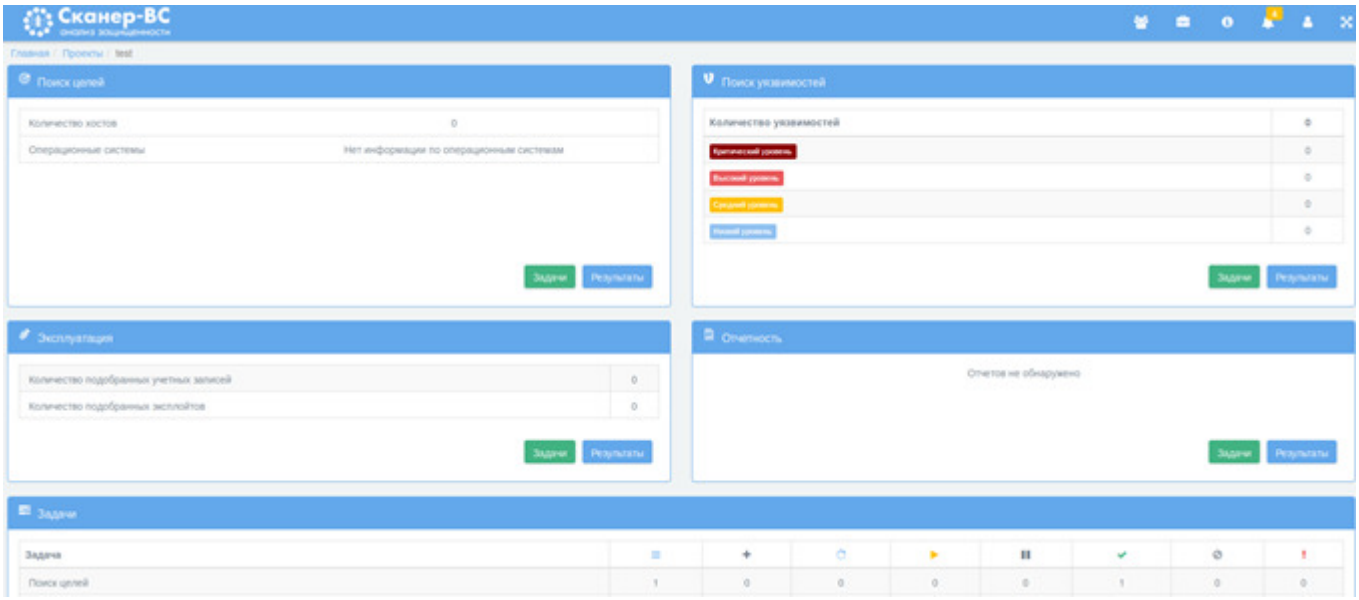


Рисунок 34 – Интерфейс проекта

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

3.3.3 Управление проектами

3.3.3.1 Общее описание

Функция управления проектами ПК «Сканер-ВС», определяется правами (ролью) назначенными Оператору.

Оператор с ролью «Пользователь» может работать только со своими проектами, которые созданы в его учетной записи. К проектам других пользователей у Оператора с ролью «Пользователь» доступа нет.

Роль «Администратор» и «Суперпользователь» позволяет Оператору, помимо функций «Пользователя», управлять проектами созданными другими пользователями.

3.3.3.2 Управление задачами

3.3.3.2.1 Общее описание

В процессе администрирования (управления) ПК «Сканер-ВС», Оператор выполняет задачи по управлению проектами. Функционал ПК «Сканер-ВС», реализующий возможность управления

задачами проектов, доступен Операторам, которым назначена роль «Пользователь», «Администратор» и «Суперпользователь».

В рамках управления задачами проектов Оператор может выполнить:

– поиск целей (пп. 3.3.6.2);

– поиск уязвимостей (пп. 3.3.6.3);

– эксплуатацию (пп. 3.3.6.4);

– отчетность (пп. 3.3.6.5);

– задачи (пп. 3.3.6.6).

Для управления задачами ПК «Сканер-ВС» предназначен специальный интерфейс, доступ к которому осуществляется нажатием в левой части веб-интерфейса по разделу «Проекты» или нажатием кнопки «Проекты» в верхнем правом углу веб-интерфейса (рис. 31). Далее необходимо выбрать проект из рабочей области элемента «Проекты», нажатием на необходимый проект (рис. 32), после чего будет открыт интерфейс проекта.

Вид интерфейса проекта представлен на рисунке (рис. 35).

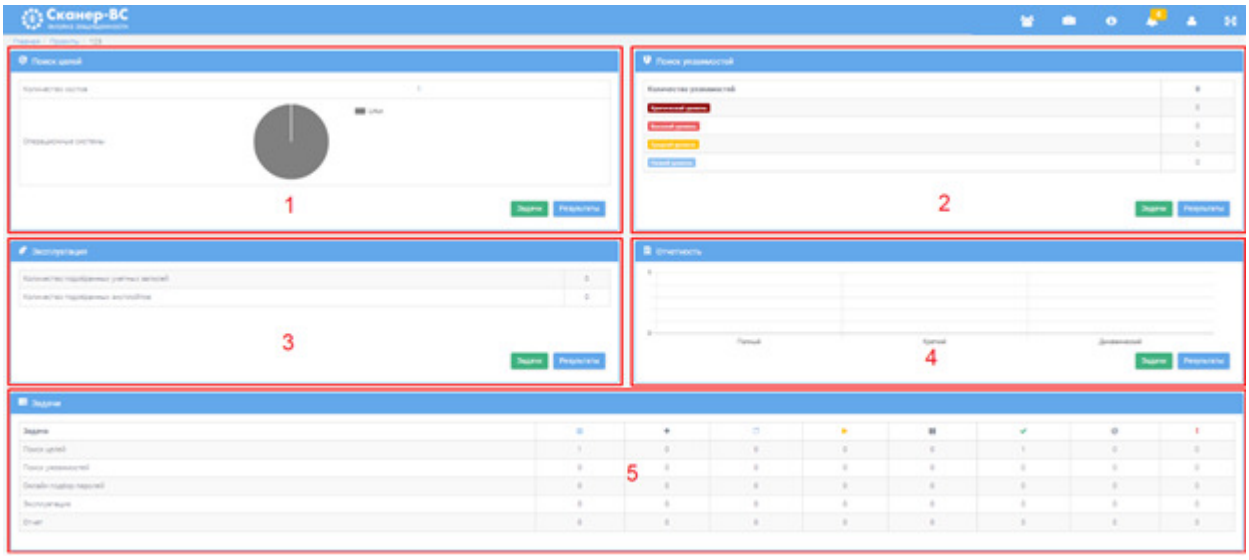


Рисунок 35 – Интерфейс проекта

Интерфейс проекта содержит следующие элементы:

1. Поиск целей (пп. 3.3.6.2).
2. Поиск уязвимостей (пп. 3.3.6.3).
3. Эксплуатация (пп. 3.3.6.4).
4. Отчетность (пп. 3.3.6.5).

5. Задачи (пп. 3.3.6.6).

3.3.3.2.2 Вкладка «Задачи»

В рамках задач по тестированию защищенности Оператор использует следующие элементы интерфейса проекта:

– поиск целей (пп. 3.3.6.2);

– поиск уязвимостей (пп. 3.3.6.3);

– эксплуатацию (пп. 3.3.6.4);

– отчетность (пп. 3.3.6.5).

При выполнении тестирования защищенности ПК «Сканер-ВС» используется специальный интерфейс, доступ к которому осуществляется нажатием кнопки «Задачи» (в секторе с номером 1-4 на рисунке (рис. 35), после чего откроется вкладка «Задачи» (рис. 36).

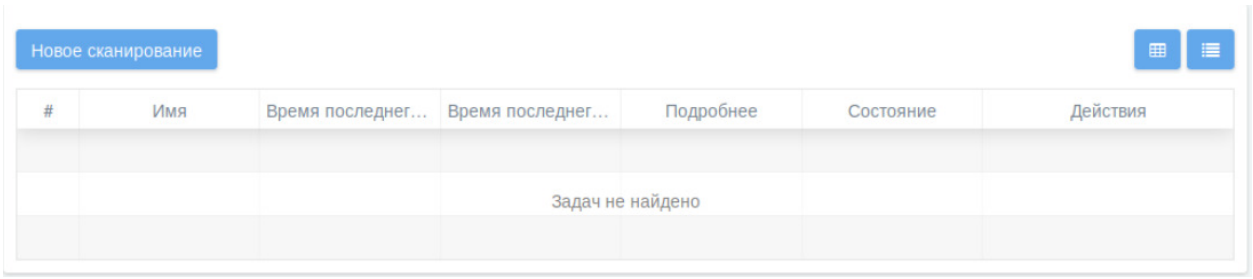


Рисунок 36 – Вкладка «Задачи»

Во вкладке «Задачи» находится таблица, которая содержит в себе следующие данные:

– номер задачи;

– имя задачи;

– время последнего запуска;

– время последнего завершения;

– подробные данные о задаче;

– состояние задачи;

– действия с задачей.

Для создания задачи необходимо нажать кнопку нового сканирования в верхнем левом углу таблицы.

Во вкладке «Задачи» есть два способа отображения данных по задаче: общий и подробный. В подробном режиме удобно просматривать статус задачи, если использовалась настройка «Разбивать на подзадачи».

Чтобы перейти в подробный режим необходимо нажать кнопку списка в верхнем правом углу таблицы (рис. 37).

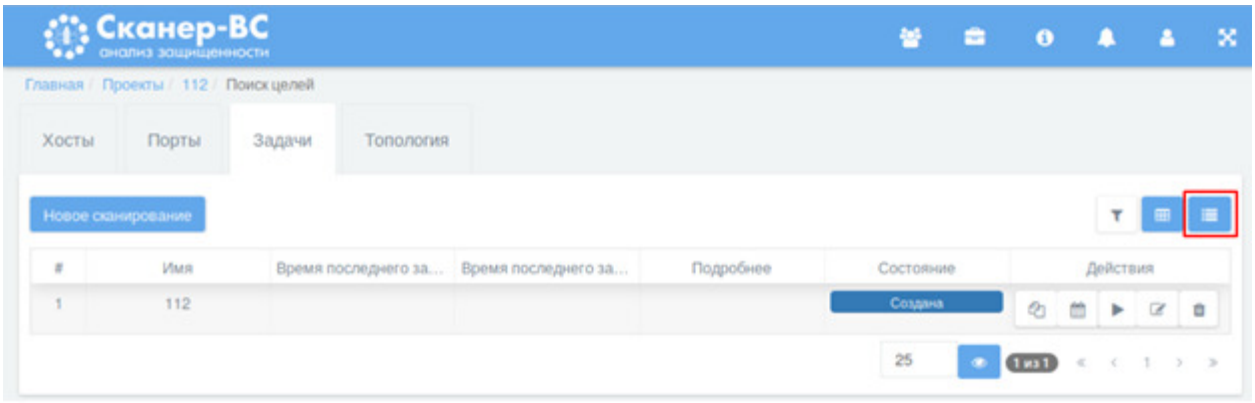


Рисунок 37 – Включение режима подробного отображения

Пример отображения рабочего пространства в подробном режиме показан на рисунке (рис. 38). Для развертывания задачи необходимо нажать на темно-серую стрелку соответствующей задачи, раскроется список подзадач, представленный на рисунке (рис. 39). Для Оператора доступны следующие действия при работе с подзадачами: «Запустить», «Отменить», «Приостановить». Задачи, которые были созданы без параметра «Разбивать на подзадачи» развернуть нельзя, поэтому стрелка будет светло-серого цвета (рис. 38).

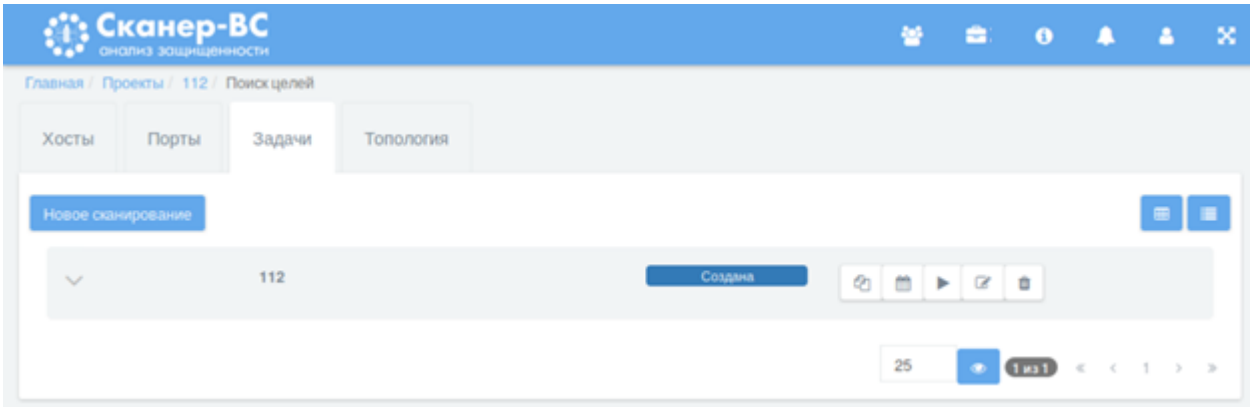


Рисунок 38 – Подробный режим отображения

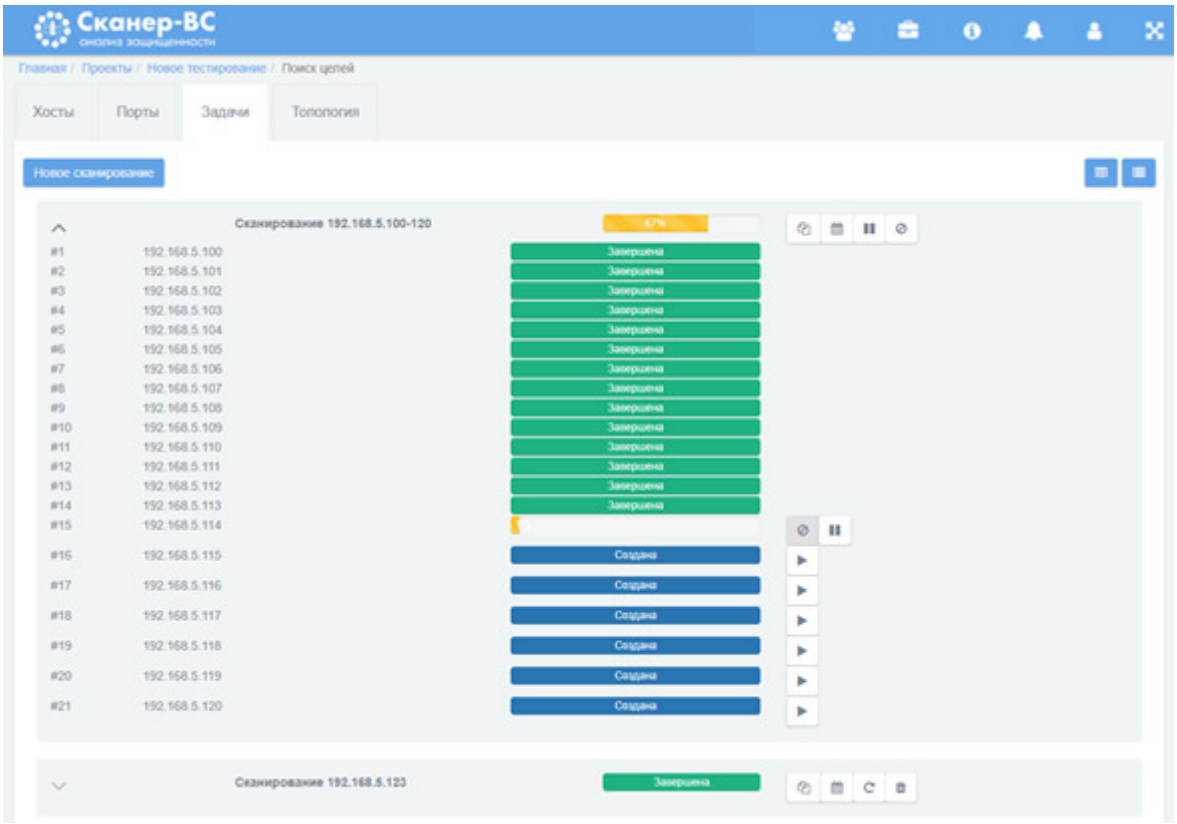


Рисунок 39 – Подзадачи

При задании диапазона IP-адресов в качестве целей, ПК «Сканер-ВС» предложит использовать дополнительную настройку «Разбивать на подзадачи» (рис. 39).

Примечание. Для больших диапазонов IP-адресов рекомендуется обязательно использовать данную настройку, так как при возникновении трудностей в сканировании отдельных узлов, данные узлы можно будет пропустить вручную и не потерять результаты других подзадач.

После создания задачи на сканирование, во вкладке «Задачи» в таблице появится номер задачи, ее имя, текущий статус (цветной индикатор с комментарием) и перечень доступных действий. Перечень возможных состояний задач и доступных действий представлен в таблице (см. Таблица 2).

Таблица 2 – Перечень состояний задач и доступных действий

Состояние задачи	Цвет	Доступные действия
Создана	Синий	– клонировать; – запланировать; – запустить; – редактировать;

Состояние задачи	Цвет	Доступные действия
		– удалить;
В обработке	Синий	– клонировать; – запланировать
В процессе	Желтый	– клонировать; – запланировать; – приостановить; – отменить
Пауза	Синий	– клонировать; – запланировать; – возобновить; – отменить
Завершена	Зеленый	– клонировать; – запланировать; – повторить; – удалить
Отменена	Серый	– клонировать; – запланировать; – повторить; – удалить
Ошибка	Красный	– клонировать; – запланировать; – повторить; – удалить

Для получения подробной информации о задаче нужно нажать на строку таблицы, в которой она находится.

После нажатия откроется интерфейс описания задачи (рис. 40).

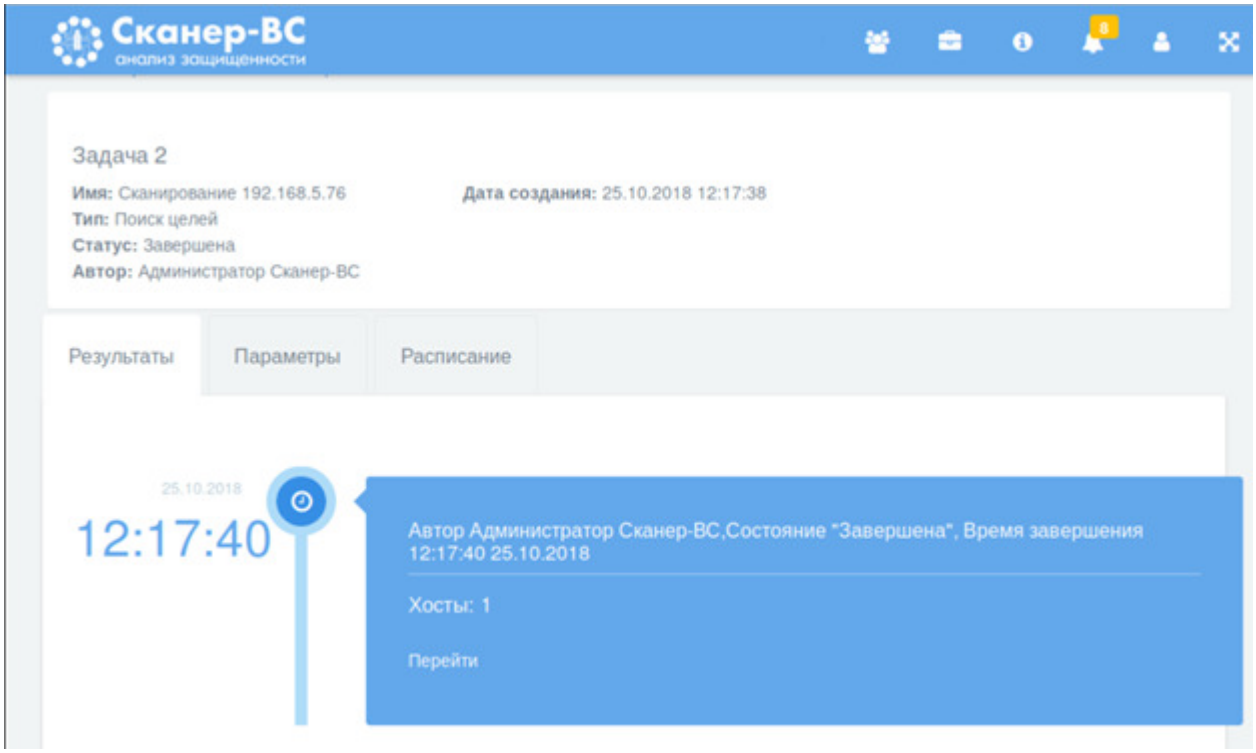


Рисунок 40 – Интерфейс описания задачи

Интерфейс содержит следующие вкладки:

– результаты;

– параметры;

– расписание.

Для получения подробной информации по задаче необходимо нажать левой кнопкой мыши на конкретную задачу во вкладке «Задачи», откроется интерфейс с информацией о задаче, как на рисунке (рис. 41).

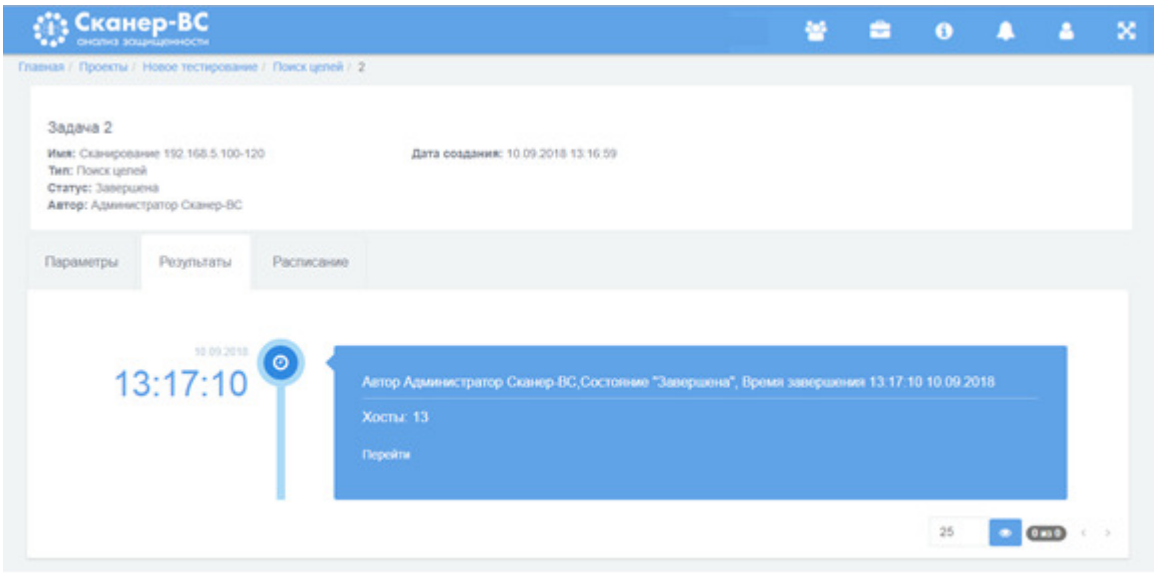


Рисунок 41 – Интерфейс с информацией о задаче

Во вкладке «Результаты» содержатся результаты сканирования каждого запуска задачи (рис. 41). Во вкладке «Параметры» содержится подробная информация о параметрах запущенной задачи (рис. 42). Во вкладке «Расписание» содержатся правила по расписанию запуска задачи (рис. 43).

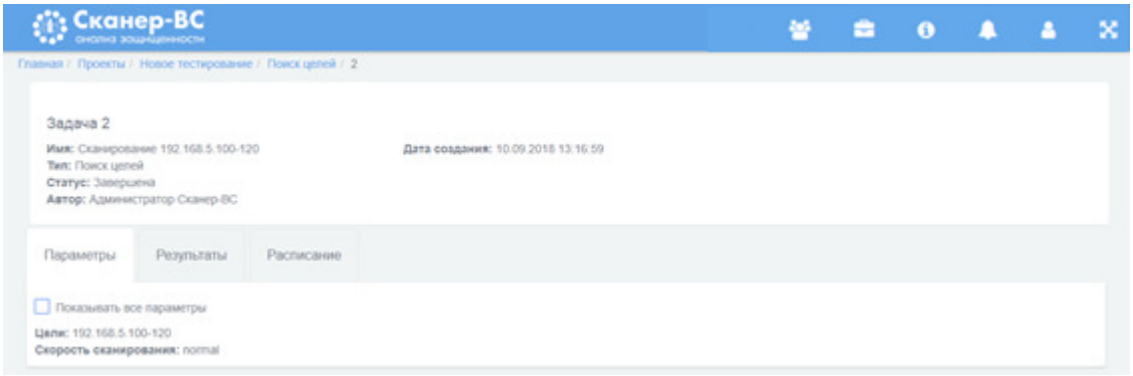


Рисунок 42 – Параметры задачи

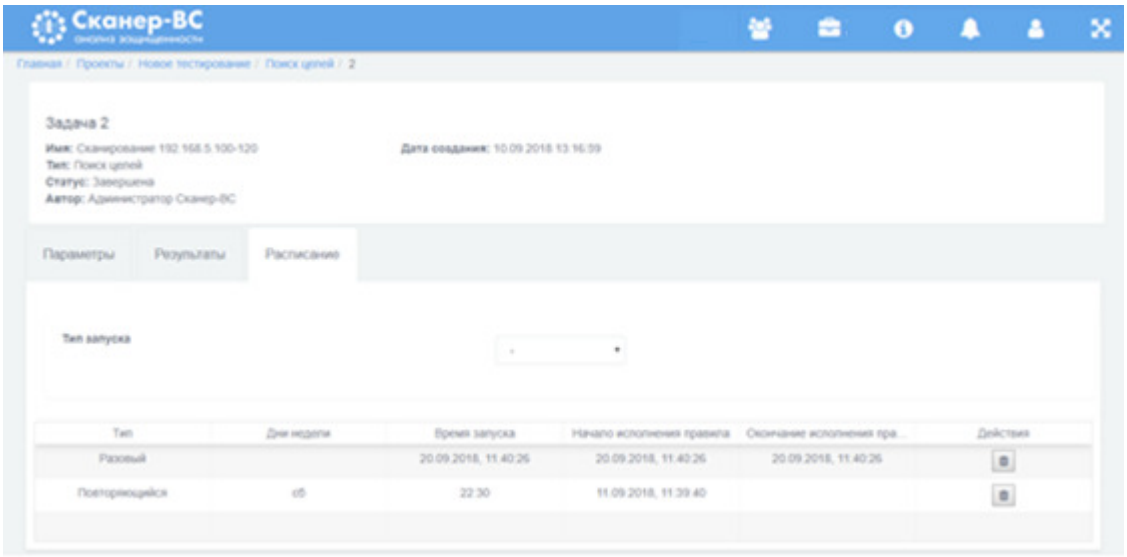


Рисунок 43 – Расписание задачи

Для перехода к результатам сканирования конкретного запуска необходимо во вкладке «Результаты» нажать на соответствующую строчку с информацией по нему. В рабочем окне появятся результаты запуска задачи, а также подробная информация по возникшим ошибкам (если имеются) во вкладке «Ошибки» (рис. 44).

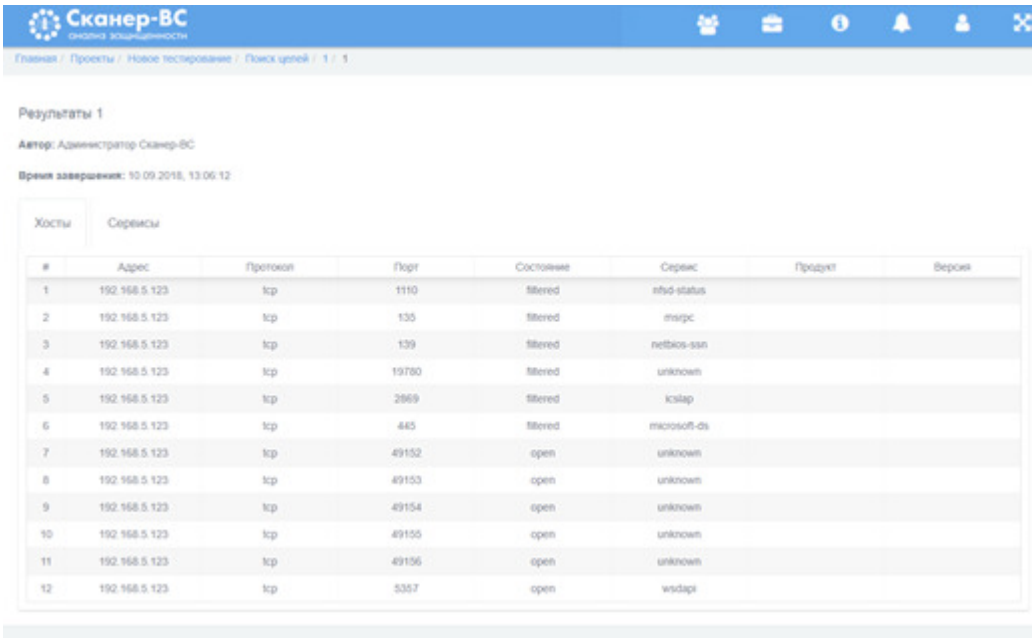


Рисунок 44 – Результаты запуска задачи

Подробная информация об управлении расписанием выполнения задач представлена в подпункте 3.3.3.2.4.

3.3.3.2.3 Настройка целей для сканирования

При создании задачи на новое сканирование (при поиске целей и поиске уязвимостей) настраиваются цели для сканирования. 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 необходимо нажать кнопку «Импорт целей из активов», отметить нужные IP-адреса (если IP-адрес выбран, рядом с ним в пустом квадрате появится галочка) или нажать кнопку «Выделить все» (все IP-адреса в поле будут отмечены автоматически). Затем необходимо нажать кнопку «Выбрать» и отмеченные IP-адреса появятся в поле «Цели».

Для загрузки целей сканирования из файла необходимо подготовить соответствующий список целей поиска уязвимостей в формате TXT, где одна строка должна содержать только один IP-адрес компьютера, сети или подсети. Затем нужно нажать кнопку «Импорт целей из файла» и в открывшемся окне выбрать файл с импортируемым списком, далее нажать кнопку «Открыть». Перечень целей сканирования появится в поле «Цели».

3.3.3.2.4 Управление расписанием выполнения задач

Запланировать задачу можно двумя способами: во вкладке «Задачи» и во вкладке «Расписание» конкретной задачи.

Во вкладке «Задачи» (см. пп. 3.3.3.2.2) в столбце «Действия» необходимо нажать кнопку «Запланировать», откроется диалоговое окно добавления правила (рис. 45). Далее нужно выбрать тип запуска: разовый или повторяющийся. Если был выбран разовый запуск, то далее необходимо настроить дату и время запуска и нажать кнопку «Добавить правило». Правило появится в сводной таблице правил по задаче (рис. 46). Если выбран повторяющийся запуск, то далее необходимо выбрать дни недели повторений, время запуска, дату начала исполнения правила, дату окончания исполнения правила и нажать кнопку «Добавить правило». Правило появится в сводной таблице правил по задаче (рис. 46). Любое правило можно удалить, для этого необходимо нажать кнопку «Удалить» в столбце «Действия».

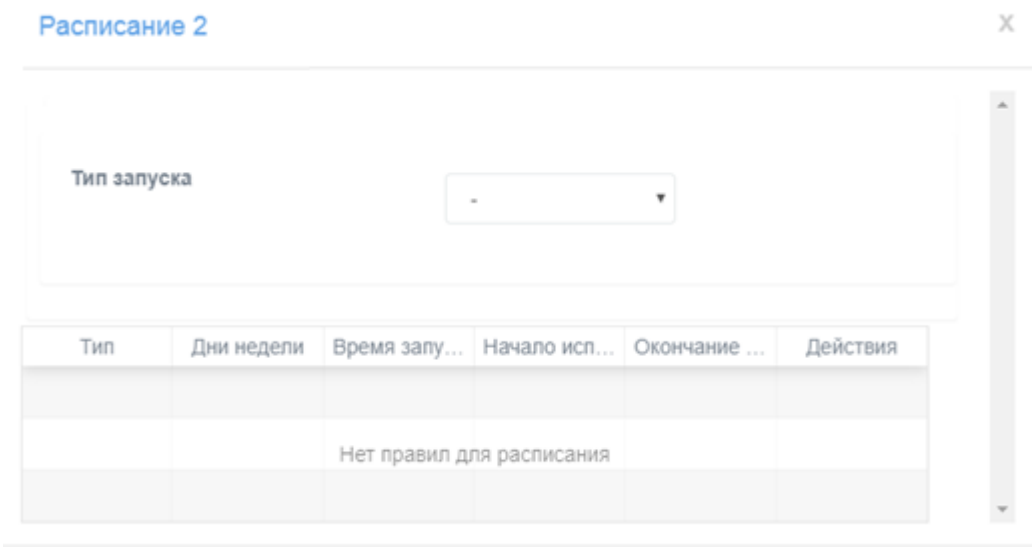


Рисунок 45 – Добавление правила

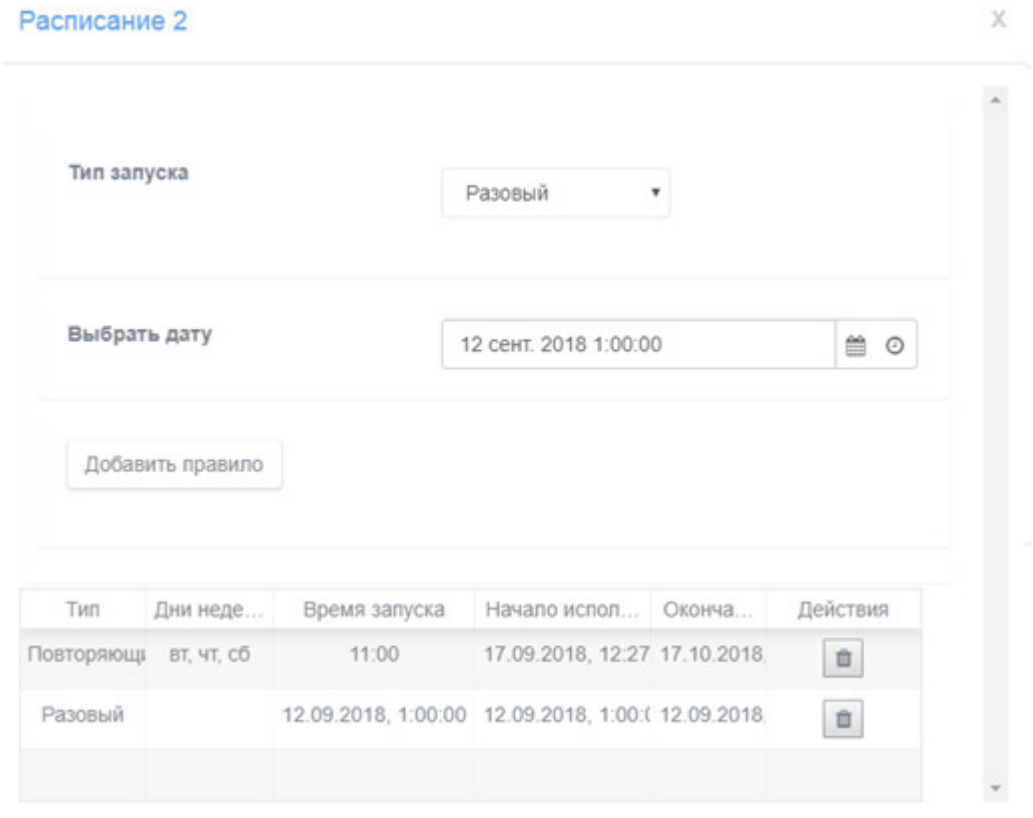


Рисунок 46 – Результат добавления правил

Запланировать задачу аналогичным способом можно, также, во вкладке «Расписание» конкретной задачи (рис. 43). Порядок добавления правила аналогичен описанному выше первому способу.

Независимо от результатов сканирования любую задачу можно перезапустить или дублировать. Для этого необходимо нажать кнопку «Дублировать» или «Повторить» (рис. 47), расположенные справа от индикатора статуса сканирования.

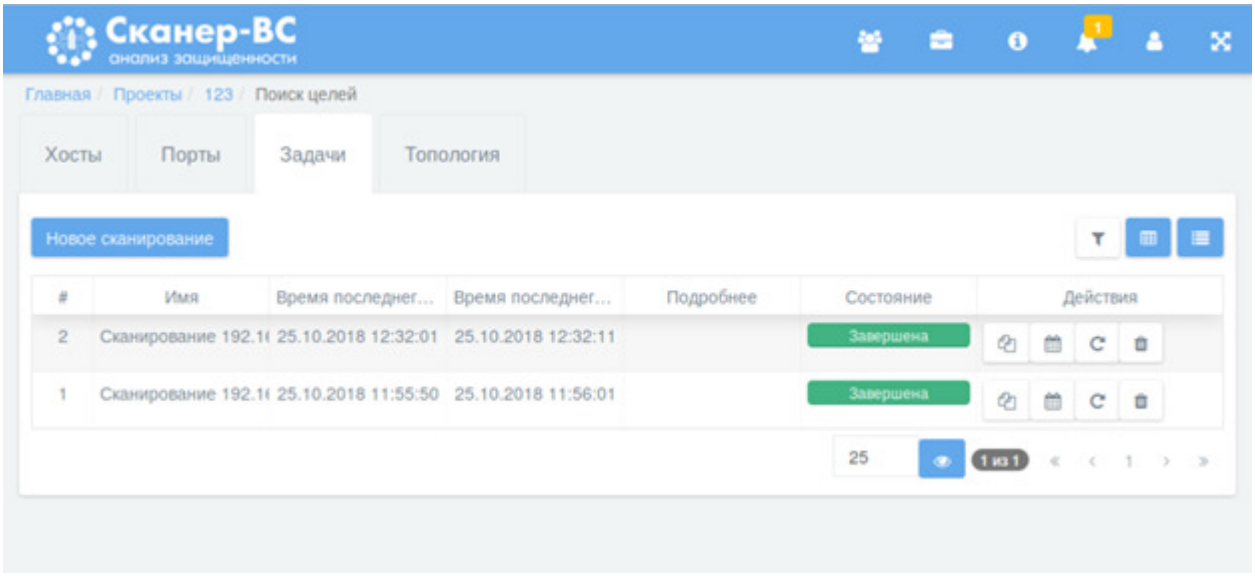


Рисунок 47 – Процесс сканирования

Для получения подробной информации об ошибке в процессе выполнения задачи, 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.

Изменение статуса выполнения задачи будет отражено в правом верхнем углу веб-интерфейса (кнопка Уведомления) (рис. 48).

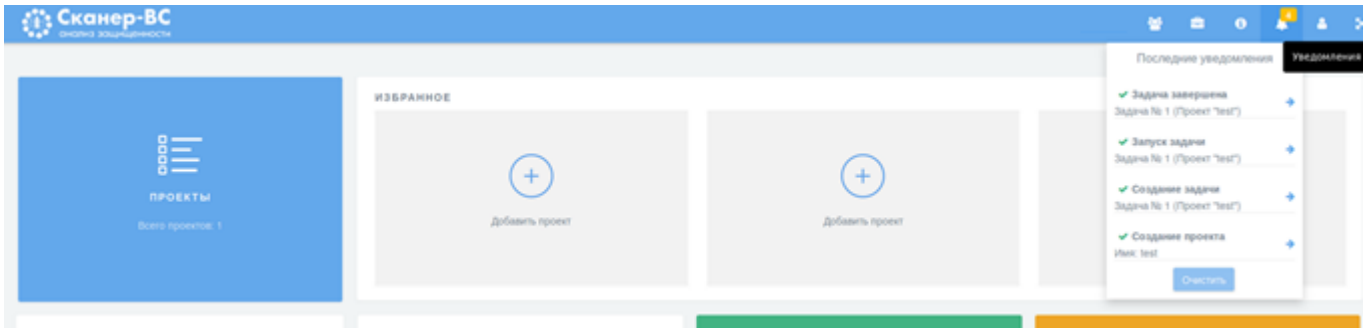


Рисунок 48 – Уведомления

3.3.3.2.5 Элемент «Задачи»

Элемент «Задачи» предназначен для просмотра статуса созданных задач (рис. 49).

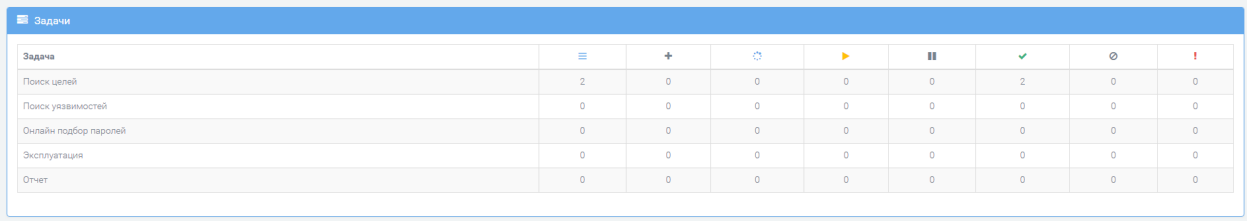


Рисунок 49 – Элемент «Задачи»

Элемент «Задачи» содержит таблицу, в столбцах которой содержатся следующие данные о задачах:

– тип задачи;

– сумма всех имеющихся задач;

– созданные задачи;

– задачи, находящиеся в обработке;

– активные задачи;

– приостановленные задачи;

– завершенные задачи;

– отмененные задачи;

– ошибки при выполнении задач.

3.3.4 Удаление проекта

Для удаления проекта в левой части главной страницы ПК «Сканер-ВС» необходимо нажать левой кнопкой мыши по разделу «Проекты» (рис. 31) или нажать на пиктограмму «Проекты» на панели управления.

В открывшемся интерфейсе нужно нажать на значок «крестик» в правом верхнем углу того проекта, который необходимо удалить. После нажатия появится окно с просьбой подтвердить удаление проекта (рис. 50).

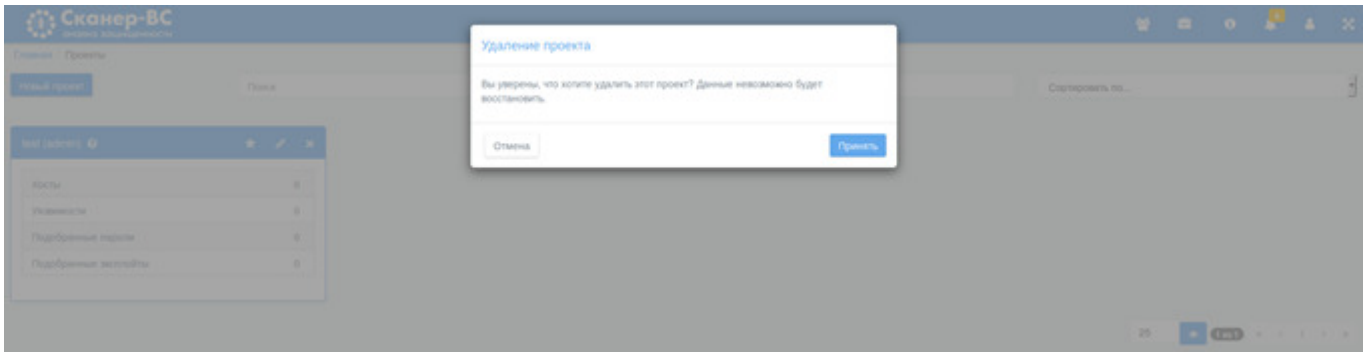


Рисунок 50 – Окно с просьбой подтвердить удаление проекта

Далее для удаления проекта необходимо нажать кнопку «Принять», если же по каким-либо причинам проект удалять не требуется, нужно нажать кнопку «Отмена».

3.3.5 Управление ресурсами

3.3.5.1 Общее описание

В процессе администрирования ПК «Сканер-ВС», Оператор выполняет задачи по управлению ресурсами. Функционал ПК «Сканер-ВС», реализующий возможность управления ресурсами, доступен Операторам, которым назначена роль «Пользователь», «Администратор» или «Суперпользователь».

В рамках задач по управлению ресурсами Оператор может выполнить:

– управление плагинами (пп. 3.3.5.2);

– управление политиками (пп. 3.3.5.3);

– управление словарями (пп. 3.3.5.4);

– управление списками портов (пп. 3.3.5.5);

– управление эксплойтами (пп. 3.3.5.6).

Для управления ресурсами ПК «Сканер-ВС» предназначен специальный интерфейс «Ресурсы», доступ к которому осуществляется нажатием на раздел «Ресурсы» на главном экране.

Вид интерфейса «Ресурсы» представлен на рисунке (рис. 51).

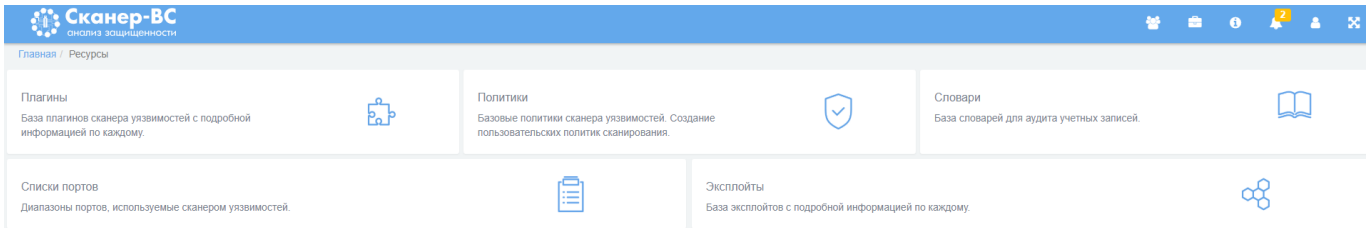


Рисунок 51 – Вид интерфейса «Ресурсы»

Интерфейс «Ресурсы» содержит следующие элементы:

– плагины (пп. 3.3.5.2);

– политики (пп. 3.3.5.3);

– словари (пп. 3.3.5.4);

– списки портов (пп. 3.3.5.5);

– эксплойты (пп. 3.3.5.6).

3.3.5.2 Управление плагинами

Управление плагинами осуществляется через специализированный интерфейс «Плагины». Для доступа в интерфейс «Плагины» необходимо выполнить следующие действия:

– открыть раздел «Ресурсы»;

– войти в интерфейс «Плагины».

Вид интерфейса «Плагины» представлен на рисунке (рис. 52).

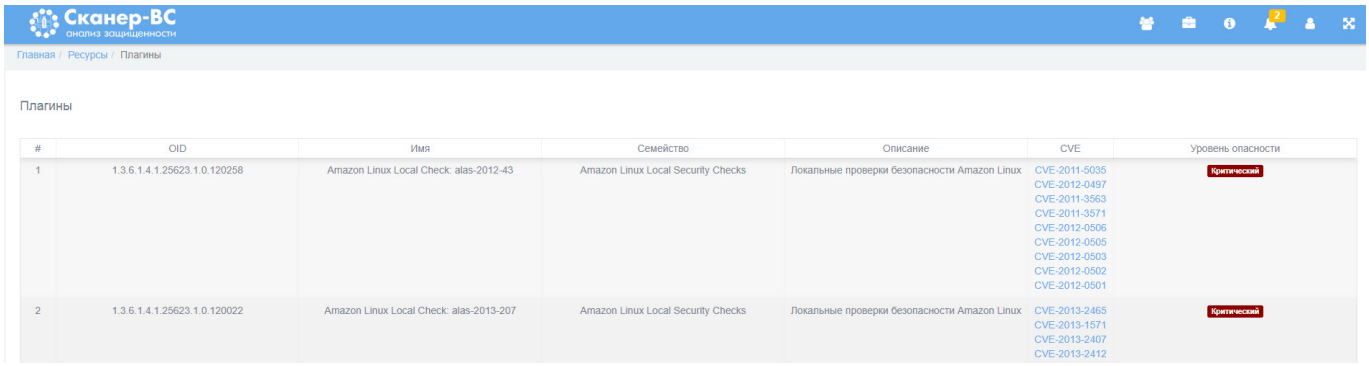


Рисунок 52 – Интерфейс «Плагины»

В данном интерфейсе присутствует таблица с семью столбцами. Каждый столбец содержит информацию о плагине. В таблице представлены следующие данные о плагинах (слева направо):

– номер строки плагина в таблице;

– OID плагина (уникальный идентификатор);

– имя плагина;

– семейство плагина;

– описание плагина;

– номер плагина в базе данных общеизвестных уязвимостей информационной безопасности (CVE);

– уровень опасности плагина.

Для получения более подробной информации о плагине необходимо нажать на строку, в которой находится плагин.

Вид интерфейса описания плагина представлен на рисунке (рис. 53).

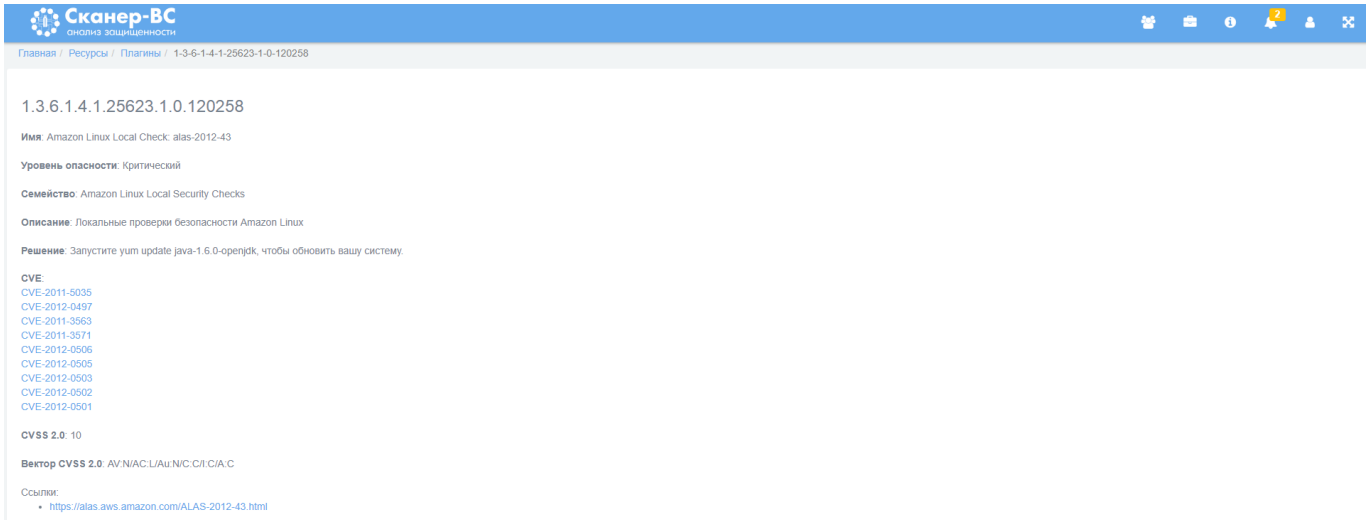


Рисунок 53 – Интерфейс описания плагина

В интерфейсе описания плагина содержится следующая информация:

– имя плагина;

– уровень опасности плагина;

– семейство плагина;

– описание плагина;

– решение для устранения уязвимости;

– CVE;

– BDU (если идентификатор присутствует);

– CVSS (оценка уязвимости);

– ссылки на подробное описание плагина.

3.3.5.3 Управление политиками

Управление политиками осуществляется через специализированный интерфейс. Для входа в интерфейс необходимо выполнить следующие действия:

– войти в раздел «Ресурсы»;

– выбрать интерфейс «Политики».

Вид интерфейса «Политики» представлен на рисунке (рис. 54).

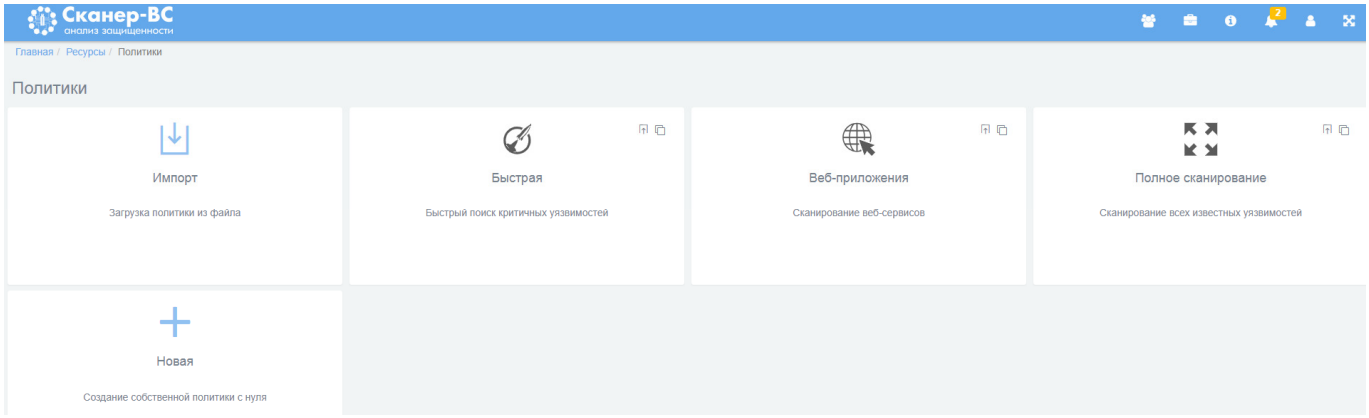


Рисунок 54 – Интерфейс «Политики»

В данном интерфейсе содержатся следующие разделы:

– Импорт (пп. 3.3.5.3.1);

– Политика быстрого сканирования (пп. 3.3.5.3.2);

– Политика сканирования веб – приложений (пп. 3.3.5.3.3);

– Политика полного сканирования (пп. 3.3.5.3.4);

– Новая политика (пп. 3.3.5.3.5).

3.3.5.3.1 Импорт

Импорт предназначен для загрузки собственной политики сканирования из файла в ПК «Сканер-ВС». Импорт осуществляется нажатием на раздел «Импорт» (рис. 55), после чего необходимо выбрать файл соответствующего формата в проводнике и нажать кнопку «Открыть».

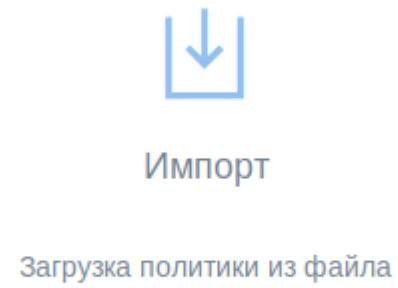


Рисунок 55 – Вид раздела «Импорт» в интерфейсе «Плагины»

3.3.5.3.2 Политика быстрого сканирования

Политика быстрого сканирования предназначена для быстрого поиска критичных уязвимостей. Вход для просмотра политики быстрого сканирования осуществляется нажатием на раздел политики «Быстрая» (рис. 56).

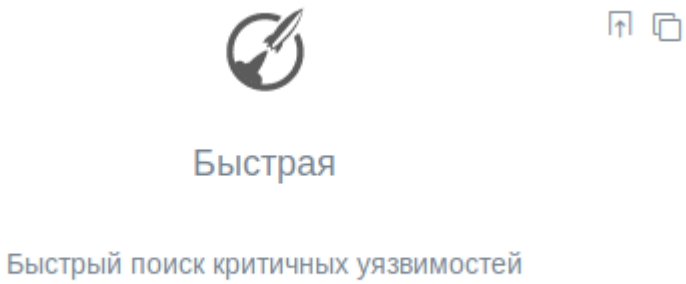


Рисунок 56 – Вид раздела политики «Быстрая» в интерфейсе «Плагины»

В правом верхнем углу политики «Быстрая» в разделе «Плагины» (рис. 56) есть две пиктограммы. Данные пиктограммы отвечают за экспорт политики и ее дублирование.

Вид интерфейса политики быстрого поиска представлен на рисунке (рис. 57).

Рисунок 57 – Интерфейс политики быстрого поиска

В данном интерфейсе содержится информация о политике и присутствует таблица с тремя столбцами. Каждый столбец содержит информацию об используемых данной политикой плагинах. В интерфейсе политики быстрого поиска представлена следующая информация:

– имя политики;

– описание политики;

– является ли политика пользовательской;

– количество используемых в политике плагинов.

В таблице интерфейса содержится следующая информация об используемых плагинах:

– семейства плагинов, используемых в данной политике;

– общее число плагинов в семействе;

– общее число плагинов, используемых в семействе.

3.3.5.3.3 Политика сканирования веб-приложений

Политика сканирования «Веб-приложения» предназначена для сканирования веб-сервисов. Вход для просмотра политики сканирования веб-приложений осуществляется нажатием на раздел политики «Веб-приложения» (рис. 58).

Рисунок 58 – Раздел политики «Веб-приложения» в интерфейсе «Политики»

В правом верхнем углу политики «Быстрая» в разделе «Плагины» (рис. 56) есть две пиктограммы. Данные пиктограммы отвечают за экспорт политики и ее дублирование

Вид интерфейса политики «Веб-приложения» представлен на рисунке (рис. 59).

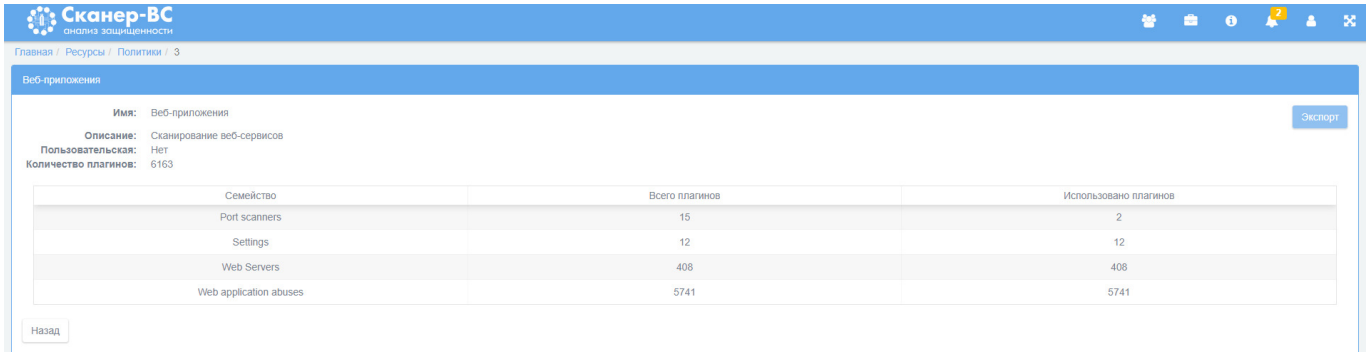


Рисунок 59 – Интерфейс политики «Веб-приложения»

В данном интерфейсе содержится информация о политике и присутствует таблица с тремя столбцами. Каждый столбец содержит информацию об используемых данной политикой плагинах. В интерфейсе политики «Веб-приложения» представлена следующая информация:

– имя политики;

– описание политики;

– является ли политика пользовательской;

– количество используемых в политике плагинов.

В таблице интерфейса содержится следующая информация об используемых плагинах:

– семейства плагинов, используемых в данной политике;

– общее число плагинов в семействе;

– общее число плагинов, используемых в семействе.

3.3.5.3.4 Политика полного сканирования

Политика полного сканирования предназначена для сканирования всех известных уязвимостей. Вход для просмотра политики полного сканирования осуществляется нажатием на раздел политики «Полное сканирование» (рис. 60).

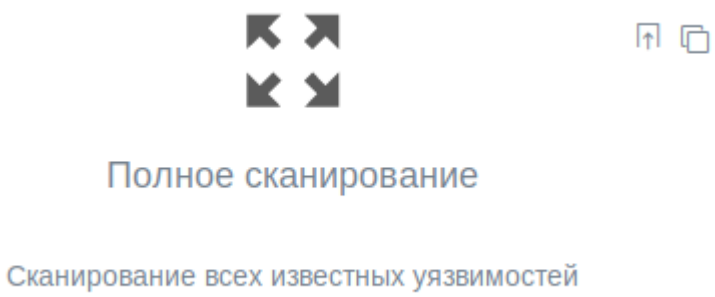


Рисунок 60 – Раздел политики «Полное сканирование» в интерфейсе «Политики»

Вид интерфейса «Полное сканирование» представлен на рисунке (рис. 61).

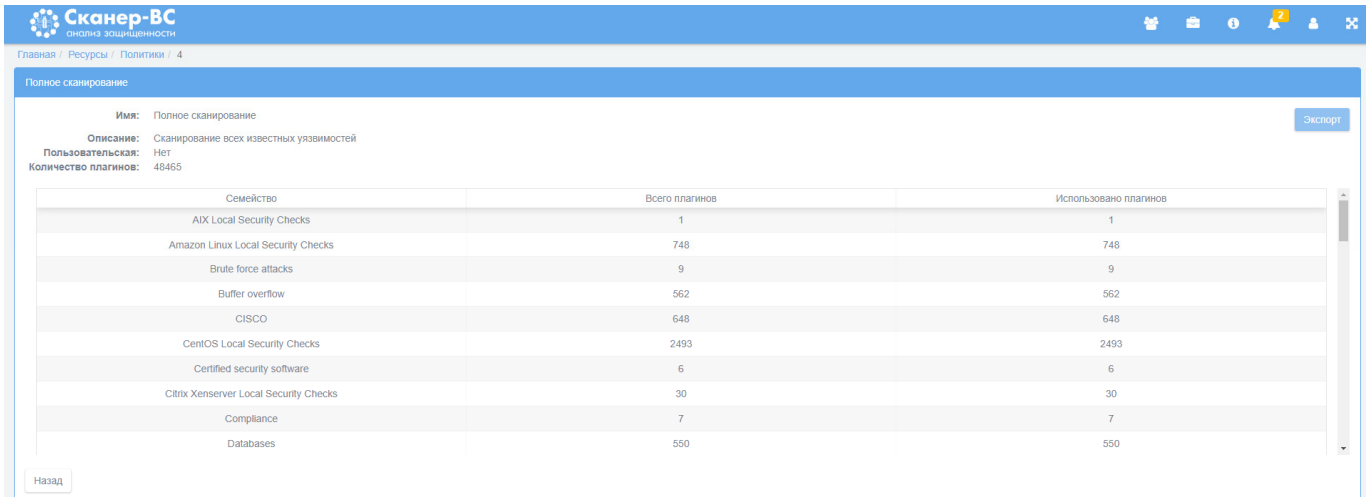


Рисунок 61 – Интерфейс «Полное сканирование»

В данном интерфейсе содержится информация о политике и присутствует таблица с тремя столбцами. Каждый столбец содержит информацию об используемых данной политикой плагинах. В интерфейсе политики «Веб-приложения» представлена следующая информация:

– имя политики;

– описание политики;

– является ли политика пользовательской;

– количество используемых в политике плагинов.

В таблице интерфейса содержится следующая информация об используемых плагинах:

– семейства плагинов, используемых в данной политике;

– общее число плагинов в семействе;

– общее число плагинов, используемых в семействе.

3.3.5.3.5 Новая политика

Интерфейс создания политики «Новая» предназначен для создания новой политики сканирования.

Вход для создания новой политики сканирования осуществляется нажатием на раздел создания политики «Новая» (рис. 62).

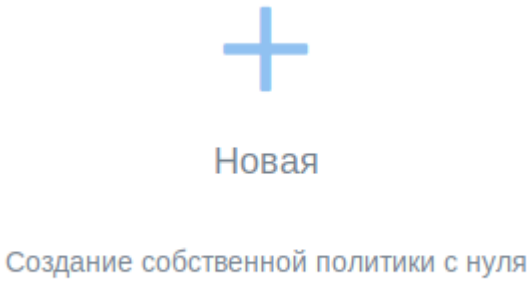


Рисунок 62 – Раздел создания политики «Новая» в интерфейсе «Политики»

Вид интерфейса создания политики «Новая» представлен на рисунке (рис. 63).

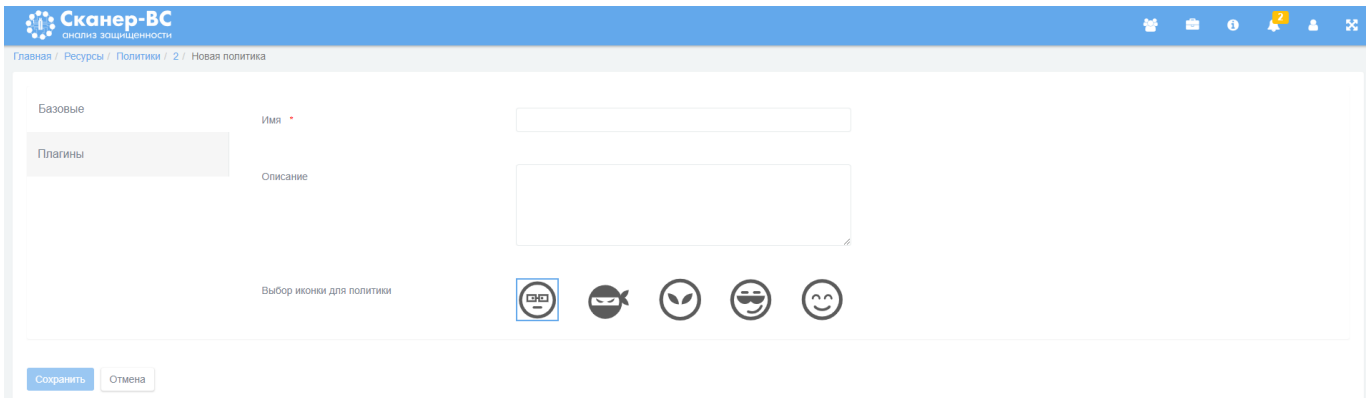


Рисунок 63 – Интерфейс создания политики «Новая» (вкладка «Базовые»)

В данном интерфейсе осуществляется создание новой политики сканирования. В интерфейсе присутствуют две вкладки:

– Базовые;

– Плагины.

Вкладка «Базовые» открывается автоматически при входе в интерфейс создания политики и содержит следующие поля для базовых настроек создания новой политики:

– Имя политики;

– Описание политики;

– Выбор иконки для политики.

Поле ввода: «Имя» является обязательными к заполнению и отмечено знаком «*» (звездочка).

Поле ввода «Имя» предназначено для ввода имени новой политики сканирования.

Поле ввода «Описание политики» предназначено для ввода описания политики сканирования.

Поле «Выбор иконки для политики» предназначено для выбора иконки политики, отображаемой в интерфейсе «Плагины».

Вкладка «Плагины» представлена на рисунке (рис. 64).

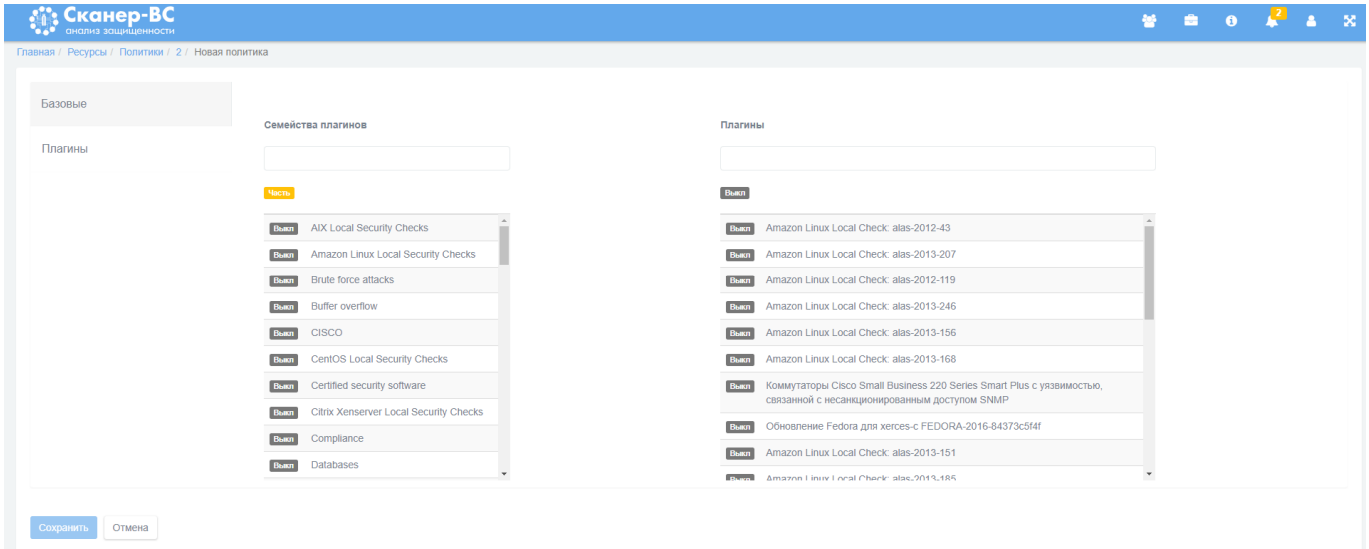


Рисунок 64 – Интерфейс создания политики «Новая» (вкладка «Плагины»)

Вкладка «Плагины» содержит окно выбора семейств плагинов для новой политики. По умолчанию в новой политике уже подключены несколько обязательных плагинов из двух семейств, без которых сканирование выполняться не будет:

– Port scanners;

– Settings.

Для включения семейства плагинов необходимо нажать кнопку «Выкл» возле него. Когда кнопка сменит свой цвет и обозначение на «Вкл», это будет обозначать, что семейство плагинов подключено к политике.

Если необходимо выбрать определенные плагины из семейства, то необходимо нажать на семейство плагинов, после чего появится окно с плагинами из данного семейства. Затем нужно будет нажать кнопку «Выкл» возле необходимых плагинов для их включения.

После завершения настроек новой политики сканирования необходимо нажать кнопку «Сохранить». Если по каким-то причинам создание новой политики не планируется необходимо нажать кнопку «Отмена».

После создания, пользовательскую политику можно экспортировать, дублировать и удалить, воспользовавшись соответствующими пиктограммами в правом верхнем углу раздела политики.

3.3.5.4 Управление словарями

Управление словарями осуществляется через специализированный интерфейс. Для входа в интерфейс необходимо выполнить следующие действия:

– войти в раздел «Ресурсы»;

– выбрать интерфейс «Словари».

Вид интерфейса «Словари» представлен на рисунке (рис. 65).

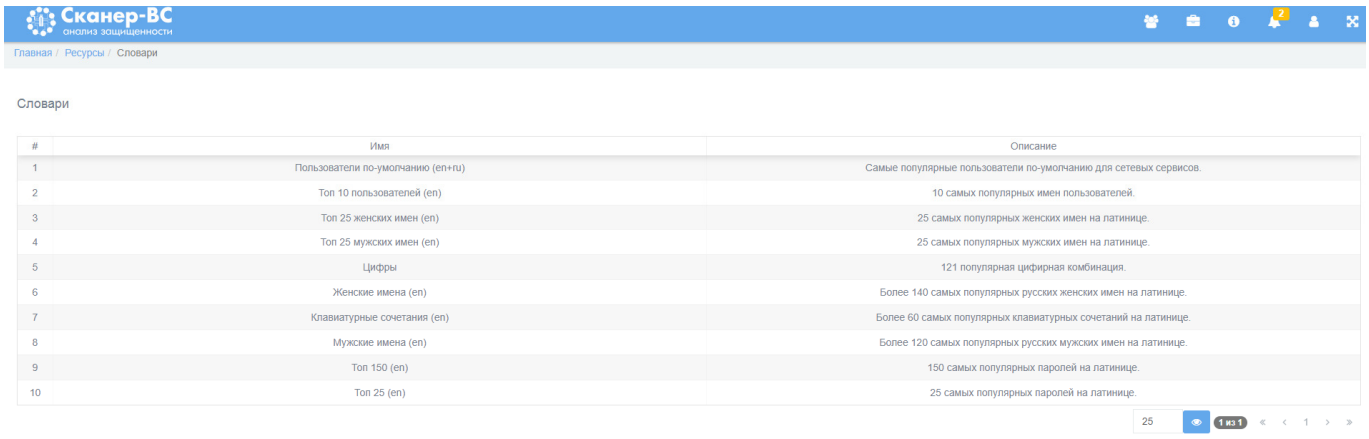


Рисунок 65 – Интерфейс «Словари»

В данном интерфейсе присутствует таблица с тремя столбцами. Каждый столбец содержит информацию о словаре. В таблице представлены следующие данные о словарях:

– порядковый номер в таблице;

– имя;

– описание.

Для более подробного описания словаря необходимо нажать на строку таблицы, в которой он находится.

Вид интерфейса с подробным описанием словаря представлен на рисунке (рис. 66).

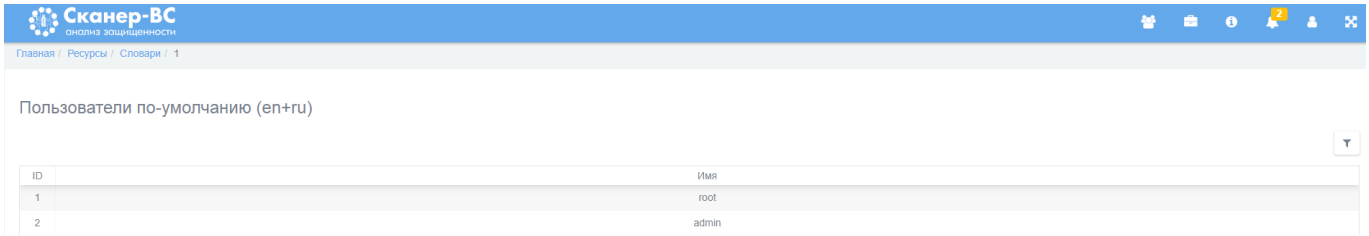


Рисунок 66 – Интерфейс с подробным описанием словаря

В интерфейсе подробного описания словаря присутствует таблица с двумя столбцами:

– номер пароля в словаре;

– имя (сам логин / пароль).

3.3.5.5 Управление списками портов

Просмотр списка портов осуществляется через специализированный интерфейс. Для входа в интерфейс необходимо выполнить следующие действия:

– войти в раздел «Ресурсы»;

– выбрать интерфейс «Списки портов».

Вид интерфейса «Списки портов» представлен на рисунке (рис. 67).

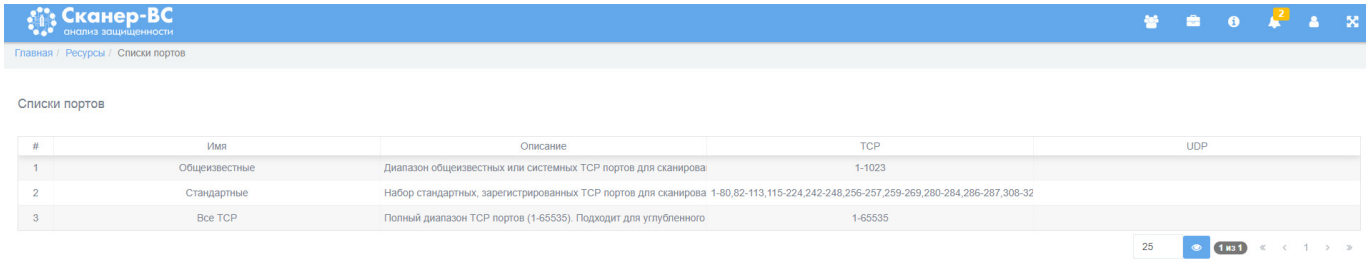


Рисунок 67 – Интерфейс «Списки портов»

В данном интерфейсе присутствует таблица с пятью столбцами. Каждый столбец содержит информацию о списке портов. В таблице представлены следующие данные о списке портов:

– номер в таблице;

– имя;

– описание;

– TCP-порты;

– UDP-порты.

3.3.5.6 Управление эксплойтами

Просмотр эксплойтов осуществляется через специализированный интерфейс. Для входа в интерфейс необходимо выполнить следующие действия:

– войти в раздел «Ресурсы»;

– выбрать интерфейс «Эксплойты».

Вид интерфейса «Эксплойты» представлен на рисунке (рис. 68).

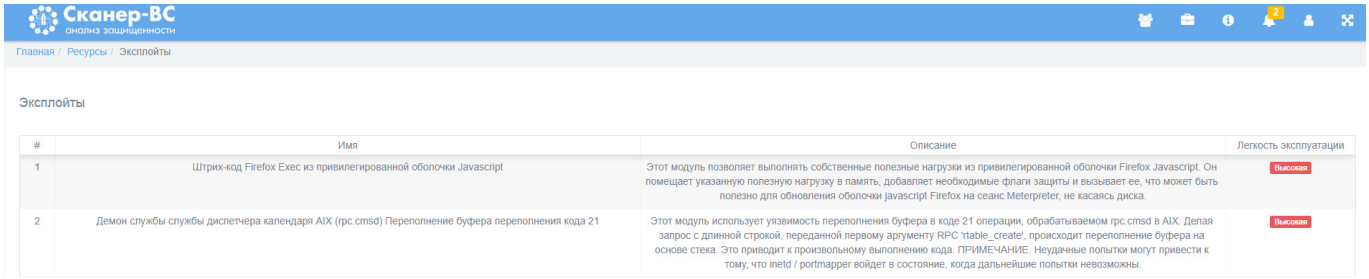


Рисунок 68 – Интерфейс «Эксплойты»

В данном интерфейсе присутствует таблица с четырьмя столбцами. Каждый столбец содержит информацию об эксплойтах. В таблице представлены следующие данные об эксплойтах:

– номер в таблице;

– имя;

– описание;

– легкость эксплуатации.

3.3.6 Тестирование защищенности

3.3.6.1 Общее описание

Для каждого тестирования защищенности 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 фазе «Отчетность» в виде сгенерированных отчетов. Для проведения тестирования защищенности пользователь может создать новый проект или, в случае продолжения, начатого ранее и сохраненного тестирования, использовать его.

В процессе администрирования ПК «Сканер-ВС», Оператор выполняет задачи по выполнению тестирования защищенности. Функционал ПК «Сканер-ВС», реализующий возможность тестирования защищенности, доступен Операторам, которым назначена роль «Пользователь», «Администратор» или «Суперпользователь».

В рамках задач по тестированию защищенности Оператор может выполнить:

– поиск целей (пп. 3.3.6.2);

– поиск уязвимостей (пп. 3.3.6.3);

– эксплуатацию (пп. 3.3.6.4);

– отчетность (пп. 3.3.6.5).

3.3.6.2 Поиск целей

3.3.6.2.1 Общее описание

В начале тестирования обязательным этапом 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 (см. пп. 3.3.6.4 «Эксплуатация»). Найденные в результате поиска целей действующие подключения с IP-адресами и задействованными TCP- и UDP-портами далее будем называть «Активами». Данные о них располагаются в секторе «Поиск целей» во 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, а также для трассировки маршрутов следования данных в сетях для построения топологии сети.

3.3.6.2.2 Поиск целей

Настройки, необходимые для запуска сканирования сети, находятся во вкладке «Базовые», где в поле ввода «Цели» Оператор задает цели сканирования: конкретный IP-адрес, множество IP-адресов, сеть или подсеть. Данное поле является обязательным к заполнению (рис. 69).

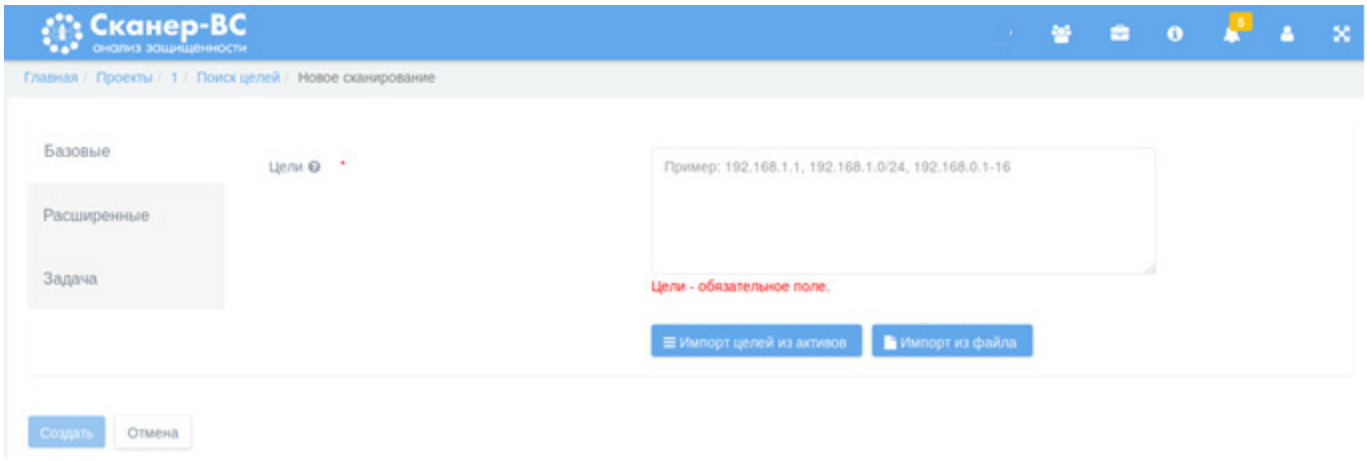


Рисунок 69 – Пример базовых настроек

Дополнительные настройки сканирования сети расположены во вкладке «Расширенные» и используются пользователем при необходимости (рис. 70).

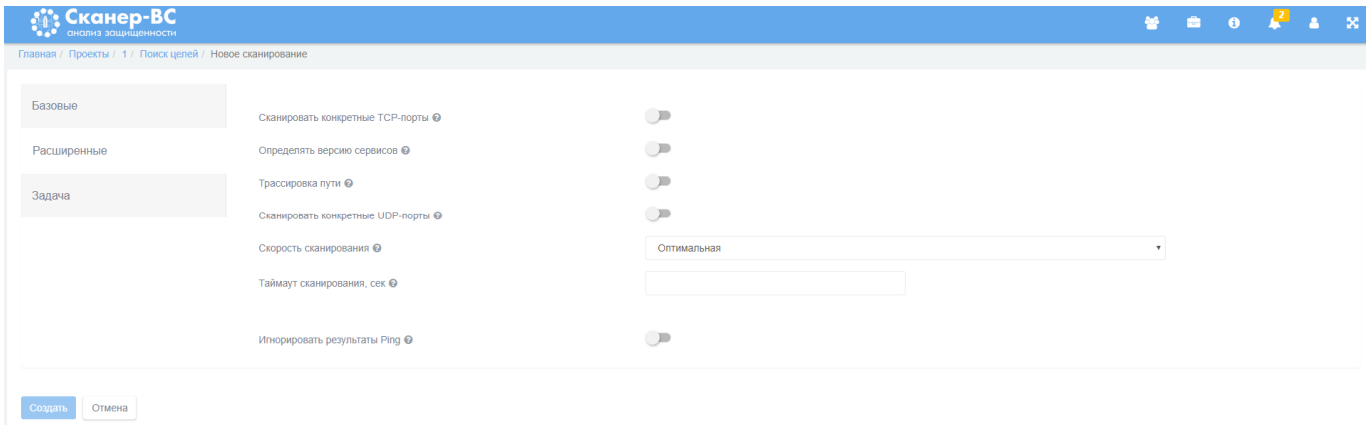


Рисунок 70 – Дополнительные настройки сканирования

Расширенный настройки представлены в виде следующих опций:

- Сканировать конкретные TCP-порты. Опция включается, если требуется сканировать нестандартные TCP-порты;
- Определять версию сервисов. Опция включается, если требуется определить версии сетевых сервисов;
- Трассировка пути. Опция включается, если необходимо отобразить трассировку пути;
- Сканировать конкретные UDP-порты. Опция используется, если требуется сканировать нестандартные UDP-порты;

Скорость сканирования. Опция включается для выбора скорости сканирования:

1) минимальная, низкая - попытка обхода систем обнаружения вторжения;
2) нормальная - незначительное использование пропускной способности сети и ресурсов;
3) оптимальная - обычный режим(рекомендуется);
4) высокая, максимальная - возможно снижение точности результатов сканирования сети.

- Таймаут сканирования, сек. Опция используется, для пропуска целевых хостов, время сканирования которых превышает установленный таймаут;
- Игнорировать результаты Ping. Опция включается, если необходимо обнаружение хостов с помощью TCP SYN вместо Ping.

Оператору рекомендуется использовать настройку «Определять версию сервисов» для определения версии сетевых сервисов, запущенных на хосте, а также настройку «Трассировка пути» для трассировки маршрутов следования данных в сетях для построения топологии сети.

Во вкладке «Задача» Оператор задает имя и описание текущего сканирования в соответствующих пустых полях (рис. 71). Если поля оставить пустыми, они будут заполнены автоматически, исходя из установленных настроек сканирования. При включении тумблера «Автозапуск» задача автоматически запуститься сразу после ее создания.

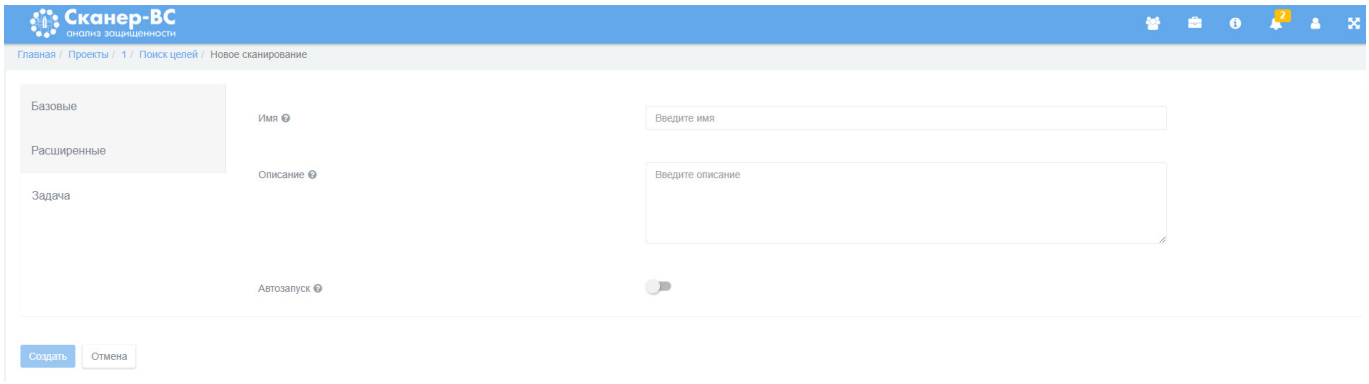


Рисунок 71 – Имя и описание сканирования

Для того, чтобы закончить создание задачи на поиск целей, необходимо нажать кнопку «Создать». Если же по каким-либо причинам проект создавать не требуется, нужно нажать кнопку «Отмена».

3.3.6.2.3 Запуск задачи

Если у задачи не настроен «Автозапуск», то для запуска задачи необходимо нажать на соответствующую пиктограмму находящейся в столбце действия, в одной строке с задачей.

Успешное завершение сканирования представлено на рисунке (рис. 72).

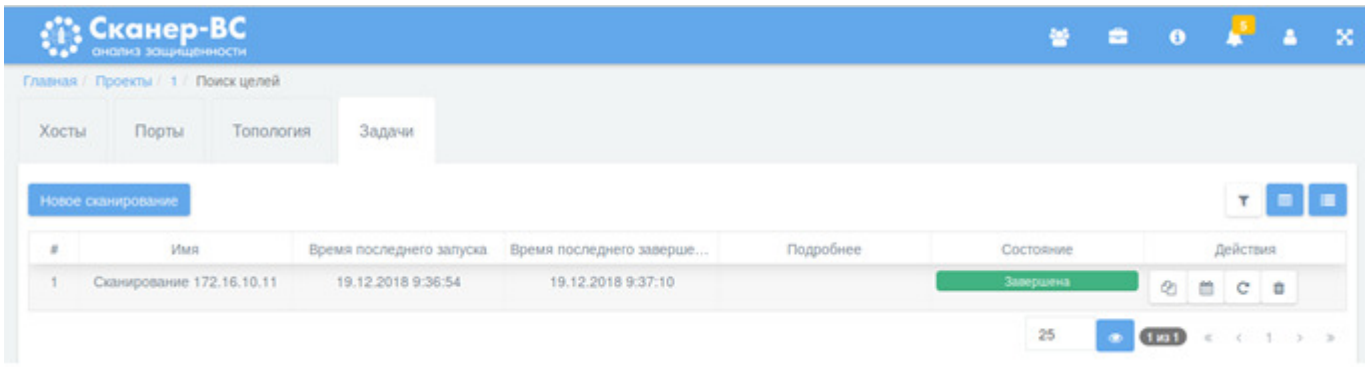


Рисунок 72 – Процесс сканирования

После завершения сканирования можно просмотреть подробную информацию о выполненной задаче (см. пп. 3.3.3.2.2).

Изменение статуса выполнения задачи будет отражено в правом верхнем углу веб-интерфейса (пиктограмма «Уведомления»).

После завершения сканирования во вкладке «Хосты» в таблице показаны IP-адрес, имя хоста, MAC-адрес, операционная система (далее – ОС) и тип устройства, который им соответствует (рис. 73).

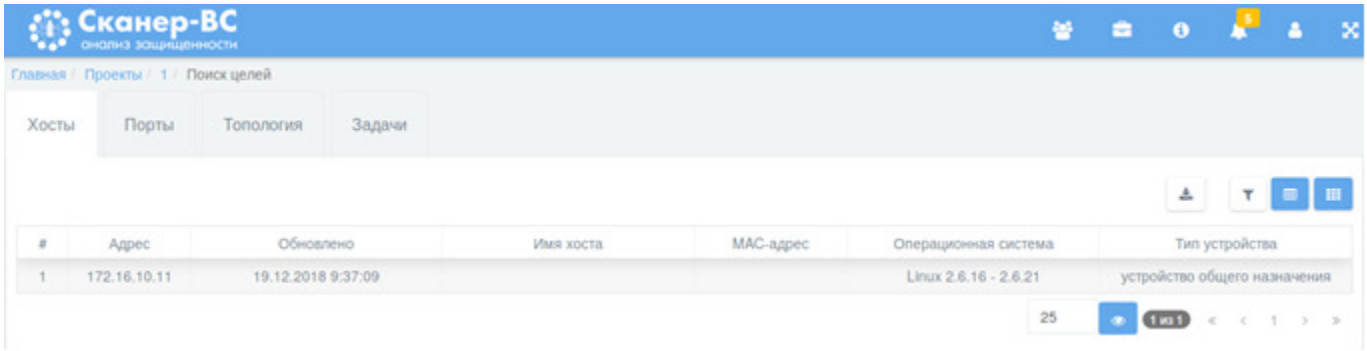


Рисунок 73 – Вкладка «Хосты»

После завершения сканирования во вкладке «Порты» появятся данные об открытых портах, запущенных сервисах, продуктах и номерах версий, которые будут сгруппированы в таблицу (рис. 74).

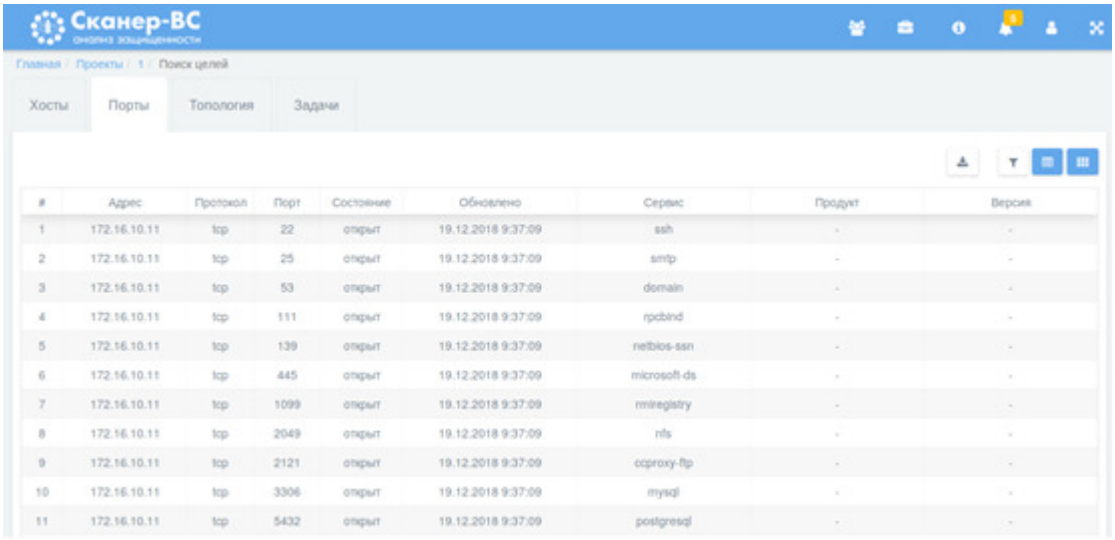


Рисунок 74 – Вкладка «Порты»

После завершения сканирования во вкладке «Топология» (рис. 75). Во вкладке приведена топология сети в виде рисунка. Слева приведены примеры значков и их значение.

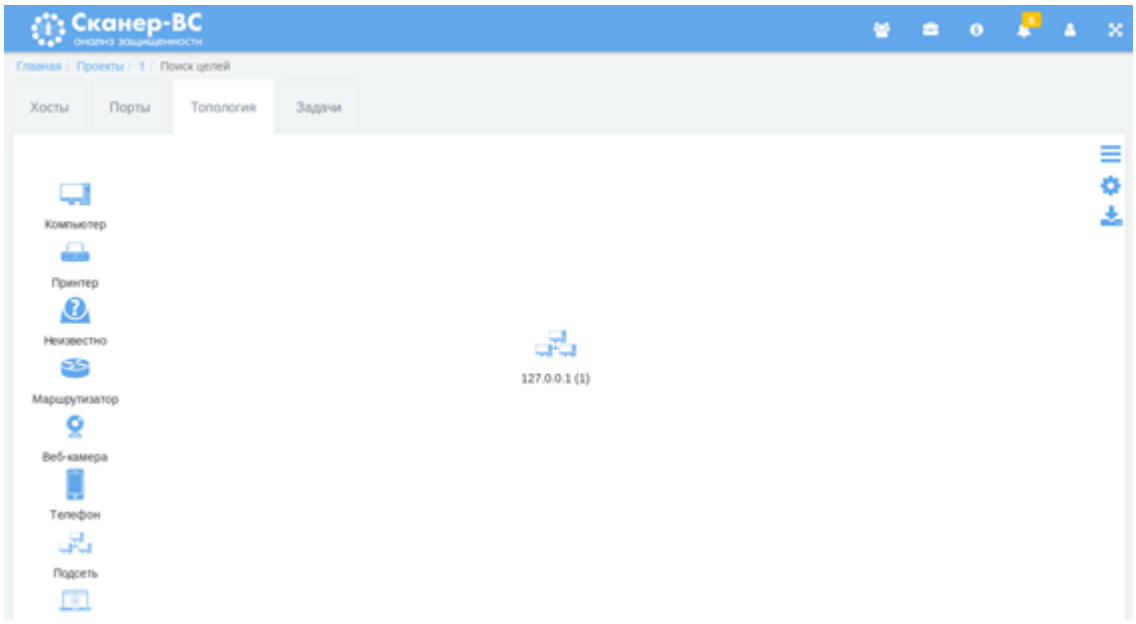


Рисунок 75 – Вкладка «Топология»

Справа находятся опции, при помощи которых можно управлять содержимым вкладки:

– « » – выбор источника отображения топологии;

– « » – выбор опции отображения топологии (анимированные значки или статические);

– « » – сохранение топологии в графический файл.

3.3.6.2.4 Завершение работы

После завершения работы «Поиск целей» состояние задачи изменится на «Завершена» (рис 76).

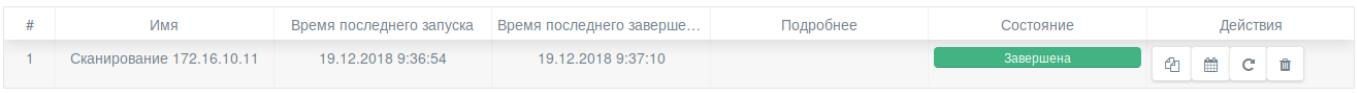


Рисунок 76 – Завершение поиска целей

Для завершенной задачи доступны следующие действия:

– « » – клонировать. Создается копия клонируемой задачи;

– «  » – запланировать. Задается дата и время запуска задачи;

– «  » – перезапустить. Задача перезапускается;

– «  » – удалить. Происходит удаление задачи из списка.

3.3.6.3 Поиск уязвимостей

3.3.6.3.1 Общее описание

Под уязвимостью программного обеспечения (далее – ПО) подразумевается дефект ПО, который может стать причиной нарушения информационной безопасности. Фаза тестирования «Поиск уязвимостей» направлена на обнаружение таких дефектов.

Дефекты делятся на разные уровни риска. Деление на уровни основано на следующей шкале, по CVSS 2.0:

– 0,1-3,9 - низкий уровень;

– 4,0-6,9 - средний уровень;

– 7,0-8,9 - высокий уровень;

– 9,0-10,0 - критический уровень.

3.3.6.3.2 Поиск уязвимостей

Настройки, необходимые для запуска поиска уязвимостей, находятся во вкладке «Базовые» (рис. 77), где Оператор задает цели поиска уязвимостей (IP-адреса проверяемых компьютеров, сетей или подсетей) и выбирает политику сканирования (набор правил сканирования): базовую (быструю, сканирование веб-сервисов, либо полное сканирование) или пользовательскую, настраиваемую Оператором. Создание пользовательской политики описано в подпункте 3.3.5.3.

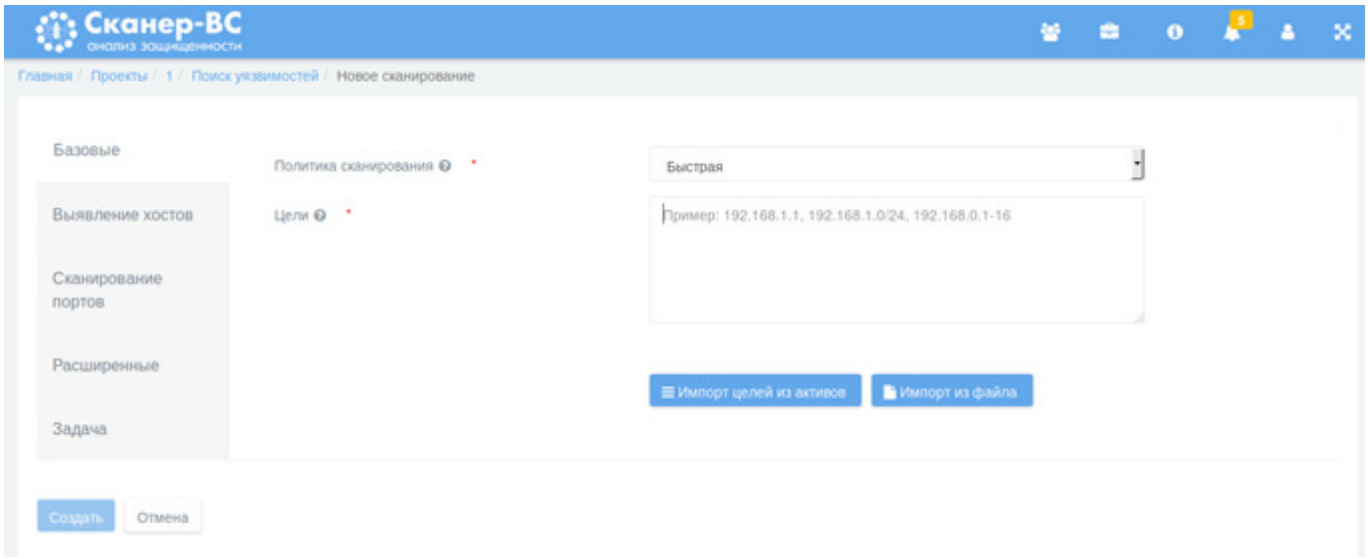


Рисунок 77 – Основные настройки сканирования

Далее необходимо выбрать политику сканирования. По умолчанию установлена «Быстрая». Если необходимо сменить политику сканирования, нужно нажать кнопку «Быстрая» (по умолчанию) и выбрать одну из базовых политик или создать свою (рис. 78). Описание создания политики приведено в пп. 3.3.5.3.5.

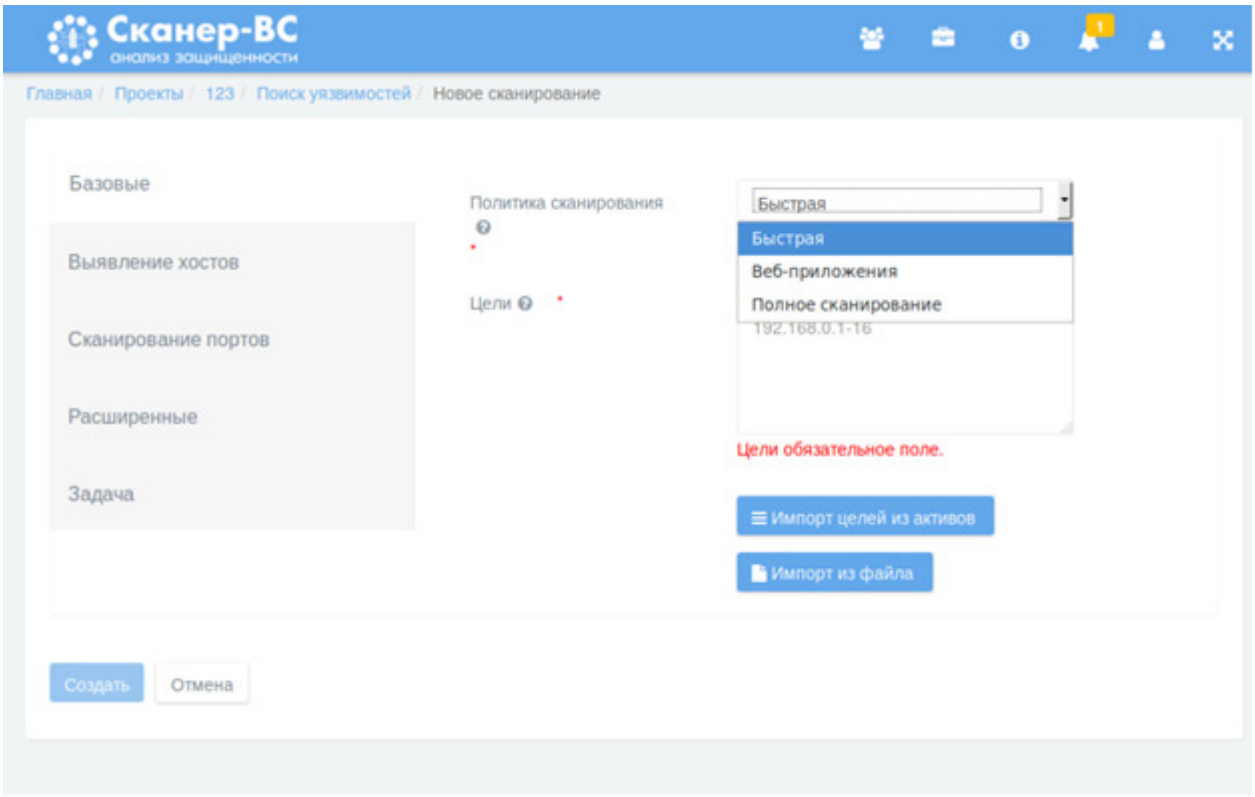


Рисунок 78 – Выбор политики сканирования

Во вкладке «Задача» (рис. 79) Оператор задает имя и описание в соответствующие пустые поля. Если поля оставить пустыми, они будут заполнены автоматически, исходя из указанных настроек сканирования.

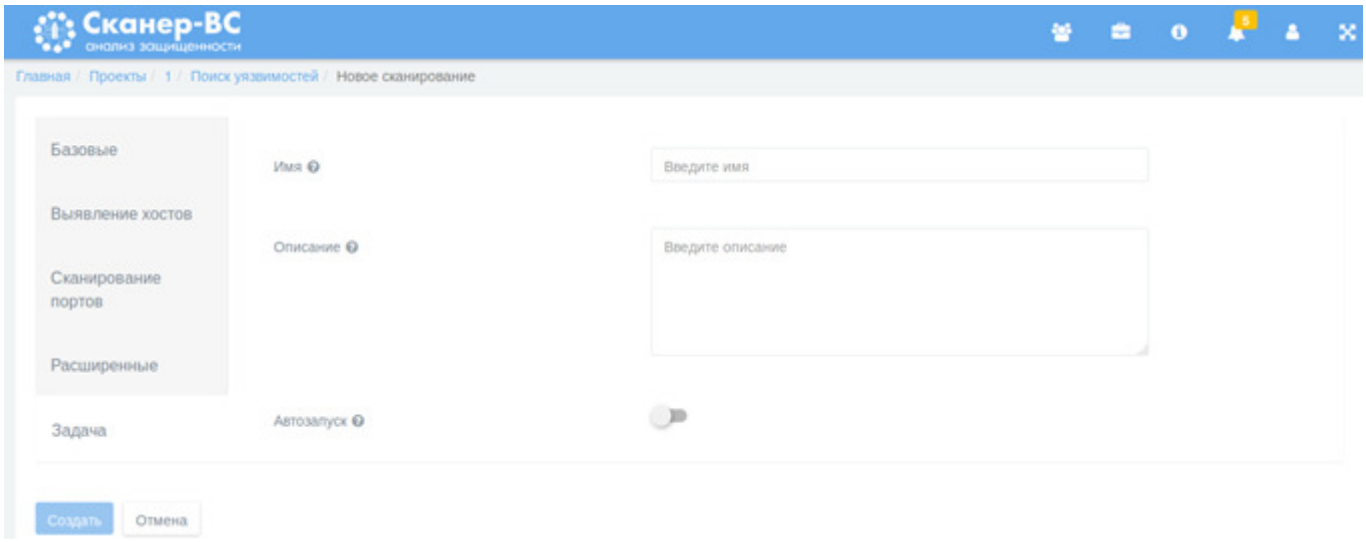


Рисунок 79 – Имя и описание сканирования

Дополнительные опции сканирования расположены во вкладках «Выявление хостов», «Сканирование портов», «Расширенные» (рис. 79) и используются Оператором при необходимости.

Опции, расположенные во вкладке «Выявление хостов»:

– Методы Ping (ARP, TCP, ICMP). Выбор метода проведения Ping-сканирования;
– Тип сети (Mixed (use RFC 1918), Private LAN, Public WAN (intemet).

Опции, расположенные во вкладке «Сканирование портов»:

– Рассматривать несканируемые, как закрытые. Отключение сканирования неизвестных портов;
– Сканировать конкретные TCP-порты. Включение сканирования нестандартных TCP-портов;
– Сканировать конкретные UDP-порты. Включение сканирования нестандартных UDP-портов;
– Порты. Выбор предустановленного диапазона портов для сканирования. Общеизвестные - сканирование будет проводиться по списку портов от 1 до 1024. Стандартные (рекомендуется) - сканирование будет проводиться по списку часто используемых портов (4481). Все - будут просканированы все порты, при выборе данной опции время сканирования может существенно увеличиться.

Опции, расположенные во вкладке «Расширенные»:

– Безопасные проверки. Опция для отключения проверок, которые могут вызвать нарушение доступности проверяемых сетевых сервисов и хостов;
– Полномочия. Опция для сканирования целевого хоста с учетной записью администратора (рекомендуется) или пользователя. Данное сканирование позволит выявить наибольшее количество уязвимостей и уменьшит количество ложных срабатываний;
– SMB. Пара логин/пароль для подключения по протоколу SMB (рекомендуется для Windows);
– SSH. Пара логин/пароль для подключения по протоколу SSH (рекомендуется для Linux);
– Таймаут сети, сек. Опция для установки значения тайм-аута сетевого подключения во время сканирования;
– Таймаут между запросами. Опция для установки значения тайм-аута для сетевых сокетов во время сканирования;
– Количество хостов. Максимальное количество хостов, которые будут тестироваться одновременно;

– Количество проверок. Максимальное количество проверок, которые будут выполняться одновременно с данным хостом.

Для начала процесса сканирования необходимо нажать кнопку «Создать» (рис. 79).

3.3.6.3.3 Завершение работы

После завершения сканирования в таблицу во вкладке «Задачи» будет добавлена строка, содержащая следующие поля (рис. 80):

– номер задачи;

– имя;

– время последнего запуска;

– время последнего завершения;

– подробнее;

– состояние;

– действия.

Для завершенной задачи доступны следующие действия:

– « » – клонировать. Создается копия клонируемой задачи;

– « » – запланировать. Задается дата и время запуска задачи;

– « » – перезапустить. Задача перезапускается;

– « » – удалить. Происходит удаление задачи из списка.

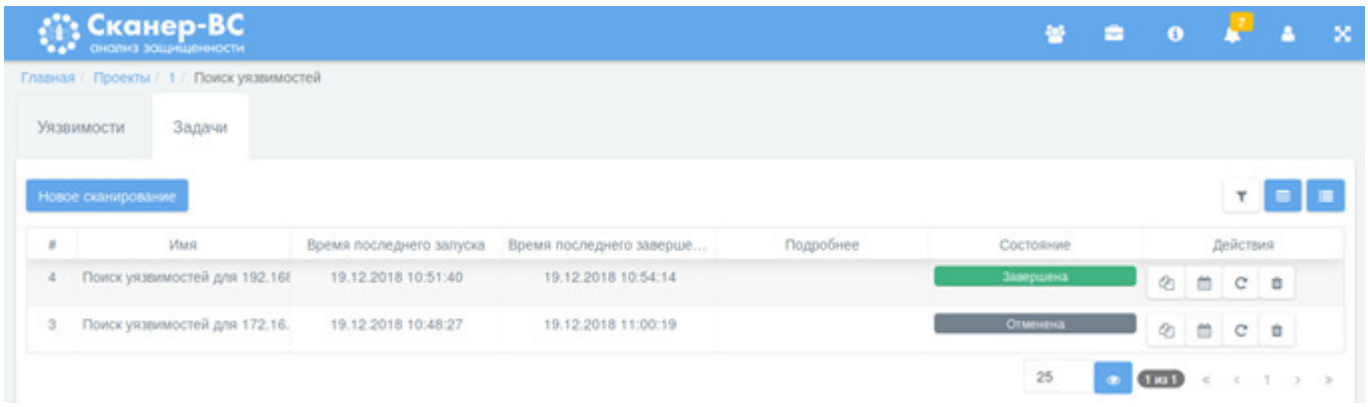


Рисунок 80 – Результат сканирования

После завершения сканирования во вкладке «Уязвимости» появятся данные об обнаруженных уязвимостях, которые будут сгруппированы в таблицу (рис. 81).

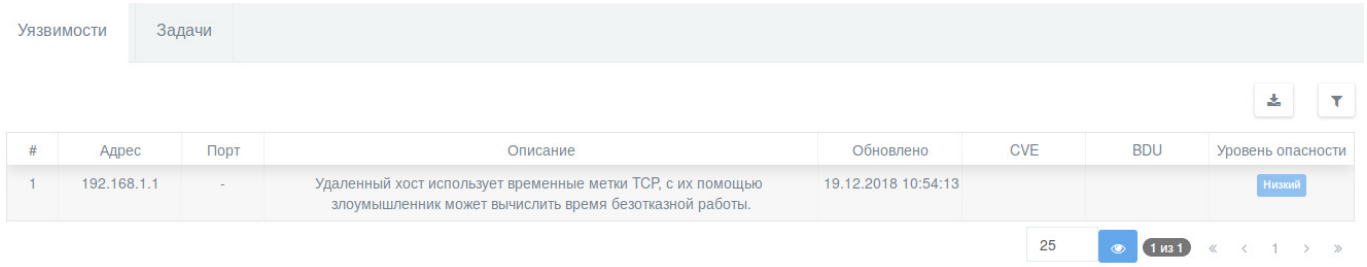


Рисунок 81 – Результаты поиска

Чтобы подробнее узнать об уязвимости, необходимо нажать на нее правой кнопкой мыши.

3.3.6.4 Эксплуатация

3.3.6.4.1 Общее описание

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

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

3.3.6.4.2 Поиск эксплойтов

Для проведения тестирования возможности несанкционированного удаленного использования ресурсов компьютера необходимо выбрать вкладку «Поиск эксплойтов» (рис. 82).

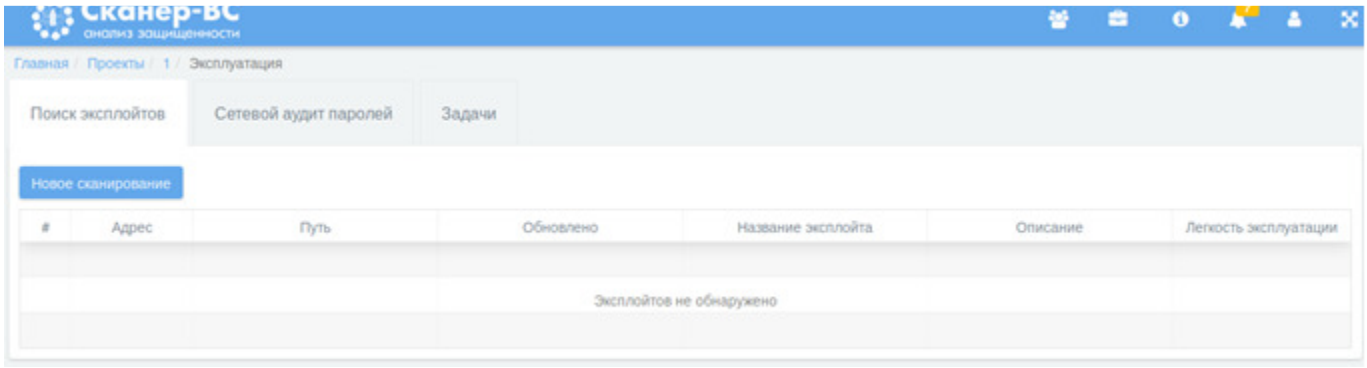


Рисунок 82 – Вкладка «Поиск эксплойтов»

После нажатия кнопки «Новое сканирование» откроется интерфейс нового поиска эксплойтов (рис. 83) с тремя вкладками настроек:

– базовые;

– расширенные;

– задача.

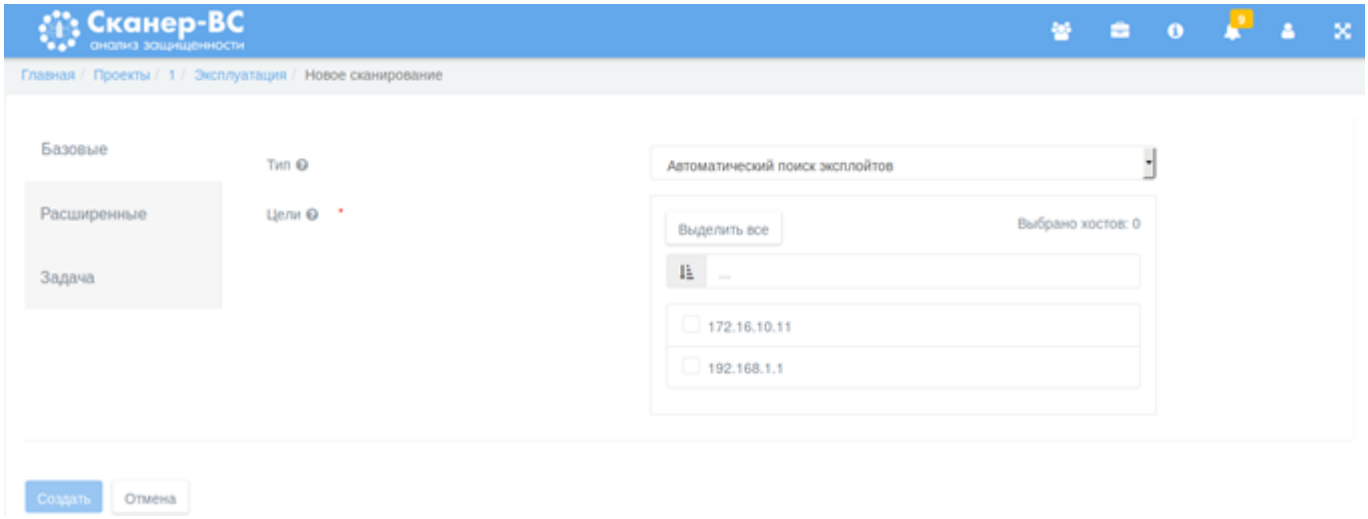


Рисунок 83 – Интерфейс нового поиска эксплойтов

Во вкладке «Базовые», в поле «Тип» необходимо выбрать тип поиска, в поле «Цель» необходимо выбрать сканируемый IP-адрес. Запуск тестирования можно произвести только для одного IP-адреса. Если перед запуском поиска эксплойтов в проекте были проведены поиск целей (с включенной функцией «Определять версии сетевых протоколов») и поиск уязвимостей, то

выберите тип поиска «Автоматический поиск эксплойтов», в ином случае нажмите кнопку «Ручной поиск эксплойтов».

При выборе автоматического поиска эксплойтов, во вкладке «Расширенные» нужно указать 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.

При выборе ручного поиска эксплойтов, во вкладке «Расширенные» в многострочное поле «Ключевые слова» необходимо ввести 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. Поиск будет производиться аналогично строгому поиску.

Во вкладке «Задача» необходимо указать имя нового сканирования, можно сделать описание и включить автозапуск задачи, сразу после создания.

После завершения настройки, для запуска тестирования необходимо нажать копку «Создать».

Результаты завершения работы приведены в пп. 3.3.6.4.4.

3.3.6.4.3 Сетевой аудит паролей

Для проведения сетевого аудита паролей необходимо перейти во вкладку «Сетевой аудит паролей» и нажать кнопку «Новое сканирование» (рис. 84).

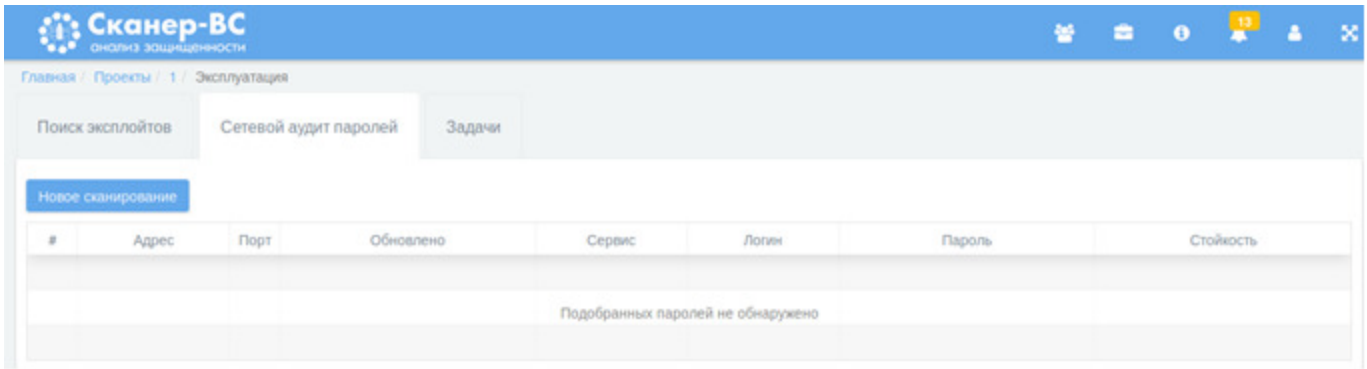


Рисунок 84 – Интерфейс запуска подбора паролей

После нажатия кнопки «Новый подбор паролей» откроется интерфейс нового подбора пароля (рис. 85) с пятью вкладками настроек:

– базовые;

– пользователи;

– пароли;

– расширенные;

– задача.

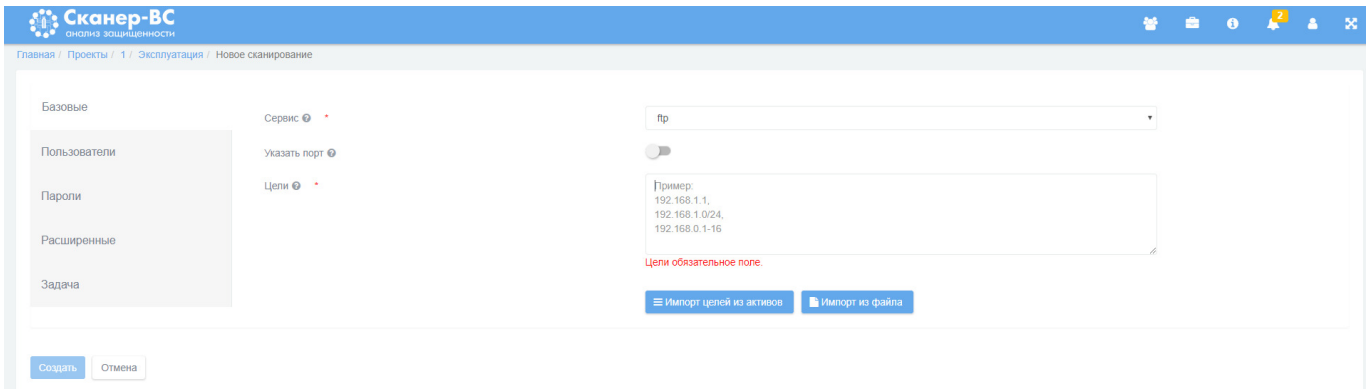


Рисунок 85 – Интерфейс нового подбора пароля

Во вкладке «Базовые» расположены базовые параметры сетевого аудита паролей: тестируемый сервис (протокол), порт (если используется порт не по умолчанию) и цели тестирования: IP-адрес, сеть или подсеть.

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

Во вкладке «Пользователи» необходимо задать идентификаторы (имена, логин) пользователей проверяемых рабочих станций. Задать их можно вручную в поле «Пользователи» или импортировать из файла в формате TXT, где одна строка документа должна содержать только одно имя. Во вкладке «Пользователи» необходимо подключить один из следующих словарей:

– Пользователи по умолчанию (en+ru);

– Топ 10 пользователей (en);

– Топ 25 женских имен (en);

– Топ 25 мужских имен (en).

Во вкладке «Пароли» в поле «Пароли» необходимо указать комбинации букв и цифр, которые будут использоваться в качестве аутентификационной информации. Каждая комбинация

должна находиться на отдельной строке. Настройки программы поддерживают загрузку паролей из файла в формате TXT, где одна строка документа должна содержать только один пароль.

Дополнительно, можно включить следующие опции:

– Проверить пустой пароль;

– Проверить пароль, совпадающий с логином;

– Проверить пароль, совпадающий с логином в обратном порядке.

Для завершения подбора паролей при первой подобранной паре имя - пароль нужно перейти во вкладку «Расширенные» и активировать функцию «Закончить подбор при первом положительном результате».

Во вкладке «Расширенные» можно указать интервал таймаута между попытками сканирования.

Во 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.

После завершения настройки, для запуска тестирования необходимо нажать копку «Создать».

Результаты завершения работы приведены в пп. 3.3.6.4.4.

3.3.6.4.4 Завершение работы

После нажатия кнопки «Запустить», во вкладке «Задачи», в таблице появится номер задачи, имя и индикатор статуса. Желтый цвет индикатора означает процесс сканирования, зеленый – завершение сканирования, красный – процесс сканирования завершен с ошибкой.

Данные с подобранными паролями появятся во вкладке «Сетевой аудит паролей».

После выполнения сетевого аудита паролей ПК «Сканер-ВС» присваивает в отчетах описание сложности паролей. Сложность пароля рассчитывается в зависимости от того, сколько времени и какие ресурсы потребуются злоумышленнику, чтобы скомпрометировать пароль:

– очень слабый - любой ПК, несколько минут;

– слабый - любой ПК, аппаратный ускоритель, одна неделя;

– нормальный - специализированный ПК, один год;

– надежный - большая скоординированная атака, более года;

– очень надежный – практически невозможно подобрать.

Данные о найденных эксплойтах появятся во вкладке «Поиск эксплойтов».

Информация о выполненной задаче появится во вкладке «Задачи» (рис. 86).

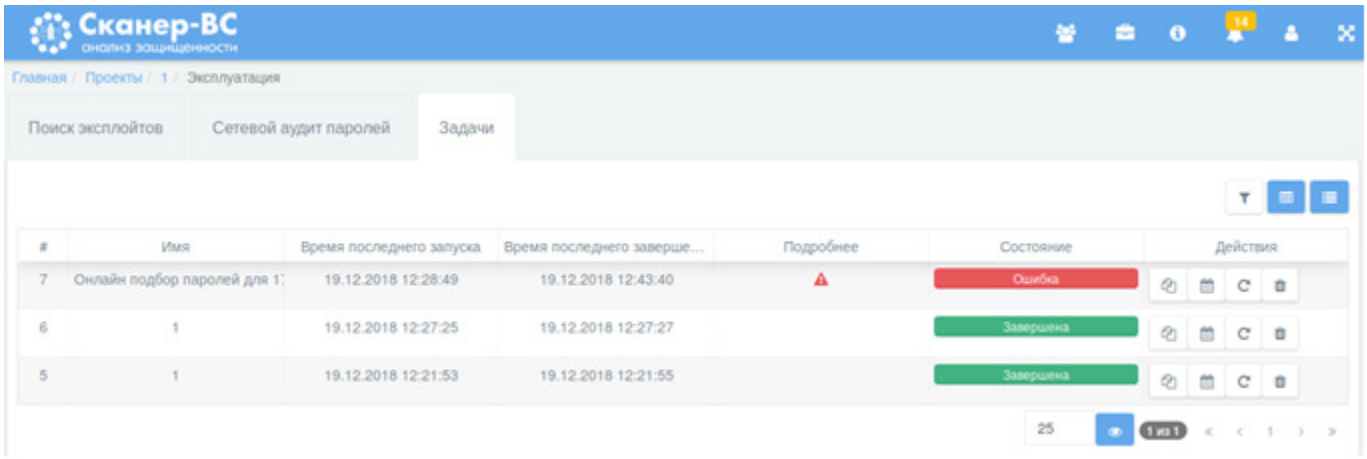


Рисунок 86 – Данные о завершенной задаче

Для завершенной задачи доступны следующие действия:

– « » – клонировать. Создается копия клонируемой задачи;

– « » – запланировать. Задается дата и время запуска задачи;

– « » – перезапустить. Задача перезапускается;

– « » – удалить. Происходит удаление задачи из списка.

3.3.6.5 Отчетность

3.3.6.5.1 Общее описание

Документирование является неотъемлемой частью анализа защищенности информационной системы. Для объединения результатов всех этапов тестирования в ПК «Сканер-ВС» используется сектор «Отчет» (номер 4 на рисунке (рис. 35), с помощью которого можно построить отчет с результатами тестирований.

3.3.6.5.2 Настройки отчета

После того как был выбран сектор «Отчет», в нем отображается страница с двумя вкладками (рис. 87).

– отчеты;

– задачи.

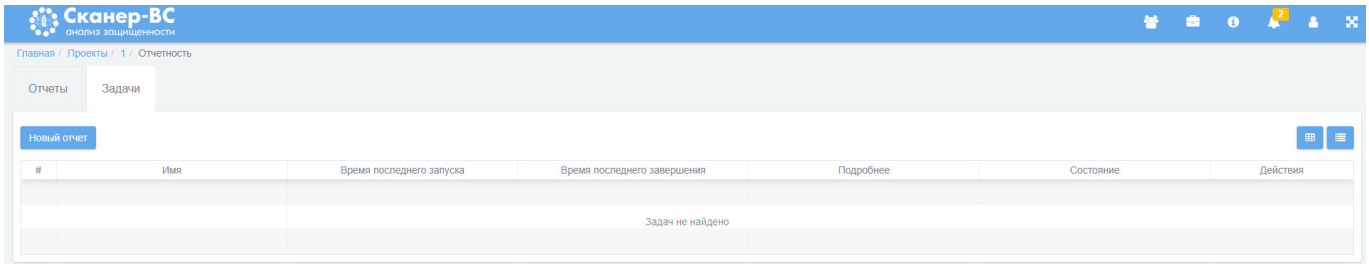


Рисунок 87 – Сектор «Отчет»

Во вкладке «Отчеты» отображаются готовые отчеты.

Во вкладке «Задачи» выполняется создание нового отчета.

Для того чтобы создать новый отчет необходимо нажать кнопку «Новый отчет». Далее откроется интерфейс создания нового отчета.

Интерфейс создания нового отчета представлен на рисунке (рис. 88).

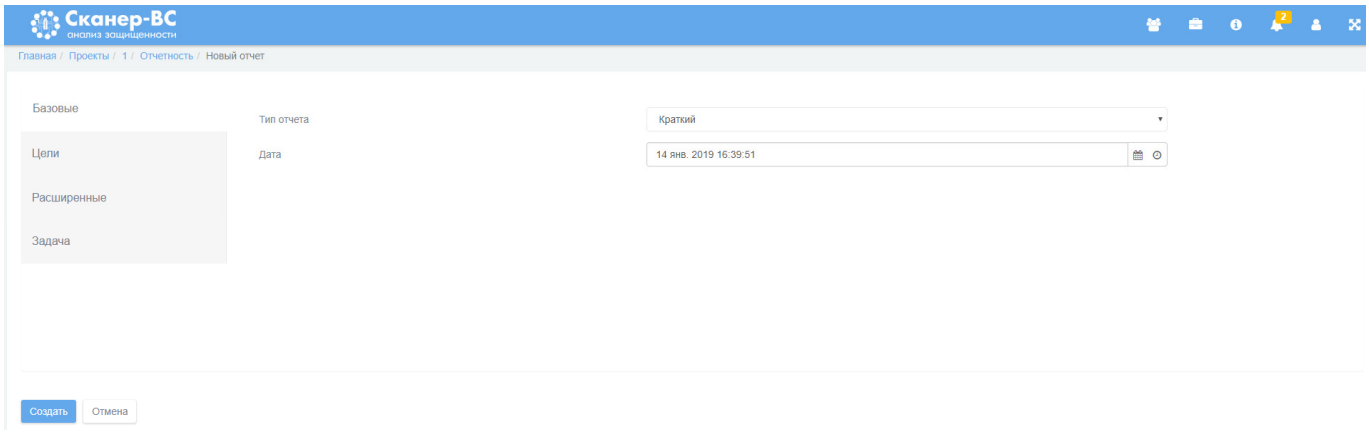


Рисунок 88 – Интерфейс создания нового отчета

В интерфейсе создания нового отчета присутствует четыре вкладки настроек:

– базовые;

– цели;

– расширенные;

– задача.

Во вкладке «Базовые» выбирается тип отчета и дата, на которую строится отчет.

Во вкладке «Цели» выполняется выбор запусков, которые должны быть отображены в отчете.

Во вкладке «Расширенные» выбираются разделы, которые будут в отчете, типы уязвимостей, а также присутствует функция маскирования пароля в отчете.

Во вкладке «Задача» необходимо указать имя нового отчета, можно сделать описание и отключить автозапуск создания отчета, сразу после настроек (опция автозапуска включена по умолчанию).

После завершения настройки, для запуска создания отчета необходимо нажать копку «Создать».

Отчет может быть:

– кратким;

– полным;

– динамическим.

Краткий отчет состоит из минимума основных сведений:

1) резюме для руководства;

2) границы проекта;

3) порты и сервисы;

4) уязвимости:

– уязвимость 1;

– уязвимость 2;

– уязвимость 3;

…..

– уязвимость n;

5) скомпрометированные учетные данные;

6) эксплойты.

В кратком отчете группировка идет по фазам. Для каждой фазы описаны результаты тестирования различных хостов.

Отчет можно экспортировать в формат HTML, PDF, DOC.

Полный отчет содержит следующие разделы:

1) резюме для руководства;

2) границы проекта;

3) тестируемый хост 1:

- порты и сервисы;
- уязвимости;
- скомпрометированные учетные данные;
- эксплойты;

4) тестируемый хост 2:

- порты и сервисы;
- уязвимости;
- скомпрометированные учетные данные;
- эксплойты;

…..

5) тестируемый хост n:

- порты и сервисы;
- уязвимости;
- скомпрометированные учетные данные;
- эксплойты.

В полном отчете группировка идет по хостам, для каждого хоста описаны результаты тестирования каждой фазы.

Отчет можно экспортировать в формат HTML, PDF, DOC.

Динамический отчет содержит следующие разделы:

- резюме для руководства;
- границы проекта;
- порты и сервисы;
- уязвимости;
- скомпрометированные учетные данные;
- эксплойты.

Динамический отчет строится только по одному хосту на любом заданном периоде. Данный отчет позволяет сравнить уровень защищенности одного хоста в динамике.

Отчет можно экспортировать в формат HTML, PDF, DOC.

3.3.6.5.3 Завершение работы

Результатом завершения работы в Разделе «Отчеты» служит созданный список отчетов (Краткий, Полный, Динамический) по текущему проекту с возможностью экспорта в форматы HTML, PDF, DOC.

3.3.6.6 Задачи

В Разделе «Задачи» представлен перечень всех задач проекта (рис. 89):

– поиск целей;

– поиск уязвимостей;

– эксплуатация;

– отчетность.

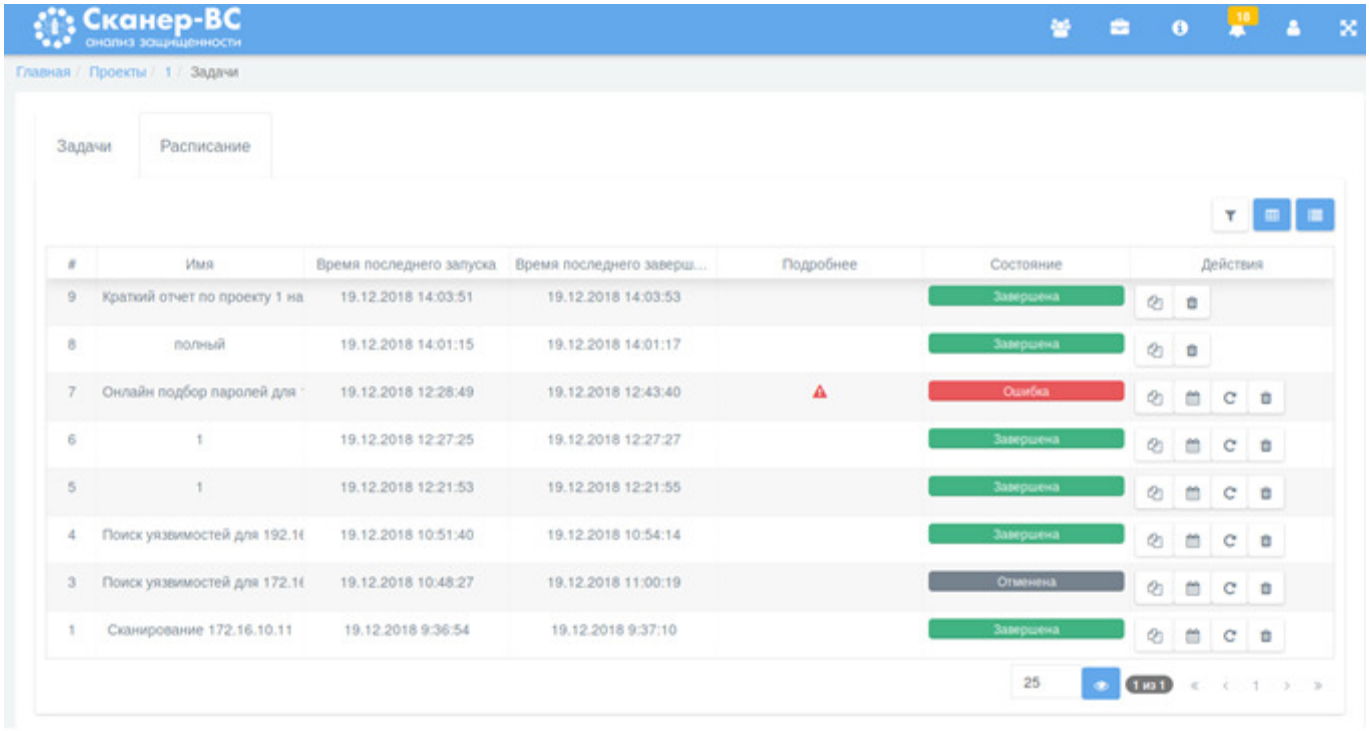


Рисунок 89 – Раздел «Задачи»

Перечень задач представлен в табличном виде. Раздел разделен на две вкладки:

– задачи;

– расписание.

3.3.6.6.1 Вкладка «Задачи»

Вкладка «Задачи» объединяет в себе информацию по всем разделам проекта.

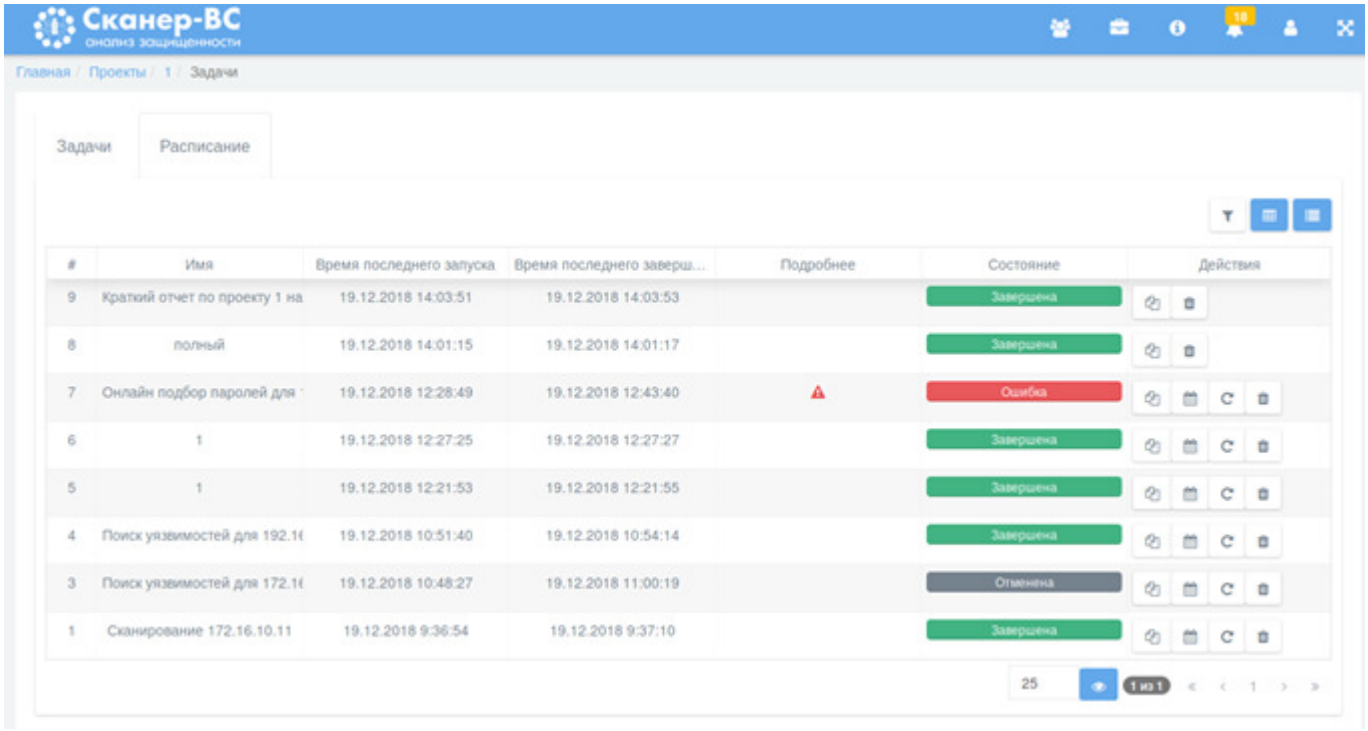


Рисунок 90 – Вкладка «Задачи»

В таблице (см. Таблица 3) содержится описание столбцов вкладки «Задачи».

Таблица 3 – Описание полей вкладки «Задачи»

Название столбца	Описание
Порядковые номер	Порядковый номер задачи в таблице
Имя	Название задачи
Время последнего запуска	Время последнего запуска задачи
Время последнего завершения	Время последнего завершения задачи
Подробнее	Показывает запланирована ли задача или нет
Состояние	Состояние задачи
Действия	Разрешенные действия с задачей

Для задачи доступны следующие действия:

– « » – клонировать. Создается копия клонируемой задачи;

– « » – запланировать. Задается дата и время запуска задачи;

– « » – перезапустить. Задача перезапускается;

– « » – удалить. Происходит удаление задачи из списка.

Для просмотра подробной информации по задаче необходимо нажать на интересующую задачу.

Для создания или редактирования задач необходимо перейти в соответствующие разделы.

3.3.6.6.2 Вкладка «Расписание»

Во вкладке «Расписание» (рис. 91) представлены только запланированные задачи.

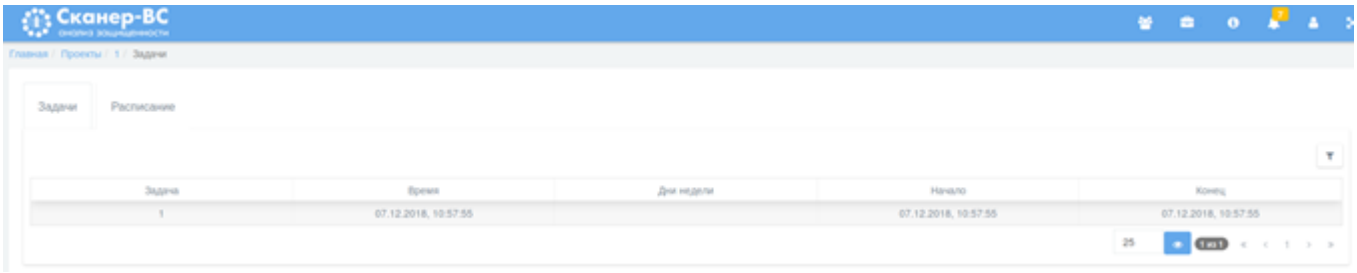


Рисунок 91 – Вкладка «Расписание»

В таблице (см. Таблица 3) содержится описание столбцов вкладки «Расписание».

Таблица 4 – Описание полей вкладки «Расписание»

Название столбца	Описание
Задача	Название задачи
Время	Запланированное время
Дни недели	Запланированные дни недели, если есть
Начало	Начало следующего запуска
Конец	Завершение следующего запуска

Для просмотра подробной информации по задаче необходимо нажать на интересующую задачу.

3.3.6.6.3 Завершение работы

Раздел «Задачи» сугубо информационный и не позволяет редактировать представленную в нем информацию, кроме общих действий:

– « » – клонировать. Создается копия клонируемой задачи;

– « » – запланировать. Задается дата и время запуска задачи;

– « » – перезапустить. Задача перезапускается;

– « » – удалить. Происходит удаление задачи из списка.

Результатом завершения работы раздела «Задачи» можно считать автоматически построенный список всех задач по проекту.

3.4 Информация

В разделе «Информация» (рис. 92) приведены такие сведения, как:

– Продукт;

– Разработчик;

– Техническая поддержка;

– Сайт продукта.

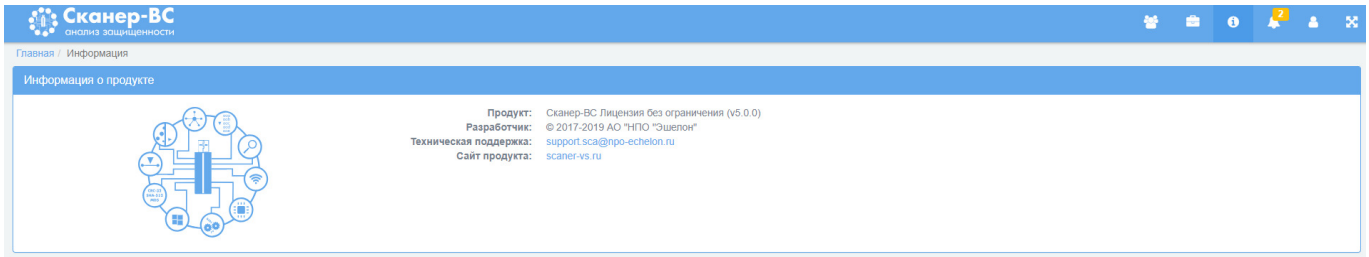


Рисунок 92 – Раздел «Информация»

В раздел «Информация» можно перейти, нажав на пиктограмму « » на панели навигации.

3.5 Уведомления

Инструмент «Уведомления» не является отдельным разделом с отдельным рабочим окном. Инструмент «Уведомления» указывает на наличие непрочитанных уведомлений для Оператора.

Количество уведомлений отображается на пиктограмме «Уведомления» в числовом виде (рис. 93).

Рисунок 93 – Пример наличия непрочитанных уведомлений

При нажатии на пиктограмму «Уведомления», на панели навигации, открывается всплывающее окно со списком непрочитанных уведомлений (рис. 94).

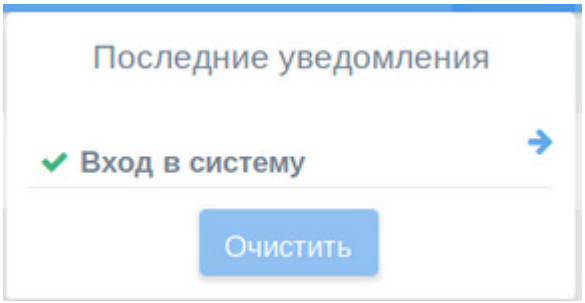


Рисунок 94 – Всплывающее окно

Для работы с уведомлениями Оператору доступны следующие действия:

– переход к источнику уведомления;

– очистка всех уведомлений.

Для перехода к источнику уведомления, Оператор должен нажать на значок « » .

Примечание. Существует группа системных уведомлений, переход к которым невозможен.

Для очистки всех уведомлений, Оператор должен нажать кнопку «Очистить» во всплывающем окне.

Настройка получения уведомлений происходит в профиле пользователя, в разделе «Личная информация» (п. 3.6.2).

3.6 Личная информация

Инструмент «Личная информация» не является отдельным разделом с отдельным рабочим окном. Инструмент «Личная информация» предназначен для общей настройки ПК «Сканер-ВС».

В инструмент «Личная информация» можно перейти по пиктограмме «  » на панели навигации.

Инструмент «Личная информация» выполнен в форме всплывающего окна (рис. 95).

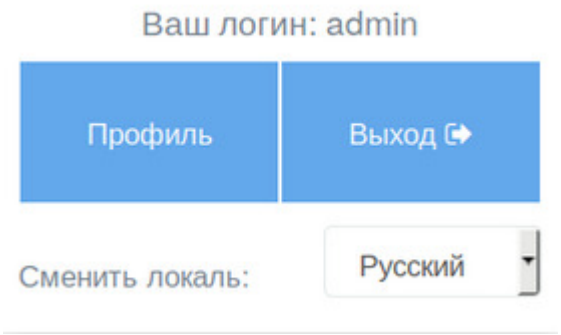


Рисунок 95 – Всплывающее окно «Личная информация»

Инструмент «Личная информация» позволяет Оператору выполнить следующие действия:

– получить информацию о текущем профиле ПК «Сканер-ВС»;

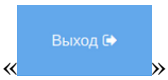
– сменить язык ПК «Сканер-ВС» (Сменить локаль);

– войти в профиль;

– выйти из ПК «Сканер-ВС».

Информация о профиле доступна вверху всплывающего окна (рис. 95) и отображается в виде: «Ваш логин: xxx». Где, xxx – это название профиля.

ПК «Сканер-ВС» доступен в двух языках (локалях): Русский, English. Выбор локалей доступен внизу всплывающего окна в виде выпадающего списка «Сменить локаль:».

Выход из ПК «Сканер-ВС» осуществляется по нажатию кнопки « 

». После выхода Оператор попадает в окно авторизации (рис. 1).

При нажатии кнопки « 

», Оператор переходит в рабочее окно личного кабинета (рис. 96).

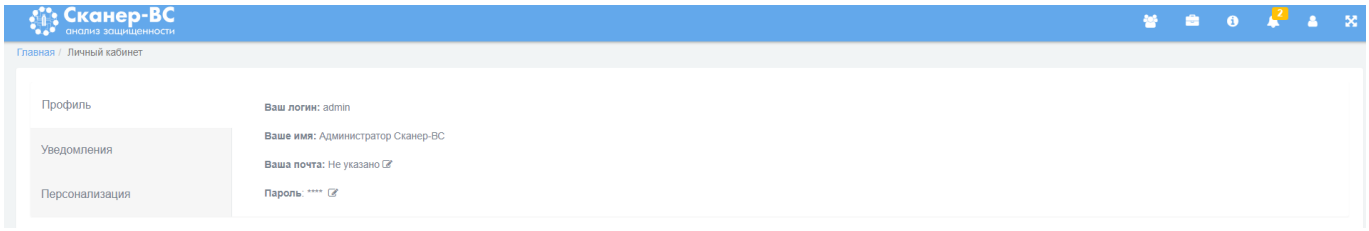


Рисунок 96 – Личный кабинет

В личном кабинете присутствуют следующие вкладки:

– Профиль;

– Уведомления;

– Персонализация.

3.6.1 Вкладка «Профиль»

Во вкладке «Профиль» (рис. 96) отображается информация о профиле Оператора:

– логин;

– имя;

– ваша почта (электронная почта);

– пароль.

«Логин» и «Имя» задается в разделе «Администрирование» при создании нового пользователя (см. пп. 3.2.2.2).

Электронную почту и пароль можно изменить, нажав на значок « ».

После ввода нового адреса электронной почты нажать кнопку «Сохранить» (рис. 97).

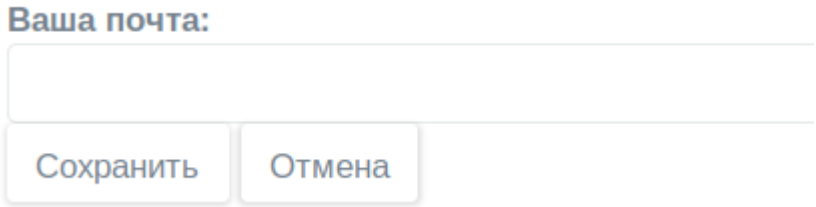


Рисунок 97 – Окно ввода электронной почты

При изменении пароля открывается форма смены пароля (рис. 98).

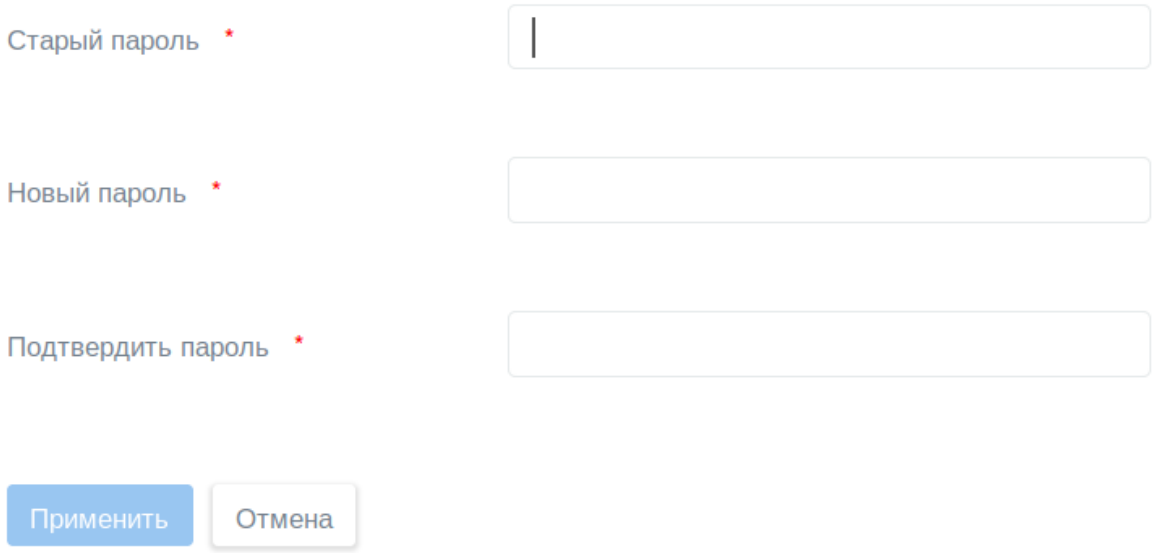


Рисунок 98 – Форма смены пароля

Значком «*» (звездочка) помечены поля обязательные к заполнению.

Правила создания нового пароля описаны в подпункте 3.2.2.2.

После завершения ввода нового пароля нажать кнопку «Применить». Если все действия выполнены правильно, то откроется всплывающее окно с подтверждением смены пароля (рис. 99).

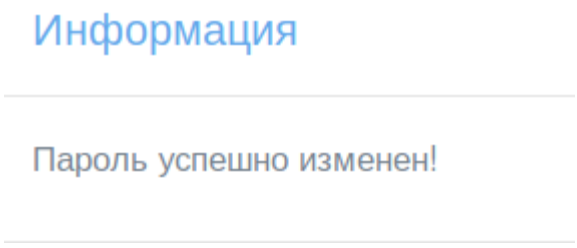


Рисунок 99 – Подтверждение смены пароля

3.6.2 Вкладка «Уведомления»

Вкладка «Уведомления» (рис. 100) разделена на вкладки «События» и «Правила».

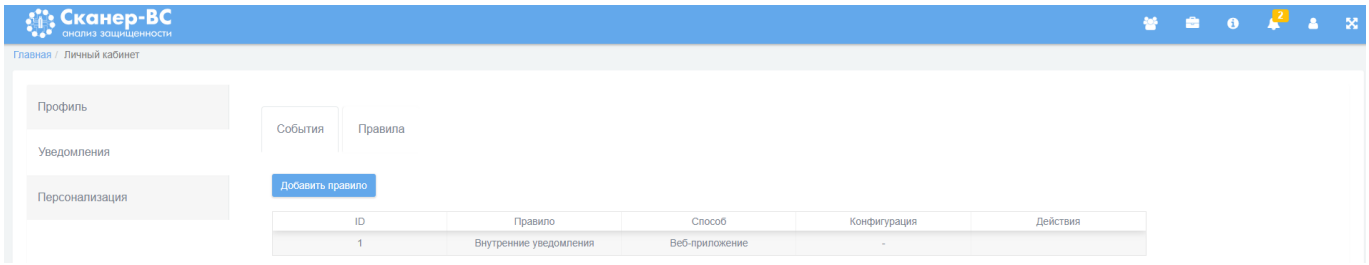


Рисунок 100 – Рабочее окно вкладки «Уведомления»

3.6.2.1 Вкладка «Правила»

Вкладка «Правила» (рис. 101) предназначена для добавления правил для событий.

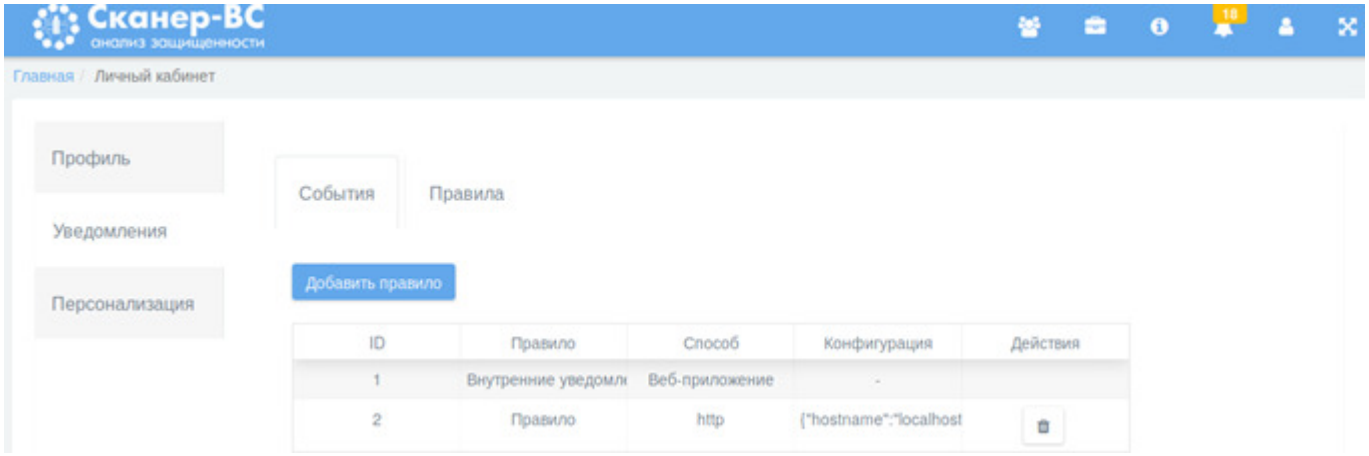


Рисунок 101 – Вкладка «Способы»

Во вкладке «Правила», в виде таблицы, представлен перечень правил. Перечень содержит следующие графы:

– ID – Порядковый номер правила;

– правило – название правила;

– способ – способ уведомления;

– конфигурация – краткая конфигурация правила;

– действия – разрешенные действия с правилом.

Правило можно упорядочивать, нажав на заголовок столбца таблицы.

Правило можно удалить, нажав на иконку « » в столбце таблицы «Действия».

Правило «Внутреннее уведомление» удалить невозможно. Оно является в ПК «Сканер-ВС» правилом по умолчанию.

Для создания нового правила необходимо нажать кнопку «Добавить правило». Откроется форма добавления нового сервера (рис. 102).

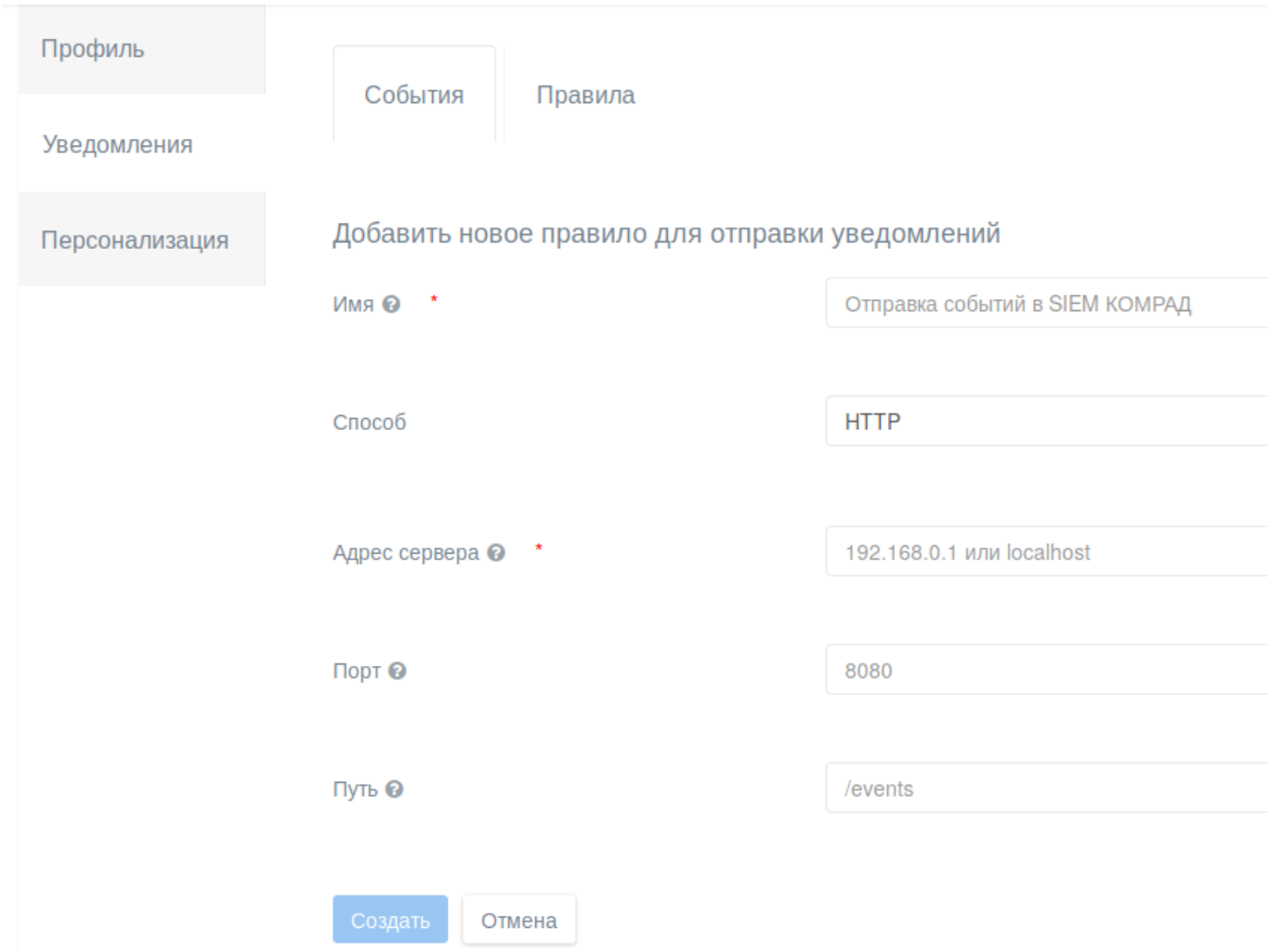


Рисунок 102 – Форма добавления нового сервера

Форма содержит следующие поля:

– Имя – название правила отправки уведомлений;

– Способ – способ доставки уведомления;

– Адрес сервера – IP-адрес (без протокола) сервера, на который будут отправляться уведомления;

– Порт – порт, на который будут отправляться уведомления;

– Путь – адрес директории на сервере, в которой будут сохраняться уведомления (автоматически не создается).

Если вся информация заполнена правильно, то необходимо нажать кнопку «Создать» для сохранения изменений или «Отмена» для выхода из формы добавления нового сервера.

Значком «*» (звездочка) помечены поля обязательные к заполнению.

Значок « » информирует о наличии подсказки по данному полю.

При удачном сохранении, правило автоматически появляется в перечне правил вкладки «Правила» и в перечне событий во вкладке «События».

3.6.2.2 Вкладка «События»

Вкладка «События» представлена в виде таблицы (рис. 100). В левой ее части содержится перечень событий, по которым ПК «Сканер-ВС» отправляет уведомления. В правой части таблицы содержатся правила уведомления.

По умолчанию, в ПК «Сканер-ВС», создано правило «Внутренние уведомления», которое выводит уведомления о событиях на пиктограмму «». Все события в этом правиле включены.

В таблице содержатся следующие события:

– вход в систему;

– выход из системы;

– создание пользователя;

– изменение информации о пользователе;

– изменение привилегий пользователя;

– блокировка пользователя;

– разблокировка пользователя;

– обновление пароля пользователя;

– удаление пользователя;

– создание проекта;

– удаление проекта;

– редактирование проекта;

– создание задачи;

– редактирование задачи;

– удаление задачи;

– запуск задачи;

– запуск задачи по планировщику;

– приостановление задачи;

– возобновление задачи;

– отмена задачи;

– планирование задачи;

– задача завершена;

– задача отменена;

– задача завершена с ошибкой.

Значок « ✔ » показывает, что событие включено, а значок « ✖ » - выключено. Для включения или выключения события достаточно кликнуть левой кнопкой мыши на самом значке.

Добавление правил для событий происходит во вкладке «Правила» (см. пп. 101).

3.6.3 Вкладка «Персонализация»

Вкладка «Персонализация» (рис. 103) содержит настройки по персонализации следующих элементов ПК «Сканер-ВС»:

– форма поиска целей;

– форма поиска уязвимостей;

– форма подбора паролей;

– форма автоматического поиска эксплойтов;

– форма ручного поиска эксплойтов;

– форма создания проекта;

– гибкая настройка языков.

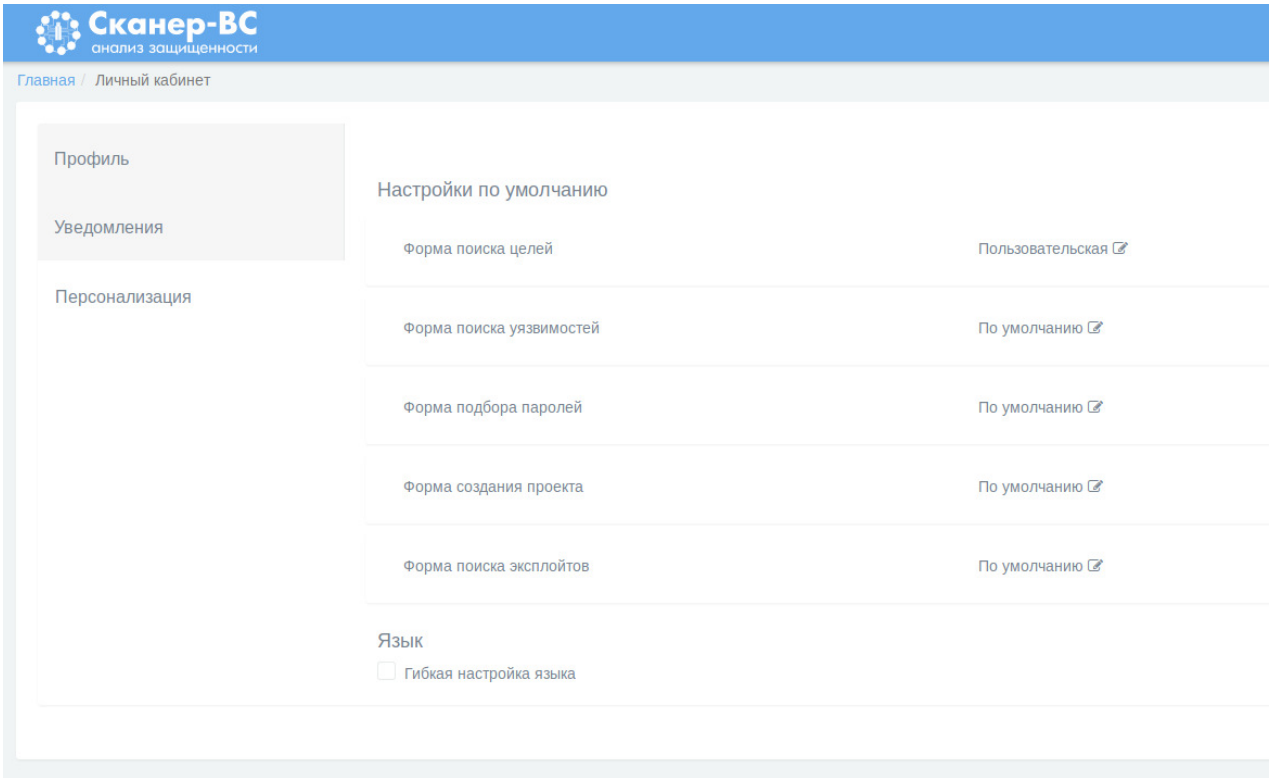


Рисунок 103 – Вкладка «Персонализация»

Настройки персонализации можно изменить, нажав на значок « ».

После изменения и сохранения настроек надпись «По умолчанию» изменится на «Пользовательская» (рис. 103).

3.6.3.1 Форма поиска целей

На рисунке (рис. 104) представлена форма поиска целей.

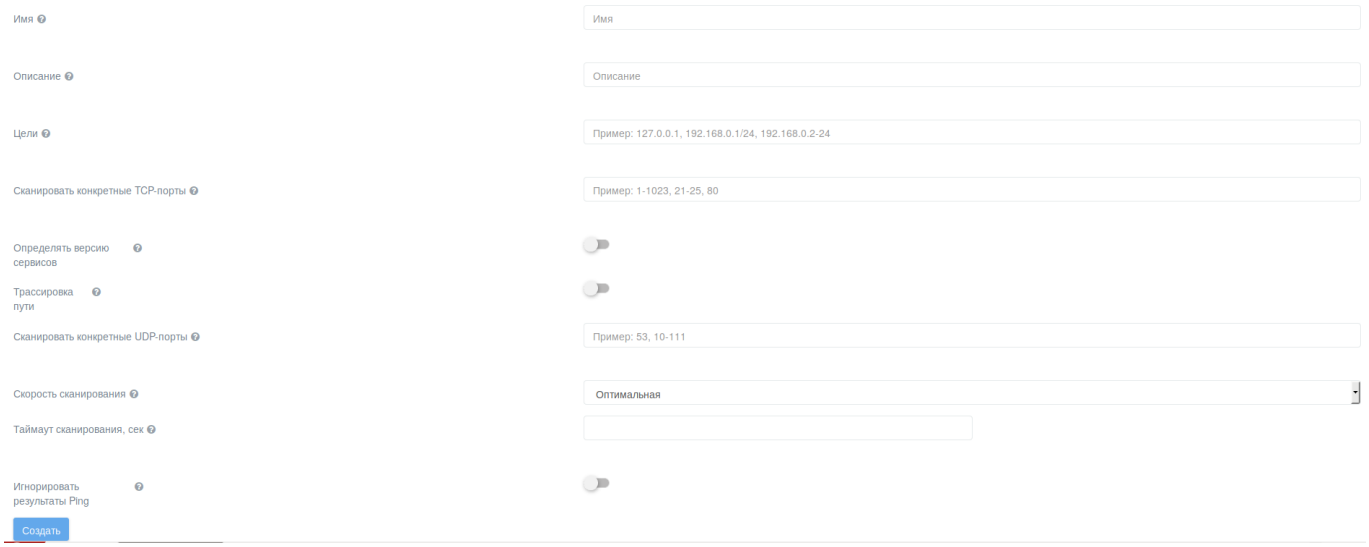


Рисунок 104 – Форма поиска целей

В таблице (см. Таблица 5) представлено описание полей формы поиска целей.

Таблица 5 – Описание полей формы поиска целей

Параметр	Описание
Имя	Имя задачи
Описание	Описание задачи
Цели	IP-адреса
Сканировать конкретные TCP-порты	Параметр для сканирования нестандартных TCP-портов или диапазонов TCP-портов
Определять версию сервисов	Параметр определения версии сетевых сервисов
Трассировка пути	Параметр включения трассировки пути
Сканировать конкретные UDP-порты	Параметр для сканирования нестандартных UDP-портов или диапазонов UDP-портов
Скорость сканирования	Выбор скорости сканирования: – минимальная, низкая - попытка обхода систем обнаружения вторжения; – нормальная - незначительное использование пропускной способности сети и ресурсов; – оптимальная - обычный режим (рекомендуется); – высокая, максимальная - возможно снижение точности результатов сканирования сети

Параметр	Описание
Таймаут сканирования, сек	Настройка для пропуска целевых хостов, время сканирования которых превышает установленный таймаут
Игнорировать результаты Ping	Настройка для обнаружения хостов с помощью TCP SYN вместо Ping

Значок « » информирует о наличии подсказки по данному полю.

Для сохранения результатов необходимо нажать кнопку «Создать».

3.6.3.2 Форма поиска уязвимостей

На рисунке (рис. 105) представлена форма

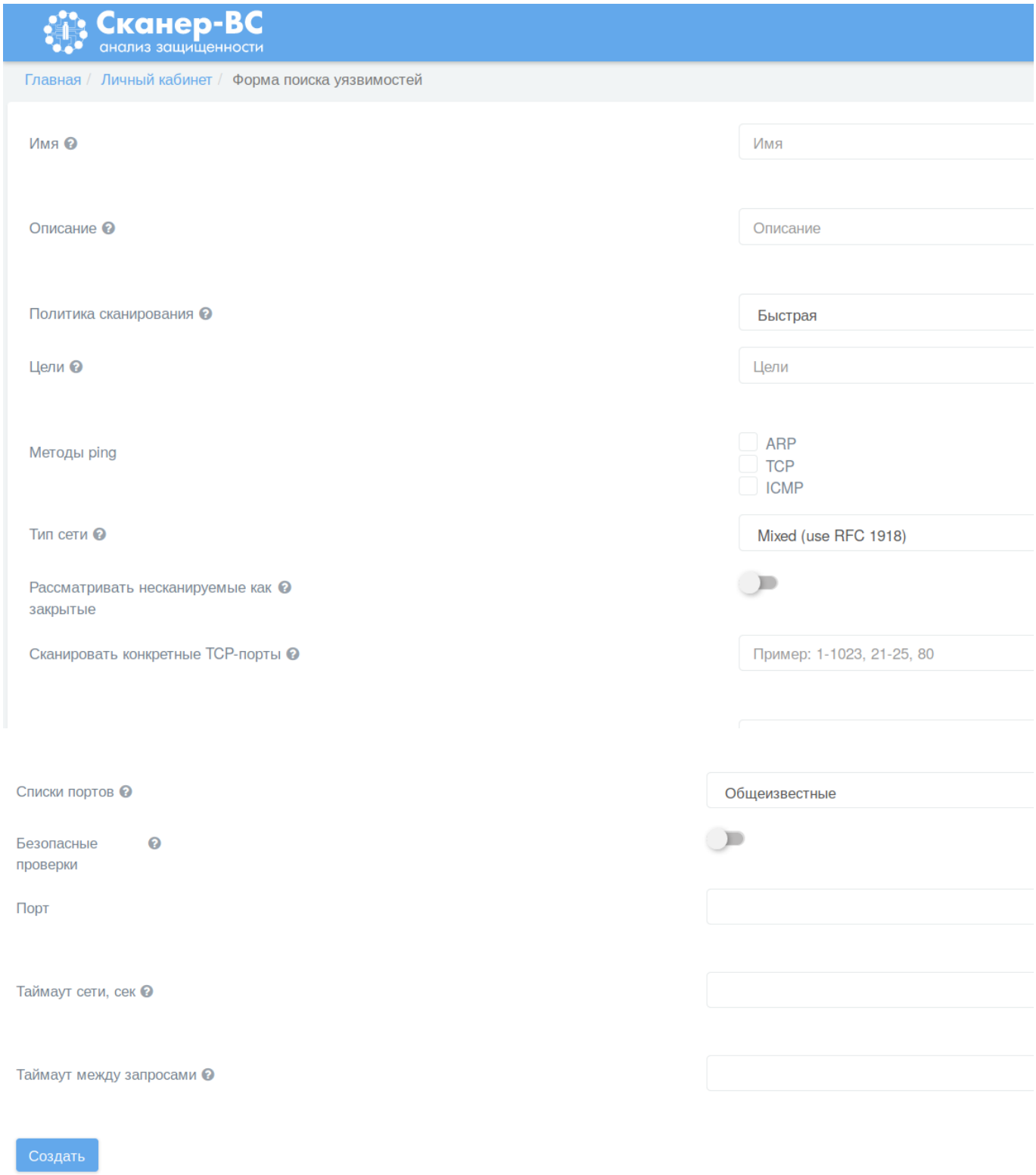


Рисунок 105 – Форма поиска уязвимостей

В таблице (см. Таблица 6) представлено описание полей формы поиска уязвимостей.

Таблица 6 – Описание полей формы поиска уязвимостей

Параметр	Описание
Имя	Имя задачи
Описание	Описание задачи
Политика сканирования	Политика сканирования определяет перечень сетевых проверок безопасности, которые будут запущены в ходе сканирования уязвимостей. Выберите одну из предустановленных или создайте собственную в подпункте 3.3.5.3
Цели	IP–адрес
Методы ping	Параметр выбора метода ping: – ARP; – TCP; – ICMP
Тип сети	Параметр, указывающий тип сети
Рассматривать несканируемые, как закрытые	Настройка отключения сканирования неизвестных портов
Сканировать конкретные TCP-порты	Параметр для сканирования нестандартных TCP-портов или диапазонов TCP-портов
Сканировать конкретные UDP-порты	Параметр для сканирования нестандартных UDP-портов или диапазонов UDP-портов
Списки портов	Параметр выбора предустановленного диапазона портов для сканирования. Общеизвестные - сканирование будет проводиться по списку портов от 1 до 1024. Стандартные (рекомендуется) - сканирование будет проводиться по списку часто используемых портов (4481). Все - будут просканированы все порты, при выборе данной опции время сканирования может существенно увеличиться
Безопасные проверки	Параметр для отключения проверок, которые могут вызвать нарушение доступности проверяемых сетевых сервисов и хостов
Порт	Перечень портов
Таймаут сети, сек	Параметр для пропуска целевых хостов, время сканирования которых превышает установленный таймаут

Параметр	Описание
Таймаут между запросами	Параметр для установки значения тайм-аута для сетевых сокетов во время сканирования

Значок « » информирует о наличии подсказки по данному полю.

Для сохранения результатов необходимо нажать кнопку «Создать».

3.6.3.3 Форма подбора паролей

На рисунке (рис. 106) представлена форма подбора паролей.

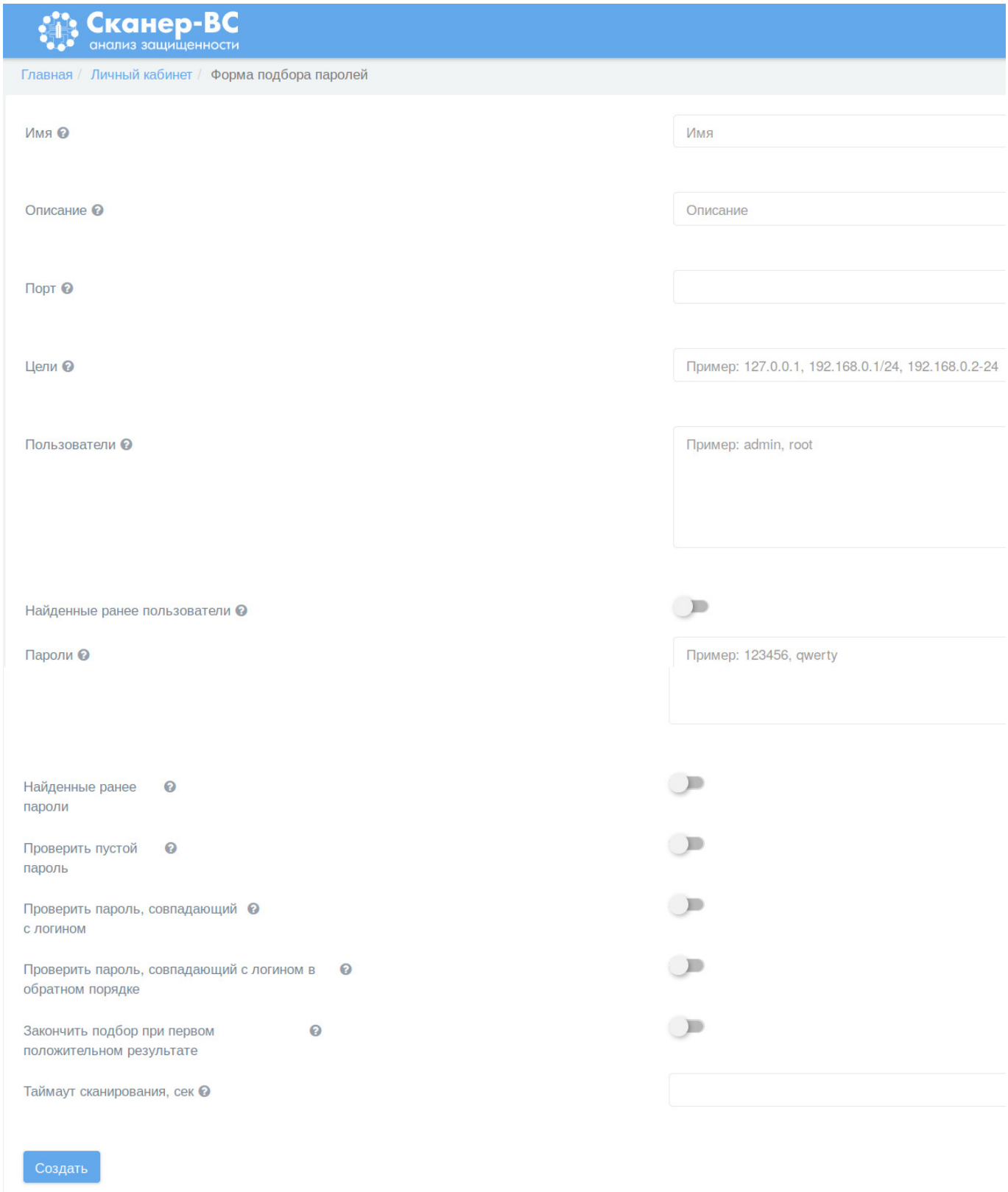


Рисунок 106 – Форма подбора паролей

В таблице (см. Таблица 7) представлено описание полей формы подбора паролей.

Таблица 7 – Описание полей формы подбора паролей.

Параметр	Описание
Имя	Имя задачи
Описание	Описание задачи
Порт	Номер порта, если сетевой сервис использует нестандартный порт
Цели	Перечень IP-адресов
Пользователи	Перечень имен учетных записей пользователей, к которым будет осуществляться подбор паролей
Найденные ранее пользователи	Параметр чтобы включения в проверки ранее найденных имен пользователей
Пароли	Перечень применяемых пользователями паролей
Найденные ранее пароли	Параметр включения проверки ранее найденных паролей
Проверить пустой пароль	Параметр включения проверки пустых паролей
Проверить пароль, совпадающий с логином	Параметр включения проверки паролей, совпадающих с логином
Проверить пароль, совпадающий с логином в обратном порядке	Параметр включения проверки паролей, совпадающих с логином в обратном порядке
Закончить подбор при первом положительном результате	Параметр прерывания подбора пароля после первого найденного
Таймаут сканирования, сек	Параметр включения таймаута между попытками

Значок « » информирует о наличии подсказки по данному полю.

Для сохранения результатов необходимо нажать кнопку «Создать».

3.6.3.4 Форма поиска эксплойтов

На рисунке (рис. 107) представлена форма поиска эксплойтов

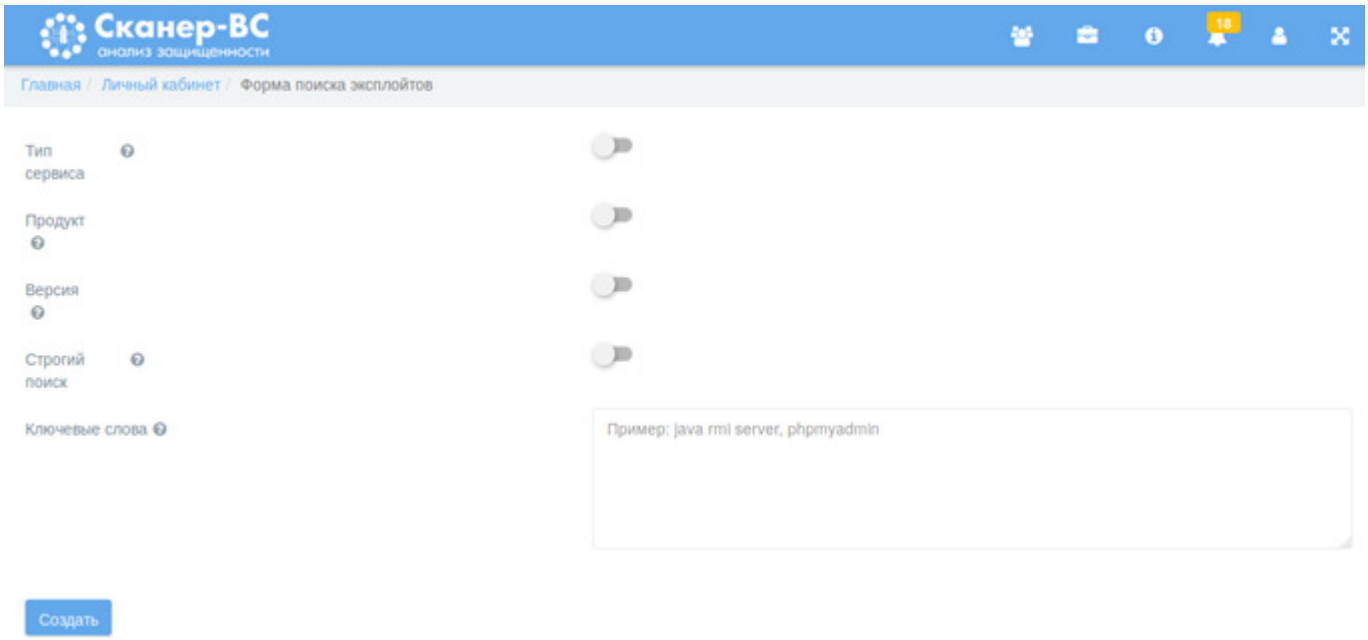


Рисунок 107 – Форма поиска эксплойтов

В таблице (см. Таблица 8) представлено описание полей формы поиска эксплойтов.

Таблица 8 – Описание полей формы поиска эксплойтов

Параметр	Описание
Тип сервиса	Параметр для включения поиска по найденным типам сервисов
Продукт	Параметр для включения поиска по найденным продуктам
Версия	Параметр для включения поиска по найденным версиям продуктов
Строгий поиск	параметр для поиска только тех эксплойтов, которые подходят по всем заданным параметрам поиска. По умолчанию данная опцию выключена и осуществляется поиск эксплойтов, для которых выполняется хотя бы один из критериев поиска
Ключевые слова	Параметр для задания ключевых слов, фрагментов текста, которые должны обязательно присутствовать в названии, описании или других данных эксплойта

Значок « » информирует о наличии подсказки по данному полю.

Для сохранения результатов необходимо нажать кнопку «Создать».

3.6.3.5 Гибкая настройка языков

На рисунке (рис. 108) представлена форма гибкой настройка языков.

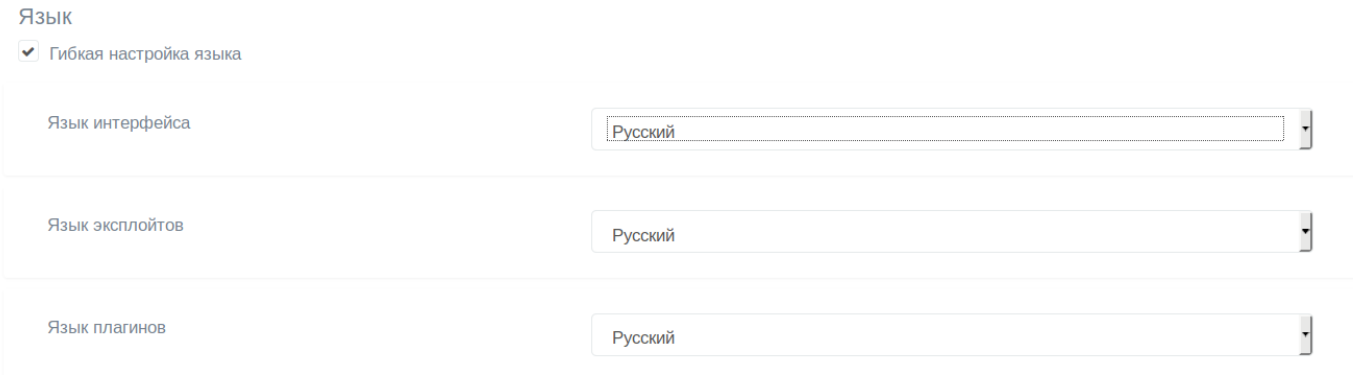


Рисунок 108 – Гибкая настройка языков

В таблице (см. Таблица 9) представлено описание полей формы гибкой настройка языков.

Таблица 9 – Описание полей формы гибкой настройка языков

Параметр	Описание
Язык интерфейса	Параметр выбора языка интерфейса: – Русский; – English
Язык эксплойтов	Параметр выбора языка эксплойтов: – Русский; – English
Язык плагинов	Параметр выбора языка плагинов: – Русский; – English

4 СООБЩЕНИЕ ОПЕРАТОРУ

Тексты сообщений, выдаваемых в ходе выполнения программы, представлены в таблице (см. Таблица 10).

Таблица 10 – Сообщения Оператору

Сообщение	Описание
«Вышел срок действия лицензии»	Данное сообщение появляется, если срок действия лицензии программного комплекса истек.
«Вы действительно хотите уничтожить выбранные объекты?»	Сообщение о подтверждении удаления найденной остаточной информации на выбранном носителе
«Вы действительно хотите уничтожить выбранные объекты?»	Сообщение о подтверждении удаления выбранных каталогов, папок, подпапок, файлов
«Следующие каталоги: являются системными и будут пропущены.»	Сообщение о невозможности удаления системных файлов
«Отчет успешно построен. Нажмите «ОК», чтобы открыть его.»	Сообщение о построение отчета

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

Сокращение	Расшифровка
BIOS	(англ. Basic input / output system) Базовая система ввода / вывода
ID	(англ. Identification data) Идентификатор
SVGA	(англ. Super video graphics array) Графический видеоадаптер
UEFI	(англ. Unified extensible firmware interface) Унифицированный расширяемый интерфейс встроенного (базового) программного обеспечения
USB	(англ. Universal serial bus) Универсальная последовательная шина
WEP	(англ. Wired equivalent privacy) Алгоритм для обеспечения безопасности беспроводных сетей
Wi-Fi	(англ. Wireless fidelity) Беспроводная сеть
WPA	(англ. Wi-Fi protected access) Алгоритм для обеспечения безопасности беспроводных сетей
ИС	Информационная система
ОС	Операционная система
ПО	Программное обеспечение