УТВЕРЖДЕН
НПЕШ.00606-01 90-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВО АНАЛИЗА ЗАЩИЩЕННОСТИ «СКАНЕР-ВС»

Руководство пользователя

Часть 3

НПЕШ.00606-01 90-2

Листов 290

2025

АННОТАЦИЯ

Настоящее руководство пользователя распространяется на «Программный комплекс «Средство анализа защищенности «Сканер-ВС» НПЕШ.00606-01 (далее – изделие или ПК «Сканер-ВС»).

Изготовитель, разработчик и производитель изделия: акционерное общество «НПО «Эшелон» (юридический адрес: 107023, г. Москва, ул. Электрозаводская, д. 24, стр. 1, тел.: 8 (495) 223-23-92, эл. почта: support.sca@cnpo.ru).

В документе содержатся следующие сведения:

– назначение программы (п. 1 настоящего документа);

– условия выполнения программы (п. 3 и 4 настоящего документа);

– описание функций и особенностей эксплуатации изделия (п. 5 настоящего документа);

– сообщения оператору (п. 8 настоящего документа).

ПК «Сканер-ВС» состоит из нескольких (в зависимости от исполнения) функционально независимых составных частей в соответствии с таблицей 1.

Таблица 1 – Состав ПК «Сканер-ВС»

№ исполнения / Компонент	1	2	3	4	5	6	7	8	9
Программное обеспечение «Сканер-ВС» версии 5	+	+	–	–	+	–	–	–	–
Программное обеспечение «Сканер-ВС» версии 6	–	–	+	+	+	–	–	–	–
Программное обеспечение «Сканер-ВС» версии 7 редакция «Base»	–	–	–	–	–	+	–	+	–
Программное обеспечение «Сканер-ВС» версии 7 редакция «Enterprise»	–	–	–	–	–	–	+	–	+
Программный компонент «Инспектор» версии 3	–	+	–	–	+	–	–	+	+
Программный компонент «Инспектор» версии 4	–	–	–	+	+	–	–	+	+

В документе содержатся сведения о назначении, функциях и особенностях эксплуатации ПК «Сканер-ВС» в 6, 7, 8 и 9 вариантах исполнения.

Сведения о назначении, функциях и особенностях эксплуатации изделия в 1, 2 и 5 вариантах исполнения содержатся в документе НПЕШ.00606-01 90 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Руководство пользователя. Часть 1».

Сведения о назначении, функциях и особенностях эксплуатации изделия в 3, 4 и 5 вариантах исполнения содержатся в документе НПЕШ.00606-01 90-1 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Руководство пользователя. Часть 2».

Настоящий документ предназначен для пользователя ПК «Сканер-ВС».

Под пользователем понимается любое лицо, допущенное до эксплуатации изделия с ролями «Пользователь» и/или «Администратор».

Организация-разработчик оставляет за собой право без дополнительного уведомления вносить в руководство пользователя изменения, связанные с улучшением изделия. Актуальная версия документации публикуется в новой редакции руководства пользователя и на сайте компании.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

BIOS	—	(англ. *Basic Input/Output System*) – базовая система ввода / вывода
CISA	—	(англ. *Cybersecurity and Infrastructure Security Agency*) – организация, поддерживающая авторитетный источник уязвимостей, которые были эксплуатированы в реальных условиях
CSV	—	(англ. *Comma-Separated Values*) – текстовый формат, предназначенный для представления табличных данных
HTML	—	(англ. *HyperText Markup Language*) – стандартизированный язык разметки документов в сети Интернет
ID	—	(англ. *Identification Data*) – идентификатор
KEV	—	(англ. *Known Exploited Vulnerabilities*) – это каталог известных эксплуатируемых уязвимостей в области кибербезопасности, которые активно используются. Он служит для оперативного реагирования на реальные угрозы и своевременного устранения уязвимостей, прежде чем они будут эксплуатированы
NIST	—	(англ. *National Institute of Standards and Technology*) – Национальный институт стандартов и технологий, разрабатывающий и поддерживающий технологические стандарты, руководства, передовые практики и другие ресурсы по кибербезопасности
NVD	—	(англ. *National Vulnerability Database*) – база данных уязвимостей, созданная Национальным институтом стандартов и технологий (NIST)
TCP	—	(англ. *Transmission Control Protocol*) – один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных
UDP	—	(англ. *User Datagram Protocol* – протокол пользовательских датаграмм) – один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета
UEFI	—	(англ. *Unified extensible Firmware Interface*) – унифицированный расширяемый интерфейс встроенного (базового) программного обеспечения
USB	—	(англ. *Universal Serial Bus* – универсальная последовательная шина) – последовательный интерфейс для подключения периферийных устройств к вычислительной технике
АРМ	—	автоматизированное рабочее место
БУ	—	база уязвимостей
ОС	—	операционная система
ПО	—	программное обеспечение
ПУ	—	пользовательская уязвимость
ФСТЭК России	—	федеральная служба по техническому и экспортному контролю

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

ПК «Сканер-ВС» предназначен для автоматизированного анализа (контроля) защищенности информации.

ПК «Сканер-ВС» для работы в значимых объектах критической информационной инфраструктуры 1 категории, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования 2 класса.

Программное обеспечение «Сканер-ВС» (далее – Сканер-ВС) предназначен для поиска уязвимостей программного обеспечения (далее – ПО), сканирования сетевых узлов и сервисов, идентификации операционной системы (далее – ОС) и приложений, трассировки сетевых маршрутов для построения топологии сети, сбора информации при помощи активного подключения к исследуемому узлу, проверки стойкости сетевых паролей и настроек программного обеспечения на соответствие требованиям безопасности.

Сканер-ВС обеспечивает инвентаризацию ресурсов сети, определение состояния TCP- и UDP-портов в диапазоне от 1 до 65535, идентификацию операционных систем и сетевых приложений, трассировку маршрутов следования данных для построения топологии сети.

Сканер-ВС осуществляет поиск уязвимостей автоматизировано или по расписанию, задаваемому пользователем.

Сканер-ВС осуществляет автоматическое или ручное обновление базы данных уязвимостей с помощью встроенной утилиты «Центр обновлений».

Сканер-ВС осуществляет подбор паролей по словарям для учетных записей пользователей для следующих сетевых сервисов: imap, imaps, mssql, mysql, pop3, pop3s, postgres, rdp, redis, smtp, smtps, snmp, ssh, telnet, vnc.

Сканер-ВС осуществляет активное подключение к исследуемым узлам для сбора информации.

Сканер-ВС осуществляет проверку настроек программного обеспечения на соответствие требованиям безопасности.

Сканер-ВС обеспечивает формирование отчетов по результатам проверок в форматах HTML.

Сканер-ВС обеспечивает идентификацию и аутентификацию пользователей Сканер-ВС.

Компонент «Инспектор» предназначен для тестирования функций безопасности при проведении аттестации автоматизированных систем.

Компонент «Инспектор» обеспечивает тестирование механизмов очистки оперативной памяти ОС специального назначения «Astra Linux Special Edition» и запоминающих устройств рабочей станции.

Компонент «Инспектор» обеспечивает формирование отчетов по результатам проверок в формате HTML.

Примечание. Сканер-ВС не предназначен для сканирования разных активов с одинаковыми FQDN или IP адресам в одной исследуемой подсети, так как в таком случае Сканер-ВС не будет разделять получаемую об этих активах информацию, в результате чего произойдет смешивание информации разных активов под одним сетевым адресом, что приведет к слиянию двух разных активов в один, который будет заполнен некорректной информацией.

Сканер-ВС версии 7 редакций «Base» и «Enterprise» из состава исполнений № 6, 7, 8 и 9 реализуют следующие функции безопасности:

– обеспечение идентификации и аутентификации операторов Сканер-ВС (ИАФ.1). Аутентификация осуществляется с использованием паролей, а идентификация осуществляться по идентификатору (имени учетной записи), связанному с учётной записью пользователя Сканер-ВС;

– обеспечение управления идентификаторами операторов Сканер-ВС (ИАФ.3). При добавлении нового пользователя должен генерироваться и присваиваться создаваемой учетной записи пользователя уникальный идентификатор. При удалении

существующей учетной записи пользователя Сканер-ВС, соответствующие этой учетной записи пользователя логин и пароль должны удаляться;

– обеспечение управления средствами аутентификации Сканер-ВС (ИАФ.4). Управление средствами аутентификации выполняется под учетной записью пользователя
с ролью «Администратор»;

– обеспечение защиты обратной связи при вводе аутентификационной информации (ИАФ.5). Ввод пароля при аутентификации защищен от визуальной демонстрации (вводимые символы пароля отображаются условными знаками «•»), а также осуществляется защита от копирования пароля из формы;

– обеспечение управления учетными записями операторов Сканер-ВС (УПД.1). Управление учетными записями операторов Сканер-ВС выполняется под учетной записью пользователя с ролью «Администратор»;

– обеспечение разграничения доступа на основе ролевой модели (УПД.2). В Сканер-ВС реализовано разграничение доступа на базе ролевой модели для операторов с ролями «Администратор» и «Пользователь»;

– обеспечение блокирования сеанса доступа в Сканер-ВС после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10). Производится разрыв сессии по истечению установленного времени бездействия пользователя или по его команде и автоматический переход к окну авторизации в Сканер-ВС;

– обеспечение запрета любых действий операторов до идентификации и аутентификации (УПД.11). В Сканер-ВС реализован механизм запрета любых действий неавторизованных операторов за исключением непосредственной идентификации и аутентификации в Сканер-ВС;

– обеспечение сбора и записи информации о событиях безопасности Сканер-ВС (РСБ.3). Сканер-ВС производит регистрацию событий безопасности Сканер-ВС и запись информации об этих событиях в журнал аудита событий безопасности;

– обеспечение генерирования временных меток и синхронизации системного времени в Сканер-ВС (РСБ.6). Во время функционирования Сканер-ВС регистрирует и присваивает временные метки задачам, запрашиваемым операторами Сканер-ВС;

– реализация ограничения прав операторов по вводу информации в Сканер-ВС (ОЦЛ.6). В Сканер-ВС предусмотрены операторы с ролями «Пользователь» и «Администратор». Для пользователя с ролью «Администратор» нет ограничений по вводу информации в Сканер-ВС. Пользователю с ролью «Пользователь» недоступен ввод

в Сканер-ВС информации следующего характера:

а) управление учетными записями операторов Сканер-ВС;

б) управление учетными записями, используемыми для осуществления активного подключения к узлам исследуемой сети, и привязанными к ним секретами;

в) обновление базы уязвимостей Сканер-ВС. Пользователю с ролью «Пользователь» доступен только просмотр истории обновлений;

г) конфигурирование Сканер-ВС и его компонентов. Запрет конфигурирования осуществляется средствами среды функционирования Сканер-ВС.

– реализация контролирования точности, полноты и корректности данных, вводимых в информационную систему (ОЦЛ.7). В Сканер-ВС установлены лимиты на вводимые символы, а также проводится проверка на корректность введенных данных и наличие недопустимых символов в процессе ввода проверяемой информации;

– выявление уязвимости и конфигурации ПО. Для выявления (поиска) уязвимостей Сканер-ВС использует встроенную базу данных уязвимостей кода и уязвимостей конфигурации ПО. База данных уязвимостей Сканер-ВС содержит унифицированные описания уязвимостей, аналогичные содержащимся в следующих общедоступных источниках (АНЗ.1): банк данных угроз безопасности информации ФСТЭК России (https://www.bdu.fstec.ru), национальная база данных уязвимостей США «National Vulnerability Database» (https://nvd.nist.gov/), база отслеживания ошибок безопасности ОС на базе Debian GNU/Linux «Debian GNU/Linux Security Bug Tracker» (https://security-tracker.debian.org/tracker/), база данных уязвимостей информационной безопасности ОС на базе Ubuntu «Ubuntu CVE Tracker» (https://ubuntu.com/security/cve), база отслеживания ошибок безопасности ОС на базе RHEL/CentOS «RHEL/CentOS

Security Data» (https://access.redhat.com/security/data). Также в Сканер-ВС предусмотрена возможность сгенерировать отчет с описанием выявленных уязвимостей;

– контроль установки обновлений операционных систем семейства Microsoft Windows (АН3.2). Для каждого IBM PC совместимого персонального компьютера в используемой локальной сети, функционирующему на базе ОС семейства Microsoft Windows, Сканер-ВС сохраняет информацию об установленных обновлениях;

– обеспечение аудита параметров настройки и правильности функционирования ПО, а именно для каждого IBM PC совместимого персонального компьютера в используемой локальной сети Сканер-ВС сохраняет информацию об уязвимостях, связанных с настройками ПО (АН3.3);

– обеспечение инвентаризации программных и технических средств, а именно для каждого IBM PC-совместимого персонального компьютера в используемой локальной сети Сканер-ВС сохраняет информацию о типе и версии ОС, MAC адресе устройства, а также перечень установленного ПО (АН3.4).

Компонент «Инспектор» версии 3 из состава исполнений № 2, 5, 8 и 9 реализует следующие функции безопасности:

– контроль состава технических средств, ПО и средств защиты информации (АН3.4). Компонент «Инспектор» обеспечивает инвентаризацию программных и технических средств, а именно для каждого IBM PC-совместимого персонального компьютера в используемой локальной сети сохраняет информацию о версии ОС, перечень установленного ПО, параметры мониторов, центрального процессора, дисковых устройств, сетевых адаптеров, принтеров, устройств ввода информации (клавиатура, мышь), перечень подключенных USB-накопителей, перечень лицензионных ключей.

– обеспечение контроля реализации правил разграничения доступа (АН3.5 в части контроля реализации правил разграничения доступа и полномочий операторов в информационной системе). Компонент «Инспектор» обеспечивает формирование и контроль дискреционных и мандатных полномочий доступа операторов (локальных и доменных) к выбранным сетевым папкам и объектам файловой системы ОС семейства Microsoft Windows, в том числе с учетом настроек СЗИ Secret Net Studio, СЗИ Secret Net Studio-C, СЗИ Secret Net 7, СЗИ НСД Dallas Lock 8.0-K, СЗИ Dallas Lock 8.0-C;

– компонент «Инспектор» обеспечивает формирование и контроль дискреционных и мандатных полномочий доступа локальных операторов к выбранным объектам файловой системы ОС специального назначения «Astra Linux Special Edition»;

– контроль целостности ПО (ОЦЛ.1). Компонент «Инспектор» обеспечивает контрольное суммирование заданных файлов, папок, подпапок, съемных носителей и накопителей на жестких магнитных дисках;

– контроль уничтожения информации и обеспечение поиска остаточной информации на машинных носителях (ЗНИ.8). Компонент «Инспектор» обеспечивает поиск остаточной информации на машинных носителях информации, а также определяет директорию файла с найденной информацией.

Компонент «Инспектор» версии 4 из состава исполнений № 4, 5, 8 и 9 реализует следующие функции безопасности:

– контроль состава технических средств и ПО (АНЗ.4). Компонент «Инспектор» обеспечивает инвентаризацию программных и технических средств, а именно для каждого IBM PC-совместимого персонального компьютера в используемой локальной сети сохраняет информацию о версии ОС, перечень установленного ПО, параметры мониторов, центрального процессора, дисковых устройств, сетевых адаптеров, принтеров, устройств ввода информации (клавиатура, мышь), перечень подключенных USB-накопителей, перечень лицензионных ключей;

– обеспечение контроля реализации правил разграничения доступа (АНЗ.5 в части контроля реализации правил разграничения доступа и полномочий операторов в информационной системе). Компонент «Инспектор» обеспечивает формирование и контроль дискреционных и мандатных полномочий доступа операторов (локальных и доменных) к выбранным сетевым папкам и объектам файловой системы ОС специального назначения «Astra Linux Special Edition»;

– контроль целостности ПО (ОЦЛ.1). Компонент «Инспектор» обеспечивает контрольное суммирование заданных файлов, папок, подпапок, съемных носителей и накопителей на жестких магнитных дисках;

– контроль уничтожения информации и обеспечение поиска остаточной информации на машинных носителях (ЗНИ.8). Компонент «Инспектор» обеспечивает поиск остаточной информации на машинных носителях информации, а также определяет директорию файла с найденной информацией, в целях контроля гарантированного уничтожения остаточной информации на машинных носителях.

Условные обозначения мер защиты информации указаны в соответствии со следующими нормативными документами:

– приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;

– приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

2. ФУНКЦИОНАЛЬНЫЕ ОТЛИЧИЯ СКАНЕР-ВС ВЕРСИИ 7 РЕДАКЦИЙ «BASE» И «ENTERPRISE»

Программное обеспечение «Сканер-ВС» версии 7 редакция «Enterprise» – это расширенная редакция Сканер-ВС с набором функций, позволяющих пользователю более подробно настраивать шаблоны аудита и создавать конфигурации пользовательских уязвимостей.

Программное обеспечение «Сканер-ВС» версии 7 редакция «Base» – это отдельный дистрибутив с «базовой» редакцией ПО. Данная редакция не содержит функций, позволяющих пользователю самому создавать шаблоны аудита конфигурации, а также пользовательские уязвимости. В редакции «Base» также недоступен импорт шаблонов с сайта обновлений (отсутствует возможность скачать их и по лицензии). Пользователь может использовать только предустановленные шаблоны для ОС Astra Linux 1.5/1.6/1.7 и Windows 11.

Подробно функциональные отличия Сканер-ВС версии 7 редакций «Base» и «Enterprise» представлены в таблице 2.

Таблица 2 – Отличия Сканер-ВС версии 7 редакций «Base» и «Enterprise»

Функция	Сканер-ВС 7 «Enterprise»	Сканер-ВС 7 «Base»
Исследование сети	+	+
Пользовательские скрипты	+	+
Сетевая инвентаризация	+	+
Поиск уязвимостей	+	+
Пользовательская база уязвимостей	+	–
Аудит конфигурации	+	+
Создание/редактирование шаблонов аудита конфигурации	+	–
Сетевой подбор паролей	+	+
Подсистема отчетов	+	+
Импорт шаблонов аудита	+	–
Лицензия	+	+

3. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

Установка и первичная настройка Сканер-ВС осуществляется администратором.

Условия выполнения Сканер-ВС на автоматизированном рабочем месте (далее – АРМ) указаны в документе НПЕШ.00606-01 91-1 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Руководство администратора. Часть 2».

Примечание. Любые действия, непосредственно проводимые с АРМ, необходимо осуществлять в соответствии с документацией на этот АРМ.

4. ВЫПОЛНЕНИЕ ПРОГРАММЫ

4.1. Общие сведения

В Сканер-ВС предусмотрены операторы с ролями «Пользователь» и «Администратор».

Пользователь с ролью «Администратор» не имеет ограничений по вводу информации в Сканер-ВС, за исключением изменения конфигураций компонентов Сканер-ВС.

Пользователю с ролью «Пользователь» не доступны в отношении Сканер-ВС следующие действия:

– добавление новых операторов;

– управление учетными записями и их секретами, используемыми для осуществления активного подключения к узлам исследуемой сети;

– выполнение обновлений базы уязвимостей;

– управление пользовательскими скриптами;

– управление пользовательскими уязвимостями;

– изменение настроек аудита (доступно только для просмотра);

– изменение конфигурации компонентов.

4.2. Запуск Сканер-ВС

Для запуска Сканер-ВС необходимо выполнить следующие действия:

– получить АРМ с установленным на него Сканер-ВС с комплектом документации. Инструкция изменения порядка загрузки в UEFI и различных типах BIOS для запуска с Live-носителя представлена в приложении 1 настоящего документа;

– запустить АРМ в соответствии с эксплуатационной документацией на него;

– запустить встроенный терминал «Fly» ОС специального назначения Astra Linux Special Edition 1.7;

– перейти к каталогу /usr/bin/ с помощью команды `cd /usr/bin`;

– произвести подсчет контрольных сумм неизменяемых исполняемых файлов Сканер-ВС в соответствии с инструкцией, приведенной в НПЕШ.00606-01 30 «Сканер-ВС. Формуляр»;

– проверить функционирование сервиса Сканер-ВС с помощью команды `systemctl status scanner`;

– проверить, что в выводе результатов выполнения команд проверки функционирования сервисов указан статус «Active»;

– подключиться к веб-интерфейсу Сканер-ВС в соответствии с п. 4.3 настоящего документа.

4.3. Подключение к веб-интерфейсу Сканер-ВС в «стандартном режиме»

Для подключения к веб-интерфейсу Сканер-ВС в «стандартном режиме» необходимо выполнить следующие действия:

– включить АРМ в соответствии с эксплуатационной документацией на него;

– открыть браузер и в адресной строке ввести IP-адрес Сканер-ВС, а именно: **https://localhost/** (для удаленного подключения к Сканер-ВС вместо «localhost» необходимо ввести IP-адрес АРМ, на которую был установлен Сканер-ВС);

– перейти по введенному IP-адресу;

– далее в окне браузера отобразится окно авторизации Сканер-ВС (рис. 1).

5. ВЕБ-ИНТЕРФЕЙС Сканер-ВС

5.1. Общее описание веб-интерфейса Сканер-ВС

После подключения к Сканер-ВС в браузере отобразится окно авторизации, где пользователь должен ввести логин и пароль (рис. 1).

Функции управления (администрирования) Сканер-ВС определяются правами, назначенными оператору. В Сканер-ВС предусматриваются роли «Администратор» и «Пользователь».

В Сканер-ВС есть предустановленная учетная запись с ролью «Администратор» с логином: admin и паролем: admin. Данная учетная запись является уникальной. Рекомендуется немедленно после первой авторизации сменить пароль для предустановленной учетной записи на надежный и сохранить данный пароль, так как для данной учетной записи в целях безопасности пароль восстановить невозможно.

Для получения логина и пароля для авторизации в Сканер-ВС обратитесь к своему оператору с ролью «Администратор».

Окно авторизации

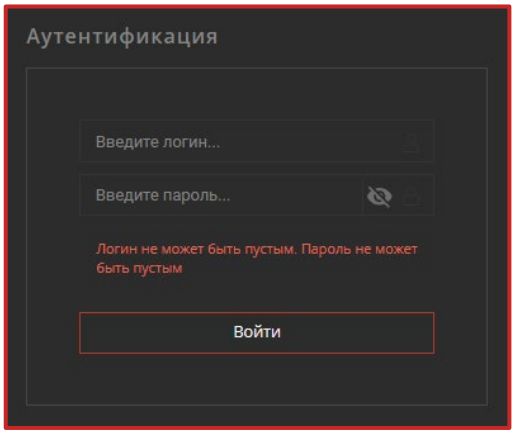


Рис. 1

При успешной авторизации в веб-интерфейсе будет отображена главная страница Сканер-ВС (рис. 2).

Главная страница Сканер-ВС

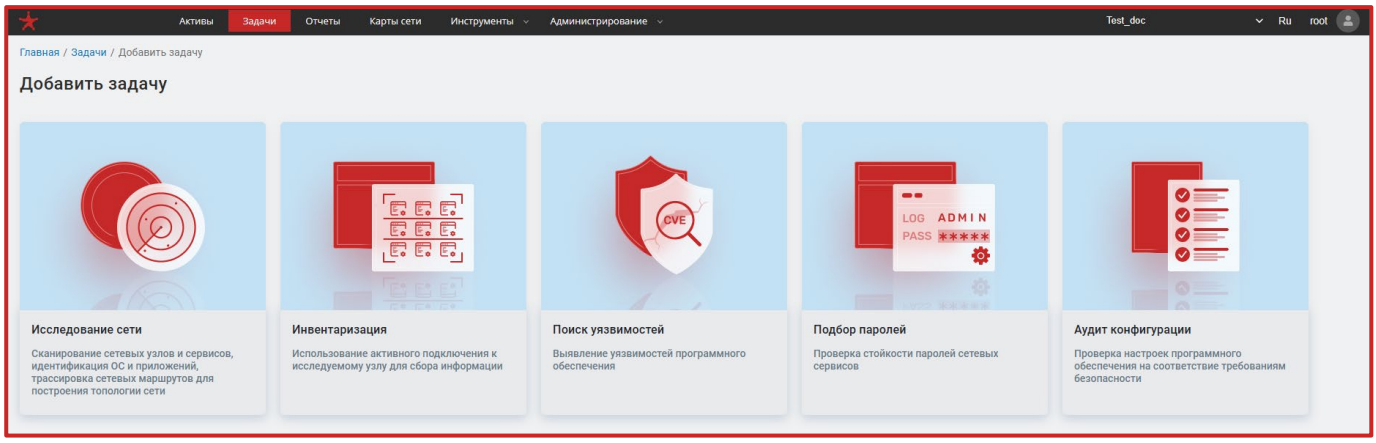


Рис. 2

Веб-интерфейс Сканер-ВС содержит два основных блока элементов:

– «Панель навигации» (рис. 3);

– «Рабочее окно» (рис. 4).

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

– «Активы»;

– «Задачи»;

– «Отчеты»;

– «Карты сети»;

– «Инструменты»;

– «Администрирование» (доступно только для пользователя с ролью «Администратор»);

– меню выбора проекта (пример на рис. 3 – «Test_doc»);

– меню выбора языка интерфейса;

– имя текущего пользователя (пример на рис. 3 – «root»);

– меню управления учетной записью пользователя (значок на рис. 3).

Панель навигации

Рис. 3

Блок «Рабочее окно» (рис. 4) является основной рабочей областью интерфейса Сканер-ВС, в котором отображаются основные задачи с кратким их описанием, выполнение которых обеспечивает анализ сети с точки зрения информационной безопасности.

Рабочее окно

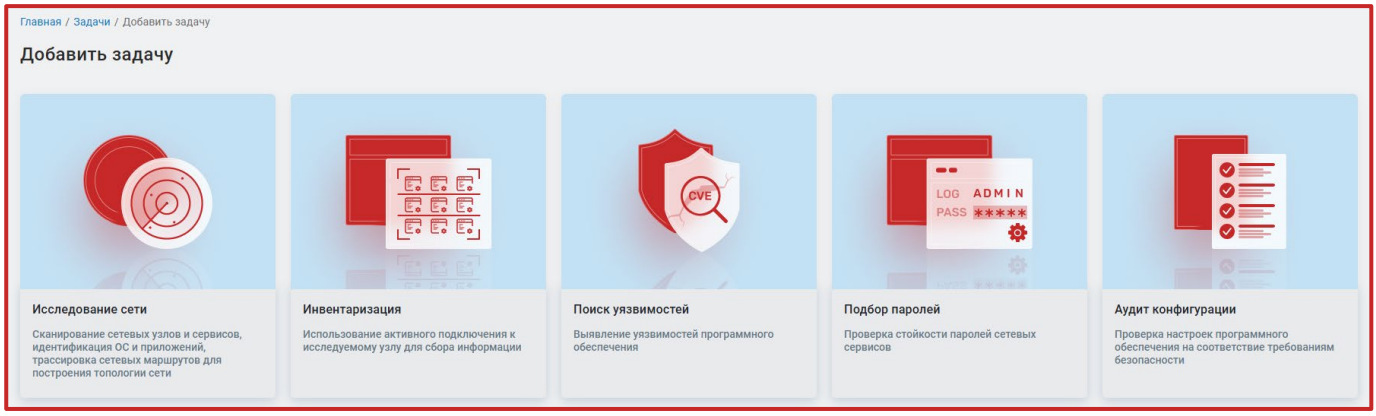


Рис. 4

Веб-интерфейс изделия поддерживает унифицированный механизм отображения данных в табличном формате, при этом оператору предоставляется возможность:

– управлять данными таблицы;

– экспортировать данные из таблицы.

5.1.1. Иконки, используемые в графическом интерфейсе

В таблице 3 представлено назначение стандартных иконок, используемых в графическом интерфейсе Сканер-ВС.

Таблица 3 – Используемые иконки и их назначение

Иконка	Назначение
Иконки, общие для всего веб-интерфейса	
	Удаление
	Удалить неиспользуемые
	Настройка отображения столбцов таблиц
	Поиск
	Фильтрация
	Перейти на следующую страницу
	Перейти на предыдущую страницу
	Подтвердить / Выбрать
	Отменить / Закрыть
	Раскрытие параметров
	Скачать / Скачать данные в формате CycloneDX
	Загрузить / Загрузить данные в формате CycloneDX
	Экспортировать / Экспортировать в .csv
	Импортировать
	Редактировать
	Скопировать / Дублировать
	Расписание
	Показать дополнительные параметры
	Приостановить / Пауза
	Отменить / Остановить
	Запустить
	Меню управления учетной записью пользователя
	Сортировка данных в таблице по возрастанию значений параметра
	Сортировка данных в таблице по убыванию значений параметра
	Скачать текст ошибки выполнения команд
	Уровень критичности
	Всплывающая подсказка

Иконка	Назначение
	Всплывающая краткая документация по использованию функции
	Индикатор наличия эксплойта
	Индикатор наличия опасного эксплойта (CISA KEV)
	Отметить как ложное срабатывание
	Индикатор отметки уязвимых пакетов ложными
	Выбор директории через дерево каталогов
	Объединить
	Одновременная проверка подключений
	Перейти в режим редактирования чувствительной информации
Иконки, используемые для отображения типа устройства в картах сети	
	Сетевое ПО
	Сетевое оборудование
	Офисное оборудование
	Десктопное оборудование
	Мобильные устройства
	Другой тип оборудования, не относящийся к описанным группам
	Межсетевой экран
	Виртуальная машина
	Коммутатор
	Сетевой концентратор
	Терминал
	Оборудование IP телефонии
	Веб-камера
	Сетевой принтер

5.1.2. Экспорт данных из таблиц

Иконка экспорта данных из таблицы «  » предназначена для экспорта данных из таблицы в формате «.csv» на текущий АРМ.

Выбор полей для скачивания реализован посредством настройки отображения столбцов таблицы (п. 5.1.4). Установленная галочка (активный чекбокс « ☑ ») у поля с именем столбца в настройках означает, что в скачанных данных будут содержаться данные из этого столбца.

После активации чекбокса у необходимых настроек, выбора данных и нажатия иконки экспорта может открыться (в зависимости от настроек браузера) окно подтверждения для скачиваемых данных (рис. 5).

Примечание. Экспортируются **только выбранные на текущей отображаемой странице** строки таблицы. Выбранные ранее строки на других страницах остаются таковыми после завершения экспорта.

Окно подтверждения экспорта данных из таблицы в браузере

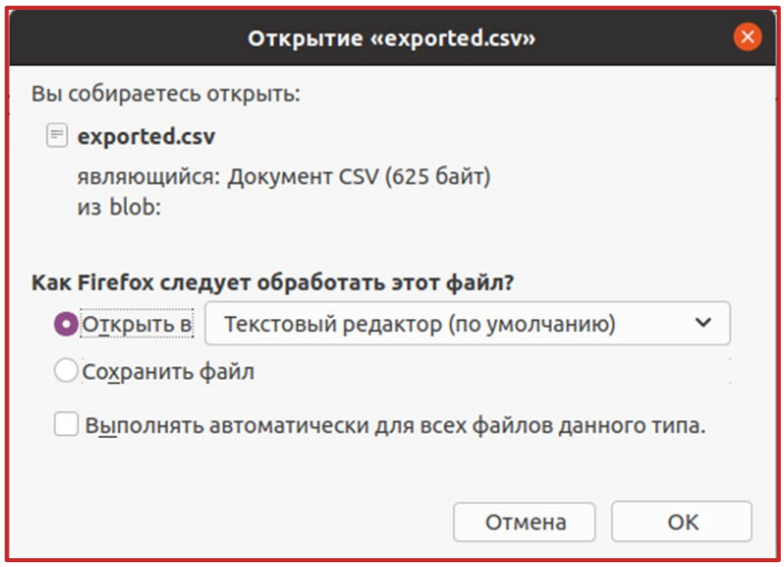


Рис. 5

При появлении данного окна необходимо нажать кнопку «Ок» для экспорта и последующего отображения данных в формате «.csv» без скачивания файла или кнопку «Отмена» для возврата в предыдущее окно Сканер-ВС. В случае необходимости загрузки данных непосредственно на жесткий диск АРМ выберите опцию «Сохранить файл», а затем нажмите кнопку «Ок».

Примечание. Экспортированные данные из таблиц рекомендуется открывать в стандартном приложении «Блокнот» или его аналогах.

5.1.3. Фильтр элементов таблицы

Иконка фильтра элементов таблицы («») предназначена для настройки отображения данных, содержащихся в таблице.

При нажатии на иконку фильтра появляются строки для выбора данных, по которым будут отфильтрованы данные в таблице.

После применения фильтра рядом с иконкой «» отобразится красный круг, сигнализирующий о том, что в таблице отображены только те данные, которые соответствуют примененному фильтру.

Так же в Сканер-ВС предусмотрена функция фильтрации элементов таблиц, связанных с отображением активов, по тегам, а именно таблица активов (п. 5.4 настоящего документа), окно импорта активов для проведения задач (рис. 55).

Для применения фильтрации активов по тегу необходимо нажать на соответствующий тег.

В списке всех задач оператору доступна возможность фильтрации по наличию активов в каждой задаче. Для этого необходимо нажать кнопку «» на верхней панели таблицы и в выпадающем справа блоке указать необходимые активы, используя кнопку «Импорт из активов » (рис. 6).

Блок «Фильтр»

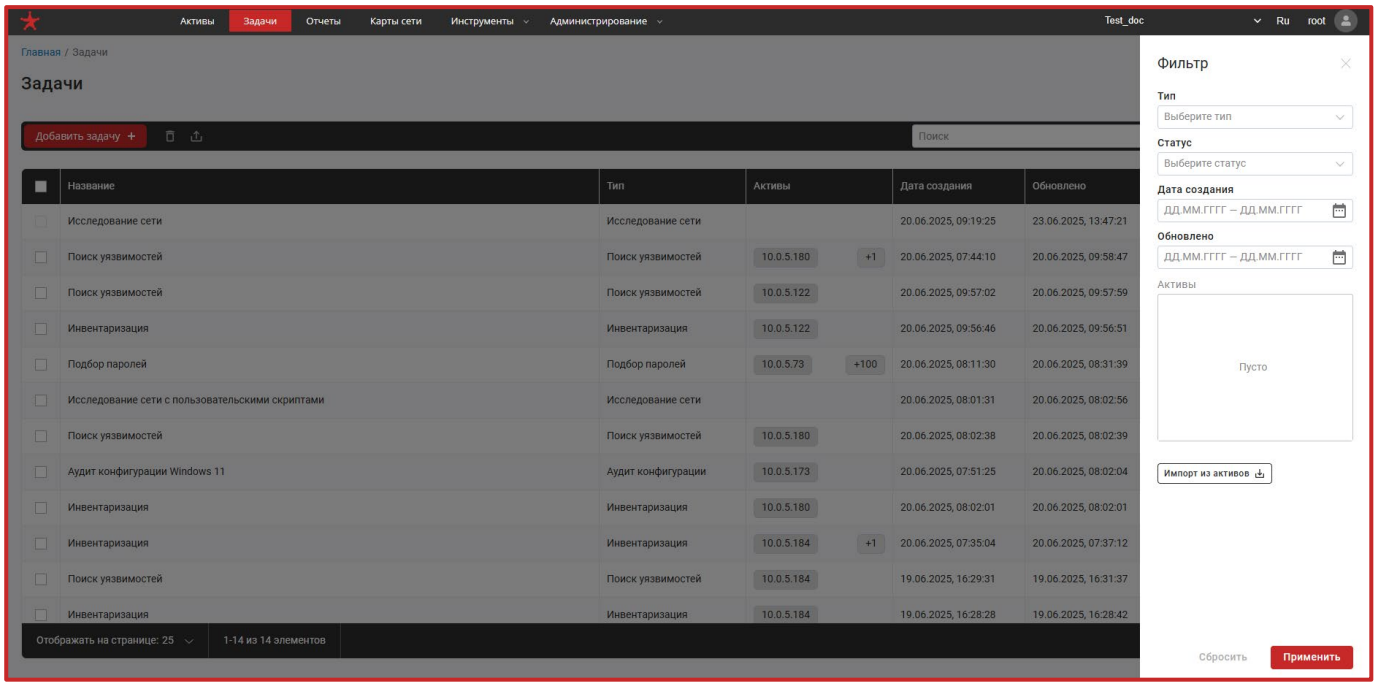


Рис. 6

После применения фильтрации список задач обновится, отобразив только те задачи, в которых используется хотя бы один указанный актив. Если фильтр не применен, столбец «Активы» будет недоступен.

Для сброса фильтра элементов таблицы необходимо повторно нажать на иконку фильтра, после чего, в открывшемся окне фильтра последовательно нажать кнопку «Сбросить» и кнопку «Применить» внизу окна «Фильтр».

5.1.4. Настройка отображения столбцов таблиц

Иконка отображения столбцов таблиц («⚙») предназначена для выбора отображения требуемых колонок выбранной таблицы (рис. 7), а также для выбора колонок (полей), данные из которых, можно скачать из таблицы (см. п. 5.1.2).

Пример настройки отображения столбцов таблицы

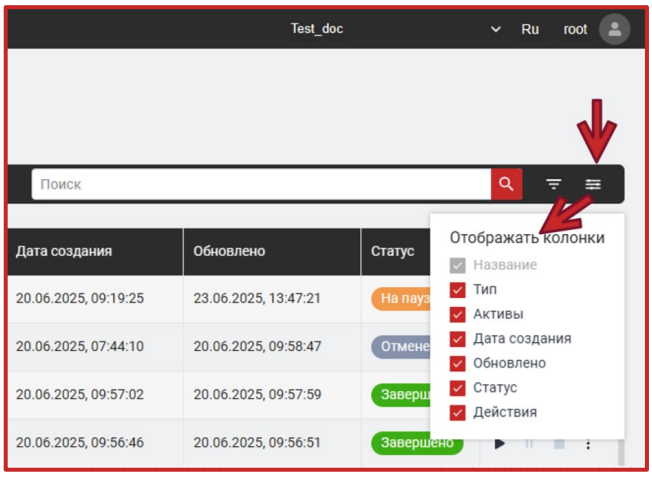


Рис. 7

Выбрать/убрать отображение столбца можно нажатием на его название или поле выбора «☐» рядом с его названием. После чего выбранный столбец отобразится в таблице, а в настройках отображения появится «☑» рядом с добавленным столбцом.

При большом количестве отображаемых в таблицах столбцов информация в ячейках может обрезаться. В таком случае в конце текста отображается троеточие, а при наведении курсора на ячейку, информация в которой не поместилась, в Сканер-ВС отображается всплывающее окно с отображением полной информации текущей ячейки.

5.1.5. Сортировка данных в таблицах

Во всех вкладках Сканер-ВС предусмотрена функция сортировки данных в таблицах по какому-либо критерию. Для сортировки данных необходимо нажать на надпись, соответствующую интересующему параметру в строке заголовка таблицы.

После чего данные в таблице будут отсортированы по этому параметру в порядке убывания. Для сортировки данных по этому же параметру, но в порядке возрастания необходимо повторно нажать на ту же надпись, соответствующую этому параметру.

При третьем нажатии на тот же параметр сортировка возвращается к значению по умолчанию (данные сортируются по дате добавления).

5.1.6. Поиск данных в таблицах

В Сканер-ВС предусмотрена функция поиска по какому-либо заранее известному параметру данных в таблицах каждой функциональной вкладки. Для поиска данных необходимо ввести корректный заранее известный параметр поиска данных, например, для вкладки «Активы» ввести название какого-либо актива в строку поиска на панели навигации. После чего нажать на кнопку поиска.

При нажатии кнопки поиска Сканер-ВС произведет сопоставление введенного параметра всем данным из таблицы и, в случае совпадения параметра данным из таблицы, отобразит только те данные, которые соответствуют условиям поиска. В противном случае в Сканер-ВС отобразится сообщение «Нет данных», что сигнализирует об отсутствии совпадений по введенному параметру.

5.1.7. Управление отображением данных в таблицах

В Сканер-ВС предусмотрен функционал управления отображением данных в таблицах. Этой цели служит нижняя панель в зоне данных таблиц (рис. 8).

Панель управления отображением данных

Рис. 8

Сканер-ВС позволяет оператору:

– настроить количество отображаемых строк в таблице (поле «Отображать на странице» на рис. 8);

– определить количество строк таблицы, отображенных на текущей странице, и общее количество строк (надпись «1-7 из 7 элементов» на рис. 8);

– переходить на интересующую страницу таблицы сразу с одновременной передачей информации об общем количестве страниц (поле «1 из 1 страницы» на рис. 8);

– переходить между страницами таблицы по одной (кнопки «◀» и «▶» на рис. 8).

5.2. Меню управления учетной записью пользователя

5.2.1. О программе

Для ознакомления с информацией о Сканер-ВС предназначен специальный интерфейс, переход к которому осуществляется нажатием на иконку «👤» на панели навигации, и далее в выпадающем списке нажатием пункта «О программе» (рис. 9).

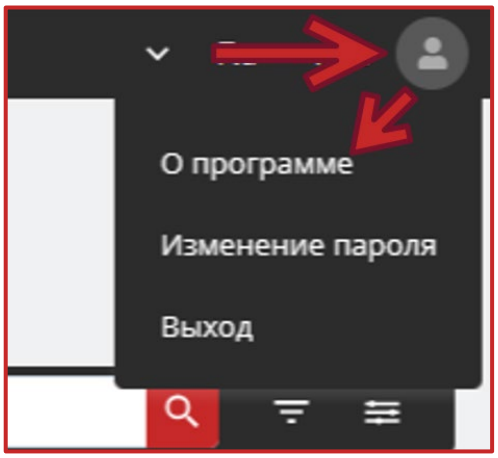


Рис. 9

Окно ознакомления с информацией о продукте представлено на рис. 10.

Окно «О программе»

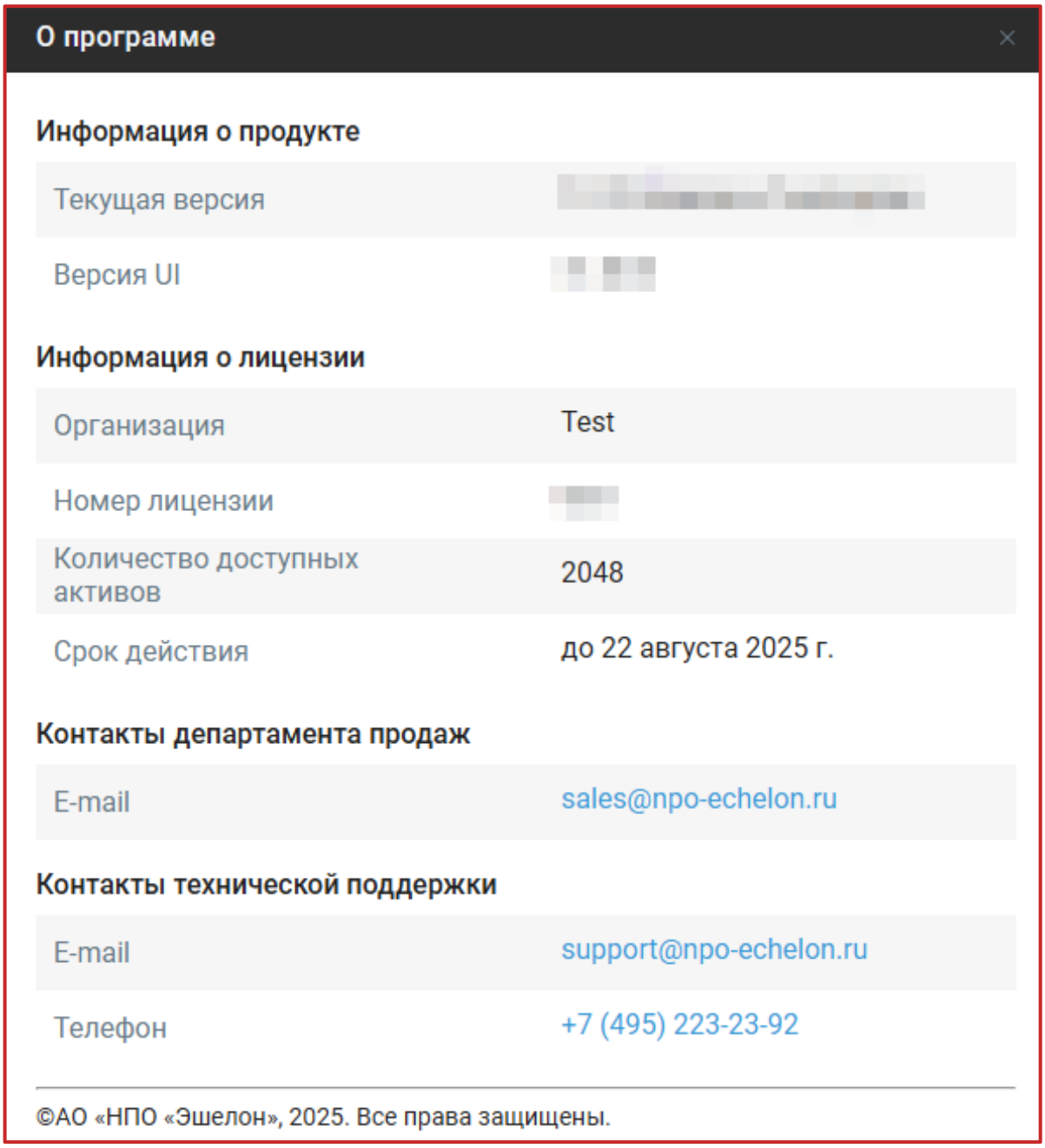


Рис. 10

В окне «О программе» содержатся следующие данные:

– информация о продукте:

а) текущая версия;

б) версия UI.

– информация о лицензии:

а) организация;

б) номер лицензии;

в) количество доступных активов;

г) срок действия.

– контакты департамента продаж:

а) e-mail.

– контакты технической поддержки:

а) e-mail;

б) телефон.

5.2.2. Изменение пароля

В Сканер-ВС предусмотрена функция смены пароля пользователя с ролью «Пользователь». Для смены пароля пользователя необходимо навести курсор на иконку «» на панели навигации, и далее в выпадающем списке выбрать пункт «Изменение пароля» (рис. 11).

Изменение пароля

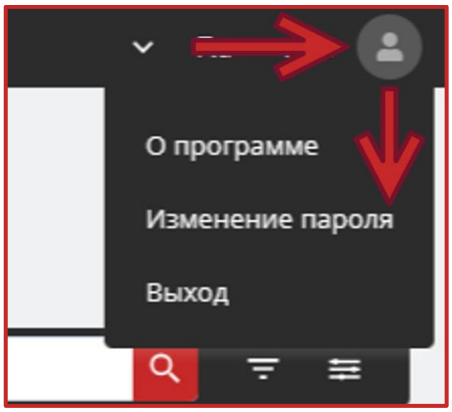


Рис. 11

После перехода в меню смены пароля пользователя в Сканер-ВС отобразится окно «Изменение пароля» (рис. 12).

Окно «Изменение пароля»

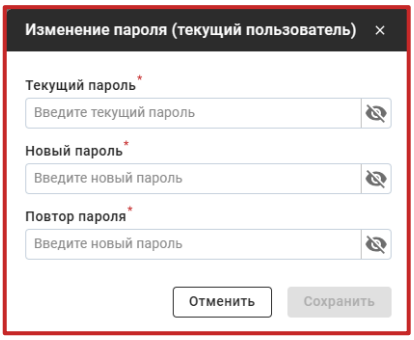


Рис. 12

Для смены пароля пользователя необходимо заполнить все поля, представленные на рис. 12. После чего нажать на кнопку «Сохранить», которая станет активной.

Для отмены смены пароля необходимо нажать на крестик в правом верхнем углу окна или кнопку «Отменить».

Если по каким-либо причинам оператору с ролью «Пользователь» не удается авторизоваться в системе, то это может быть связано с вводом неверного пароля. В таком случае рекомендуется обратиться к своему администратору для сброса пароля.

5.2.3. Выход

Для разрыва текущей сессии пользователя необходимо навести курсор на иконку «  » на панели навигации, и далее в выпадающем списке выбрать пункт «Выход» (рис. 13).

Выход из Сканер-ВС

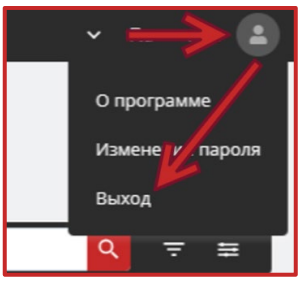


Рис. 13

После чего произойдет разрыв текущей сессии пользователя и переход к окну авторизации Сканер-ВС.

5.3. Проекты

5.3.1. Общее описание

Сканер-ВС всегда функционирует в рамках какого-либо проекта. В том случае, если новый проект никогда не создавался, то функционирование Сканер-ВС происходит в созданном по умолчанию проекте.

Проекты позволяют оператору систематизировать активы по какому-либо критерию и в последствии проводить задачи, выполняемые Сканер-ВС не для всей сети сразу, а для отдельных групп ее активов.

Для выбора проекта необходимо нажать на поле с названием текущего проекта (см. рис. 3 – «Проект_01»). При этом откроется выпадающий список доступных для выбора избранных проектов (рис. 14).

Выбор проекта

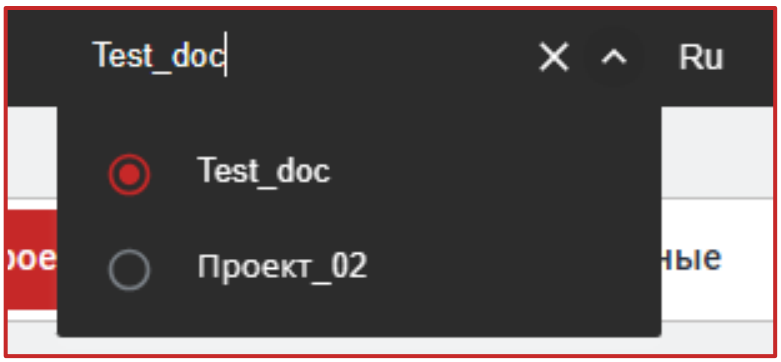


Рис. 14

Для быстрого выбора проекта из избранных для последующей работы необходимо нажать на строку с названием проекта. Пустой кружок закрасится красным цветом, а в окне с надписью «Выберите проект» отобразится название выбранного проекта. При переключении между проектами Сканер-ВС автоматически переходит к вкладке «Активы» (п. 5.4 настоящего документа) выбранного проекта с обновлением страницы.

Проект представляет собой совокупность всех данных, относящихся к текущему тестированию. Проект включает в себя информацию о данных тестирования (активы, уязвимости) и результаты тестирования (сгенерированные отчеты), а также оценку влияния уязвимостей на информационные системы на основе показателя ФСТЭК согласно методическому документу ФСТЭК России «Методика оценки уровня критичности уязвимостей программных и программно-аппаратных средств», утвержденному 28 октября 2022 года.

Для расчета оценки влияния уязвимостей на информационные системы на основе показателя ФСТЭК необходимо предварительно провести задачу «Поиск уязвимостей» (см. п. 5.5.5) для активов каждого проекта. Далее необходимо перейти во вкладку «Проекты» – данная оценка обновится автоматически.

Для перехода к вкладке «Проекты» необходимо нажать на меню «Инструменты» и в открывшемся списке выбрать пункт «Проекты» (рис. 15).

Переход ко вкладке «Проекты»

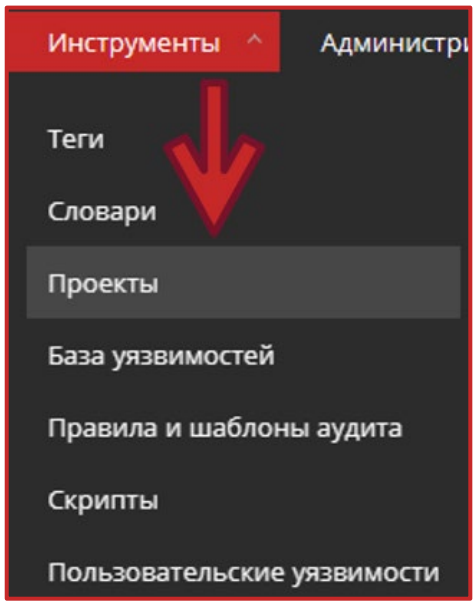


Рис. 15

После выбора пункта «Проекты» в Сканер-ВС отобразится вкладка «Проекты» (рис. 16). Для проведения тестирования пользователь может создать новый проект или использовать существующий.

Вкладка «Проекты»

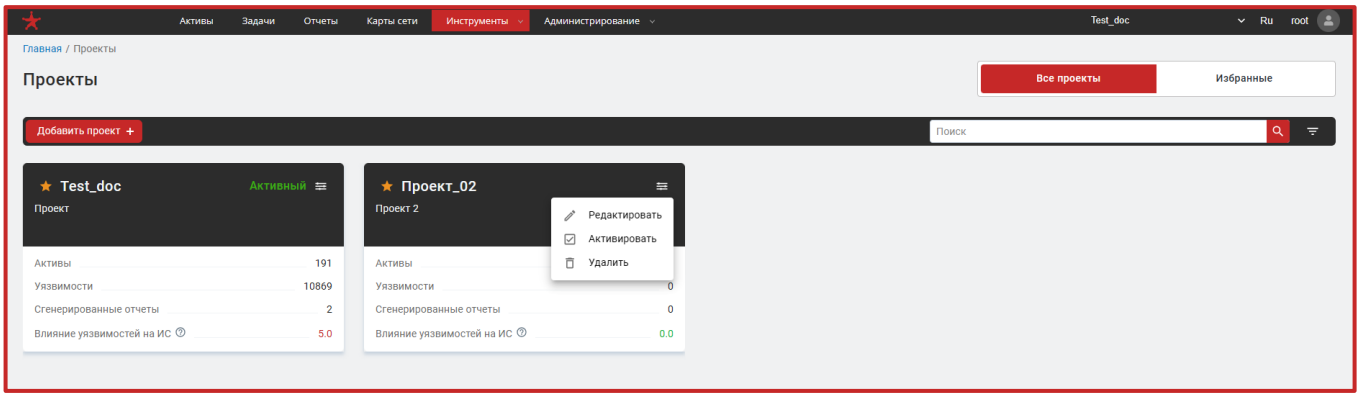


Рис. 16

Функции управления проектами в Сканер-ВС доступны для учетных записей операторов с ролями «Пользователь» и «Администратор».

В рамках управления проектами пользователь может использовать следующие функции:

– создание проекта (п. 5.3.2 настоящего документа);

– редактирование проекта (п. 5.3.3 настоящего документа);

– удаление проекта (п. 5.3.4 настоящего документа);

– выбор проекта в качестве активного для текущей сессии (п. 5.3.5 настоящего документа);

– сортировка отображения проектов « » (п. 5.3.6 настоящего документа).

В Сканер-ВС предусмотрена возможность управления отображением проектов. В верхнем правом углу вкладки «Проекты» можно выбрать какие проекты отображать из следующих вариантов:

– все проекты;

– избранные.

Для отображения всех проектов необходимо нажать на кнопку «Все проекты», для отображения только избранных – на кнопку «Избранные». Добавление проекта в избранные происходит кликом левой кнопки мыши на звездочку в левом верхнем углу карточки проекта рядом с названием проекта (рис. 17).

Карточка проекта

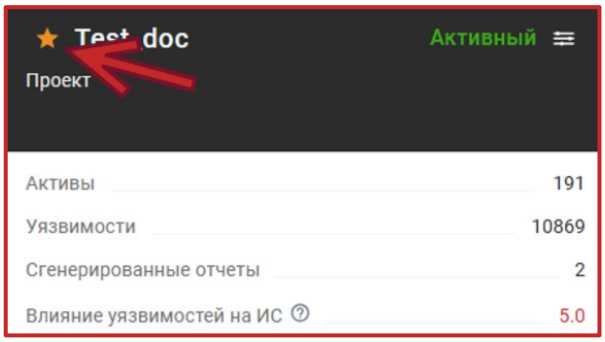


Рис. 17

После клика на звездочку проект добавится в избранные, а звездочка закрасится.

5.3.2. Создание проекта

Для создания нового проекта необходимо нажать на кнопку «Добавить проект +». При нажатии на кнопку «Добавить проект +» откроется окно «Добавление проекта» (рис. 18).

Окно «Добавление проекта»

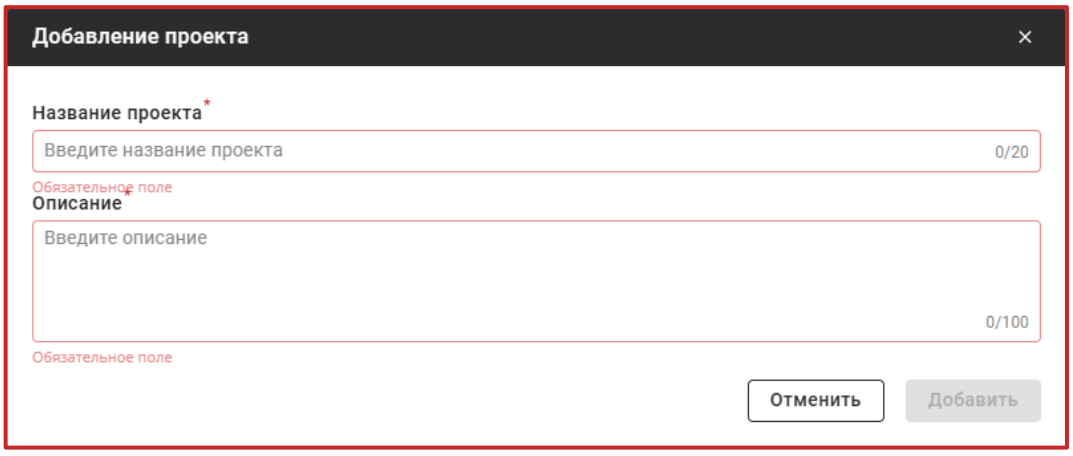


Рис. 18

Наименование проекта записывается в поле «Название проекта» и должно быть уникальным для каждого проекта. Поле «Описание» служит для удобства идентификации проектов. Оба поля являются обязательными для заполнения.

5.3.3. Редактирование проекта

Для редактирования проекта необходимо кликнуть левой кнопкой мыши на значок настроек «  » в правом верхнем углу проекта, который предстоит изменить, и во всплывшем окне нажать «Редактировать» (рис. 16).

При нажатии на «Редактировать» откроется окно редактирования проекта (рис. 19).

Окно «Редактирование проекта»

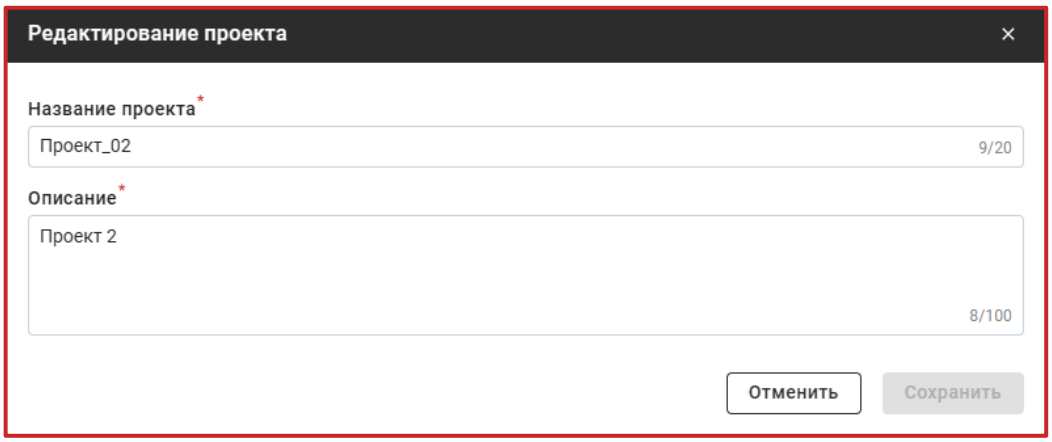


Рис. 19

После внесения изменений в название или описание проекта необходимо нажать на кнопку «Сохранить», которая станет активной для подтверждения внесенных изменений. В противном случае необходимо нажать кнопку «Отменить».

5.3.4. Удаление проекта

Для удаления проекта необходимо кликнуть левой кнопкой мыши на значок настроек «  » в правом верхнем углу проекта, который предстоит удалить, и во всплывшем окне нажать «Удалить» (рис. 16).

При нажатии «Удалить» Сканер-ВС отобразит всплывающее окно подтверждения удаления проекта. Для удаления проекта необходимо нажать на кнопку «Удалить», в противном случае – «Отменить». После подтверждения удаления проекта в Сканер-ВС отобразится сообщение об успешном его удалении.

5.3.5. Выбор проекта в качестве активного

В Сканер-ВС предусмотрена возможность выбора проекта в качестве активного (в рамках которого будет производится дальнейшая работа) не только из списка избранных проектов, но и со вкладки «Проекты» меню «Инструменты».

Для выбора проекта необходимо кликнуть левой кнопкой мыши на значок настроек « » в правом верхнем углу проекта, и во всплывшем окне нажать «Активировать» (рис. 16).

5.3.6. Сортировка отображения проектов

В Сканер-ВС предусмотрена функция сортировки отображения проектов по следующим критериям (рис. 20):

– сначала избранные;

– сначала новые;

– сначала старые.

Сортировка проектов

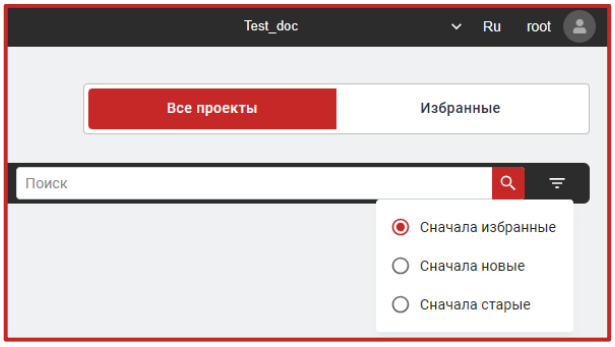


Рис. 20

Помимо настраиваемой сортировки проектов в Сканер-ВС предусмотрена автоматическая сортировка по избранным проектам. Проекты, помеченные пользователем как избранные отображаются первыми, т.е. при отображении всех проектов в таблице проектов – слева и сверху будут отображаться сначала избранные проекты, а уже за ними все остальные с учетом критериев ручной сортировки, заданной оператором.

5.4. Активы

Актив в контексте информационной безопасности – это сущность (сетевой узел рассматриваемой сети), имеющая ценность для организации, использующаяся для достижения целей организации, являющаяся объектом защиты и атаки с целью нарушения свойств безопасности.

В Сканер-ВС используется понятие информационного актива, под которым понимается конечное или сетевое устройство, имеющее IP-адрес в локальной вычислительной сети.

5.4.1. Общее описание

Перед началом работы обязательным этапом является поиск целей – обзор локальной сети, к которой подключен Сканер-ВС, с целью выявления объектов тестирования для следующих фаз проверки. Поиск целей производится путем сканирования IP-адресов и портов (TCP- и UDP-портов) устройств, присоединенных к локальной сети. Без поиска невозможно использовать все функции Сканер-ВС, в частности, невозможно использовать поиск уязвимостей (п. 5.5.5 настоящего документа). Найденные в результате данного исследования сети (п. 5.5.3 настоящего документа) цели будут называться «Активы».

Каждому активу присваивается свой уникальный набор параметров, получаемых в ходе выполнения задач Сканер-ВС. Параметры активов располагаются во вкладке «Активы» в виде таблицы (рис. 21).

Активы можно добавлять ручным методом, процесс добавления нового актива описан в п. 5.4.4 настоящего документа.

Вкладка «Активы»

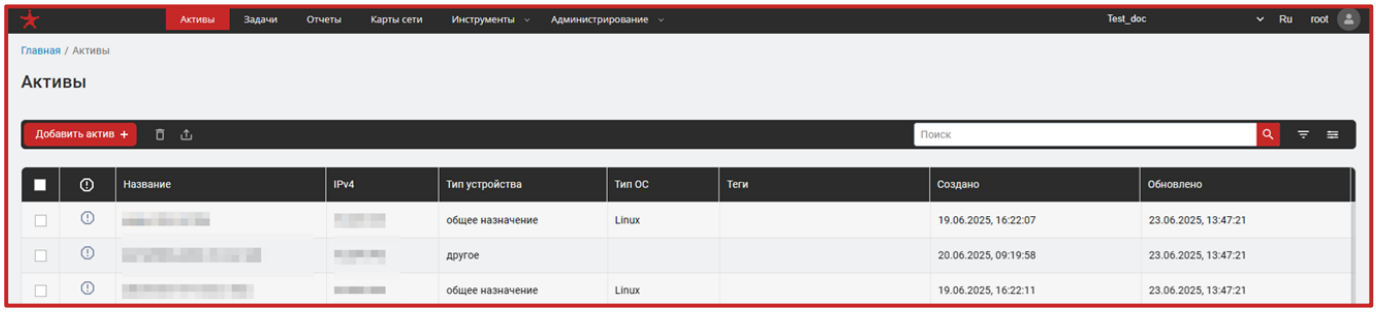


Рис. 21

5.4.2. Описание интерфейса

Интерфейс вкладки «Активы» условно можно разделить на три зоны (рис. 22):

1) «Зона управления активами»;
2) «Зона с заголовком таблицы активов»;
3) «Зона данных активов».

Деление на условные зоны вкладки «Активы»

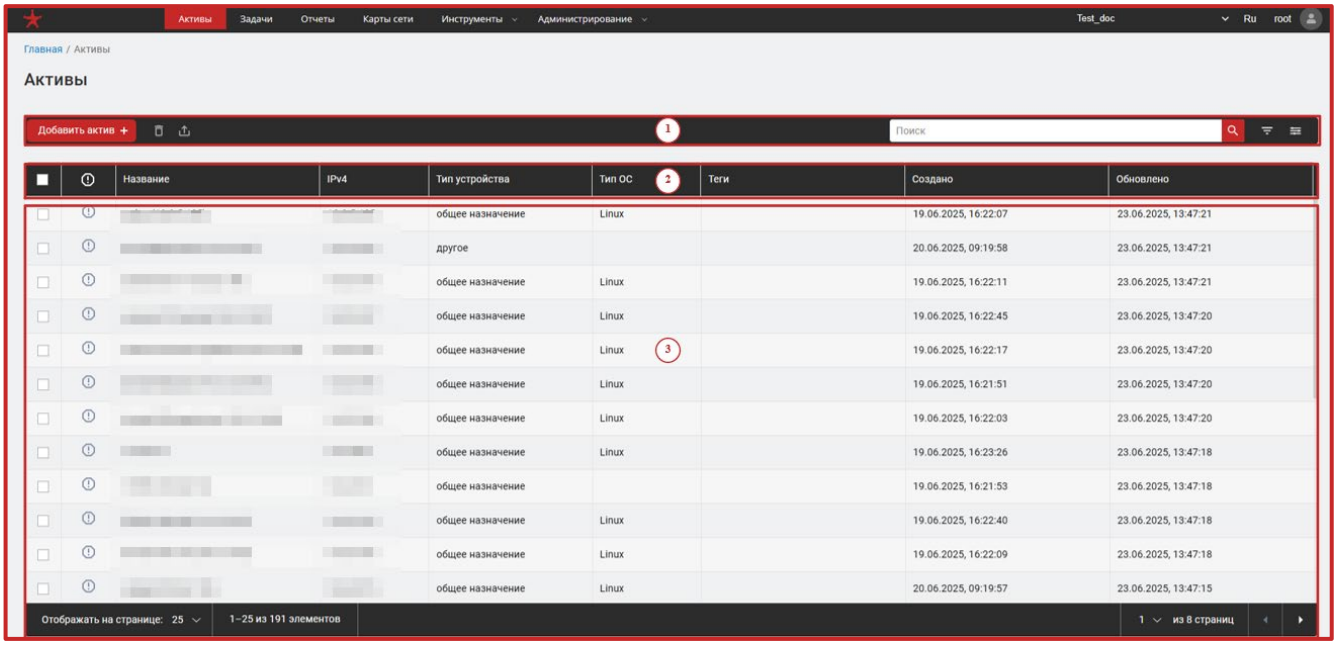


Рис. 22

5.4.3. Управление активами

Данная зона предназначена для управления активами. С ее помощью можно добавлять, удалять или экспортировать активы. Кнопки «Экспортировать в .csv» (иконка «⬆») и «Удалить» по умолчанию скрыты. Для их отображения необходимо выбрать один или несколько активов из зоны дынных активов путем однократного нажатия на поле выбора « ☐ » рядом с названием интересующего(их) актива(ов). После чего в настройках отображения появится « ☑ » рядом с выбранным(и) активом(ами).

Пример выбора нескольких из доступных активов представлен на рис. 23.

Выбор нескольких активов

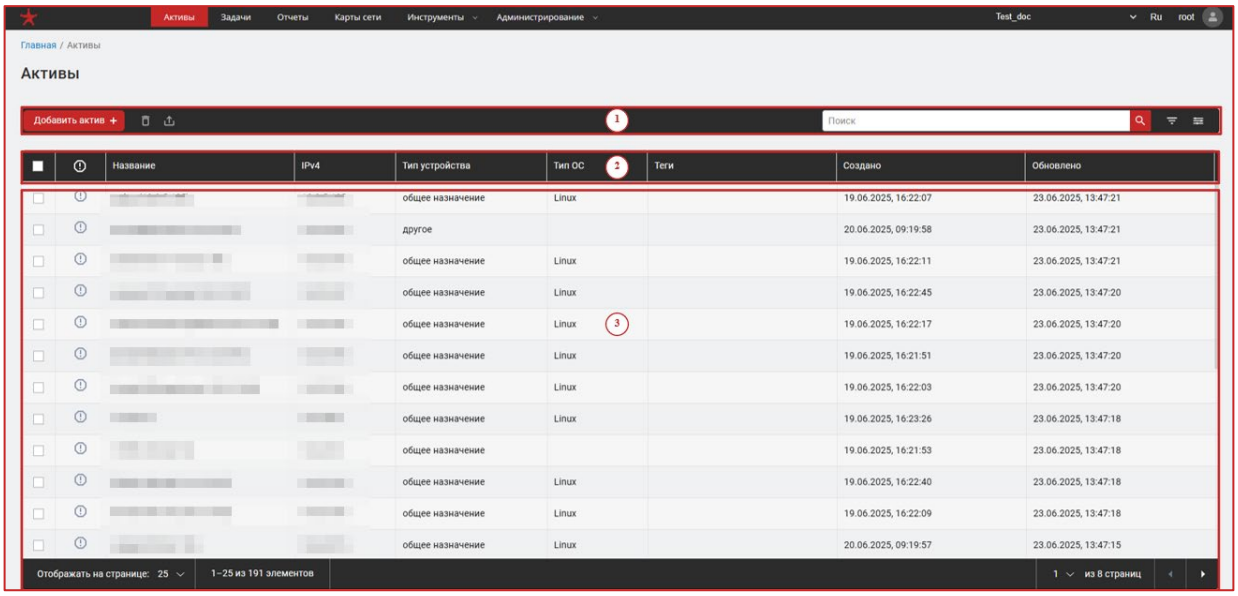


Рис. 23

Как видно из рис. 23, после выбора некоторых активов из списка отображаются кнопки «Экспортировать в .csv» и «Удалить». При нажатии на иконку «⬆» происходит экспорт данных из таблиц (п. 5.1.2 настоящего документа). При нажатии на кнопку «Удалить» отображается всплывающее окно с подтверждением удаления выбранных активов (рис. 24).

Подтверждение удаления активов

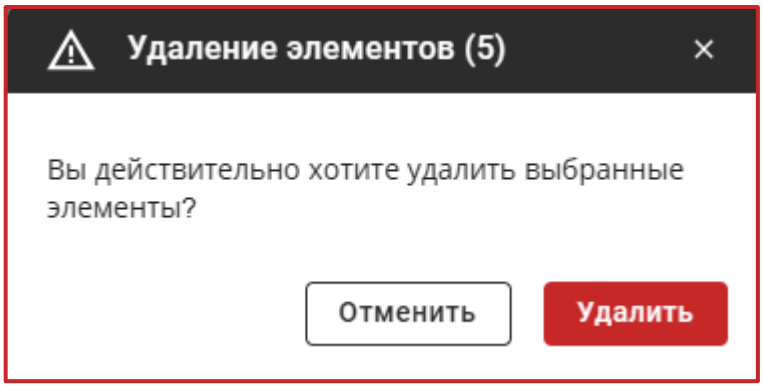


Рис. 24

Для удаления выбранных активов необходимо нажать на кнопку «Удалить», в противном случае – «Отменить».

Описание функциональных кнопок представлено в таблице 3.

5.4.3.1. Зона с заголовком таблицы активов

По умолчанию данная таблица включает в себя минимально необходимые столбцы для работы. Остальные столбы не отображаются (скрыты). Для отображения необходимых вам столбцов воспользуетесь настройкой (иконка «  ») в зоне функциональных кнопок для работы с активами.

Описание зоны с заголовком таблицы активов представлено в таблице 4.

Таблица 4 – Заголовок таблицы активов

№	Наименование	Описание актива
1	FQDN	FQDN актива. FQDN – полностью определенное имя домена, не имеющее неоднозначностей в определении
2	IPv4	IP-адрес (IPv4) актива. IP-адрес (IPv4) – запись в виде 4-х десятичных чисел (от 0 до 255), разделенных точками
3	IPv6	IP-адреса (IPv6) актива. IP-адрес (IPv6) – как правило, адрес записывается в виде восьми четырехзначных шестнадцатеричных чисел (от 0 до 9 и от A до F) разделенных двоеточиями
4	MAC	MAC-адреса актива. MAC-адрес – это уникальный идентификатор, который присваивается каждой единице сетевого оборудования и позволяет идентифицировать каждую точку подключения, каждый узел сети
5	Имя хоста	Hostname актива. Hostname – это имя, которое присваивается компьютеру
6	Тип устройства	Тип устройства актива. Категории: сервер, рабочая станция, межсетевой экран, маршрутизатор, принтер, VoIP-адаптер, WAP, другое, камера, виртуальная машина, общее назначение, мост, широкополосный маршрутизатор, игровая приставка, концентратор, балансировщик нагрузки, мультимедийное устройство, АТС, КПК, телефон, устройство питания, сервер печати, прокси-сервер, удалённое управление, устройство безопасности, специализированное, устройство хранения, коммутатор, устройство телекоммуникации, терминал, терминальный сервер, VoIP-телефон
7	Тип ОС	Тип ОС актива. Классификация типа ОС: – Не выбрано; – Windows; – Linux; – MacOS.
8	Теги	Пользовательские теги актива

№	Наименование	Описание актива
9		Уровень критичности актива. Задается пользователем и отражает важность (ценность) данного актива для инфраструктуры. Категории: – уровень критичности не определен; – низкая критичность; – средняя критичность; – высокая критичность.
10	Создано	Дата и время создания актива
11	Обновлено	Дата и время обновления информации об активе

5.4.3.2. Зона данных активов

Зона данных представляет собой таблицу с указанием данных активов, где каждая строка – это различные данные одного актива, а каждый столбец – тип данных, относящиеся к заголовку данной таблицы.

5.4.4. Добавление актива

Для добавления актива необходимо:

1) зайти на вкладку «Активы»;

2) нажать кнопку «Добавить актив» (рис. 25);

3) заполнить поля нового актива и нажать на кнопку «Создать», которая станет активной после заполнения необходимых полей (рис. 26).

Добавление нового актива

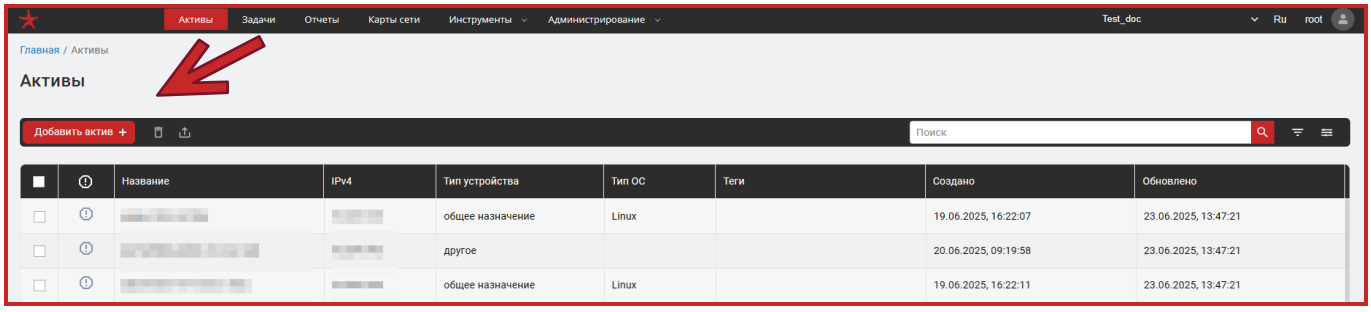


Рис. 25

Форма заполнения данных нового актива

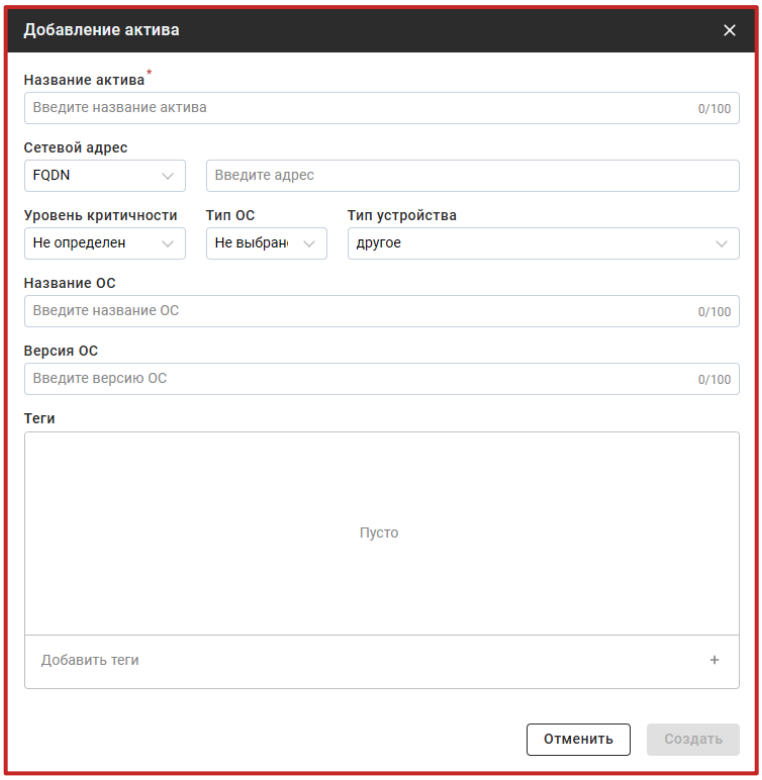


Рис. 26

Как видно из рис. 26, обязательными для заполнения являются поля «Название актива» и «Сетевой адрес». Описание параметров добавляемого актива приведено в таблице 4.

При добавлении нового актива в Сканер-ВС предусмотрены следующие варианты присвоения активу сетевого адреса:

– FQDN;

– IPv4;

– IPv6.

В Сканер-ВС предусмотрена возможность установки уровня критичности активу при его создании. Уровни критичности могут быть следующими:

– не определен (устанавливается по умолчанию);

– низкий;

– средний;

– высокий.

Помимо уровня критичности для добавляемого актива можно выбрать тип ОС из следующих вариантов:

– не выбрано (устанавливается по умолчанию);

– Windows;

– Linux;

– MacOS.

Так же в Сканер-ВС есть возможность указать тип устройства для добавляемого актива из множества представленных на данной странице вариантов.

В данном окне также предусмотрено дополнительное поле для добавления тега к создаваемому активу, которое позволит в дальнейшем, при использовании Сканер-ВС, категорировать актив по какому-либо заданному оператором критерию.

5.4.5. Карточка актива

5.4.5.1. Общее описание

При нажатии на актив открывается карточка актива, представляющая собой перечень вкладок, в каждой из которых отображается информация об определенных характеристиках актива (рис. 27), а именно:

1) «Информация»;

2) «Порты»;

3) «Прикладное ПО»;

4) «Уязвимое ПО»;

5) «Подключения».

Карточка актива

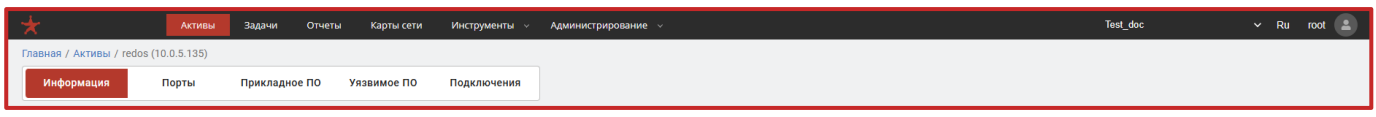


Рис. 27

5.4.5.2. Вкладка «Информация»

Данная вкладка карточки актива представляет собой полную информацию об активе (рис. 28). Она необходима для более наглядного представления данных о конкретном активе, а также для возможности их редактирования.

Вкладка «Информация» карточки актива ОС Linux

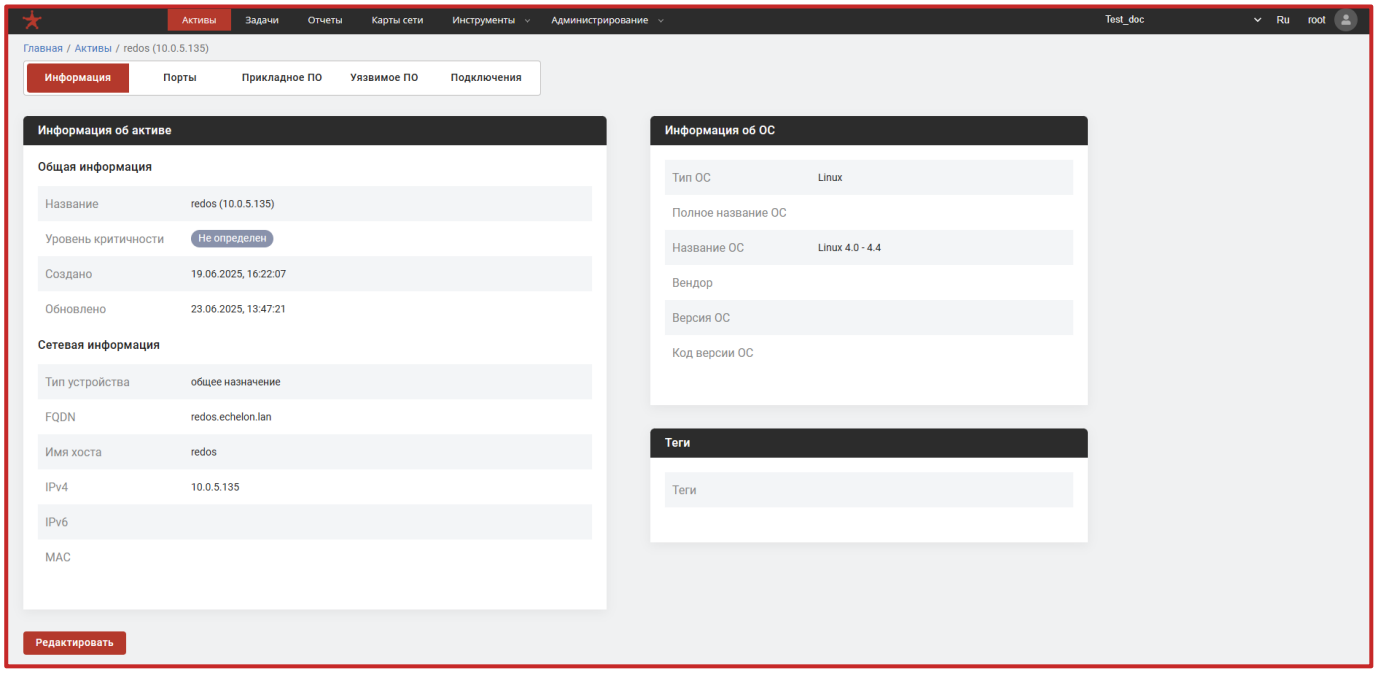


Рис. 28

В том случае, если в карточке актива, к которому применен тег, нажать на этот тег, то произойдет переход к вкладке «Активы», а данные в этой вкладке будут отображены с учетом фильтрации по выбранному тегу.

В карточке актива, функционирующего на базе ОС Windows, предусмотрено дополнительное окно «Установленные обновления» на вкладке «Информация» (рис. 29), отображающее установленные на данном активе обновления, информация о которых появляется после проведения задачи «Инвентаризация (п. 5.5.4 настоящего документа).

Вкладка «Информация» карточки актива ОС Windows

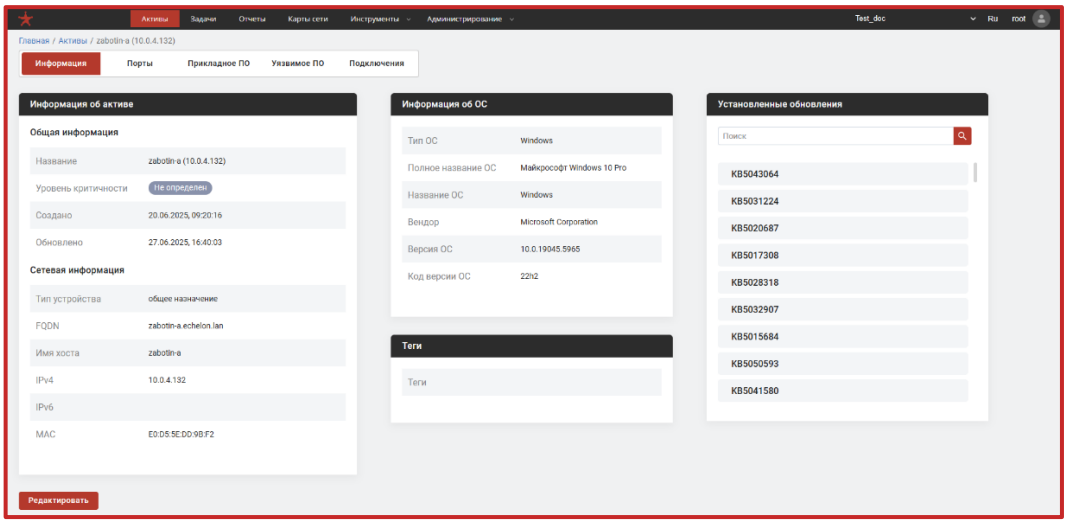


Рис. 29

5.4.5.3. Редактирование карточки актива

Изменение информации об активе позволяет своевременно и быстро производить исправление устаревшей или неправильной информации, а также дополнять ее.

Для изменения информации необходимо:

1) на вкладке «Информация» нажать на кнопку «Редактировать» (рис. 30);

Переход к редактированию информации об активе

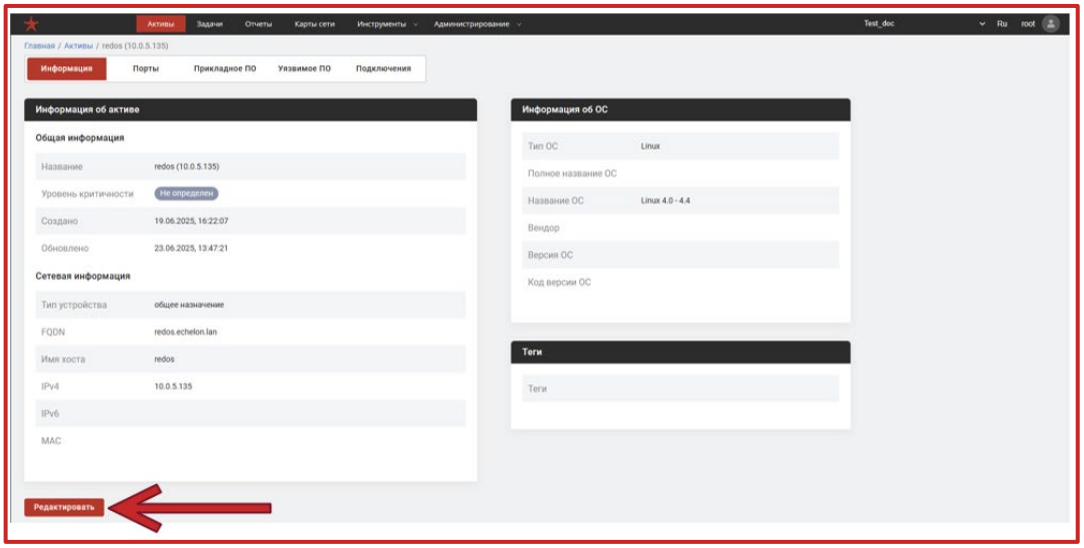


Рис. 30

2) в открывшемся окне (рис. 31) изменить необходимые поля;

Окно редактирования информации об активе

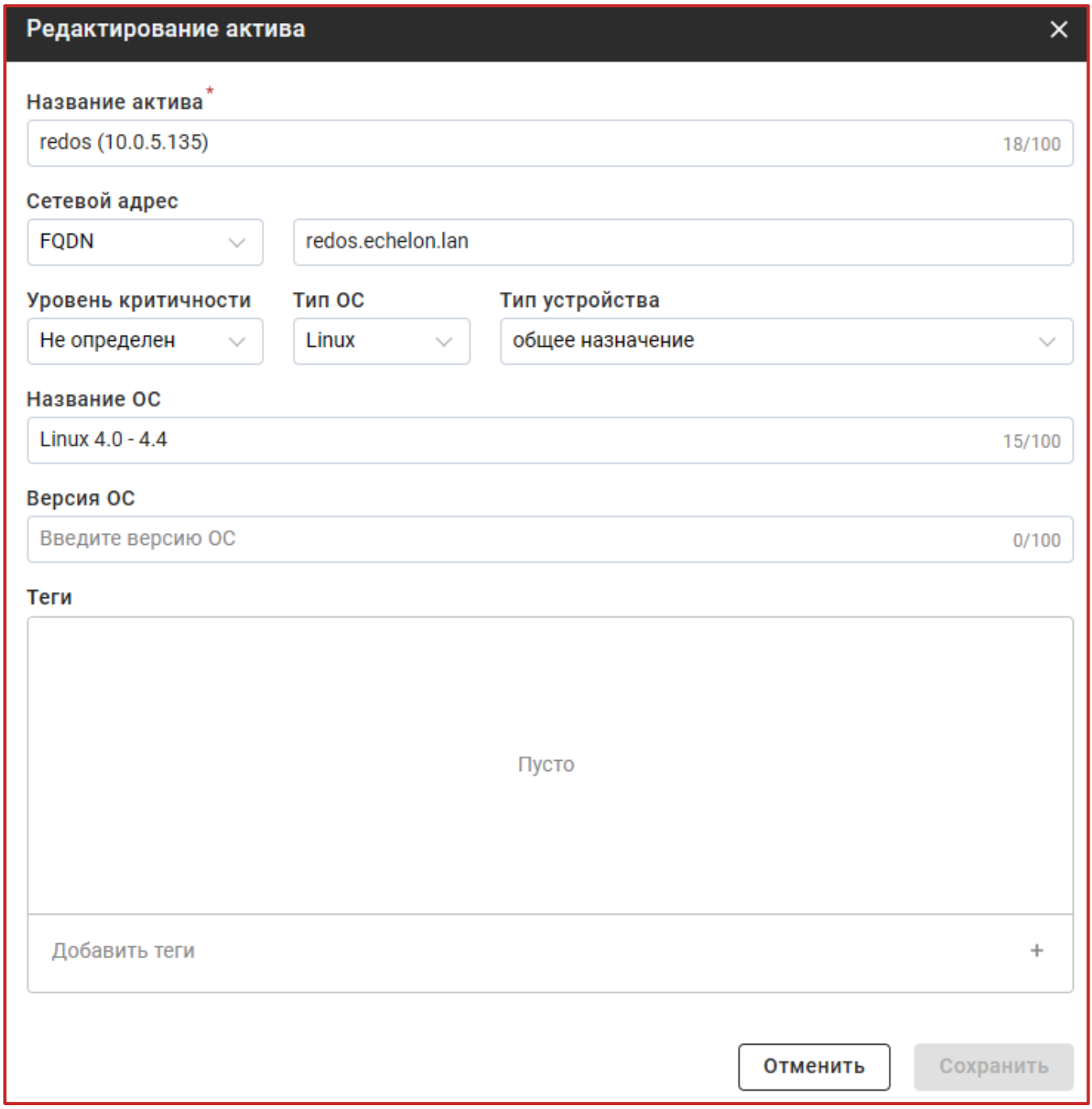


Рис. 31

3) нажать кнопку «Сохранить»;

Примечание. Кнопка «Сохранить» до внесения изменений будет заблокирована, о чем свидетельствует ее серый цвет.

4) перейти в карточку измененного актива и проверить изменения.

5.4.5.4. Порты

После завершения задачи «Исследования сети» (с включенным параметром «Сканирование портов») для указанных активов во вкладку «Порты» добавится информация по открытым портам в столбцы: «Порт», «Состояние» и «Сервис» (рис. 32).

Вкладка «Порты»

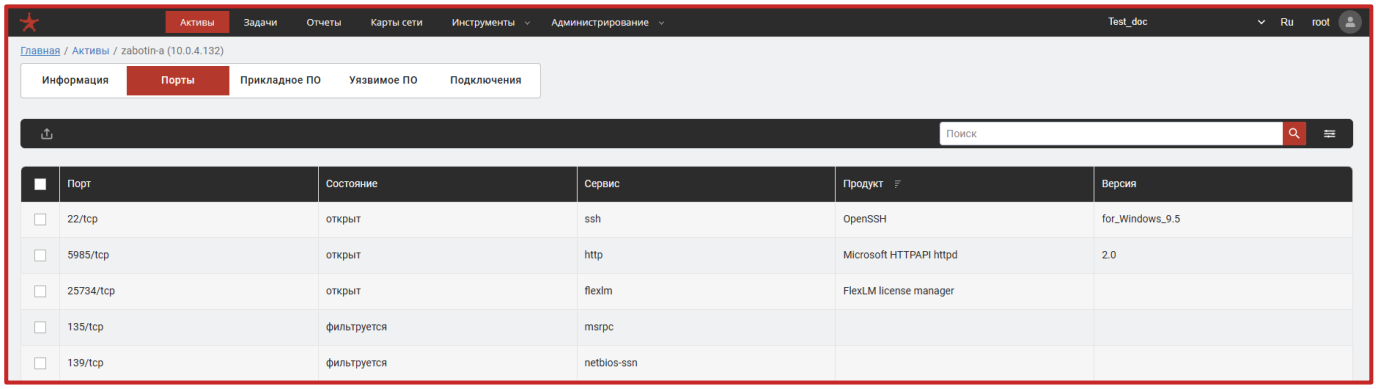


Рис. 32

Остальные данные о запущенных сервисах, продуктах, номерах версий можно получить, воспользовавшись функционалом задачи «Инвентаризация» (п. 5.5.4 настоящего документа) с включенным параметром «Сканирование портов».

5.4.5.5. Прикладное ПО

После завершения задачи «Исследование сети» по активам (п. 5.5.3 настоящего документа) (с включенным параметром «Сканирование портов») в данной вкладке отображается информация об установленном на активе прикладном ПО (рис. 33).

Дополнительную, а также более подробную информацию предоставляет выполнение задачи «Инвентаризация» по активам (п. 5.5.4 настоящего документа).

Вкладка «Прикладное ПО»

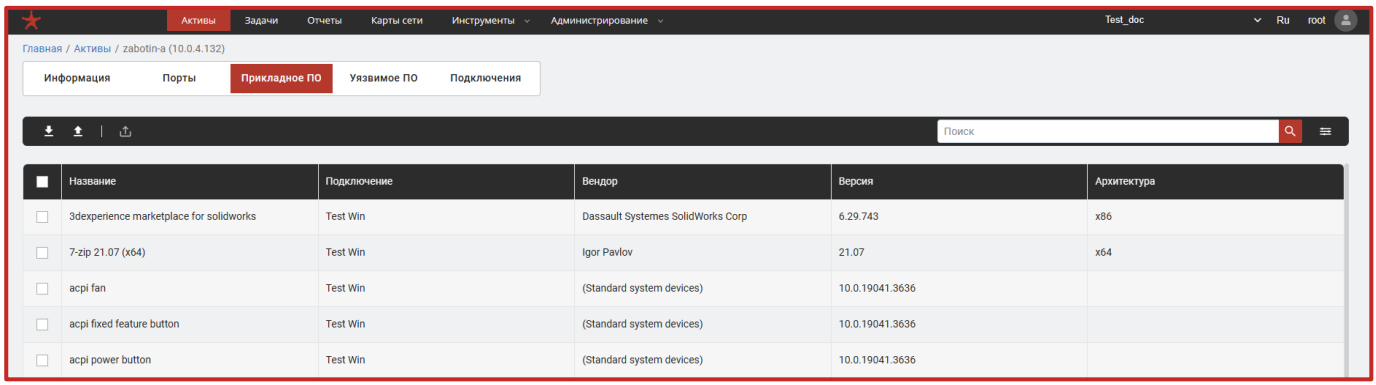


Рис. 33

На вкладке «Прикладное ПО» карточки актива отображается таблица со следующей информацией о программном обеспечении, установленном на исследуемом активе:

– «Название» – полное наименование найденного программного обеспечения;

– «Подключение» – наименование подключения актива;

– «Вендор» – наименование организации-поставщика найденного программного обеспечения;

– «Версия» – версия программного обеспечения при исследовании данного актива;

– «Архитектура» – сведения об архитектуре программного обеспечения.

На вкладке «Прикладное ПО» Сканер-ВС так же представлены иконки, обеспечивающие выполнение следующих функций:

– « » – кнопка «Скачать данные в формате CycloneDX», которая предназначена для выполнения функции экспорта списка ПО актива в формате SBOM CycloneDX, автоматически конвертируя и сопоставляя общие поля актива и компонентов, а также обрабатывая зависимости между программными пакетами для обеспечения полной совместимости с указанным стандартом;

– « » – кнопка «Загрузить данные в формате CycloneDX», которая предназначена для выполнения функции импорта списка ПО актива в формате SBOM CycloneDX;

– «  » – кнопка «Экспортировать в .csv», которая предназначена для экспорта выбранных данных из таблицы в формате «.csv» на текущий АРМ.

Примечания:

1. CycloneDX – это открытый стандарт для обмена информацией о составе ПО, который используется для анализа уязвимостей и управления безопасностью цепочки поставок за счет детального описания компонентов и их зависимостей.

2. Программные пакеты (список ПО актива) могут быть обнаружены с помощью задачи «Исследование сети», однако в этом случае список будет ограничен **только сетевыми программными пакетами**, выявленными на открытых портах. Для получения полного перечня установленного программного обеспечения рекомендуется выполнить задачу «Инвентаризация» с включенной опцией «Установленное программное обеспечение» (см. п. 5.5.4.2 настоящего документа).

5.4.5.6. Уязвимое ПО

После завершения задачи «Поиск уязвимостей» по активам (п. 5.5.5) во вкладке «Уязвимое ПО» исследованных активов появится информация об уязвимостях (рис. 34).

Вкладка «Уязвимое ПО» в карточке актива

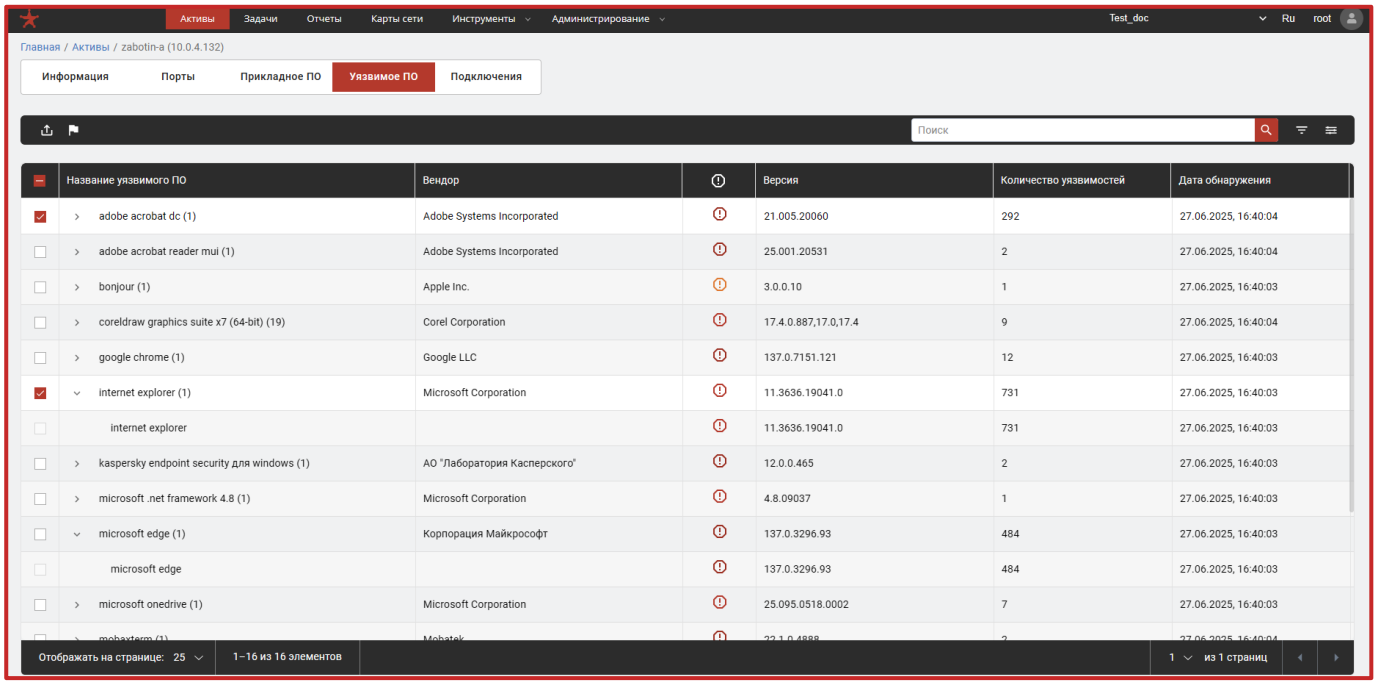


Рис. 34

На вкладке «Уязвимое ПО» Сканер-ВС отображены группы найденных уязвимых пакетов. Группировка пакетов в группы происходит по найденным уязвимостям в пакетах. Для просмотра уязвимых пакетов, входящих в состав группы необходимо нажать на иконку «›» слева от названия группы или в любом месте соответствующей строки таблицы. После чего раскроется группа найденных уязвимых пакетов (рис. 35).

Примечание. В столбце «Количество уязвимостей» указывается наибольшее количество уязвимостей среди пакетов, входящих в состав группы.

Уязвимые пакеты, входящие в состав группы

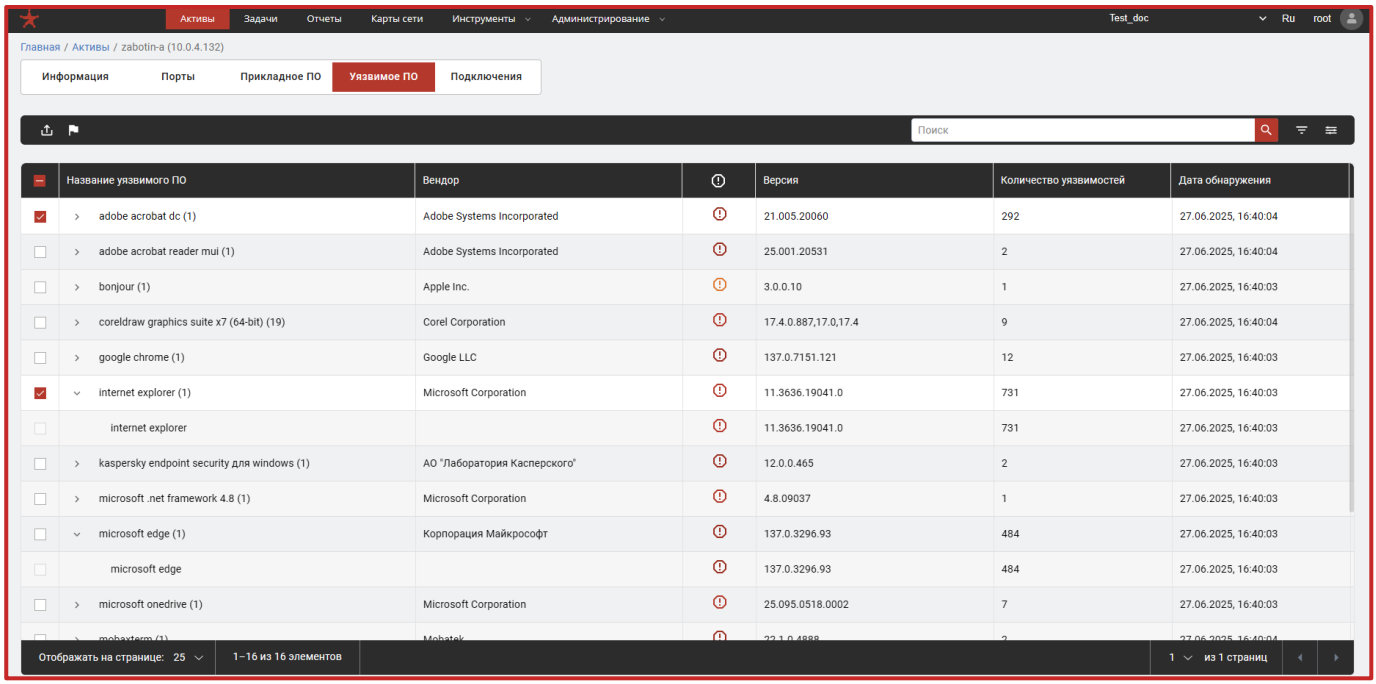


Рис. 35

Во вкладке «Уязвимое ПО» карточки актива предусмотрена возможность отметки целой группы найденных уязвимых пакетов ложной. Для отметки группы или нескольких групп уязвимых пакетов ложными необходимо выбрать отмечаемые группы и нажать на отобразившуюся иконку «⚑». После чего в отобразившемся окне подтверждения нажать «Подтвердить» для подтверждения внесения изменений, «Отменить» – для отмены.

После отметки группы уязвимых пакетов ложными в таблице уязвимого ПО отобразится значок ложных уязвимостей для отмеченных групп (рис. 36) и все пакеты, входящие в отмеченные группы, а также уязвимости в этих пометках будут отмечены ложными. При этом в карточке уязвимости отобразится сообщение «Отмечена ложной в рамках группы <имя группы>», где <имя группы> – наименование группы, которая была отмечена ложной.

Для отмены отметки группы уязвимостей ложными необходимо нажать на флажок слева от интересующей группы.

Отметка группы уязвимых пакетов ложными

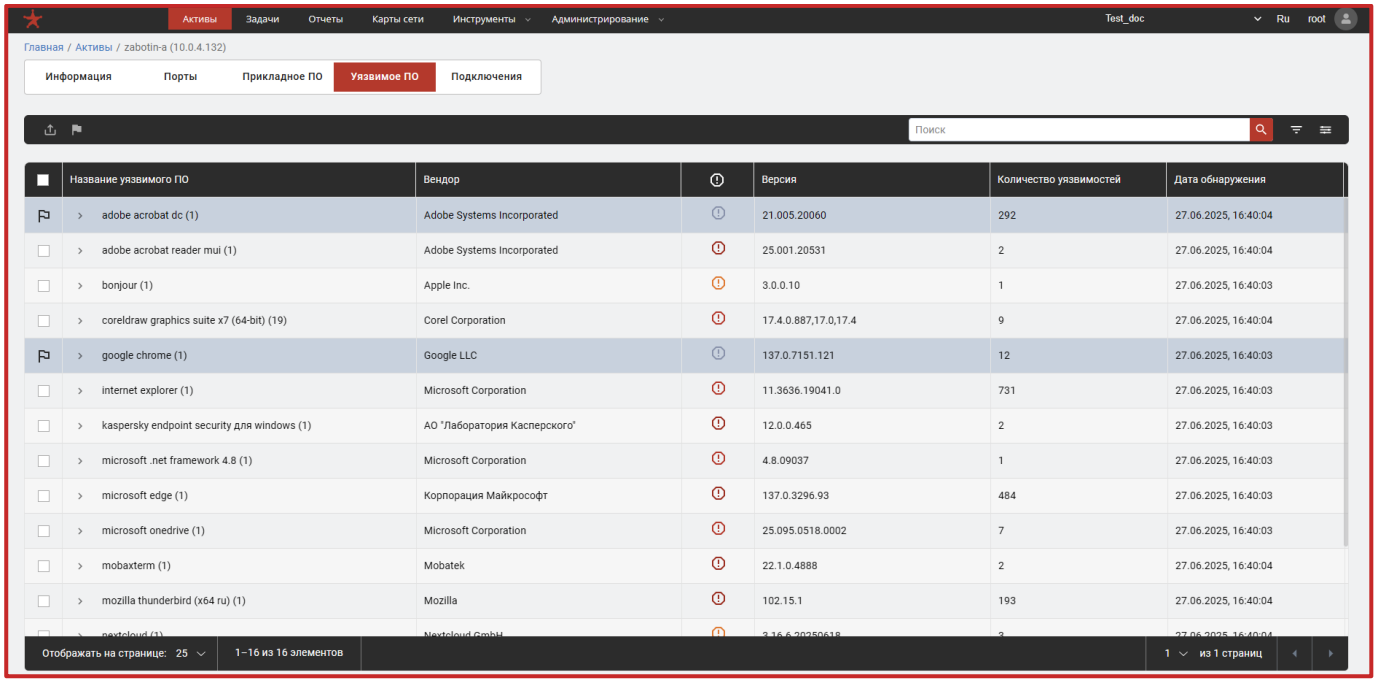


Рис. 36

Для просмотра всех найденных для конкретного ПО уязвимостей необходимо нажать на строку таблицы уязвимого ПО, после чего произойдет переход к таблице, содержащей полную информацию о найденных уязвимостях данного ПО (рис. 37), которые при необходимости можно экспортировать в формате «.csv» с помощью кнопки «⭱».

Таблица уязвимостей конкретного ПО актива

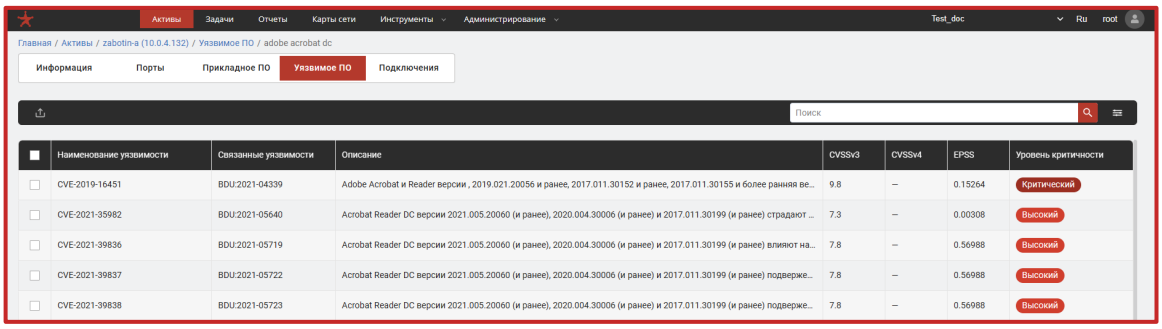


Рис. 37

Кликнув на уязвимость, можно перейти к более подробному ее описанию (карточке уязвимости) (рис. 38).

Карточка уязвимости

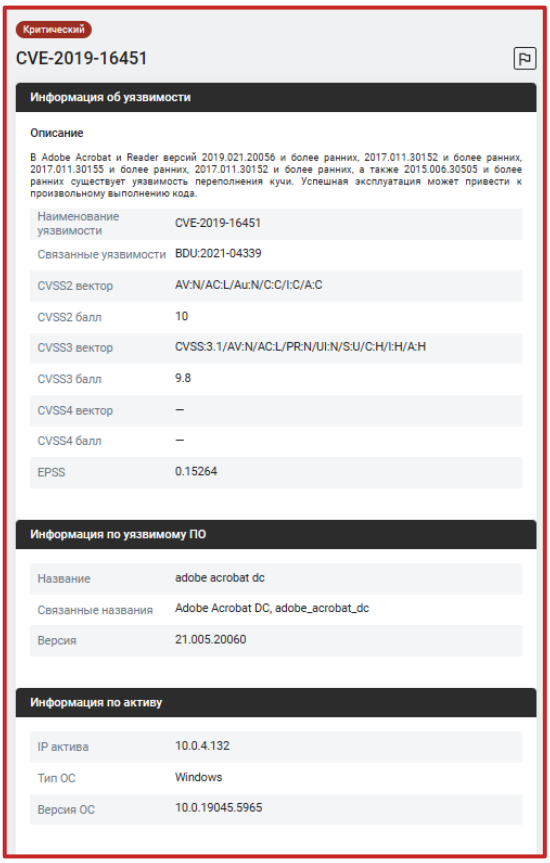


Рис. 38

При наведении мыши на CVSS вектора в карточке уязвимости отображается «Калькулятор балла» (рис. 40).

Калькулятор балла

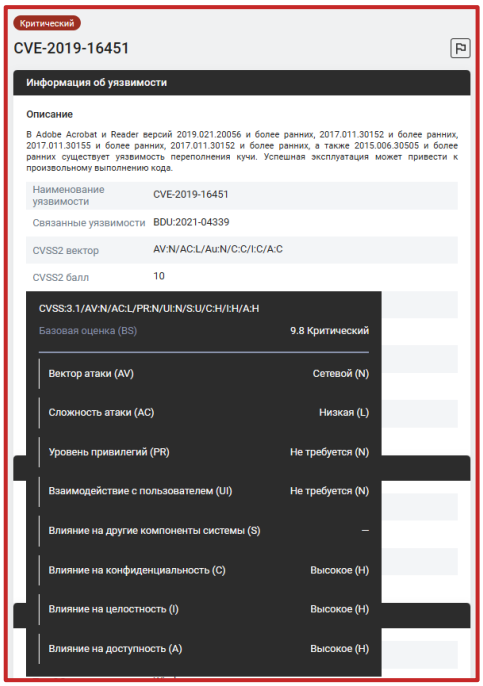


Рис. 39

По умолчанию в правой половине карточки уязвимости отображаются рекомендации по ее устранению (при наличии таких рекомендаций в официальных источниках) в вкладке «Рекомендации». При этом существует возможность исключить из результатов данную уязвимость, пометив её как ложное срабатывание.

Вкладка «Рекомендации»

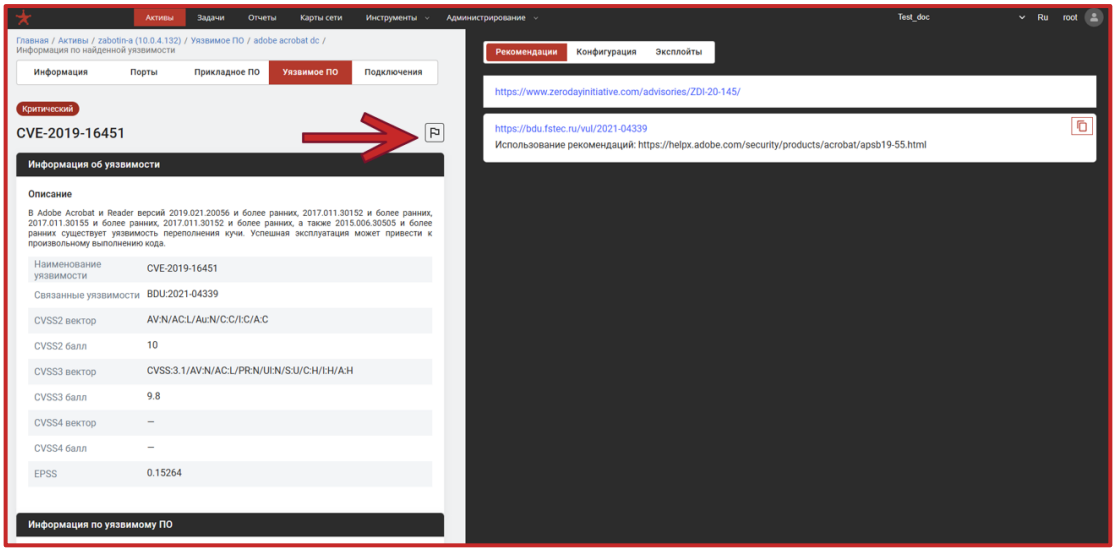


Рис. 40

Для установки отметки «Ложное срабатывание» необходимо нажать на кнопку флажка, на которую указывает стрелка на рис. 40. После нажатия на кнопку флажка отобразится всплывающее окно с настройкой отметки найденной уязвимости как ложное срабатывание (рис. 41).

Окно отметки ложного срабатывания

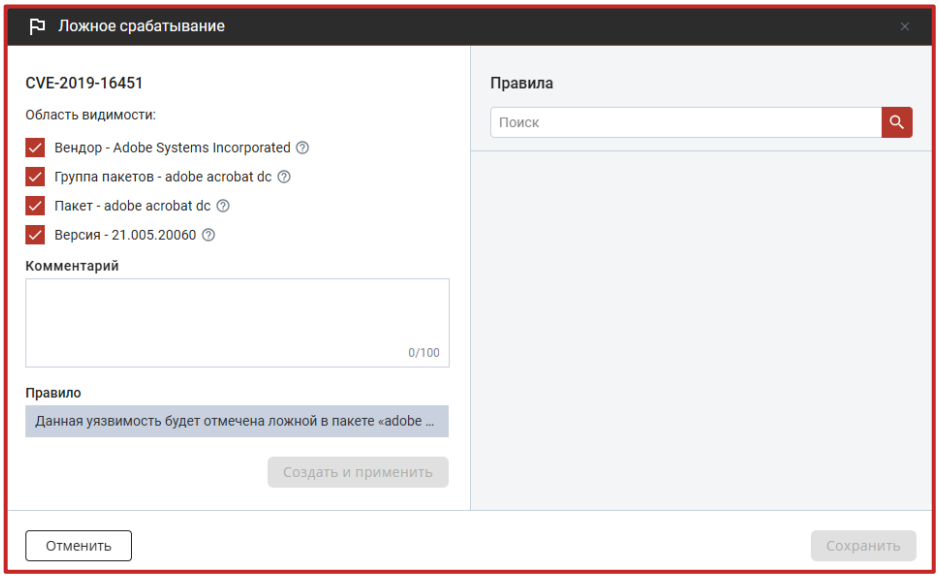


Рис. 41

Отметка уязвимости ложной происходит посредством настройки правил для конкретной уязвимости. Правила настраиваются с помощью четырех чекбоксов в зоне под названием «Область видимости».

По умолчанию все чекбоксы в окне отметки уязвимости ложной активны. В таком случае исключительно уязвимость, в карточке которой находится пользователь, будет отмечена ложной (только уязвимость для конкретной версии пакета, входящего в конкретную группу и конкретного вендора).

При деактивации чекбоксов происходит расширение области отметки уязвимости ложной. Существуют следующие варианты:

– все чекбоксы активны;

– деактивирована опция «Версия» – уязвимость будет отмечена ложной для всех версий ПО конкретного пакета, входящего в состав конкретной группы и конкретного вендора;

– деактивированы опции «Версия» и «Пакет» – уязвимость будет отмечена ложной для всех версий ПО и всех пакетов, входящих в конкретную группу конкретного вендора;

– деактивированы опции «Версия», «Пакет» и «Группа» – уязвимость будет отмечена ложной для всех версий ПО, всех пакетов во всех группах конкретного вендора;

– деактивированы все опции – уязвимость будет отмечена ложной для всех версий ПО, всех пакетов, во всех группах и всех вендоров, т.е. для всего узла исследуемой сети.

При настройке правила отметки уязвимости ложной в окне «Правило» отображается подсказка для пользователя. Для просмотра всего правила целиком необходимо навести на данное окно курсор мыши, после чего правило будет отображено во всплывающем окне (рис. 42). После настройки правила отметки уязвимости ложной необходимо добавить комментарий и нажать на кнопку «Создать и применить», которая станет активной. Созданное правило отобразится в правой части окна отметки уязвимости ложной (рис. 42). Для завершения отметки уязвимости ложной необходимо нажать на кнопку «Сохранить».

Примечание. Уязвимости, отмеченные пользователем как ложное срабатывание, в отчётах отображаться не будут, причём как в кратком, так и в полном. Отчёты описаны в п. 5.6 настоящего руководства.

Создание правила отметки уязвимости ложной

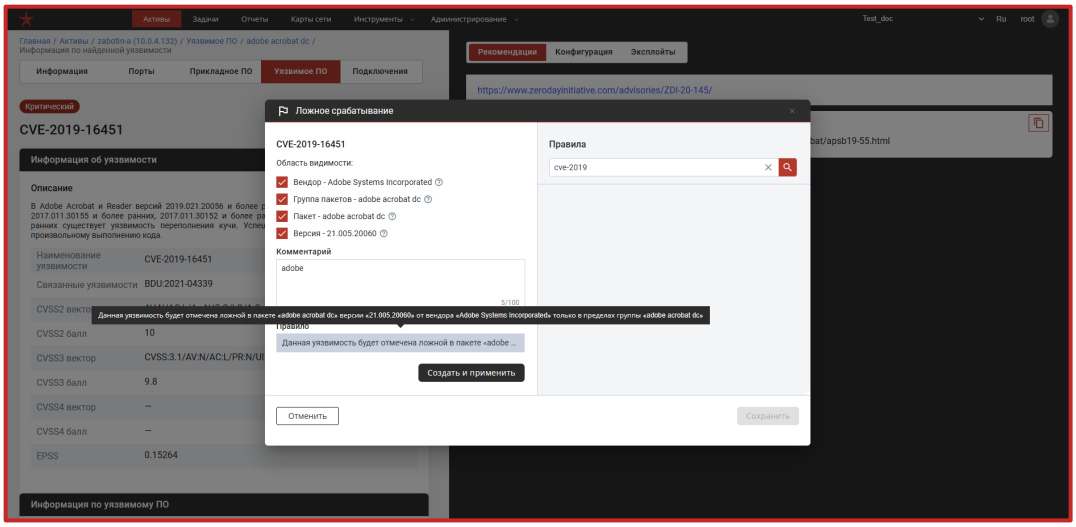


Рис. 42

После установки отметки «Ложное срабатывание» для найденной уязвимости флажок ложного срабатывания отобразится в таблице найденных уязвимостей, а соответствующая ей строка таблицы поменяет свой цвет. В карточке уязвимости появится новое поле с пометкой о ложном срабатывании и комментарием, оставленным оператором (рис. 43).

Примечание. В том случае если все найденные уязвимости в пакете будут отмечены пользователем как ложные срабатывания, то и на вкладке «Уязвимое ПО» в карточке актива (см. рис. 34) весь пакет будет отображаться аналогично отдельно взятой уязвимости конкретного ПО, для которой была сделана пометка ложного срабатывания, а количество найденных уязвимостей для этого пакета станет равным нулю.

Карточка уязвимости, помеченная как «Ложное срабатывание»

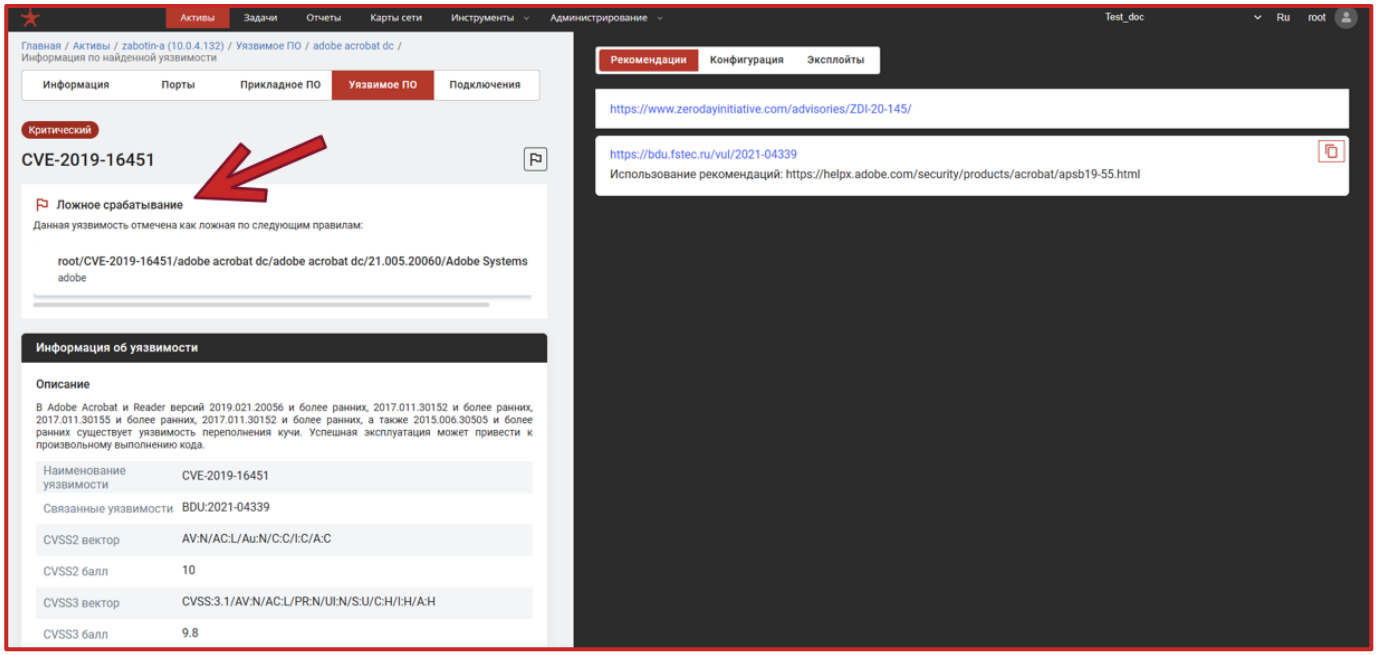


Рис. 43

Карточка уязвимости также описана в п. 5.8.4.2 настоящего документа.

Карточка пользовательской уязвимости 5.8.7.3 настоящего документа.

Для удаления отметки «Ложное срабатывание» необходимо еще раз нажать на кнопку флажка. После чего отобразится окно отметки уязвимости ложной, в котором для удаления данной отметки необходимо нажать кнопку удаления для соответствующего правила отметки уязвимости ложной (рис. 44) и затем нажать кнопку «Сохранить».

Удаление правила отметки уязвимости ложной

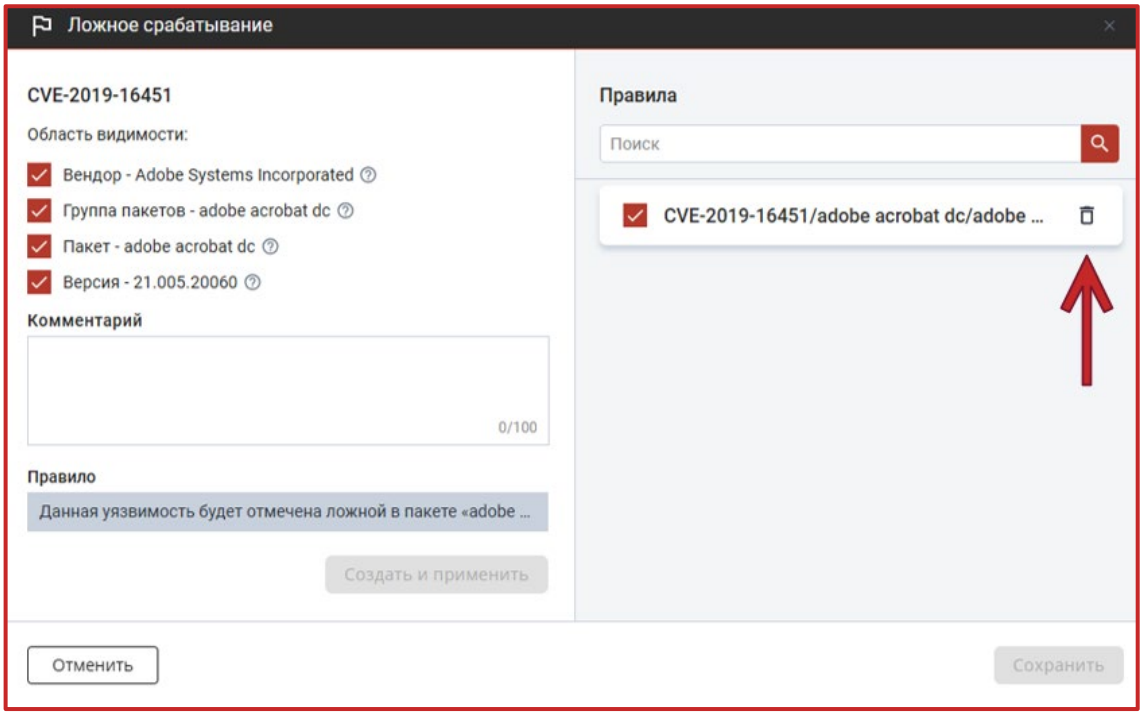


Рис. 44

Для перехода на страницу описания рекомендации по устранению выявленной уязвимости необходимо кликнуть на ссылку в поле рекомендации после чего откроется новая страница в браузере, содержащая рекомендации по устранению выявленной уязвимости.

Для просмотра данных об уязвимой версии найденного ПО необходимо нажать на кнопку «Конфигурация» в правой половине окна карточки уязвимости (рис. 45).

Конфигурация уязвимости

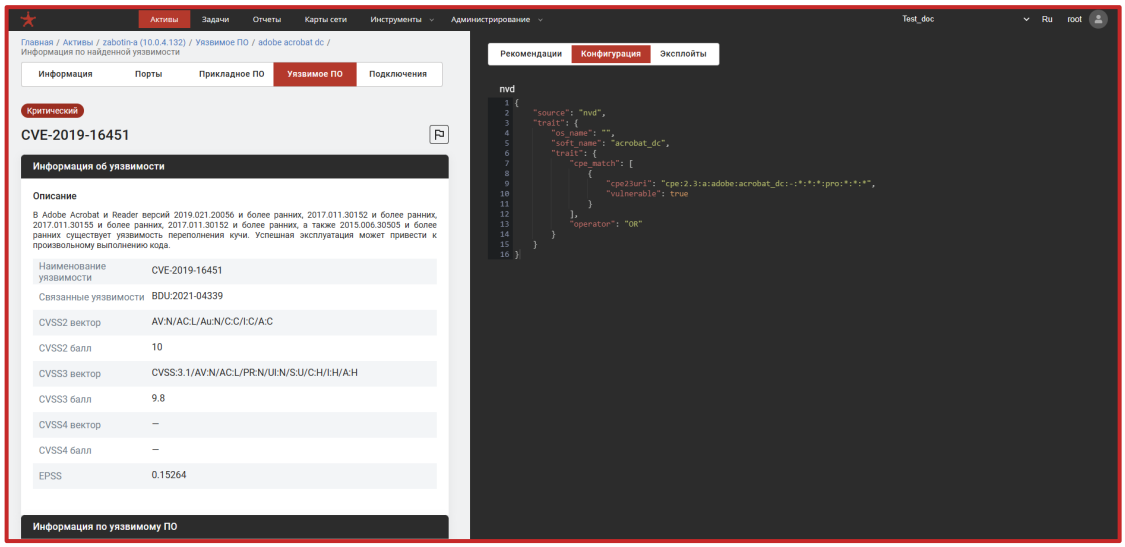


Рис. 45

Для просмотра эксплойтов, с помощью которых злоумышленник может организовать атаку на актив исследуемой сети необходимо нажать на кнопку «Эксплойты» в правой половине окна карточки уязвимости (рис. 46).

Эксплойты уязвимости

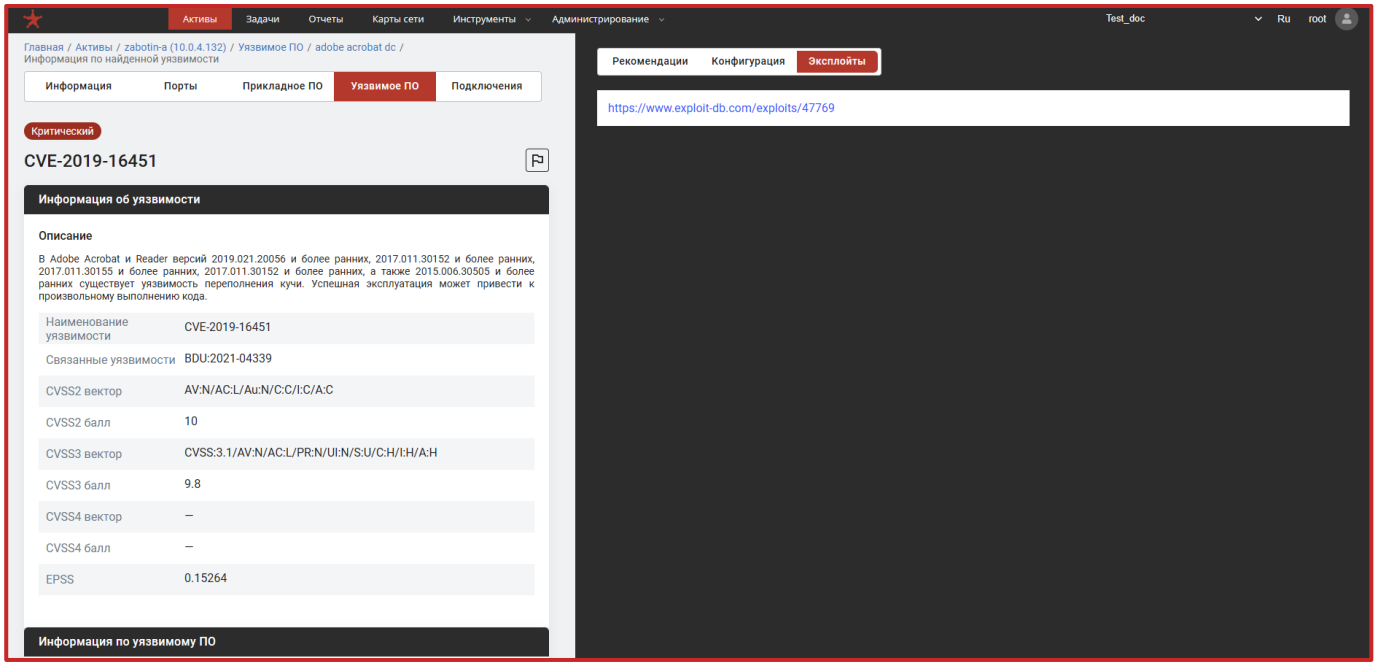


Рис. 46

5.4.5.7. Подключения

Вкладка «Подключения» (рис. 47) применяется для отображения информации о подключениях актива, а также для добавления новых подключений для дальнейшего проведения задач «Инвентаризация» и «Аудит конфигурации».

Вкладка «Подключения»

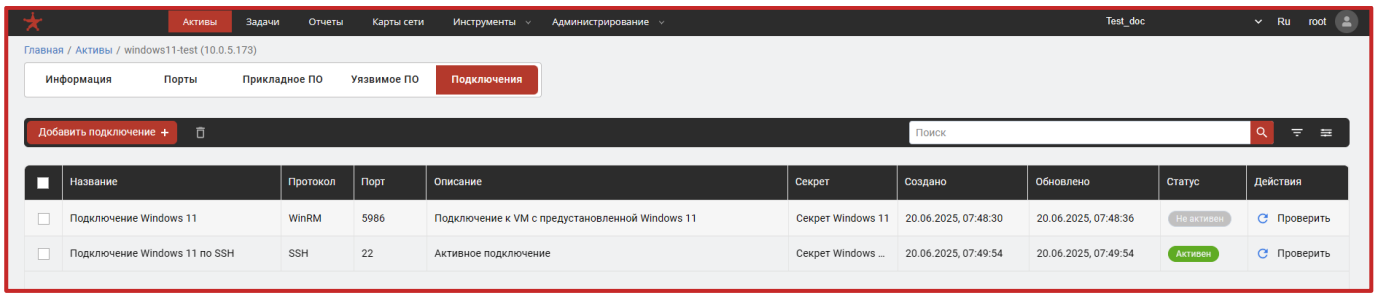


Рис. 47

Данная вкладка содержит следующую информацию:

– «Название» – название подключения;

– «Протокол» – информация об используемом в подключении протоколе обмена информацией;

– «Порт» – порт протокола;

– «Описание» – описание подключения, задаваемое оператором;

– «Секрет» – секрет, связанный с подключением;

– «Создано» – дата и время создания;

– «Обновлено» – дата и время обновления;

– «Статус» – информация о статусе подключения;

– «Проверить» – проверка подключения.

Для добавления нового подключения необходимо нажать на кнопку «Добавить подключение», после чего откроется окно для ввода параметров создаваемого подключения (рис. 48).

Окно «Настройки подключения»

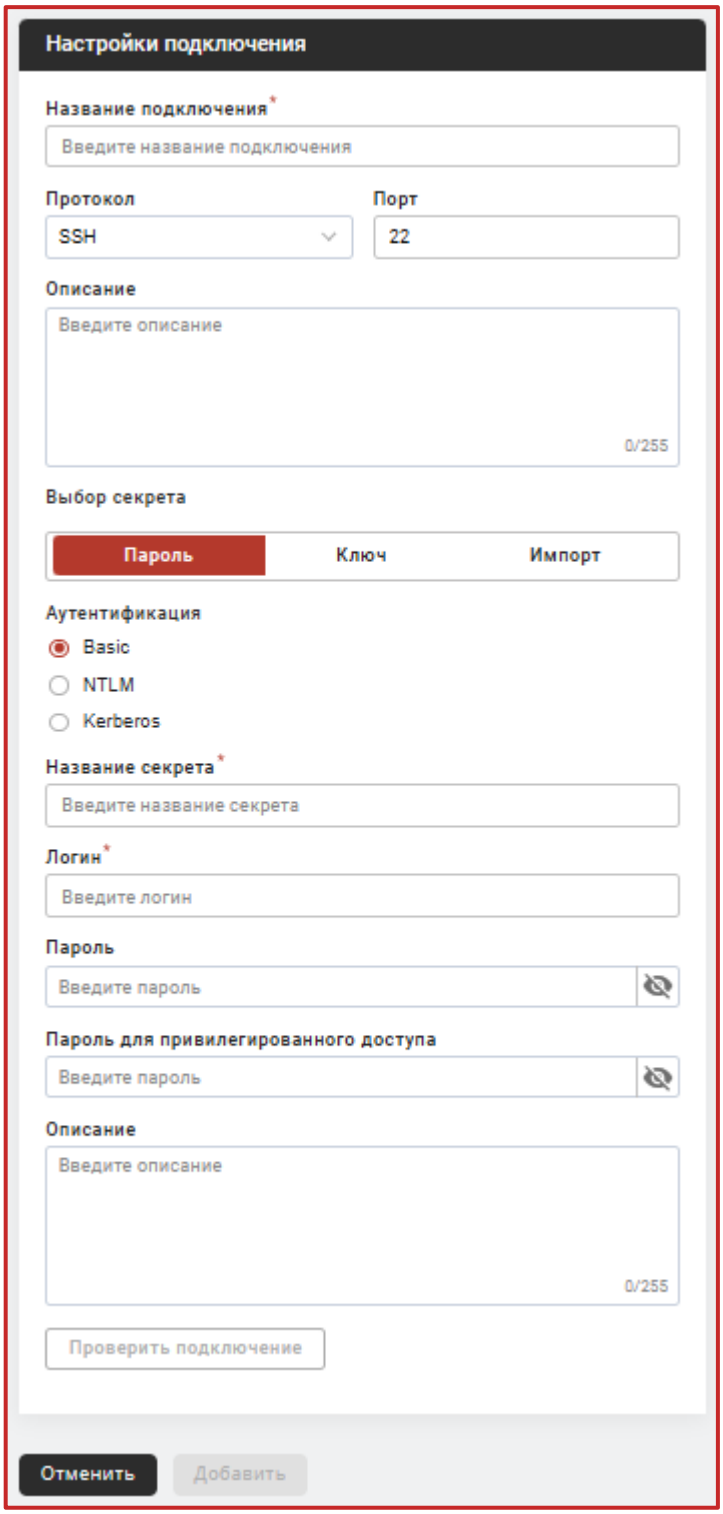


Рис. 48

Процессы настройки, редактирования и удаления подключений подробно описаны в пп. 5.9.2.1.2, 5.9.2.1.3 настоящего руководства.

5.5. Задачи

В рамках задач по анализу защищенности оператору предоставляются следующие функции Сканер-ВС:

– «Исследование сети» (п. 5.5.3);

– «Инвентаризация» (п. 5.5.4);

– «Поиск уязвимостей» (п. 5.5.5);

– «Подбор паролей» (п. 5.5.6);

– «Аудит конфигурации» (п. 5.5.7).

При проведении анализа защищенности Сканер-ВС используется специальный интерфейс, доступ к которому осуществляется нажатием кнопки «Задачи» на панели навигации (рис. 49), после чего откроется вкладка «Задачи».

Переход ко вкладке «Задачи»

Рис. 49

5.5.1. Общее описание

Вкладка «Задачи» представляет собой таблицу (рис. 50).

Вкладка «Задачи»

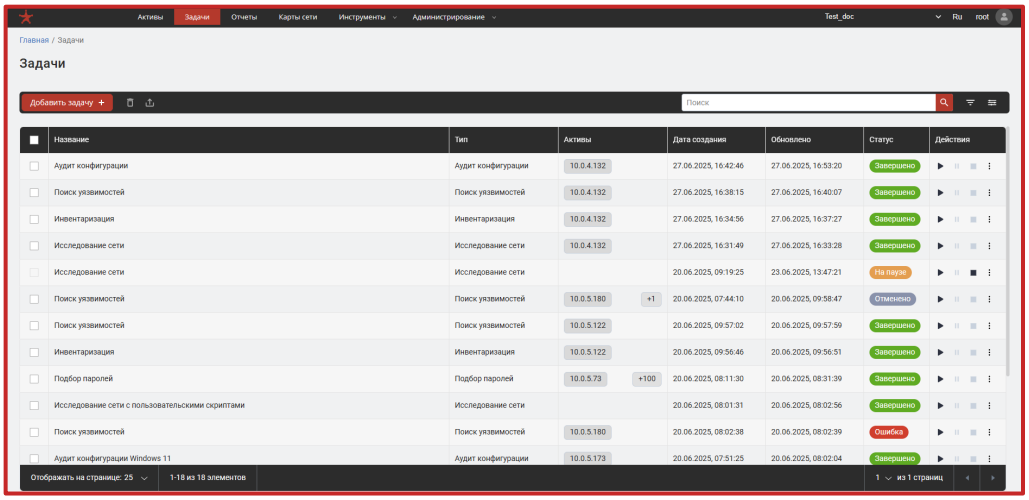


Рис. 50

Вкладка «Задачи» содержит в себе следующие данные:

– «Название» – наименование задачи, задаваемое пользователем при настройке;

– «Тип» – тип выполненной задачи:

а) «Исследование сети»;

б) «Инвентаризация»;

в) «Поиск уязвимостей»;

г) «Подбор паролей»;

д) «Аудит конфигурации».

– «Активы» – отображает цели проведения задачи;

– «Дата создания» – дата и время создания задачи;

– «Обновлено» – дата и время последнего запуска или обновления настроек задачи;

– «Статус» – информация о статусе задачи:

а) «Создано»;

б) «В процессе»;

в) «На паузе»;

г) «Завершено»;

д) «Отменено».

– действия с задачей (столбец «Действия»):

а) запустить – « ▶ »;

б) поставить на паузу – « ⏸ »;

в) отменить – « ■ »;

г) показать выпадающий список – « ⋮ ».

При наведении курсора на знак « ⋮ » отображается меню действий над завершенной задачей:

– « Редактировать» – при нажатии на данную строку выпадающего окна Сканер-ВС отображает окно редактирования завершенной задачи. Редактирование завершенных задач описано в п. 5.5.8.1 настоящего документа;

– «Дублировать» – после нажатия на данную строку выпадающего окна выбранная задача будет скопирована со всеми настройками. Скопированная задача отобразится вверху таблицы завершенных задач со статусом «Создано»;

– «Расписание» – при нажатии на данную строку выпадающего окна Сканер-ВС отображает окно настройки запуска задачи по расписанию, описанное в п. 5.5.3.7 настоящего документа;

– «Удалить» – представляет собой функцию удаления завершенной задачи.

Для создания задачи необходимо нажать на кнопку «Добавить задачу +» в верхнем левом углу таблицы.

5.5.2. Добавление задачи

После нажатия на кнопку «Добавить задачу +» в верхнем левом углу таблицы на вкладке «Задачи» откроется окно интерфейса выбора типа задачи (рис. 51).

Окно выбора типа задачи

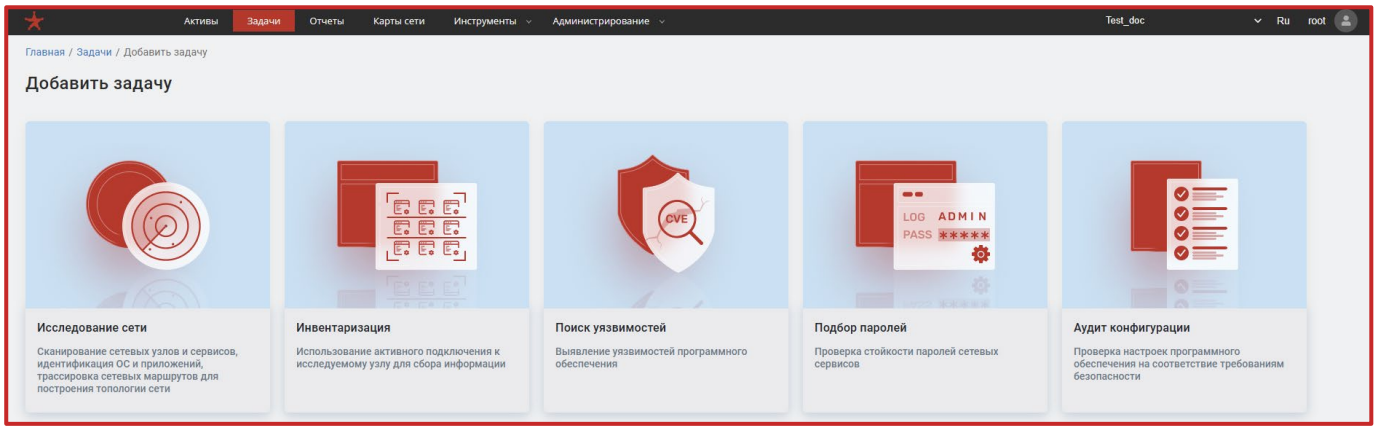


Рис. 51

5.5.3. Исследование сети

5.5.3.1. Общее описание

В начале анализа обязательным этапом является исследование сети для поиска целей – обзор локальной сети, к которой подключен Сканер-ВС, с целью выявления

объектов для следующих фаз анализа защищенности. Поиск целей производится путем сканирования IP-адресов и портов (TCP- и UDP-портов) компьютеров, присоединенных к локальной сети. Без поиска целей невозможно использовать все возможности Сканер-ВС, в частности, невозможно производить поиск уязвимостей (п. 5.5.4 настоящего документа). Найденные в результате исследования сети действующие подключения с IP-адресами и задействованными TCP- и UDP-портами далее будут называться активами. Данные о них располагаются во вкладке «Активы» в виде таблицы (п. 5.4 настоящего документа).

Дополнительно исследование сети (поиск целей) может быть использовано 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.

Для создания новой задачи исследования сети необходимо зайти на вкладку «Задачи», нажать на кнопку «Добавить задачу +», выбрать тип задачи «Исследование сети» (рис. 52).

Выбор типа задачи «Исследование сети»

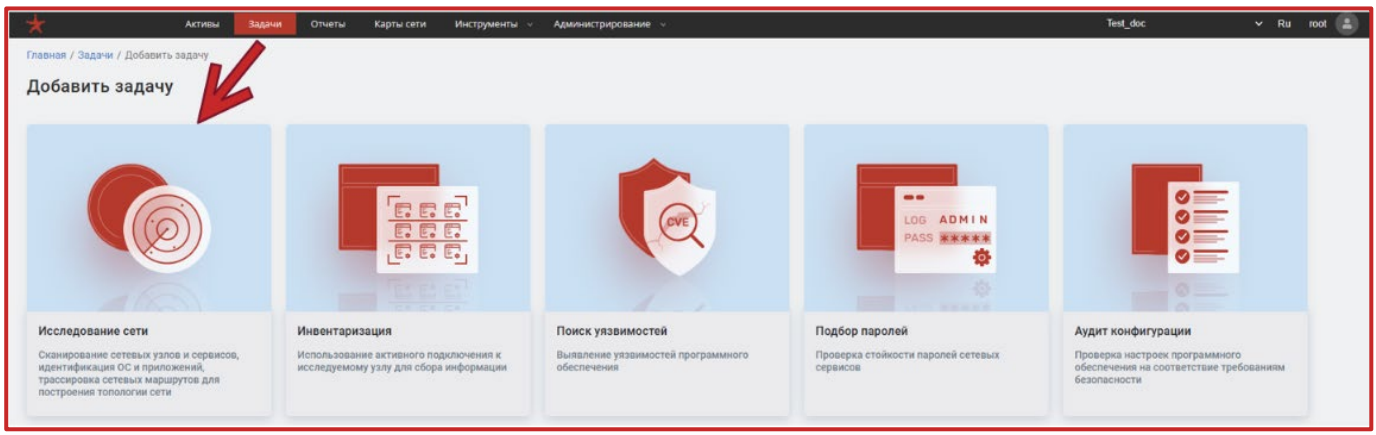


Рис. 52

Задача «Исследование сети» имеет следующие блоки настроек (рис. 53):

– «Настройки задачи»;

– «Сканирование портов»;

– «Сетевые настройки»;

– «Скрипты»;

– «Политики сканирования».

Настройки задачи «Исследование сети»

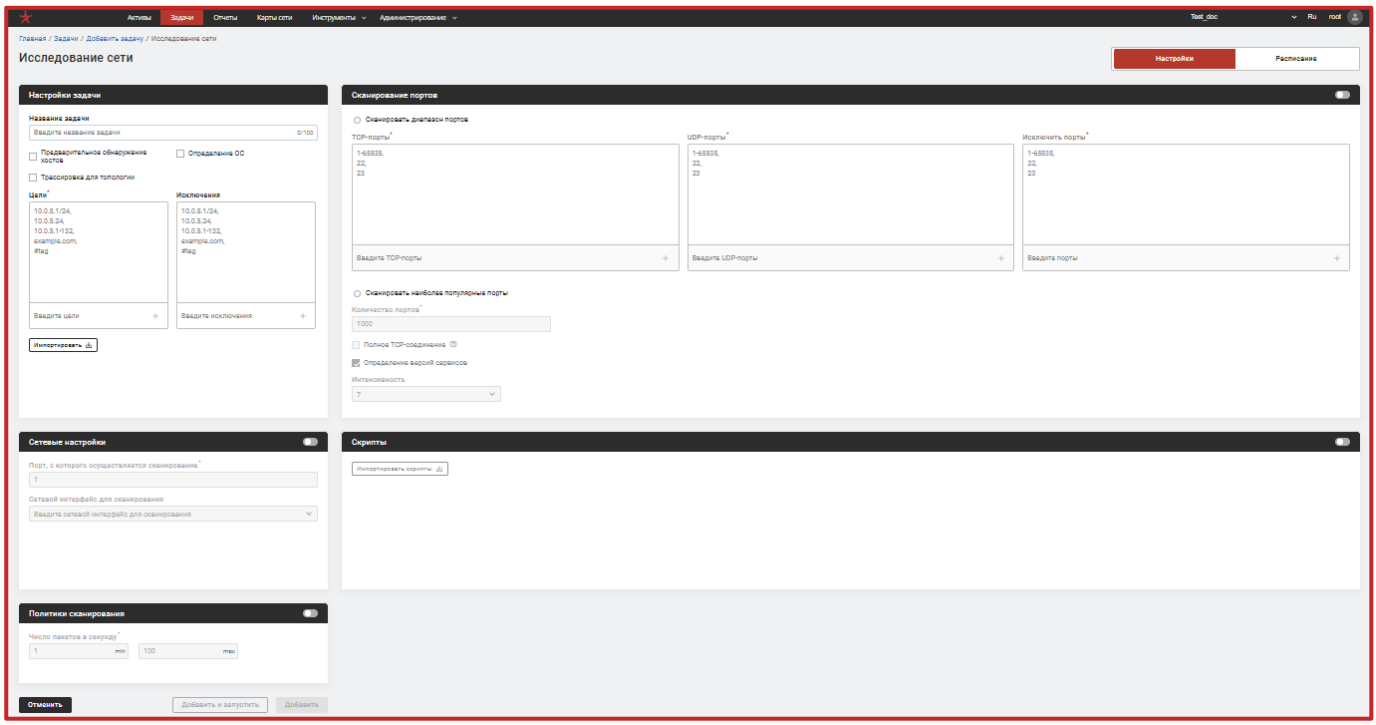


Рис. 53

5.5.3.2. Блок «Настройки задачи»

В блоке «Настройки задачи» (рис. 54) задаются следующие параметры:

– название задачи;

– опция «Предварительное обнаружение хостов»;

– опция «Определение ОС»;

– опция «Трассировка для топологии»;

– цели, для которых будет проведено исследование сети;

– исключения для исследования сети;

– загрузка целей из активов проекта (функция «Импортировать»).

Блок «Настройки задачи»

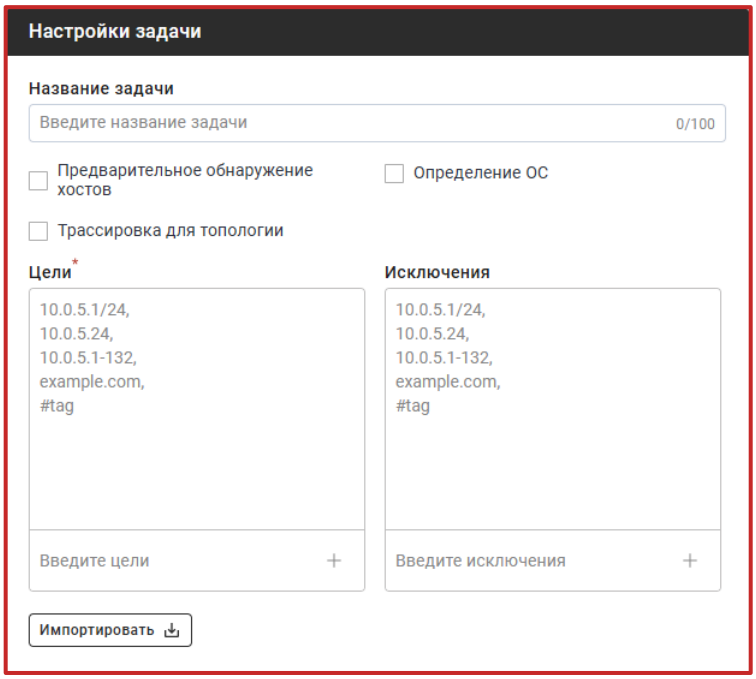


Рис. 54

Наименование задачи записывается в поле «Название задачи» и должно содержать понятное и, желательно, уникальное описание для каждой задачи данного типа. Если не указывать наименование, то по умолчанию оно примет вид: «Исследование сети».

При создании задачи на исследование сети настраиваются цели для сканирования. Цели исследования можно задавать тремя способами:

– вручную, путем ввода адреса в поле «Цели»;

– вручную, путем выбора активов, к которым применен тег;

– импортируя цели из активов.

Для добавления целей сканирования методом выбора активов с определенным тегом необходимо в поле «Адрес цели» написать выражение #′название_тега′, где ′название_тега′ – название используемого тега, заданное пользователем при создании. Теги описаны в п. 5.8.1 настоящего документа.

Примечание. Для успешного добавления активов в цели исследования с помощью тега необходимо чтобы этот тег был присвоен активам, которые добавляются в цели исследования.

Для загрузки из активов целей для сканирования необходимо нажать кнопку «Импортировать», отметить нужные для импорта активы (если актив выбран, рядом с ним в пустом чекбоксе появится галочка) или нажать на пустом чекбоксе в заголовке таблицы рядом со столбцом «Название» (все доступные для импорта активы будут отмечены автоматически). Затем необходимо нажать кнопку «Импортировать» и IP-адреса отмеченных активов появятся в поле «Цели» (рис. 55).

Импорт целей сканирования из активов

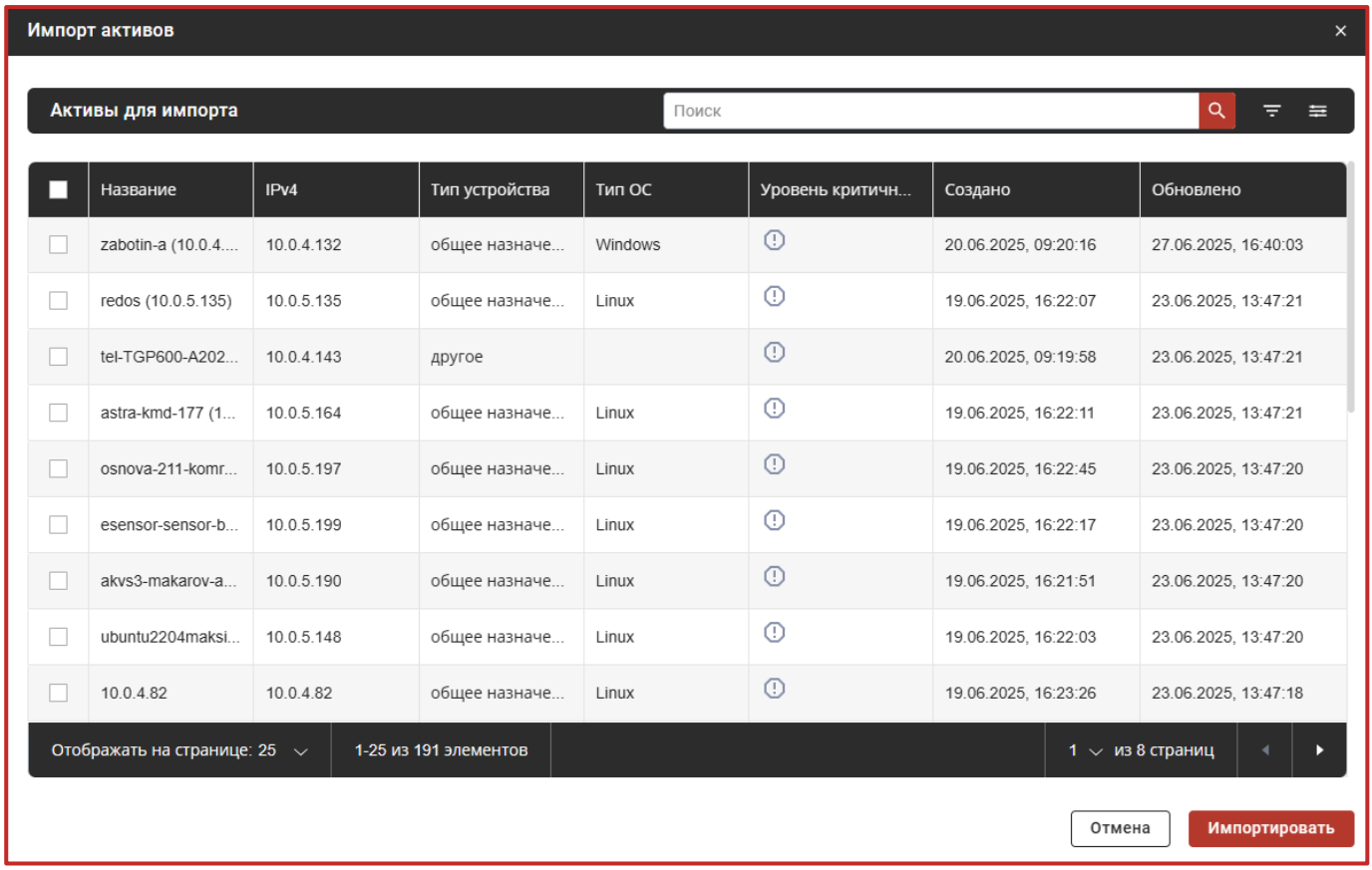


Рис. 55

Поле «Исключения» заполняется аналогично полю «Цели». При заполнении целей исследования с помощью импорта целей из активов не выбранные активы отобразятся в поле «Исключения».

Опция «Предварительное обнаружение хостов» включается, если необходимо создать список хостов заданной сети.

Опция «Определение ОС» включается в том случае, если необходимо определить тип ОС узлов исследуемой сети.

Опция «Трассировка для топологии» включается в том случае, если необходимо построить карту исследуемой сети (п. 5.7 настоящего документа).

5.5.3.3. Блок настроек «Сканирование портов»

Для включения опции «Сканирование портов» при настройке новой задачи «Исследование сети» необходимо нажать на переключатель в правом верхнем углу блока настроек «Сканирование портов» (рис. 56).

Блок настроек «Сканирование портов»

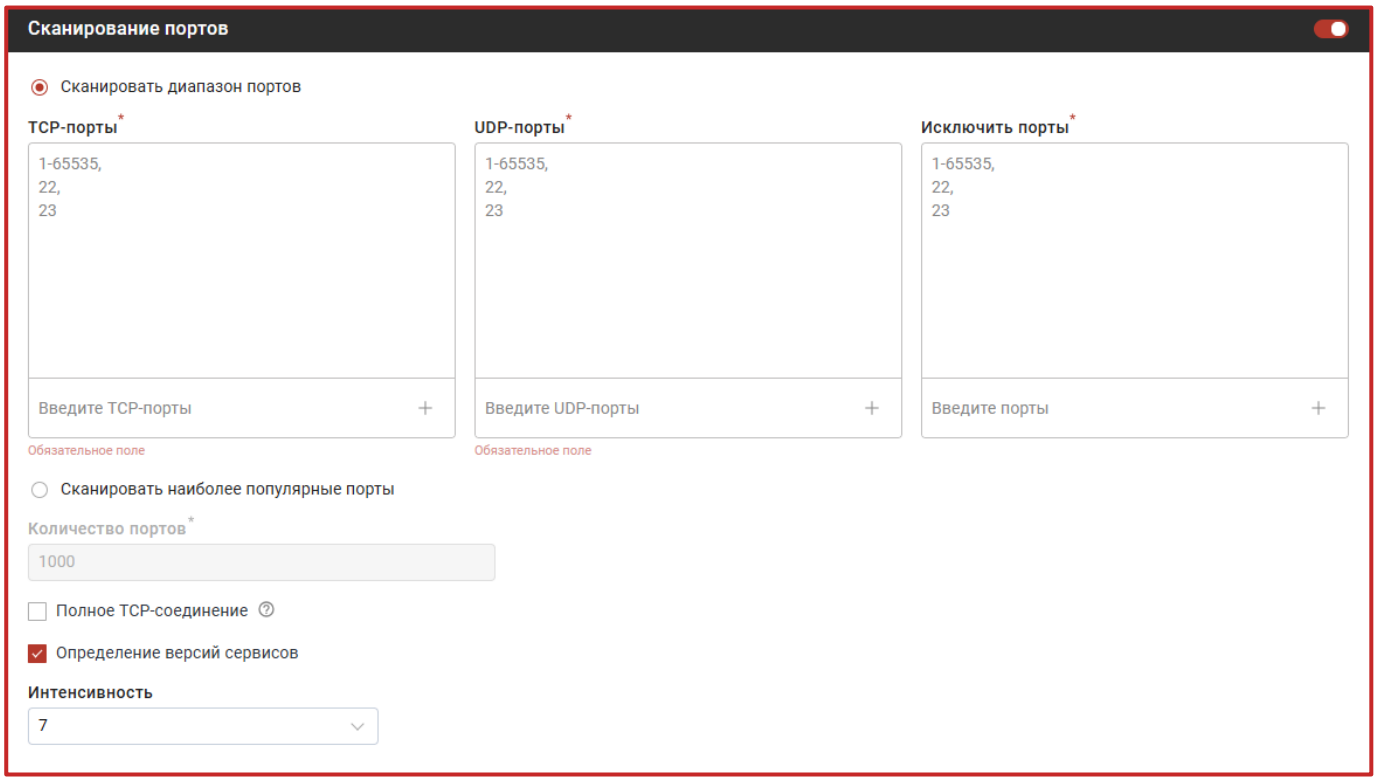


Рис. 56

Опция «Сканирование портов» предоставляет выбор режима сканирования из следующих вариантов:

– сканирование диапазона заранее заданных портов (функция «Сканировать диапазон портов»);

– сканирование популярных портов (функция «Сканировать наиболее популярные порты»).

Как видно из рис. 56, при выборе функции «Сканировать диапазон портов» необходимо указать диапазон TCP- и UDP-портов для сканирования в полях «TCP порты» и «UDP-порты» соответственно (хотя бы одно из этих полей должно быть заполнено). В случае, если необходимо не сканировать какие-либо порты или диапазон портов из сканирования, эти порты (диапазон портов) необходимо указать в поле «Исключить порты».

Примечание. Для успешного сканирования исследуемой сети через UDP порты необходимо включить настройку «Политики сканирования», описанную в п. 5.5.3.6 настоящего документа.

При выборе функции «Сканировать наиболее популярные порты» необходимо указать количество сканируемых портов в поле «Количество портов». Количество портов устанавливается ручным вводом значения при нажатии на поле, в котором указывается количество сканируемых портов, в пределах от 1 до 65535.

В Сканер-ВС реализована функция «Определение версий сервисов», функционирующих на узлах исследуемой сети. Данная функция включается автоматически при выборе опции «Сканирование портов». Так же ее можно включить или отключить вручную. Для определения версий сервисов необходимо выбрать «Интенсивность». Чем выше интенсивность, тем точнее происходит определение версий сервисов, но и возрастает риск обнаружения Сканер-ВС средствами защиты, установленными на сканируемых узлах.

При выборе функции «Полное TCP-соединение» Сканер-ВС использует TCP-сканирование с системным вызовом «connect (-sT)». Данный режим используется по умолчанию, когда недоступно полуоткрытое сканирование (SYN-сканирование). Этот метод позволяет устанавливать полное TCP-соединение и может быть менее эффективным и более заметным для целевых систем.

Примечание. При работе с мандатными метками включение функции «Полное TCP-соединение» (активация одноименного чекбокса) рекомендуется для обнаружения целевых машин с настроенными мандатными метками безопасности.

5.5.3.4. Блок настроек «Сетевые настройки»

Настройка блока «Сетевые параметры» задачи «Исследование сети» предназначена для установки сетевых параметров сканирования исследуемой сети. Блок настроек «Сетевые настройки» представлен на рис. 57.

Блок «Сетевые настройки»

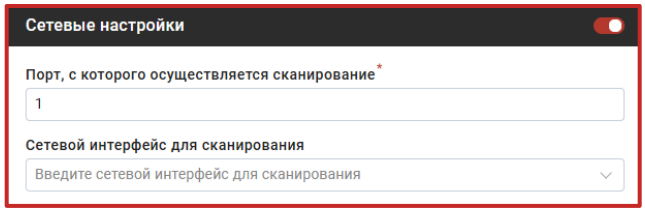


Рис. 57

В блоке настроек «Сетевые настройки» устанавливаются такие параметры как:

– порт, с которого осуществляется сканирование;

– сетевой интерфейс для сканирования.

В поле «Порт, с которого осуществляется сканирование» указывается порт, с которого будет выполняться настраиваемая задача «Исследование сети».

В поле «Сетевой интерфейс для сканирования» можно выбрать сетевой интерфейс, с помощью которого будет происходить сканирование исследуемой сети.

5.5.3.5. Блок настроек «Скрипты»

Настройка блока «Скрипты» (рис. 58) предназначена для возможности импорта системных / пользовательских скриптов и добавления для каждого опциональных аргументов. Добавленные скрипты необходимы для проведения и автоматизации расширенного процесса анализа сети и получения более полного представления безопасности активов.

Блок «Скрипты»

Рис. 58

Для активации данного блока настроек необходимо нажать на переключатель в заголовке правого верхнего угла блока. Переключатель изменит цвет, и кнопка «Выбрать из списка пользовательских скриптов» станет активна.

Нажатие на кнопку «Импортировать скрипты» позволит оператору выбрать и импортировать (рис. 59) как системный скрипт, так и написанный собственный скрипт на языке «Lua», предварительно добавленный в изделие. Системные скрипты представляют собой предустановленные в изделии по умолчанию скрипты «Nmap Scripting Engine (NSE)» в форматах «.nse» или «.lua» (подробнее о добавлении и создании пользовательских скриптов в п. 5.8.6 настоящего документа).

Примечание. Предустановленные системные скрипты аналогичны скриптам, используемым в «nmap» и для них необходимо использовать аргументы строго в соответствии с документацией на «nmap».

Всплывающая таблица импорта доступных скриптов

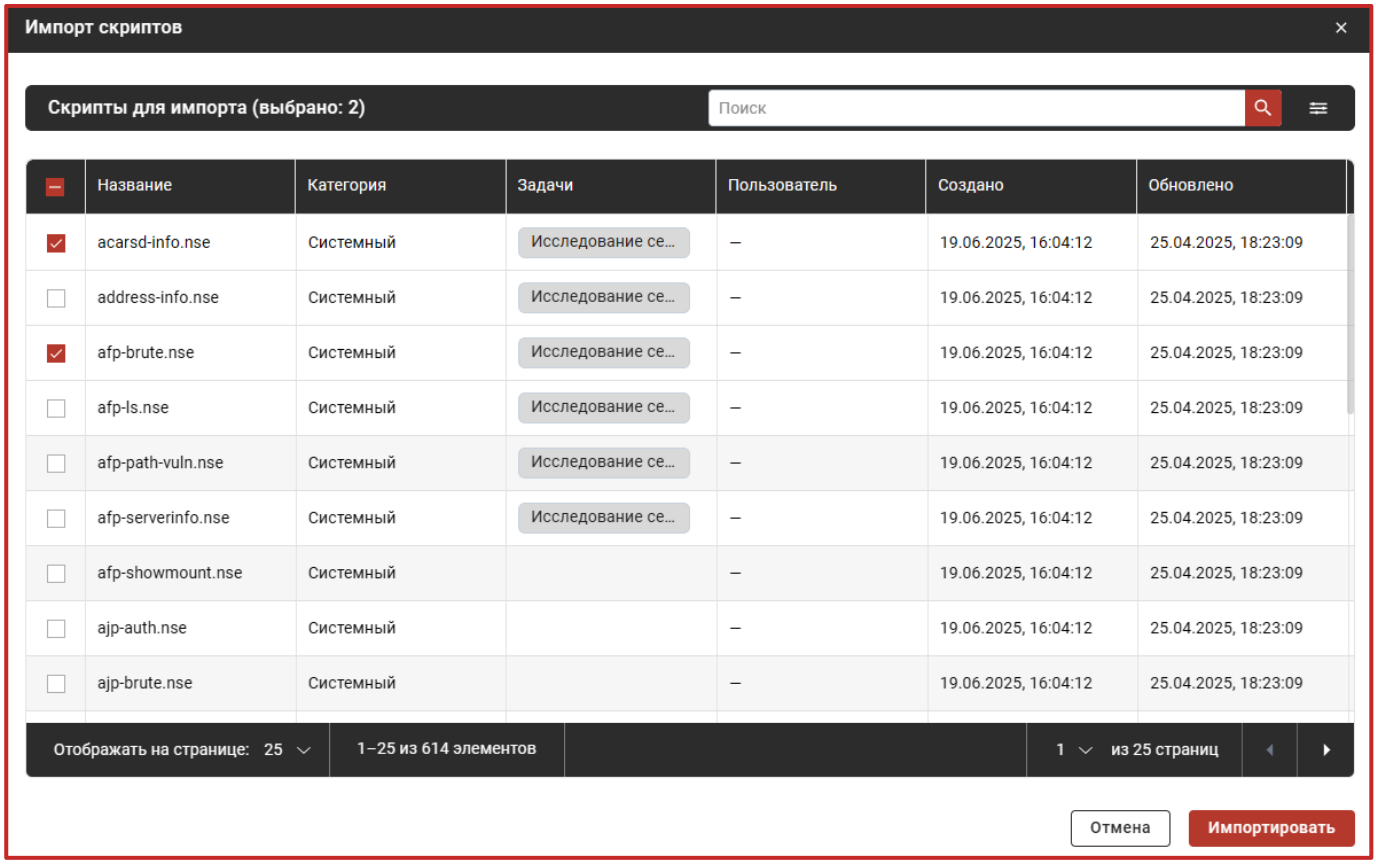


Рис. 59

Для отмены действий выбора из таблицы импорта скриптов необходимо нажать кнопку «Отмена». Для подтверждения своего выбора (после активации чекбоксов в строках с выбранными скриптами) необходимо нажать кнопку «Импортировать скрипты».

Доступные настройки блока «Скрипты»

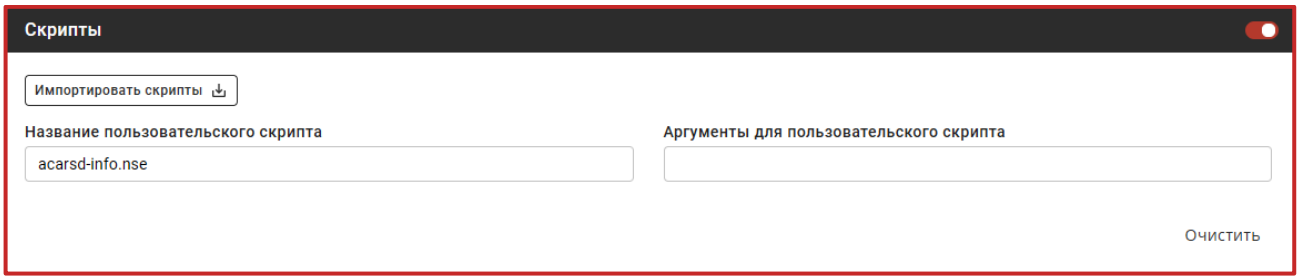


Рис. 60

При импорте хотя-бы одного скрипта из таблицы импорта пользовательских скриптов оператору станут доступны следующие дополнительные поля настроек (см. рис. 60):

– информационное поле «Название пользовательского скрипта» – предназначен для отображения полного названия импортированного оператором скрипта. Для каждого импортированного скрипта появится свое информационное поле;

– поле «Аргументы для пользовательского скрипта» – предназначен для ввода оператором параметров (аргументов), которые будут передаваться скрипту во время его выполнения для автоматизации выполнения заданных сценариев. Для каждого импортированного скрипта появится свое информационное поле;

– кнопка «Очистить» – предназначена для удаления всех ранее импортированных оператором скриптов в настройке блока «Скрипты».

5.5.3.6. Блок настроек «Политики сканирования»

Настройка блока «Политики сканирования» задачи «Исследование сети» предназначена для установки числа обрабатываемых пакетов в секунду во время сканирования исследуемой сети. Блок настроек «Политики сканирования» представлен на рис. 61.

Примечание. Настройки «Политики сканирования» следует включать только для сканирования UDP-портов. Указание минимального и максимального числа обрабатываемых пакетов в секунду может как ускорить сканирование UDP-портов, так и привести к ухудшению точности обнаружения портов или даже увеличить время выполнения задачи.

Блок «Политики сканирования»

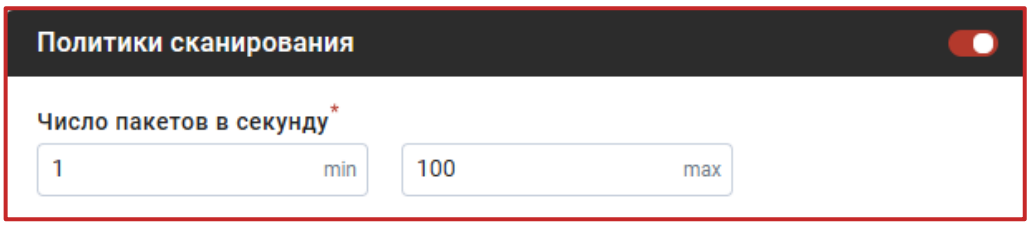


Рис. 61

5.5.3.7. Запуск задачи «Исследование сети» по расписанию

В Сканер-ВС есть опция настройки запуска задачи по расписанию (рис. 62).

Страница «Запуск задачи по расписанию»

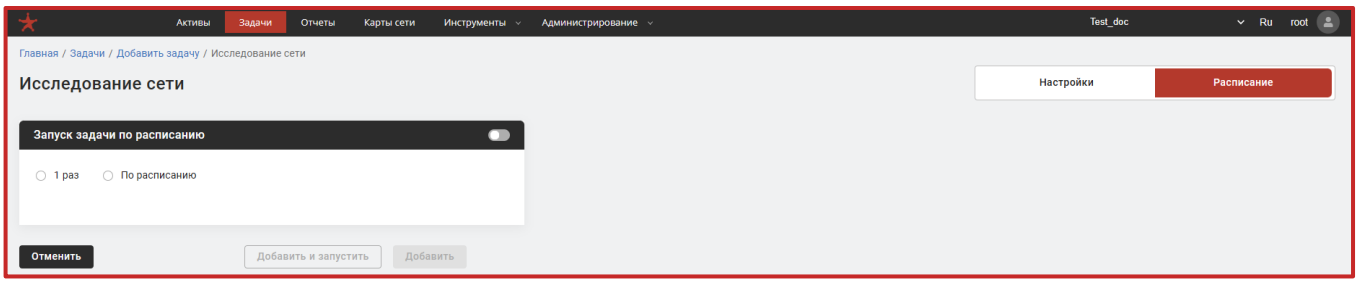


Рис. 62

Реализованы следующие варианты настройки:

– не повторять (единоразовый запуск). Настройка активна по умолчанию и срабатывает в случае, когда функция запуска выполнения задачи по расписанию выключена (см. рис. 62);

– 1 раз – с настройкой даты запуска, времени запуска и выбора временной зоны по национальной шкале времени Российской Федерации UTC (рис. 63);

Настройка запуска задачи «Исследование сети» 1 раз

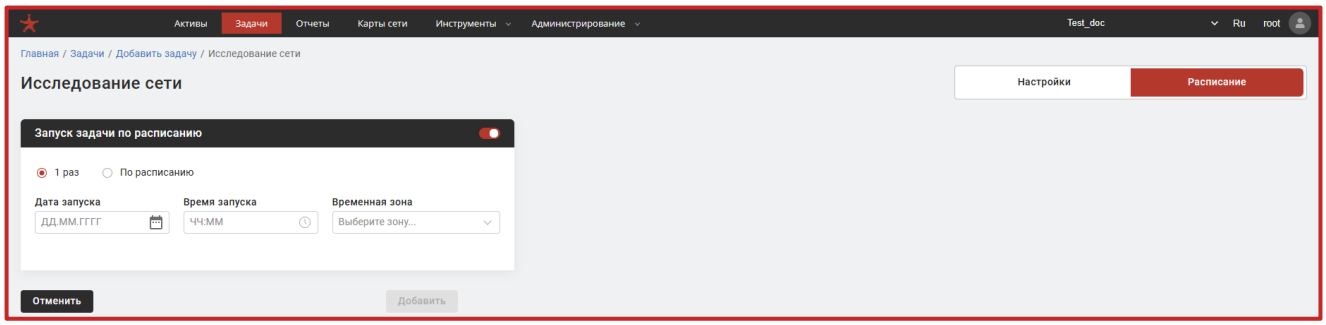


Рис. 63

– по расписанию – с настройкой по каким дням и времени запуска, а также выбора временной зоны по национальной шкале времени Российской Федерации UTC (рис. 64).

Настройка запуска задачи «Исследование сети» по расписанию

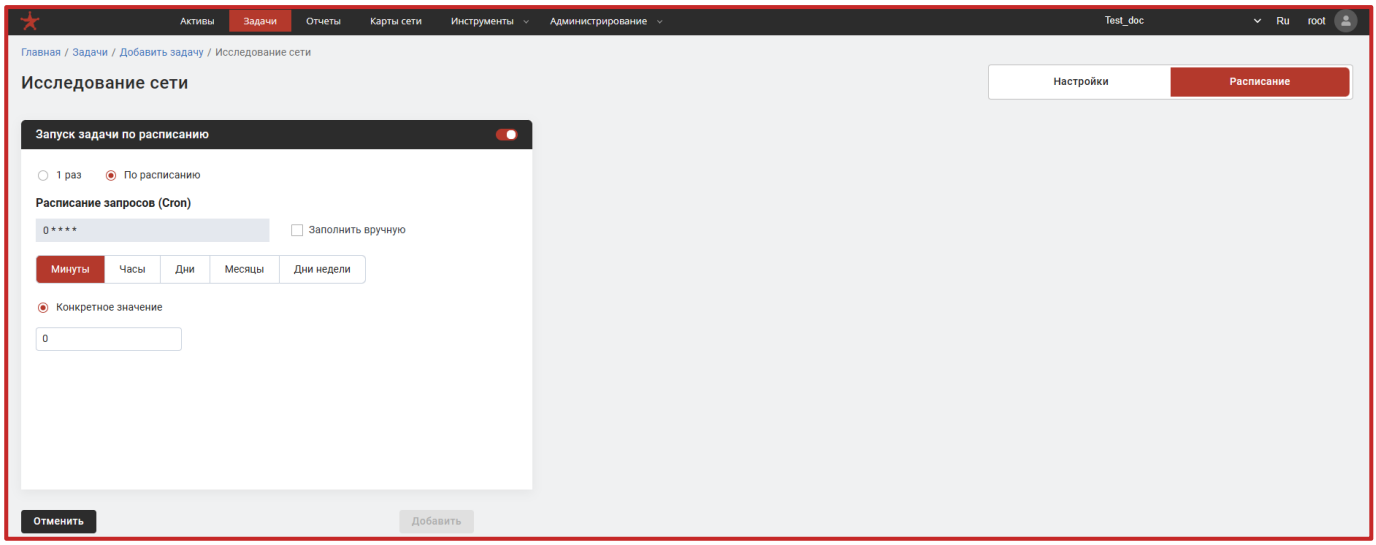


Рис. 64

При настройке запуска задачи 1 раз необходимо выбрать дату запуска, время запуска и временную зону. Установка данных параметров происходит путем поочередного нажатия на соответствующие поля. В случае установки даты запуска открывается всплывающий календарь, в котором необходимо выбрать конкретную дату запуска задачи. При выборе времени запуска открывается список доступных вариантов для запуска задачи от 00:00 до 23:45 с шагом в 15 минут. Необходимо выбрать подходящее время запуска из предложенных вариантов. При нажатии на поле «Временная зона» открывается ниспадающий список временных зон по национальной шкале времени Российской Федерации UTC), из которой необходимо выбрать подходящую для конкретной местности.

При настройке запуска задачи «Исследование сети» по расписанию необходимо установить следующие параметры:

– в какое время будет автоматически запускаться настроенная задача «Исследование сети» (поля «Минуты» и «Часы»). В случае если необходима настройка автоматического запуска выполнения задачи в определенное время, то необходимо выбрать режим «Конкретное значение» и ввести конкретное значение в поле ниже. Аналогично необходимо установить в каком часу задача будет автоматически запускаться, однако, для установки часа автоматического запуска задачи на выполнение есть функция «Каждый час». Если в поле «Часы» установлен режим «Каждый час», то данная задача «Исследование сети» будет автоматически запускаться каждый час;

– в какие дни месяца необходимо автоматически запускать задачу на выполнение (вкладка «Дни», дни устанавливаются аналогично часам). Данная вкладка предоставляет возможность настройки автоматического запуска задачи в определенные числа месяца или каждый день. По умолчанию в Сканер-ВС выбран режим «Каждый день». В случае, если необходимо настроить автоматический запуск выполнения задачи только в определенные числа месяца, необходимо выбрать режим «Конкретное значение», после чего, путем нажатия на соответствующие поля с числами месяца выбрать числа для автоматического запуска задачи на выполнение (рис. 65);

Настройка чисел месяца для автоматического запуска выполнения задачи «Исследование сети»

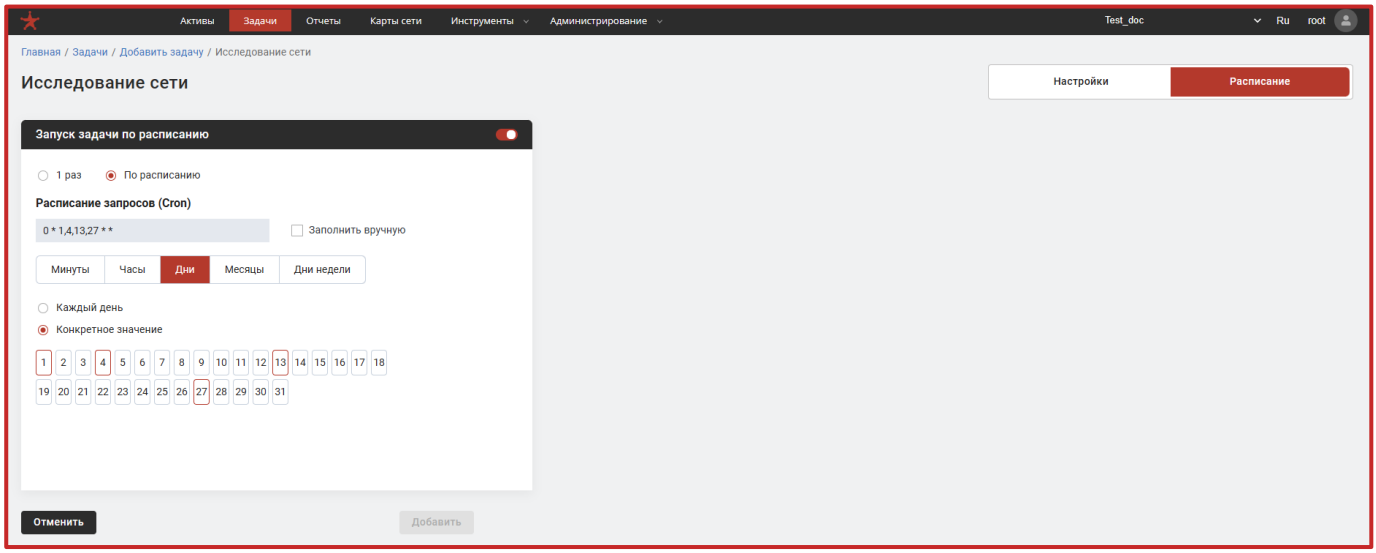


Рис. 65

– в какие месяцы года необходимо автоматически запускать задачу на выполнение (вкладка «Месяцы», месяцы устанавливаются аналогично дням месяца);

– в какие дни недели необходимо запускать задачу на выполнение (вкладка «Дни недели», дни недели в расписании задачи устанавливаются аналогично дням месяца).

Расписание запросов (поле «Cron») можно задать вручную путем ввода чисел в формате минуты, часы, дни, месяцы и дни недели, разделенные между собой пробелами. Для ручного ввода расписания необходимого нажать на чекбокс «Заполнить вручную» (рис. 65). После чего поле «Расписание запросов (Cron) станет доступно для заполнения. Для установки нескольких значений одного параметра, например, минут, необходимо ввести все необходимые значения через запятую.

После завершения настройки, для их сохранения необходимо нажать кнопку «Сохранить».

5.5.3.8. Работа с результатами выполнения задачи «Исследование сети»

В результате успешного выполнения задачи «Исследование сети» появится возможность просмотра найденных в ходе исследования хостов (рис. 66) и их портов (рис. 67) на соответствующих вкладках.

Список обнаруженных хостов после исследования сети

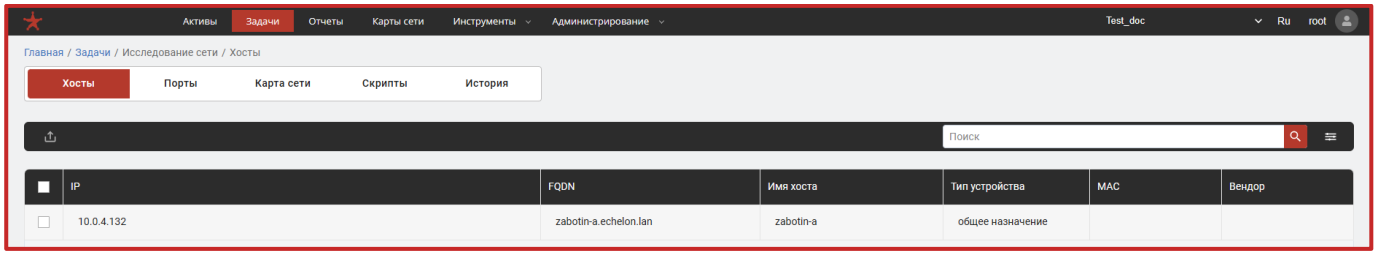


Рис. 66

Список обнаруженных портов после исследования сети

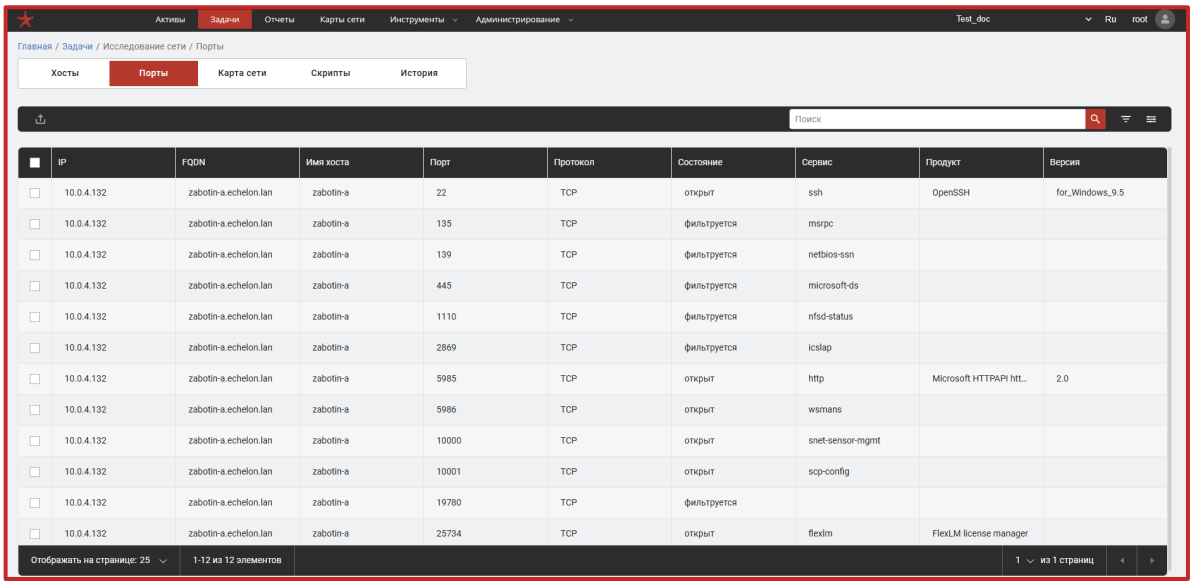


Рис. 67

При переходе во вкладку «Карта сети» отображается карта сети, исследование которой было проведено при запуске задачи. Вкладка «Карта сети» представлена на рис. 68.

Вкладка «Карта сети»

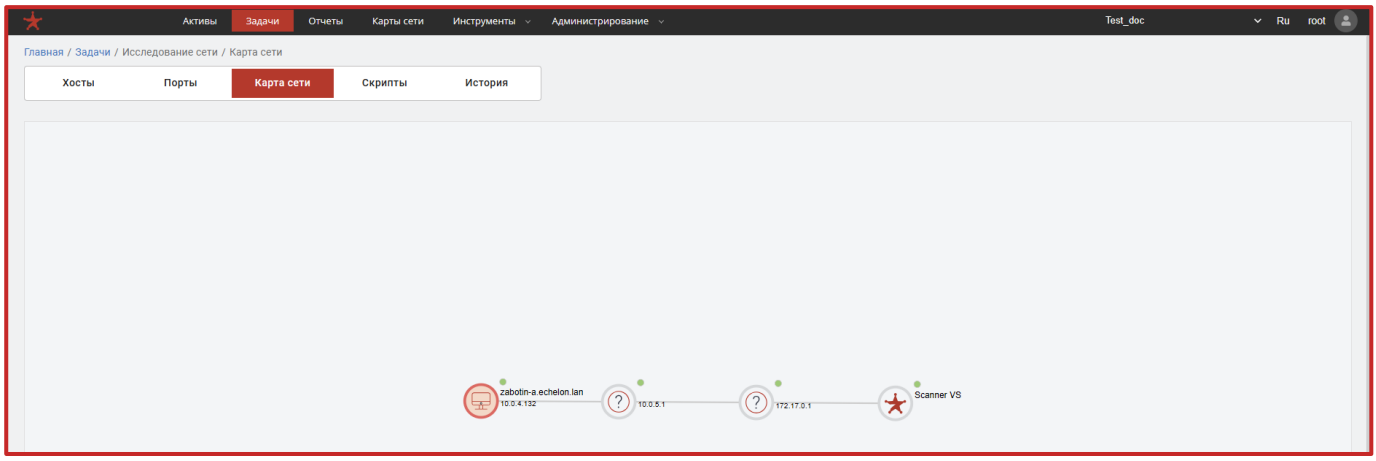


Рис. 68

На рис. 68 изображена карта сети. Узлы карты представляют собой активы, найденные в процессе исследования конкретной сети. Подробное описание карты сети представлено в п. 5.7 настоящего руководства.

В том случае, если при настройке задачи «Исследование сети» не была включена функция «Трассировка для топологии», то на данной вкладке карточки выполненной задачи вместо карты сети отобразится только иконка (узел) самого изделия.

При переходе во вкладку «Скрипты» отображается список со скриптами, которые были задействованы на активах при выполнении задачи «Исследование сети» (рис. 69).

Вкладка «Скрипты»

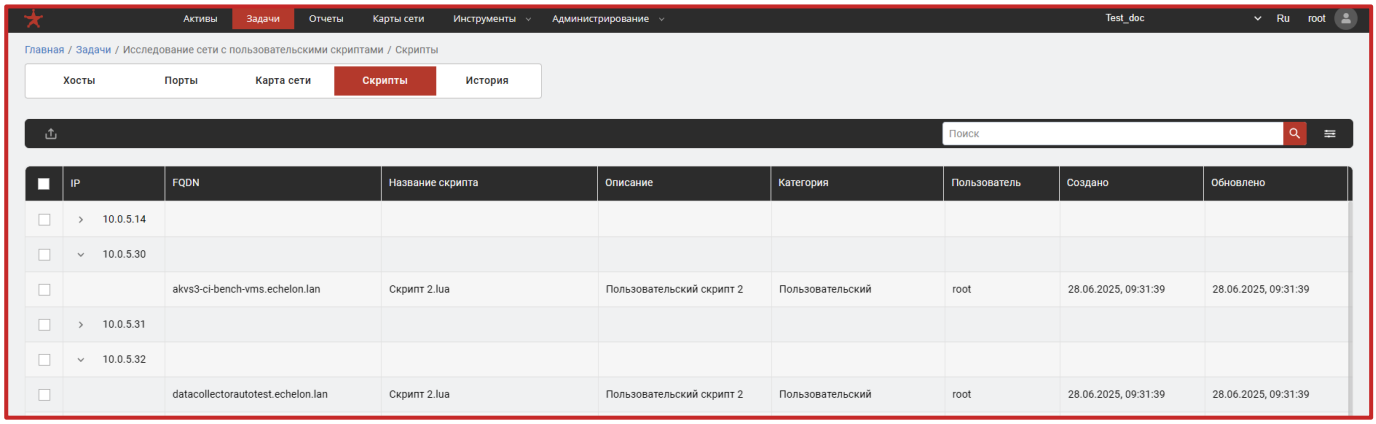


Рис. 69

Сканер-ВС позволяет пользователю просмотреть результаты выполнения выбранного скрипта (рис. 70).

Просмотр результатов выполнения пользовательского скрипта

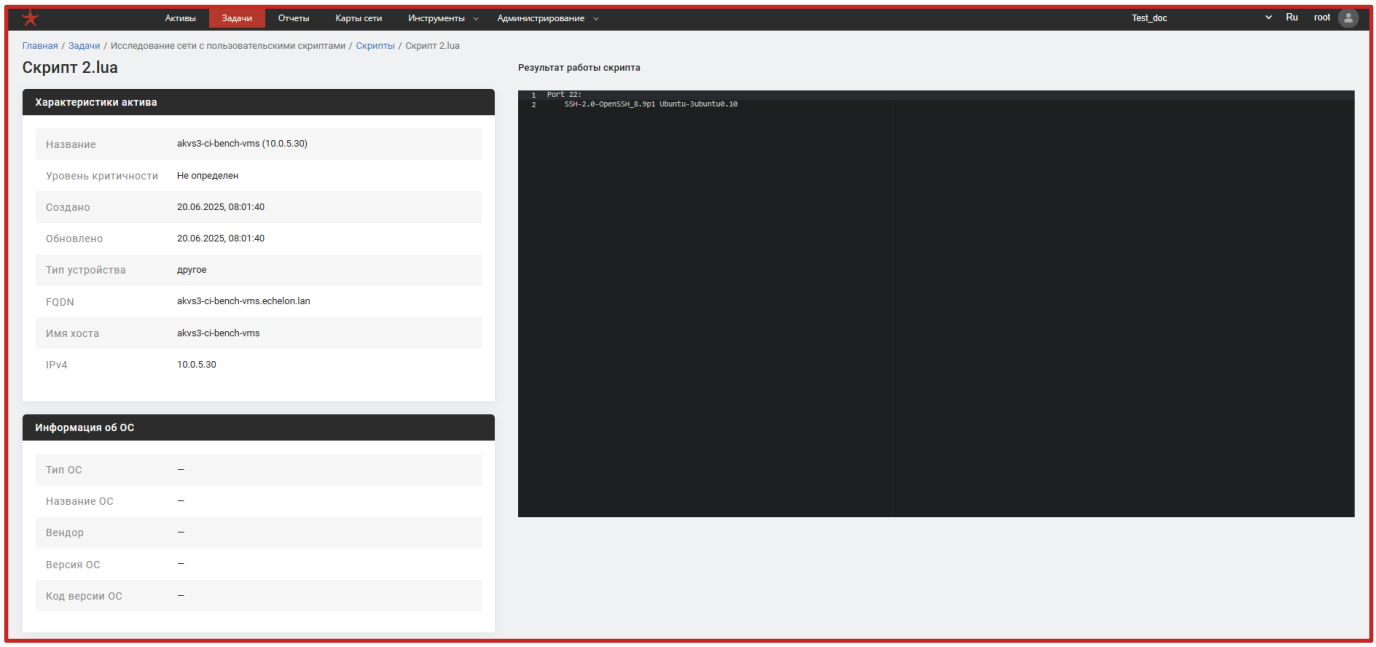


Рис. 70

После каждого запуска задачи «Исследование сети», время, дата, а также остальные параметры ее выполнения будут отображены во вкладке «История» (рис. 71).

История задачи исследования сети

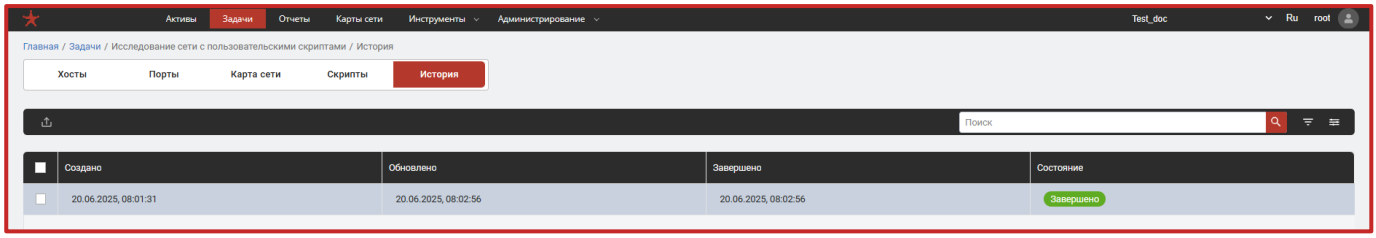


Рис. 71

Сканер-ВС позволяет пользователю просмотреть результаты не только последнего запуска задачи, но и предыдущих. Затемнение строки таблицы истории выполнения задачи показывает для какого из запусков задачи отображены результаты ее выполнения в соответствующих вкладках. Для выбора другого запуска задачи необходимо нажать левой кнопкой мыши в любом месте соответствующей строки таблицы истории выполнения задачи. Данная функция может быть полезна для отслеживания изменений, происходящих в исследуемой сети между запусками задачи.

5.5.4. Инвентаризация

5.5.4.1. Общее описание

«Инвентаризация» в изделии предназначена для активного подключения к исследуемому узлу для сбора информации безагентным способом (подключение к интересующему хосту и получение от него информации, однако, для данного способа необходимы соответствующие полномочия доступа).

«Инвентаризация» доступна только для узлов из списка активов и после успешного заведения административных учетных записей для них (п. 5.9.2.1).

Для ОС Microsoft Windows учетная запись должна быть включена в группу администраторов, для Unix систем учетная запись должна иметь права доступа «root».

При инвентаризации происходит заполнение полученных данных в карточке актива.

Для создания новой задачи на инвентаризацию необходимо зайти на вкладку «Задачи», нажать на кнопку «Добавить задачу +», выбрать тип задачи «Инвентаризация» (рис. 72).

Выбор типа задачи «Инвентаризация»

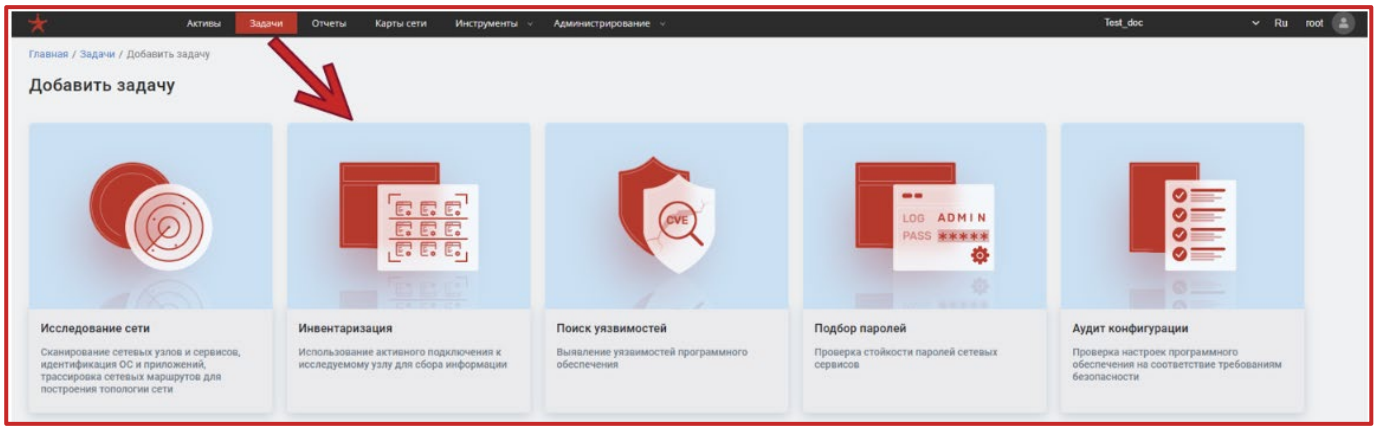


Рис. 72

Страница задачи «Инвентаризация» представлена на рис. 73.

Страница задачи «Инвентаризация»

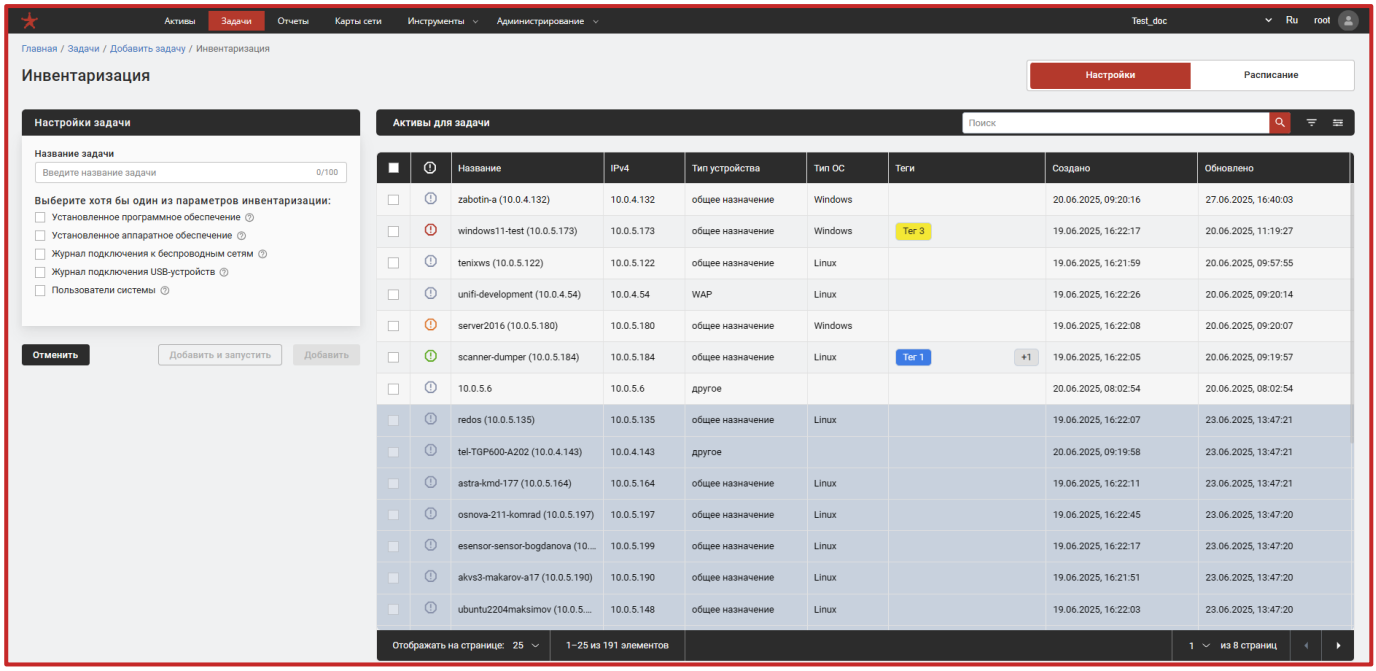


Рис. 73

Страница задачи «Инвентаризация» имеет следующие вкладки:

– «Настройки» (содержит блоки «Инвентаризация» и «Импорт активов»);

– «Расписание».

5.5.4.2. Настройка задачи «Инвентаризация»

Глубину проведения инвентаризации, сохранение и запуск задачи можно выбрать в блоке «Инвентаризация» (рис. 74).

Блок «Инвентаризация»

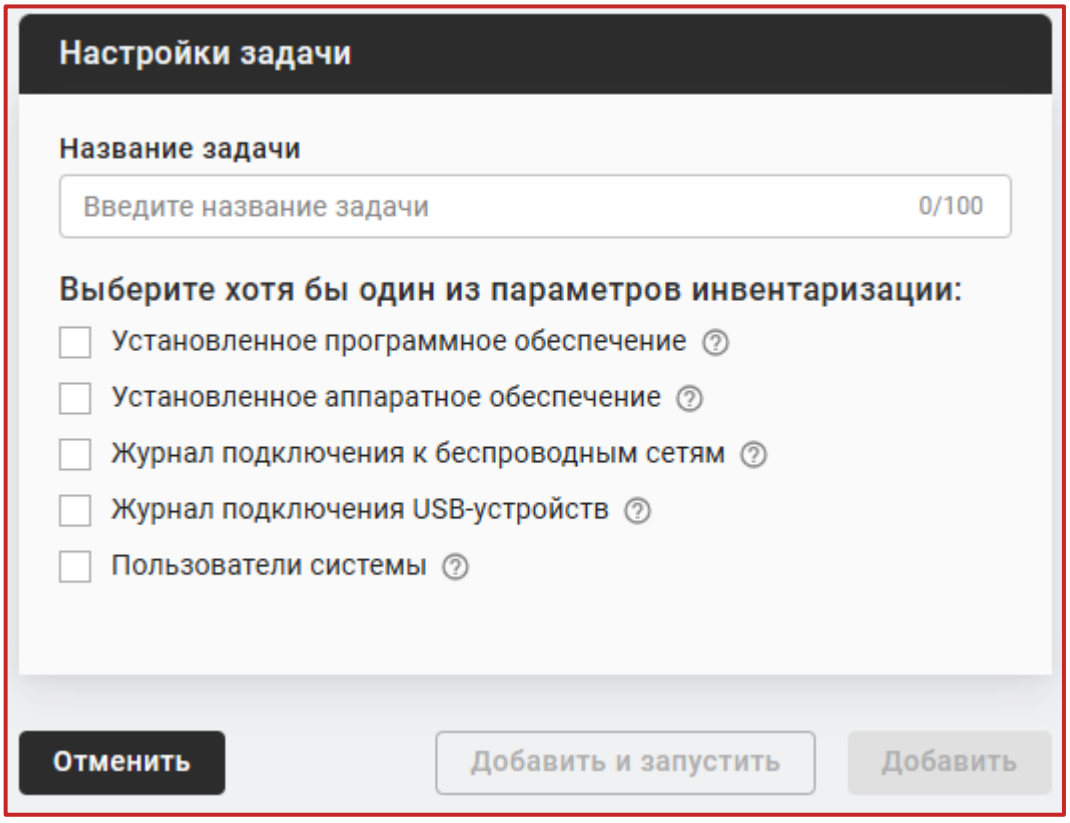


Рис. 74

Наименование задачи записывается в поле «Название задачи» и должно содержать понятное и, желательно, уникальное описание инвентаризации (см. рис. 74). Если не указывать наименование, то по умолчанию оно примет вид: «Инвентаризация».

Выполнение данной задачи заключается в проведении инвентаризации выбранных оператором активов (узлов) из таблицы импорта активов, которая находится на странице справа в блоке «Импорт активов».

При настройке проведения задачи следует активировать необходимые оператору чекбоксы с доступными параметрами «глубины инвентаризации» для более подробного получения информации о активах.

Строки таблицы импорта активов, соответствующие недоступным для выбора активам, будут отображены с затемненным фоном.

После завершения всех настроек, для их сохранения необходимо нажать кнопку «Сохранить». Для запуска задачи необходимо нажать копку «Запустить».

5.5.4.3. Результаты выполнения задачи «Инвентаризация»

В результате успешного выполнения данной задачи появится возможность просмотра таблицы с информацией об активах (узлах), по которым проводилась задача (рис. 75).

Примечание. Для проведения задачи «Инвентаризация» актива исследуемой сети необходимо создать или добавить подключение к данному активу. Не рекомендуется добавлять более одного подключения к активу, т.к. это может привести к дублированию найденного прикладного ПО для данного актива в следствии проведения задачи «Инвентаризации» сразу по всем подключенным к активу учетным записям.

Таблицы с информацией об активах (узлах)

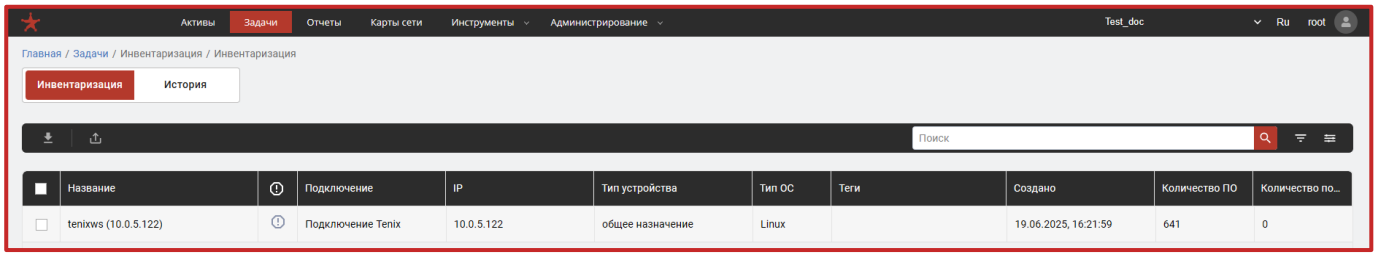


Рис. 75

Иконка «⬇» (кнопка «Скачать») активируется при выборе необходимой строки таблицы и позволяет открыть меню с выбором формата экспорта результатов инвентаризации ПО. С помощью этой функции можно автоматически конвертировать и сохранять список ПО в следующих SBOM-форматах: CycloneDX и SPDX.

Примечание. Встроенная поддержка стандарта SPDX гарантирует корректное заполнение всех обязательных полей и позволяет провести детальный аудит лицензионной информации и состава ПО. Описание формата CycloneDX представлено в п. 5.4.5.5 настоящего документа.

При нажатии на строку таблицы с информацией об активах (узлах), по которым проводилась задача, происходит переход на страницу «Результаты выполнения задачи» по конкретному активу (рис. 76).

Страница «Результаты выполнения задачи»

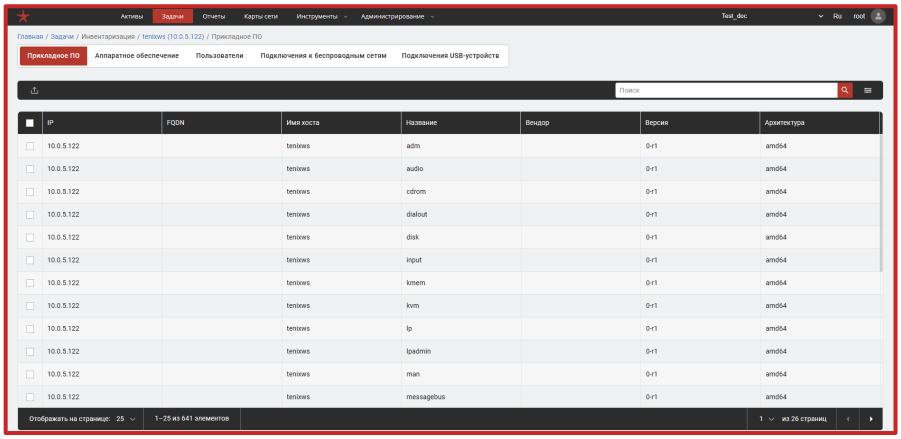


Рис. 76

При возникновении ошибок выполнения команд на активах исследуемой сети над информационной таблицей с результатами задачи предусмотрено появление кнопки «Скачать текст ошибки выполнения команд». Данная кнопка позволяет скачать файл в формате «.txt», содержащий подробную информацию о возникших ошибках.

На данной странице присутствуют следующие вкладки:

– «Прикладное ПО» – отображает результаты инвентаризации в части ПО, определенного на исследуемом активе (рис. 76);

– «Аппаратное обеспечение» – отображает результаты инвентаризации в части аппаратной конфигурации исследуемого актива (рис. 77);

Вкладка «Аппаратное обеспечение»

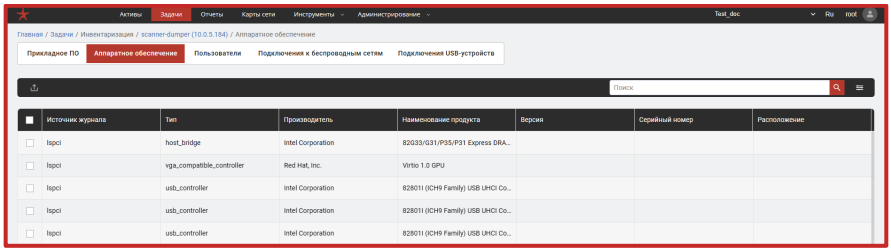


Рис. 77

При нажатии на любую строку таблицы откроется карточка аппаратного обеспечения (рис. 78), содержащая информацию о продукте.

Карточка аппаратного обеспечения

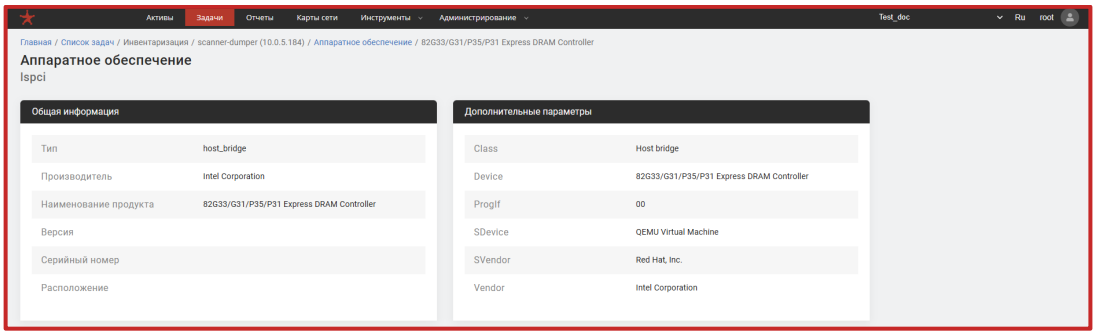


Рис. 78

– «Пользователи» – отображает результаты инвентаризации в части существующих служебных и добавленных на исследуемом активе учетных записей пользователей (рис. 79);

Вкладка «Пользователи»

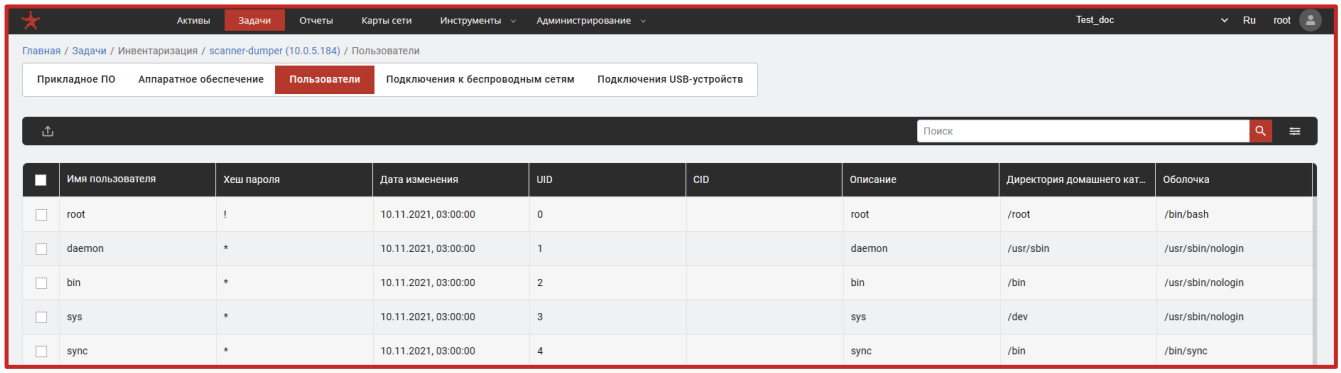


Рис. 79

– «Подключения к беспроводным сетям» – отображает результаты инвентаризации в части зафиксированных в журналах ОС актива беспроводных соединений на исследуемом узле (рис. 80). В данной вкладке ключевым и уникальным параметром является «Название сети» (SSID), а также представлена информация о идентификаторах подключения текущего сетевого профиля и типах подключения – эти параметры необходимы для агрегации истории беспроводных подключений;

Вкладка «Подключения к беспроводным сетям»

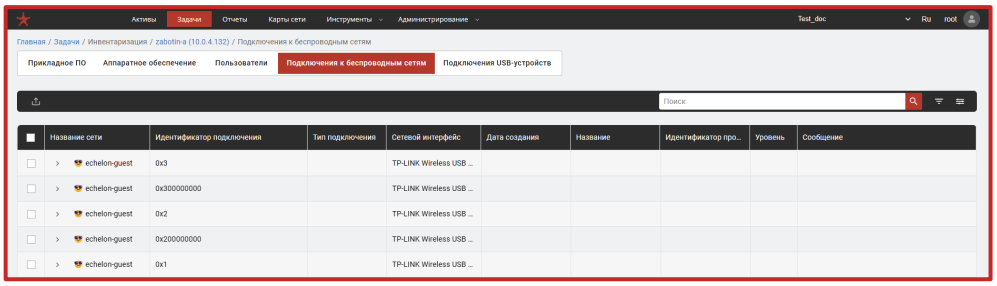


Рис. 80

– «Подключения USB-устройств» – отображает результаты инвентаризации в части обнаруженных в журналах ОС актива USB-подключений и событий, таких как подключение и отключение устройств, а также информацию о производителях и серийных номерах. Таблица включает уникальные идентификаторы устройств, их описания, производителей, серийные номера, пути в системе и время подключения (рис. 81).

Вкладка «Подключения USB-устройств»

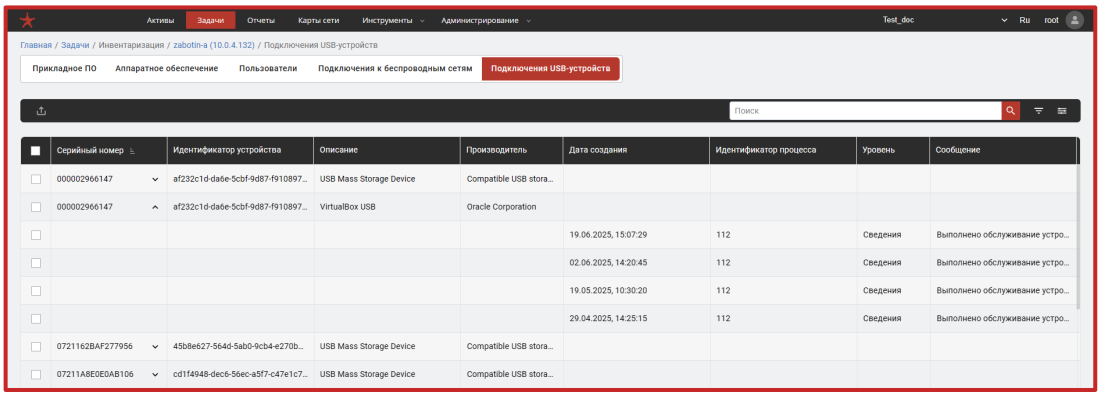


Рис. 81

После каждого запуска данной задачи, время, дата, а также остальные параметры ее выполнения будут отображены во вкладке «История». Вкладка «История» выполненной задачи «Инвентаризация» идентична одноименной вкладке задачи «Исследование сети».

Примечание. В результатах выполнения задачи «Инвентаризация» Сканер-ВС не выводятся сведения о найденных обновлениях. Данная информация сохраняется в базе данных и используется при выполнении задачи «Поиск уязвимостей», а также отображается в карточке соответствующего актива.

5.5.5. Поиск уязвимостей

5.5.5.1. Общее описание

Под уязвимостью ПО подразумевается дефект ПО, который может стать причиной нарушения информационной безопасности. Задача Сканер-ВС «Поиск уязвимостей» направлена на обнаружение таких дефектов.

Дефекты (уязвимости) делятся на разные уровни риска. В банке данных в зависимости от значения базовой оценки уязвимости V (в Сканер-ВС учитываются базовая оценка CVSS 4, CVSS 3 и CVSS 2) используются следующие уровни опасности:

– – низкий уровень, если $0,1 \leq V \leq 3,9$;

– – средний уровень, если $4,0 \leq V \leq 6,9$;

– – высокий уровень, если $7,0 \leq V \leq 8,9$;

– – критический уровень, если $9,0 \leq V \leq 10,0$;

– – уровень критичности не определен в следствии того, что в БДУ не определены ни одна из: CVSS 4, CVSS 3, CVSS 2.

Для создания новой задачи на поиск уязвимостей необходимо зайти на вкладку «Задачи», нажать на кнопку «Добавить задачу +», выбрать тип задачи «Поиск уязвимостей» (рис. 82).

Выбор типа задачи «Поиск уязвимостей»

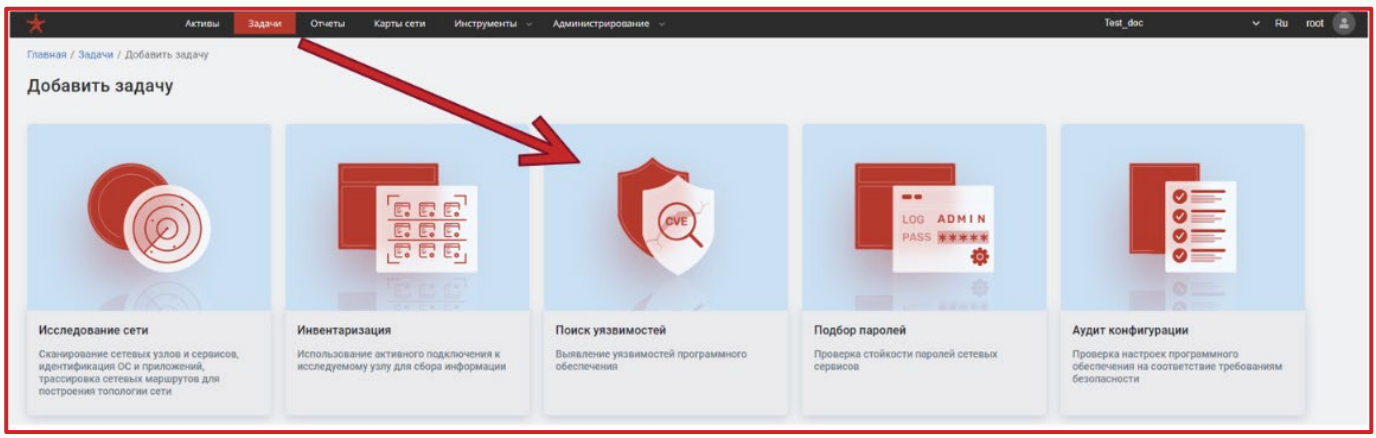


Рис. 82

Страница задачи «Поиск уязвимостей» представлена на рис. 83.

Страница задачи « Поиск уязвимостей»

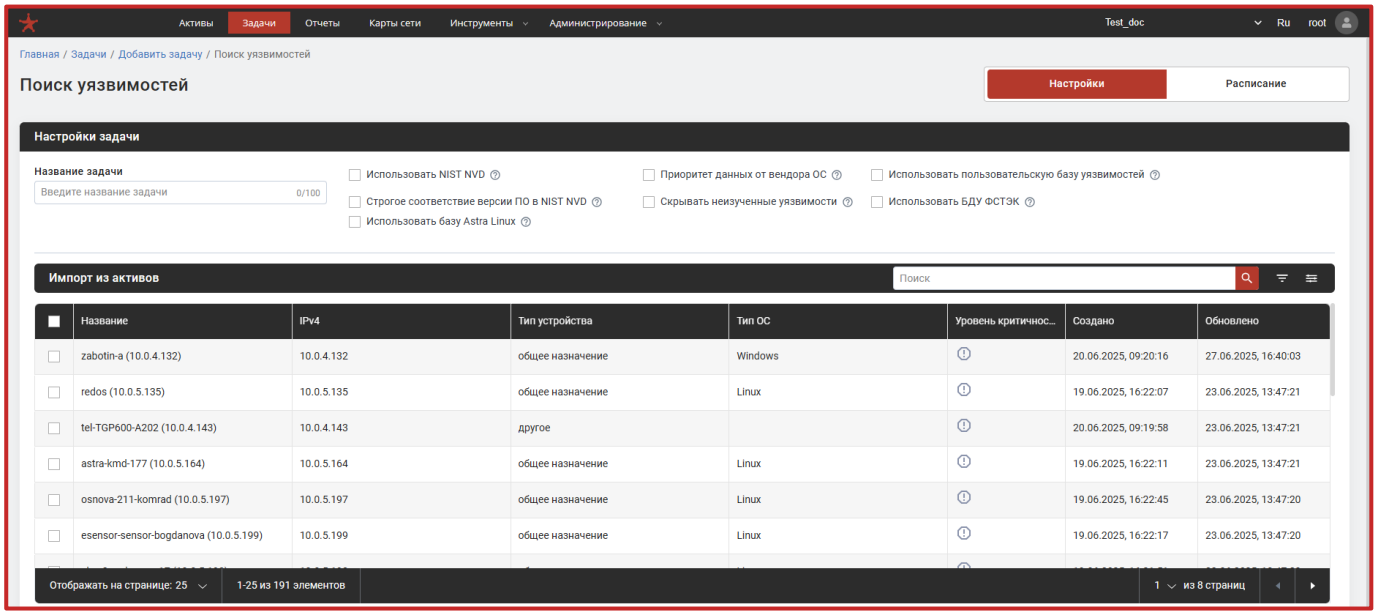


Рис. 83

Страница задачи «Поиск уязвимостей» имеет следующие вкладки:

– «Настройки» (содержит блоки «Настройки задачи» и «Импорт из активов»);

– «Расписание».

5.5.5.2. Настройка задачи «Поиск уязвимостей»

При создании задачи на поиск уязвимостей настраиваются цели для поиска. Цели поиска уязвимостей необходимо задавать, импортируя их из таблицы активов блока «Импорт активов».

Для загрузки из активов целей поиска уязвимостей необходимо отметить нужные активы (рис. 84) из таблицы активов (если актив выбран, рядом с ним в пустом чекбоксе появится галочка) или нажать на пустом чекбоксе в заголовке таблицы рядом со столбцом «Актив» (все активы в таблице будут отмечены автоматически).

Выбор активов из таблицы активов

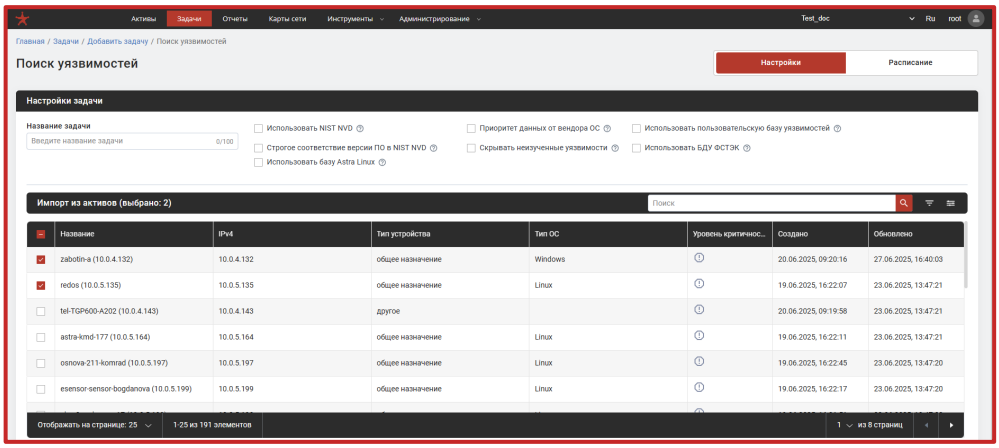


Рис. 84

В верхней части окна настроек задачи «Поиск уязвимости» есть несколько подключаемых опций:

– использовать NIST NVD. Данную опцию рекомендуется включать, если для узла под управлением Linux была проведена инвентаризация, в ходе которой была определена точная версия ОС, и для данной ОС доступны уязвимости из вендорской базы уязвимостей (Ubuntu, Debian, RedHat, Arch, Astra Linux). В этом случае по умолчанию показываются только уязвимости из соответствующей базы вендора, при включенной опции будут добавлены уязвимости из NIST NVD;

– строгое соответствие версии ПО в NIST NVD. Данную опцию рекомендуется включать, если необходимо исключить из результатов поиска уязвимостей, которые были зарегистрированы в NIST NVD с указанием того, что они применимы для всех версий программного обеспечения. Данная опция уменьшает количество ложных срабатываний;

– приоритет данных от вендора ОС. Данную опцию рекомендуется включать для актива под управлением одной из ОС Ubuntu, Debian, RedHat, Arch, Astra Linux после проведенной инвентаризации, она позволит отбросить результаты поиска уязвимостей в NIST NVD в случаях, когда для одной и той же уязвимости есть записи и в NIST NVD, и в базе уязвимостей вендора ОС. Опцию имеют смысл использовать только в случае выбранной опции «Использовать NIST NVD»;

– скрывать неизученные уязвимости. Данную опцию рекомендуется включать, если необходимо исключить из выдачи уязвимости, в описании которых отсутствует какая-либо полезная информация;

– использовать пользовательскую базу уязвимостей. Данную опцию рекомендуется включать, если необходимо совершить поиск и проверку по пользовательским описаниям уязвимостей. Для обновления списка пользовательских уязвимостей необходимо зайти в подраздел «Пользовательские уязвимости» раздела «Администрирование» (управление доступно только оператору с правами доступа «Администратор») и добавить необходимое вручную.

Примечания:

1. Использование опций «приоритет данных от вендора» и «использовать NIST NVD» при выполнении задачи «Поиск уязвимостей» на узлах с ОС семейства Windows нецелесообразно в силу того, что NIST NVD является единственной базой уязвимостей ПО для ОС семейства Windows. В таком случае результаты выполнения задачи «Поиск уязвимостей» с включенными опциями ничем не будут отличаться от результатов с выключенными.

2. Для получения наиболее точного результата выполнения задачи «Поиск уязвимостей» для узла исследуемой сети, функционирующего на базе ОС семейства Windows рекомендуется предварительно провести задачу «Инвентаризация» (п. 5.5.4 настоящего документа) для этого узла и затем провести задачу «Поиск уязвимостей» с включенной опцией «Строгое соответствие версии ПО в NIST NVD».

3. В том случае, если в результатах выполнения задачи необходимо получить уязвимости ядра RedOS, включение опции «использовать NIST NVD» является обязательным.

5.5.5.3. Запуск задачи «Поиск уязвимостей» по расписанию

Настройка расписания автоматического запуска задачи «Поиск уязвимостей» производится аналогично настройке расписания автоматического запуска задачи «Исследование сети» (п. 5.5.3.7 настоящего документа).

После завершения настройки, для их сохранения необходимо нажать кнопку «Сохранить». Для запуска задачи необходимо нажать копку «Запустить».

5.5.5.4. Работа с результатами выполнения задачи «Поиск уязвимостей»

При успешном завершении задачи «Поиск уязвимостей» оператору будет доступен результат во вкладках «Активы» и «Уязвимое ПО». Вкладка «Активы» представляет собой таблицу со списком найденных уязвимостей.

Дополнительно в таблице представлена информация о наличии уязвимости, вероятность эксплуатации уязвимости (EPSS) и список уязвимого ПО, на котором данная уязвимость была найдена (рис. 85).

Список найденных уязвимых пакетов

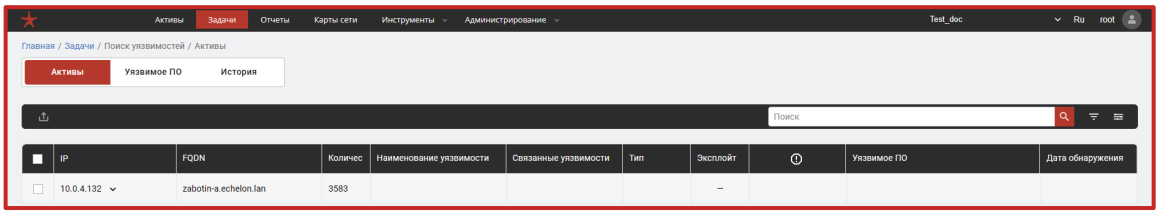


Рис. 85

При нажатии на любую из строк таблицы на вкладке «Уязвимое ПО» происходит переход к просмотру непосредственно уязвимостей, содержащихся в выбранном пакете (рис. 86).

Список уязвимостей в пакете

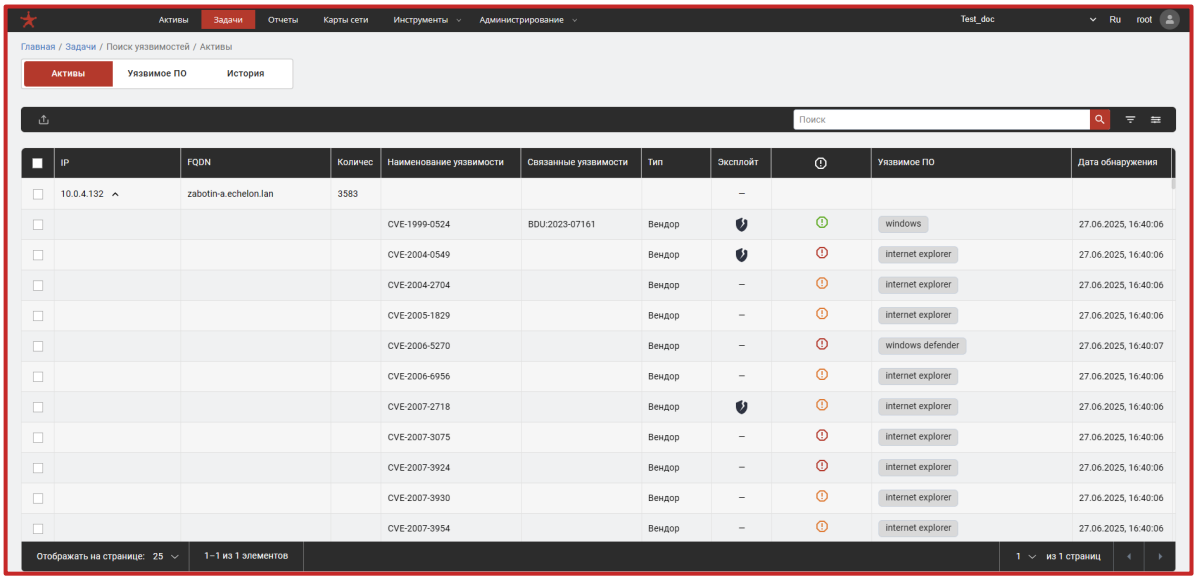


Рис. 86

При нажатии на строку, соответствующую одной из найденных уязвимостей, произойдет переход к карточке уязвимости (рис. 87), которая описана в п. 5.8.4.2 настоящего документа.

После каждого запуска данной задачи, время, дата, а также остальные параметры ее выполнения будут отображены во вкладке «История». Вкладка «История» выполненной задачи «Поиск уязвимостей» идентична одноименной вкладке задачи «Исследование сети» (подробнее в п. 5.5.3.8 настоящего документа).

Карточка найденной уязвимости

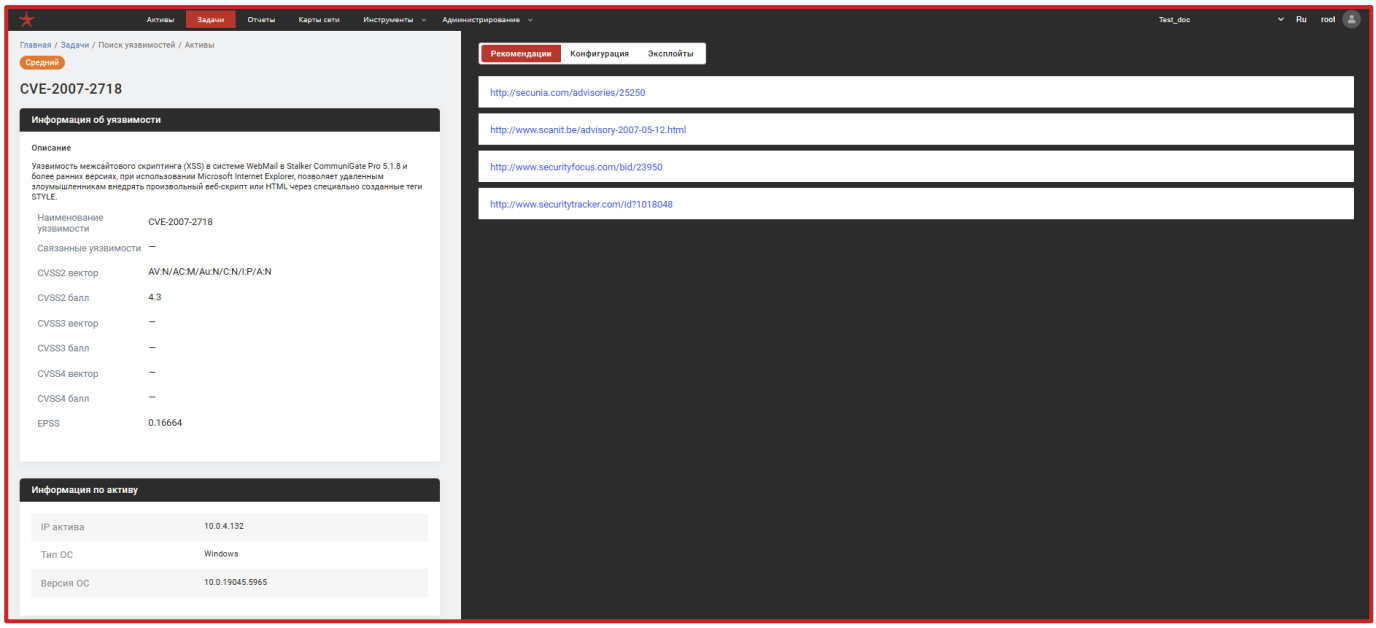


Рис. 87

5.5.6. Подбор паролей

5.5.6.1. Общее описание

Задача подбора паролей – необходима для выявления возможности получения доступа к ресурсам компьютеров в проверяемой сети путем подбора имени и пароля пользователя.

Для проведения задачи подбора пароля необходимо зайти на вкладку «Задачи», нажать на кнопку «Добавить задачу +», выбрать тип задачи «Подбор паролей» (рис. 88).

Выбор типа задачи «Подбор паролей»

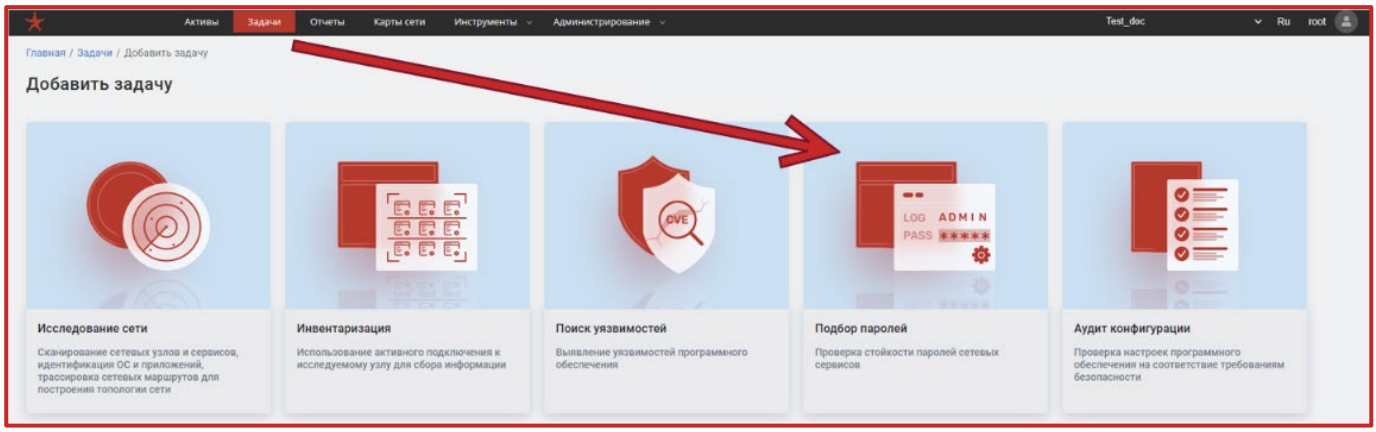


Рис. 88

Страница задачи «Подбор паролей» имеет следующие вкладки (рис. 89):

– «Настройки» (содержит блоки «Настройки задачи», «Пользователи» и «Пароли»);

– «Расписание».

Страница задачи «Подбор паролей»

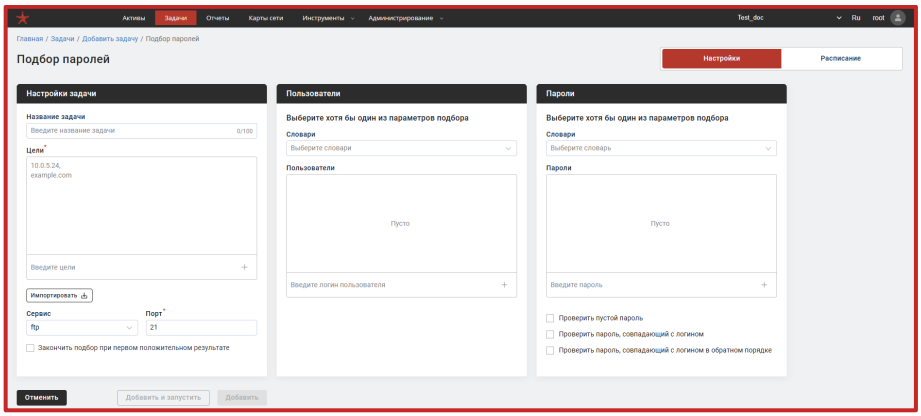


Рис. 89

5.5.6.2. Настройки задачи «Подбор паролей»

Наименование задачи записывается в поле «Название» блока «Настройка задачи» и должно содержать понятное и, желательно, уникальное описание подбора паролей (рис. 90). Если не указывать наименование, то по умолчанию оно примет вид: «Подбор паролей».

Для запуска задачи «Подбор паролей» необходимо указать активы, для которых будет совершена попытка подбора пароля. В Сканер-ВС предусмотрены следующие способы указания целей для подбора паролей:

– непосредственный ввод адреса интересующего актива в поле «Цели»;

– непосредственный ввод IP-адреса подсети в поле «Цели». В данном случае задача будет выполняться для всех доступных активов выбранной подсети;

– импорт целей из активов. Для этого способа необходимо нажать на кнопку «Импорт из активов» и аналогично импорту целей из активов для задачи «Исследование сети» (п. 5.5.3.2 настоящего документа) добавить необходимые активы в цели;

– добавление активов путем ввода тега. Для добавления целей методом выбора активов с определенным тегом необходимо в поле «Цели» написать выражение #`название_тега`, где `название_тега` – название используемого тега, заданное пользователем при создании. Теги описаны в п. 5.8.1 настоящего документа.

Блок «Настройки задачи»

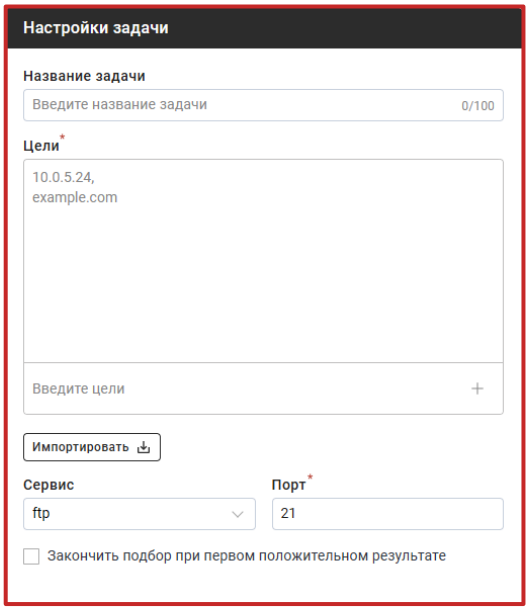


Рис. 90

После ввода IP-адреса в поле ввода «Цели» необходимо нажать на кнопку «+» рядом с ней. После чего введенный IP-адрес отобразится в поле «Цели», что символизирует о добавлении данного актива исследуемой сети в цели для задачи «Подбор паролей».

Для того, чтобы указать сервис (протокол), нужно нажать левой кнопкой мыши на выпадающий список под надписью «Сервис» и выбрать нужный вид сервиса. Перечень сервисов и стандартных портов указан в таблице 5.

Таблица 5 – Сервисы и порты

Сервис	Порт по умолчанию	Описание
imap	143	IMAP (англ. Internet Message Access Protocol) – протокол прикладного уровня для доступа к электронной почте. Порт/ID: 143/TCP
imaps	993	Тоже самое что и IMAP, только IMAP поверх SSL. Порт/ID: 993/TCP
mssql	1433	MSSQL (англ. Microsoft SQL Server) – порт, выбираемый для подключения к SQL Server. Порт/ID: 1433/TCP
mysql	3306	MySQL – протокол подключения к базе данных. Порт/ID: 3306/TCP
pop3	110	POP3 (англ. Post Office Protocol Version 3 - протокол почтового отделения, версия 3) – стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP-соединению. Порт/ID: 110/TCP
pop3s	995	Тоже самое что и POP3, только POP3 поверх SSL. Порт/ID: 995/TCP
postgres	5432	Postgres (англ. postgres database server) – порт, выбираемый для подключения к PostgreSQL. Порт/ID: 5432/TCP
rdp	3389	RDP (англ. Remote Desktop Protocol – протокол удаленного рабочего стола) – проприетарный протокол прикладного уровня, использующийся для обеспечения удаленной работы пользователя с сервером, на котором запущен сервис терминальных подключений. Порт/ID: 3389/TCP
redis	6379	Порт для подключения к Redis (англ. REmote DIctionary Server) – резидентная система управления базами данных класса NoSQL с открытым исходным кодом, работающая со структурами данных типа «ключ – значение». Порт/ID: 6379/TCP

Сервис	Порт по умолчанию	Описание
smtp	25	SMTP (англ. Simple Mail Transfer Protocol – простой протокол передачи почты) – это широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP. Порт/ID: 25/TCP, 587/TCP
smtps	465	Тоже самое что и SMTP, только SMTP поверх SSL. Порт/ID: 465/TCP
snmp	161	SNMP (англ. Simple Network Management Protocol – простой протокол сетевого управления) – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. Порт/ID: 161/UDP, 162/UDP
ssh	22	SSH (англ. Secure Shell – «безопасная оболочка») – сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Порт/ID: 22/TCP
telnet	23	TELNET (сокр. от англ. teletype network) – сетевой протокол для реализации текстового терминального интерфейса по сети (в современной форме – при помощи транспорта TCP). Порт/ID: 23/TCP
vnc	5900	Virtual Network Computing (VNC) – система удаленного доступа к рабочему столу компьютера, использующая протокол RFB (англ. Remote FrameBuffer, удаленный кадровый буфер). RFB (англ. remote framebuffer) – простой клиент-серверный сетевой протокол прикладного уровня для удаленного доступа к графическому рабочему столу компьютера. По умолчанию RFB использует диапазон: Порт/ID: от 5900/TCP до 5906/TCP.

В том случае, если нужно завершить задачу по подбору пароля при первом успешном результате, то необходимо включить опцию «Закончить подбор при первом положительном результате».

В блоке настроек «Пользователи» необходимо задать идентификаторы (имена, логин) пользователей проверяемых рабочих станций (рис. 91). Задать идентификаторы можно следующими способами:

– выбрать один из заранее подготовленных словарей пользователей в выпадающем списке «Словари»;

– ввести логины проверяемых операторов активов вручную в поле «Пользователи» и нажать «+» для добавления введенных данных.

Примечание. В Сканер-ВС можно использовать как один из описанных выше способов добавления логинов, так и оба сразу.

В Сканер-ВС добавлены следующие заранее подготовленные словари пользователей:

– Топ 15 (en);

– Топ 25 женских имен (en);

– Топ 25 мужских имен (en);

– Топ 50 (en+ru).

Ручной ввод пользователей для проверки аналогичен ручному вводу целей для подбора паролей.

Блок настроек «Пользователи»

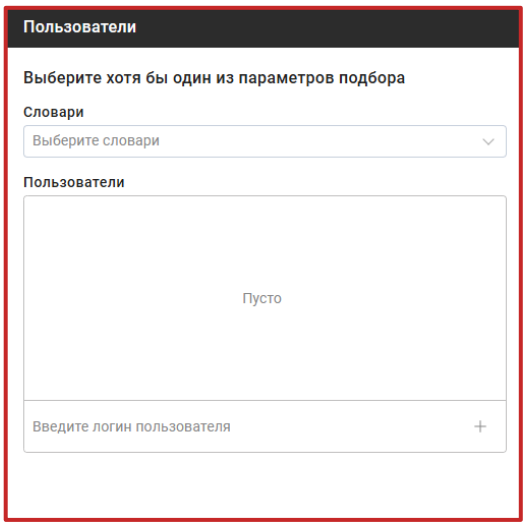


Рис. 91

Для запуска задачи «Подбор паролей» в блоке настроек «Пароли» необходимо установить какие пароли будут подбираться при запуске задачи (рис. 92). Сделать это можно следующими способами:

– подключить один из заранее подготовленных словарей в выпадающем списке «Словари»;

– вручную ввести пароли в поле «Пароли» с помощью строки «Введите пароль…»;

– выбрать одну или несколько из следующих функций, активировав соответствующий чекбокс:

а) проверить пустой пароль;

б) проверить пароль, совпадающий с логином;

в) проверить пароль, совпадающий с логином в обратном порядке.

Примечание. В блоке настроек «Пароли» можно выбрать как один из описанных выше способов установки паролей, так и все сразу или любую комбинацию способов выбора паролей для подбора и дополнительных функций.

Блок настроек «Пароли»

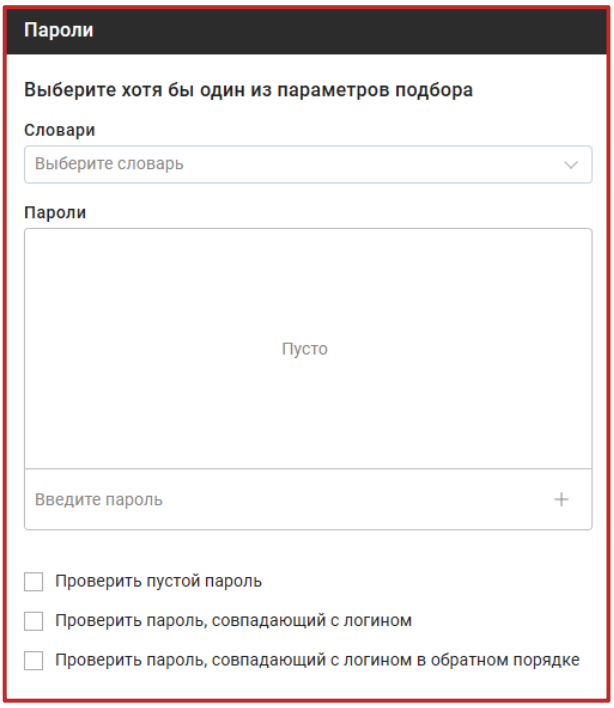


Рис. 92

В Сканер-ВС добавлены следующие заранее подготовленные словари паролей:

– цифры;

– женские имен (en);

– клавиатурные сочетания (en);

– мужские имена (en);

– топ 150 (en);

– топ 25 (en).

Ручной ввод паролей для проверки аналогичен вводу пользователей.

В том случае, если пользователем включена одна из трех опций внизу окна «Пароли», пароли, с которыми необходимо сравнивать проверяемые пароли можно не задавать.

ВАЖНО:

1. Использование больших пользовательских словарей сильно увеличивает время выполнения задачи.

2. Ввиду технических особенностей работы сервиса VNC – необходимо проводить выполнение задачи с использованием данного сервиса **несколько раз**.

5.5.6.3. Расписание задачи «Подбор паролей»

Настройка расписания автоматического запуска задачи «Подбор паролей» производится аналогично настройке расписания автоматического запуска задачи «Исследование сети» (п. 5.5.3.7 настоящего документа).

После завершения настройки, для ее сохранения необходимо нажать «Сохранить». Для запуска задачи необходимо нажать копку «Запустить».

5.5.6.4. Результаты выполнения задачи «Подбор паролей»

В результате успешного выполнения данной задачи появится возможность просмотра списка подключений, для которых были подобраны пароли (рис. 93).

Список учетных записей

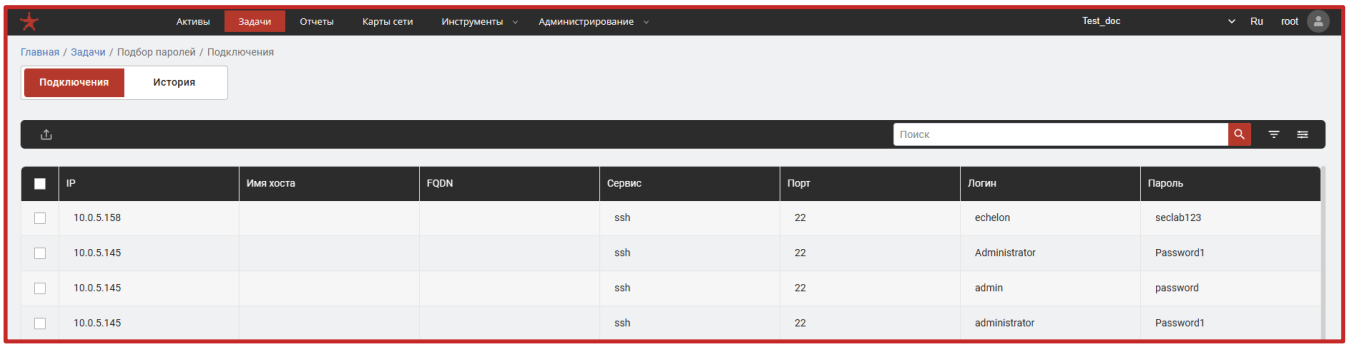


Рис. 93

После каждого запуска данной задачи, время, дата, а также остальные параметры ее выполнения будут отображены во вкладке «История». Вкладка «История» выполненной задачи «Подбор паролей» идентична одноименной вкладке задачи «Исследование сети».

5.5.7. Аудит конфигурации

5.5.7.1. Общее описание

Задача аудита конфигурации – проверка настроек программного обеспечения на соответствие требованиям безопасности. Это один из самых мощных инструментов, который можно использовать для анализа целостности системы в рамках общей стратегии безопасности. Аудит конфигурации определяет какие угрозы, связанные с настройками ПО, представляют опасность для сети и инфраструктуры. Следуя рекомендациям и исправляя параметры настройки ПО согласно результатам аудита конфигурации, можно повысить безопасность и управляемость сети.

Для ОС Microsoft Windows учетная запись должна быть включена в группу администраторов, для Unix систем учетная запись должна иметь права доступа «root».

Для проведения задачи аудита конфигурации необходимо зайти на вкладку «Задачи», нажать на кнопку «Добавить задачу +», выбрать тип задачи «Аудит конфигурации» (рис. 94).

Выбор типа задачи «Аудит конфигурации»

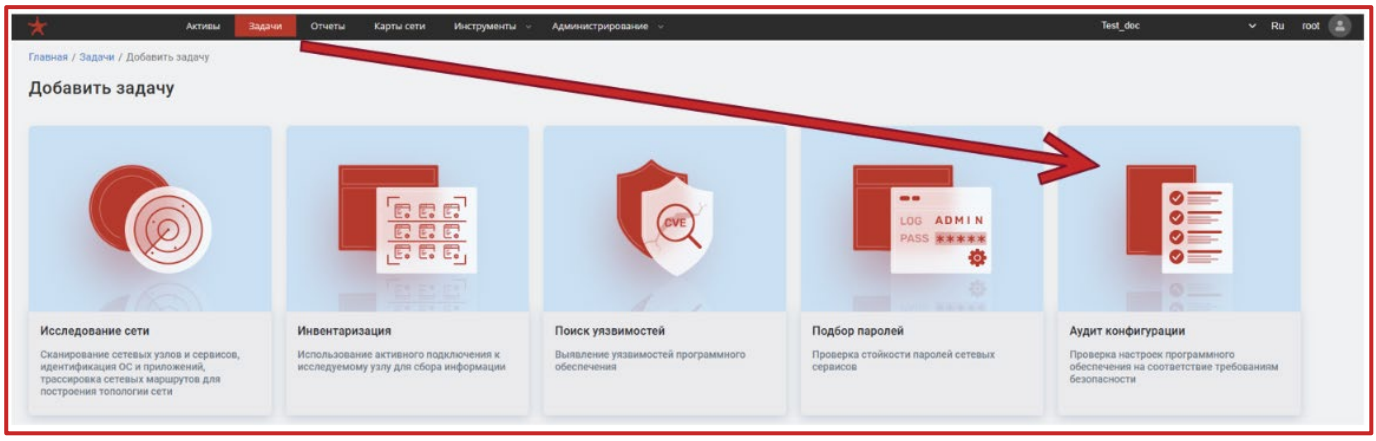


Рис. 94

Страница задачи «Аудит конфигурации» (рис. 95) имеет следующие вкладки:

– «Настройки» (содержит блоки «Настройки задачи» и «Импорт активов»);

– «Расписание».

Страница настройки задачи «Аудит конфигурации»

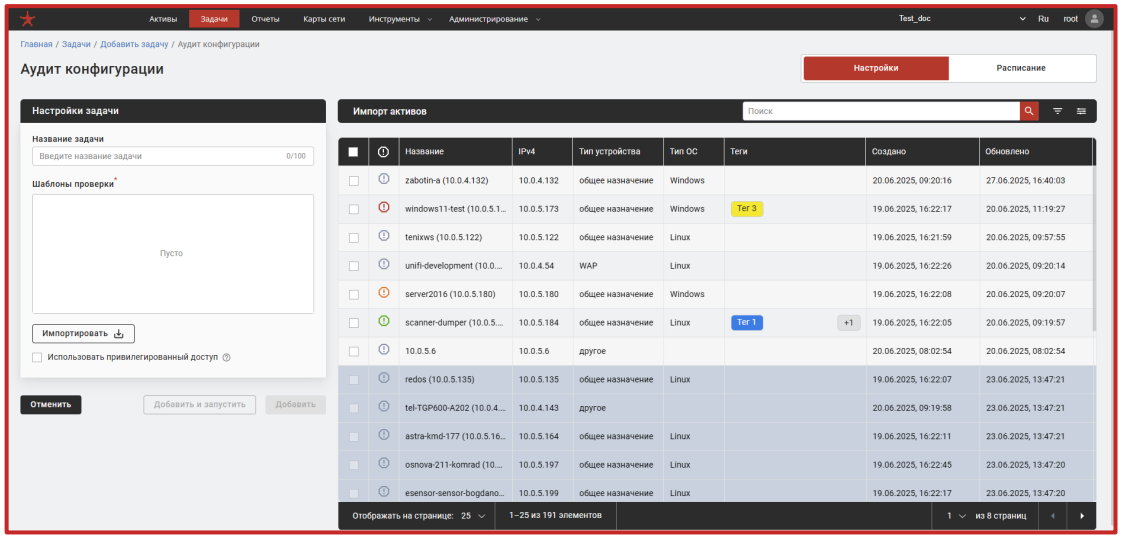


Рис. 95

5.5.7.2. Настройки задачи «Аудит конфигурации»

Конфигурации, шаблоны аудита, сохранение и запуск задачи «Аудит конфигурации» можно выбрать в блоке «Настройки задачи» (рис. 96).

Поле «Шаблоны проверки» и кнопка «Выбрать из списка шаблонов» в блоке «Настройки задачи» – **обязательная настройка** для проведения данной задачи, в котором по кнопке «Выбрать из списка шаблонов» необходимо выбрать из открывшейся таблицы ранее добавленные шаблоны для проведения аудита конфигурации. По выбранным шаблонам будет происходит проверка.

Примечание. Для запуска и проведения задачи «Аудит конфигурации» необходимо иметь хотя-бы 1 добавленный ранее шаблон проверки иначе задача не будет сохранена и/или запущена.

Блок «Настройки задачи»

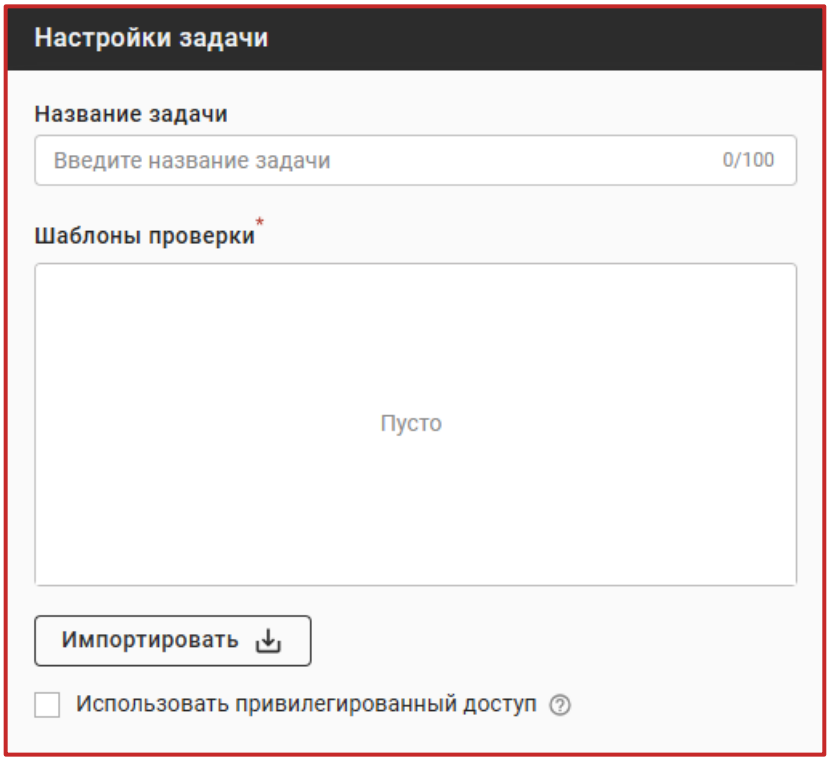


Рис. 96

Выполнение данной задачи заключается в проведении аудита конфигурации выбранных оператором активов (узлов) из таблицы импорта активов, которая находится на странице справа в блоке «Импорт активов».

Наименование задачи записывается в поле «Название задачи» блока «Настройки задачи» и должно содержать понятное и, желательно, уникальное описание аудита конфигурации. Если не указывать наименование, то по умолчанию оно примет вид: «Аудит конфигурации».

При создании задачи на аудит конфигурации активов настраиваются цели для поиска. Цели поиска уязвимостей необходимо задавать, импортируя их из активов.

Для загрузки из активов целей поиска уязвимостей необходимо отметить нужные активы из таблицы блока «Импорт активов» (если актив выбран, рядом с ним в пустом чекбоксе появится галочка) или нажать на пустом чекбоксе в заголовке таблицы рядом со столбцом «Актив» (все доступные активы в таблице будут отмечены автоматически – см. рис. 97).

Выбор всех доступных активов для задачи

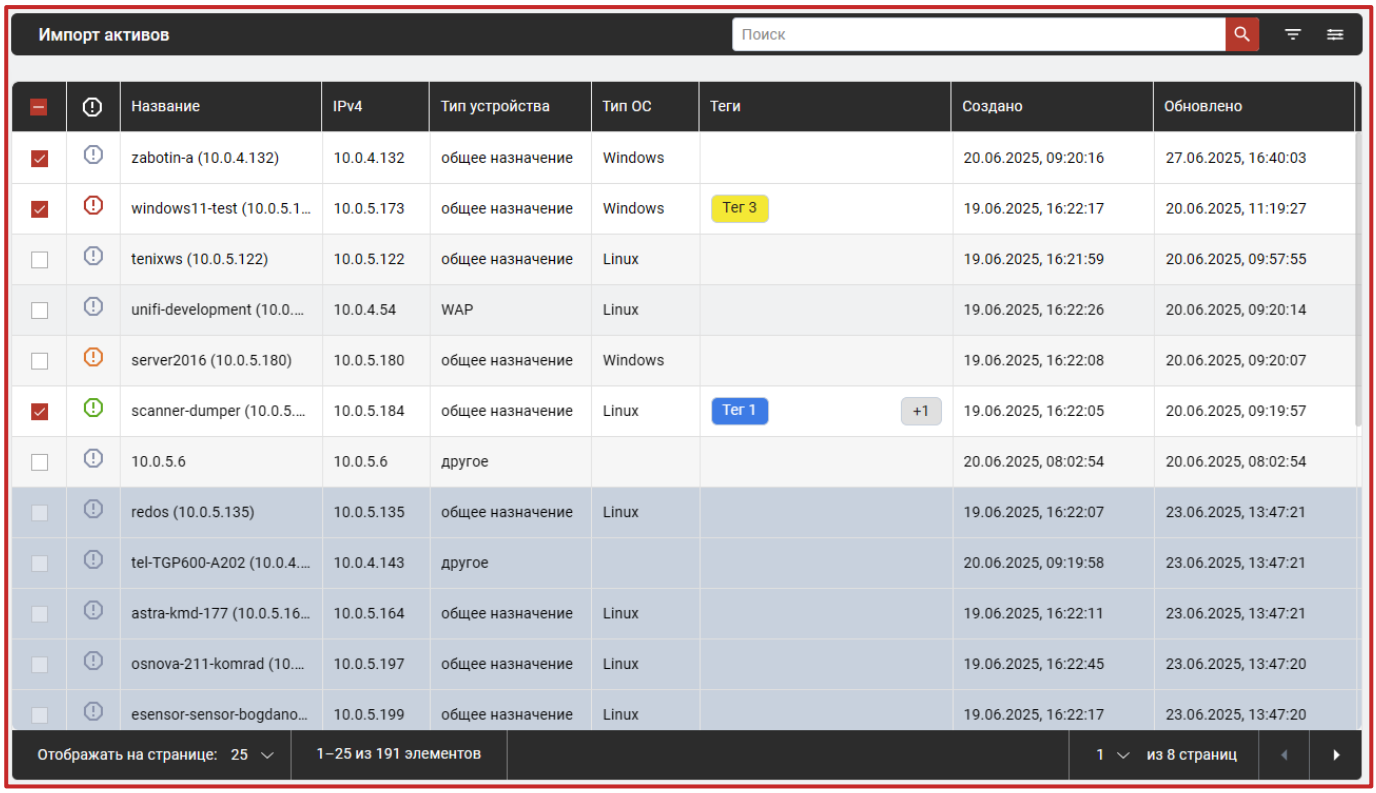


Рис. 97

5.5.7.3. Расписание задачи «Аудит конфигурации»

Настройка расписания автоматического запуска задачи «Аудит конфигурации» производится аналогично настройке расписания автоматического запуска задачи «Исследование сети» (п. 5.5.3.7 настоящего документа).

После завершения настройки, для ее сохранения необходимо нажать «Сохранить». Для запуска задачи необходимо нажать копку «Запустить».

5.5.7.4. Результаты выполнения задачи «Аудит конфигурации»

В результате успешного выполнения данной задачи появится возможность просмотра списка угроз, связанных с настройками программного обеспечения, установленного на активе, с указанием результатов проверки (рис. 98 и 99).

Результат проверки задачи аудит конфигурации

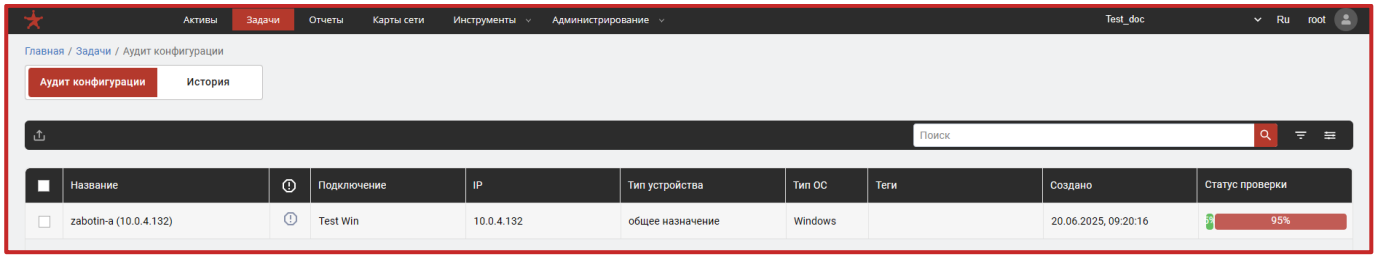


Рис. 98

Примечание. Для проведения задачи «Аудит конфигурации» актива исследуемой сети необходимо создать или добавить подключение к данному активу. Не рекомендуется добавлять более одного подключения к активу, т.к. это может привести к дублированию найденного прикладного ПО для данного актива в следствии проведения задачи «Аудит конфигурации» сразу по всем подключенным к активу учетным записям.

Список угроз, связанных с настройками ПО

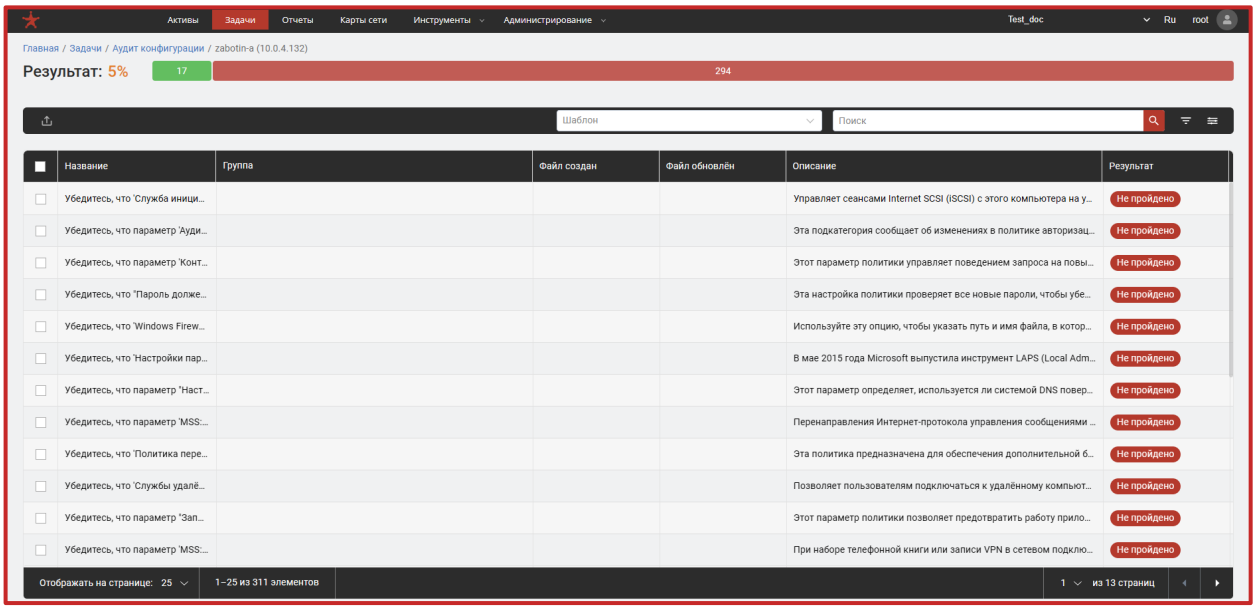


Рис. 99

В списке угроз, связанных с настройками ПО отображаются результаты проведения проверок по всем примененным при настройке задачи шаблонам аудита. Для отображения результатов прохождения проверок по какому-либо одному из шаблонов необходимо выбрать интересующий шаблон в выпадающем списке в левой части строки, расположенной над заголовком таблицы.

Кликнув на параметр, можно перейти к более подробному описанию (рис. 100).

Описание обнаруженного уязвимого ПО

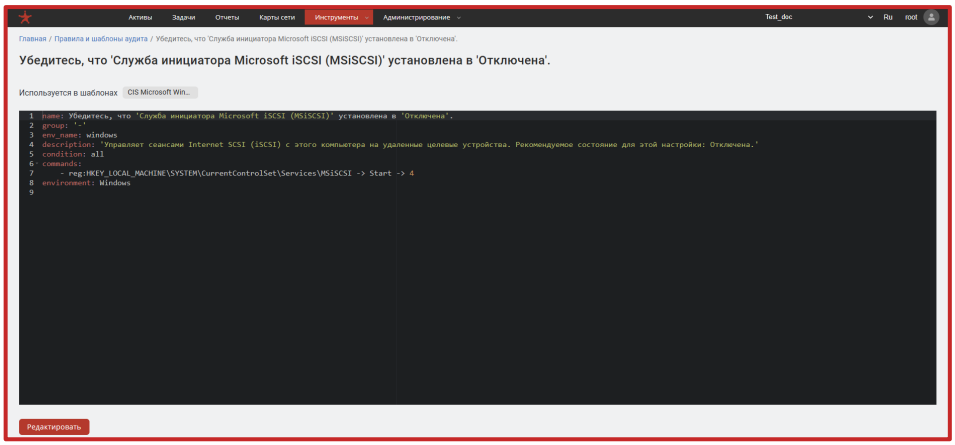


Рис. 100

После каждого запуска данной задачи, время, дата, а также остальные параметры ее выполнения будут отображены во вкладке «История» (рис. 101). Вкладка «История» выполненной задачи «Подбор паролей» идентична одноименной вкладке задачи «Исследование сети» (п. 5.5.3.8 настоящего документа).

Вкладка «История»

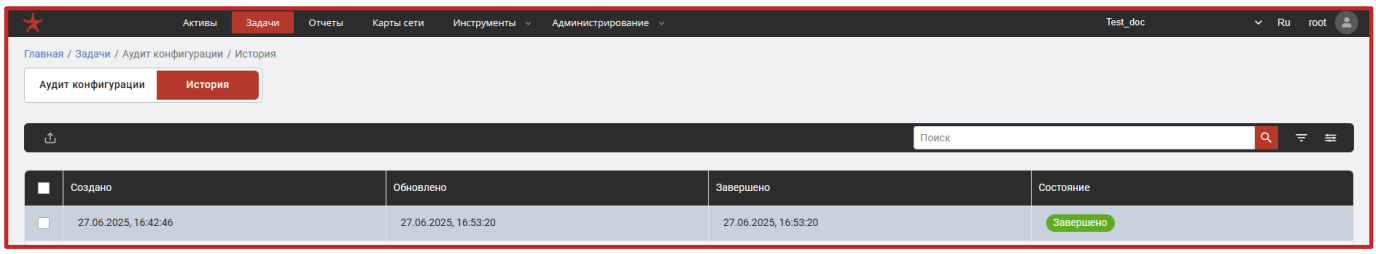


Рис. 101

5.5.8. Управление задачами

5.5.8.1. Редактирование задач

В Сканер-ВС предусмотрена возможность редактирования завершенных задач для последующего повторного их запуска с уточненными данными.

Для редактирования задачи необходимо нажать на «⋮» (рис. 102) и в открывшемся окне нажать на «Редактировать». После чего откроется окно настроек задачи, соответствующее типу редактируемой задачи.

Список задач

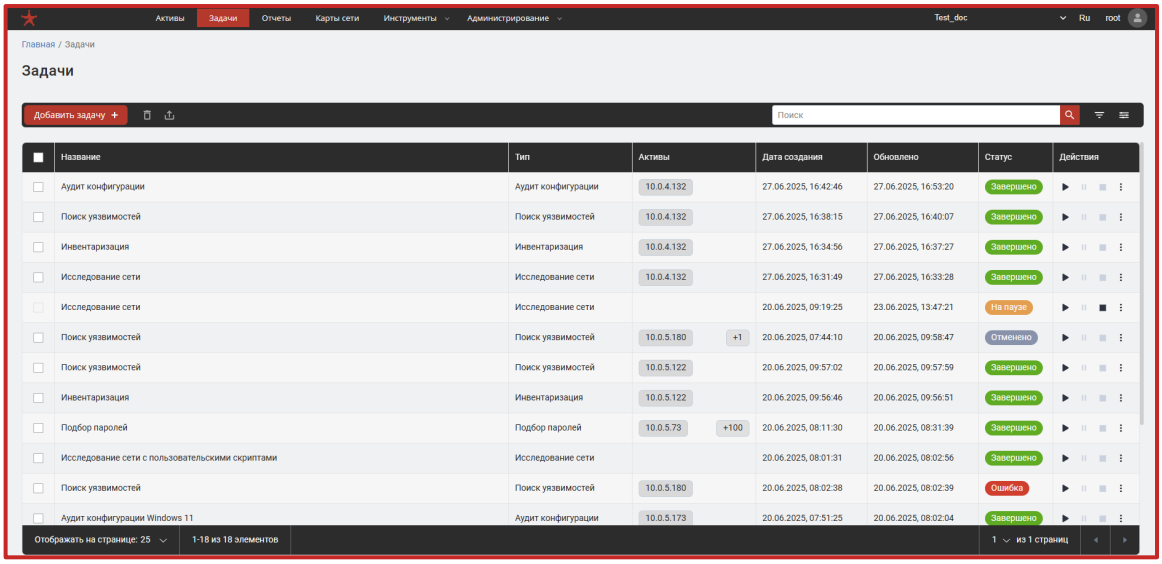


Рис. 102

В Сканер-ВС предусмотрено редактирование не только основных настроек завершенных задач, но и запуска этих задач по расписанию. Для редактирования запуска задачи по расписанию необходимо перейти на вкладку «Расписание» завершенной задачи.

После внесения изменений в настройки задачи необходимо нажать на кнопку «Сохранить» для подтверждения внесенных изменений.

Для удобства пользователя в задачах «Поиск уязвимостей», «Аудит конфигурации» и «Инвентаризация» в окне редактирования завершенных задач указываются активы исследуемой сети, для которых данные задачи проводились ранее.

5.5.8.2. Удаление нескольких задач

В Сканер-ВС наряду с удалением одной задачи из таблицы завершенных задач, описанным в п. 5.5.1 настоящего документа, предусмотрена функция удаления нескольких задач одновременно. Для этого необходимо выбрать задачи, которые необходимо удалить в таблице задач (см. рис. 50) и нажать на кнопку «Удалить». После чего в открывшемся окне подтверждения нажать кнопку «Удалить» для подтверждения удаления выбранных задач. В противном случае – кнопку «Отменить».

Примечание. Задача, находящаяся в статусе «В процессе», не может быть выбрана как для удаления, так и для импорта данных из таблицы задач.

5.6. Отчеты

Документирование является неотъемлемой частью анализа защищенности информационной системы. Для объединения результатов всех этапов проверок в Сканер-ВС используется вкладка «Отчеты» (рис. 103), с помощью которой можно построить отчет с результатами тестирований.

Переход ко вкладке «Отчеты»

Рис. 103

5.6.1. Общее описание

После того как была выбрана вкладка «Отчеты», Сканер-ВС отобразит страницу с готовыми отчетами (рис. 104).

Страница с отчетами

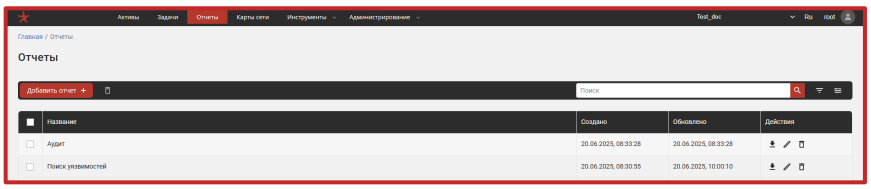


Рис. 104

Во вкладке «Отчеты» находится таблица (рис. 104), которая содержит в себе следующие данные:

– наименование отчета (столбец «Название»);

– дата и время создания отчета (столбец «Создано»);

– дата и время последнего редактирования (столбец «Обновлено»);

– действия с отчетом (столбец «Действия»):

а) скачать – « ⬇ »;

б) редактировать – « ✎ »;

в) удалить – « 🗑 ».

5.6.2. Добавление отчета

Для того, чтобы создать новый отчет необходимо нажать на кнопку «Добавить отчет +» (рис. 105).

Добавление нового отчета

Рис. 105

После нажатия на иконку «Добавить отчет +» откроется интерфейс заполнения формы для нового отчета (рис. 106).

Форма добавления нового отчета

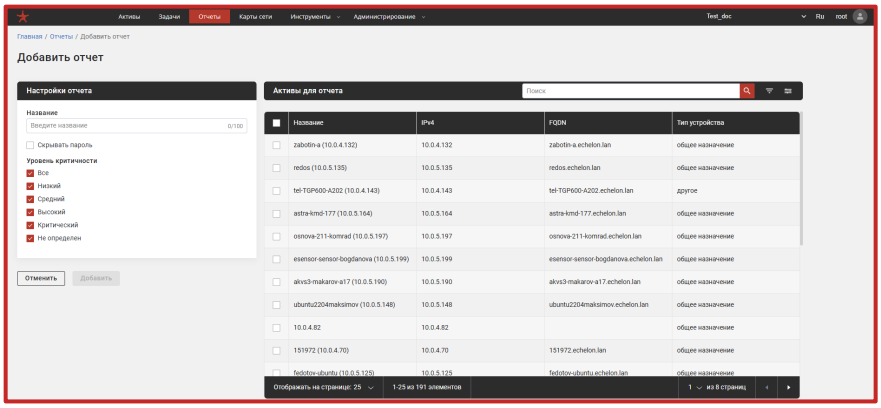


Рис. 106

Страница формы добавления нового отчета имеет следующие блоки:

– «Настройки отчета» (рис. 107);

– «Активы».

Блок «Настройки отчета»

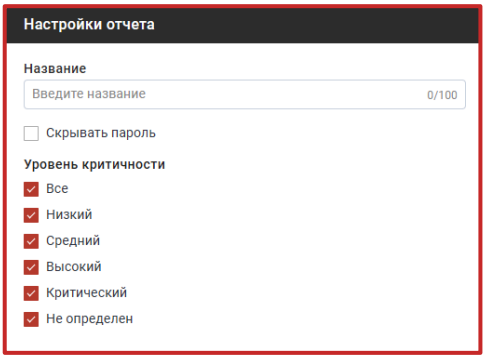


Рис. 107

Для настройки создания отчета в блоке «Настройки отчета» доступны следующие параметры:

– поле «Название» – наименование отчета должно содержать понятное и, желательно, уникальное описание. Если не указывать наименование, то по умолчанию оно примет вид: «Новый отчет»;

– чекбокс «Скрывать пароль» – при активации данной функции в сформированном отчете будут скрыты определенные изделием пароли (касаемо задачи «Подбор паролей»);

– группа чекбоксов «Уровень критичности» – содержит чекбоксы «Все», «Низкий», «Средний», «Высокий», «Критический», «Не определен» для указания уровня опасности уязвимостей.

Примечание. В Сканер-ВС нельзя создать отчет в том случае, если не выбран ни один из вариантов уровня критичности.

Блок «Активы для отчета» – представляет собой таблицу и предназначен для выбора активов, для которых будет сгенерирован отчет.

После заполнения всех обязательных полей (выбора уровня критичности и активов) появится возможность создания параметров для формирования отчета (кнопка «Создать отчет» снизу блока «Создание отчета» – станет активной). После нажатия на кнопку «Создать отчет» произойдет переход обратно к вкладке «Отчеты», а в таблице отчетов отобразиться созданный ранее отчет.

ВНИМАНИЕ!

Во время генерации отчета нельзя обновлять страницу Сканер-ВС. Обновление страницы приведет к ошибке при генерации отчета.

5.6.3. Управление отчетами

После сохранения параметров для генерации отчета, отчету будет присвоен уникальный идентификатор, а в столбцы таблицы с отчетами будут занесены необходимые данные (рис. 104).

Управлять отчетом можно посредством действий, изображенных на рис. 108.

Управление отчетами

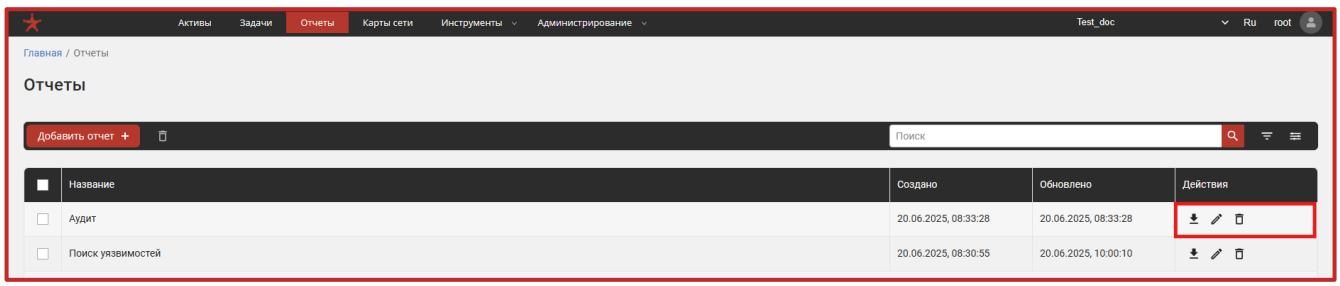


Рис. 108

При выборе действия «Скачать», появится окно «Скачать отчет» с выбором типа отчета (рис. 109). Формат для формирования отчетов в изделии: «.html».

Окно «Скачать отчет»

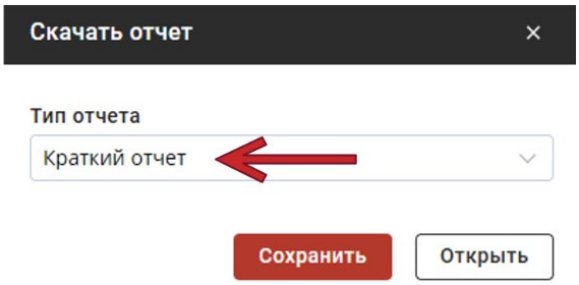


Рис. 109

При указании краткого отчета будет выведена необходимая основная информация для анализа инфраструктуры, с указанием:

– краткого резюме:

а) распределение уязвимостей по уровню критичности;

б) перечень активов, выбранных для формирования отчета;

в) распределение активов по типам ОС;

г) топ-5 наиболее уязвимых активов;

д) топ-5 программных пакетов по количеству уязвимостей.

– выявленных уязвимостей (в виде перечня обнаруженных уязвимостей с заданными при формировании отчета уровнями критичности);

– подобранных паролей (в виде перечня учетных записей, пароли к которым удалось подобрать в ходе тестирования).

При указании полного отчета будет выведена вся информация для анализа инфраструктуры, с указанием:

– резюме (формируется точно также, как и текст резюме в кратком отчете);

– информация по каждому активу, заданному при формировании отчета, с указанием:

а) общей информации (тип устройства, ОС, инвентаризация, количество обнаруженных уязвимостей на данном узле и их распределение по уровню критичности, подобранные пароли, результаты аудита конфигурации);

б) полные данные по каждой уязвимости, найденной в результате тестирования (CVE, BDU, уровень опасности, уязвимое ПО, порт, CVSS 2.0, CVSS2 вектор, CVSS 3.0, CVSS3 вектор, описание, рекомендации).

После заполнения окна «Скачать отчет» (рис. 109) появится возможность сохранения отчета, либо его открытия в браузере (рис. 110).

Титульный лист отчета в браузере

Рис. 110

При выборе действия «Редактировать» в изделии отобразится окно редактирования параметров отчета, изображенное на рис. 111.

Окно редактирования параметров отчета

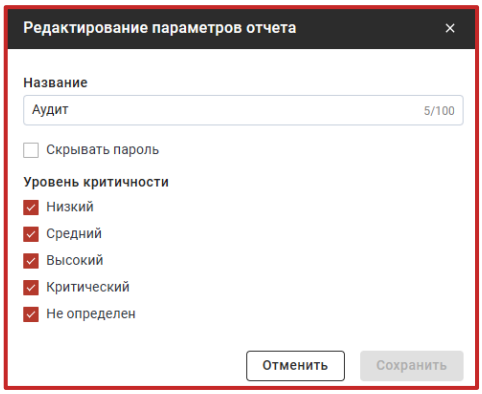


Рис. 111

После внесения изменений в параметры отчета необходимо нажать на кнопку «Сохранить», которая станет активной, для подтверждения внесенных изменений. В противном случае необходимо нажать на кнопку «Отменить».

5.7. Карты сети

Связи между активами в сети представлены в виде карты сети. Она строится на основе информации об активе или группе активов.

Для отображения топологии сети используется специальный интерфейс, доступ к которому осуществляется нажатием кнопки «Карты сети» на панели навигации, после чего откроется вкладка «Карты сети» (рис. 112).

5.7.1. Общее описание

При переходе во вкладку «Карты сети» в Сканер-ВС отображается таблица с созданными ранее картами сети (рис. 112).

Вкладка «Карты сети»

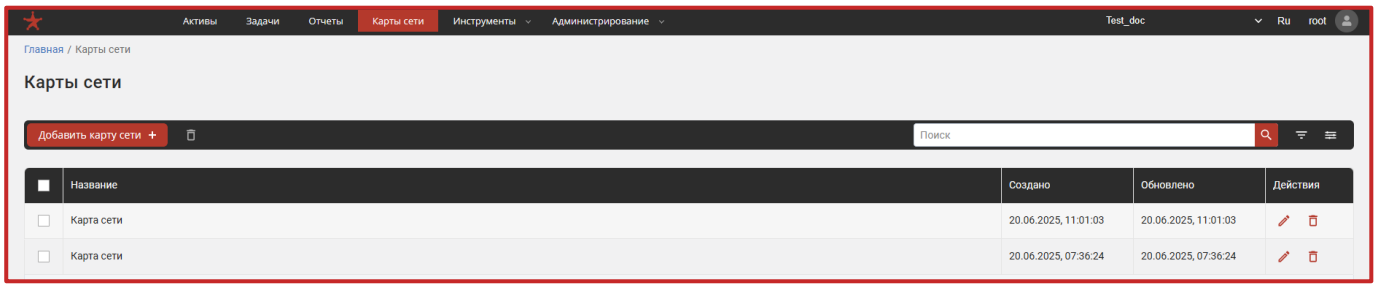


Рис. 112

В таблице карт сети отображаются созданные ранее карты сети и следующие их параметры:

– название – заданное оператором название карты сети при ее добавлении;

– создано – дата и время создания карты сети;

– обновлено – дата и время последнего обновления карты сети;

– действия – предусмотренные в изделии функции управления картой сети (редактирование и удаление).

Для добавления новой карты сети необходимо нажать на кнопку «Добавить карту сети +». После чего произойдет переход на страницу «Новая карта сети» (рис. 113).

Страница «Новая карта сети»

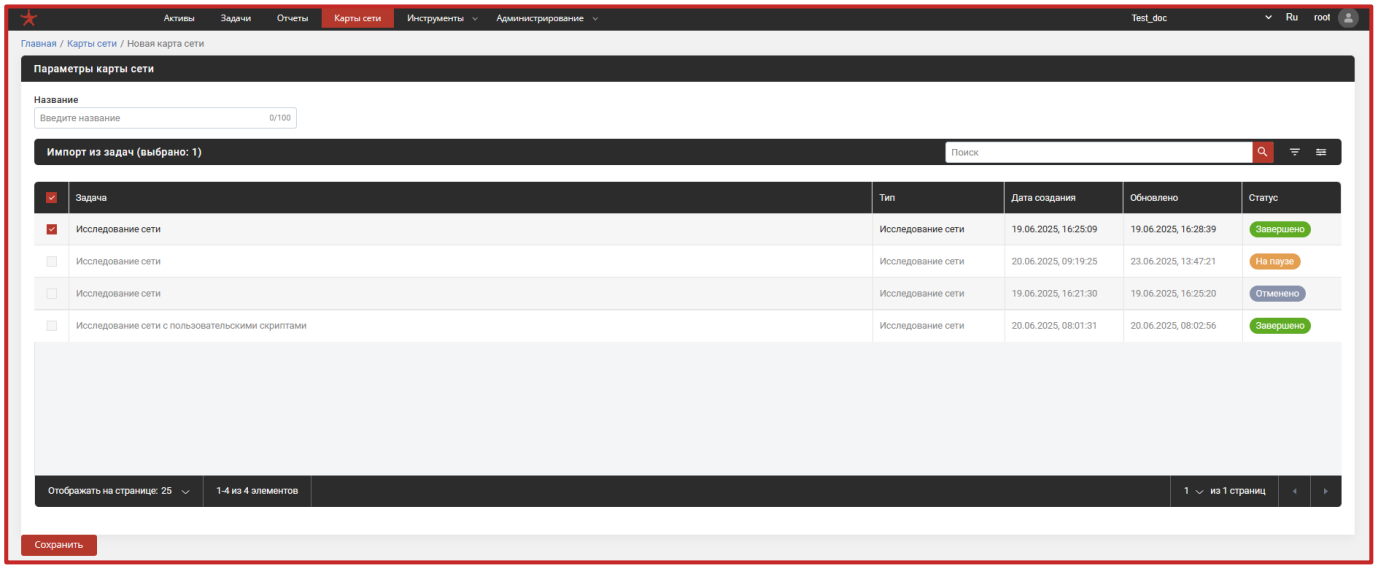


Рис. 113

Страница создания новой карты сети представляет собой таблицу, содержащую следующую информацию о завершенных задачах типа «Исследование сети» Сканер-ВС (для выбора доступны только те задачи, для которых была включена функция **«Трассировка для топологии»**):

– задача – название задачи, задаваемое пользователем при ее создании;

– тип – тип завершенной задачи (исследование сети, инвентаризация, поиск уязвимостей, подбор паролей, аудит);

– дата создания – дата и время создания завершенной задачи;

– обновлено – дата и время последнего обновления завершенной задачи (в том случае, если задача не обновлялась, то обновление будет совпадать с датой создания);

– статус – результат выполнения задачи.

Каждая строка таблицы соответствует своей завершенной задаче Сканер-ВС типа «Исследование сети».

Для создания новой карты сети необходимо выбрать доступные для данной функции задачи из таблицы «Импорт из задач» (недоступные задачи выделены серым цветом и их выбор невозможен). При создании новой карты сети, выполненные изделием задачи по умолчанию сортируются таким образом, что сперва отображаются доступные для выбора задачи, а потом уже недоступные.

После выбора задач, для которых будет построена карта сети необходимо нажать на кнопку «Сохранить» в нижнем левом углу страницы создания новой карты сети, которая станет активной.

После создания новой карты сети она отобразится в таблице во вкладке «Карты сети». Для просмотра карты сети необходимо нажать левую кнопку мыши в любом месте строки таблицы, соответствующей интересующей карте сети (рис. 112). После чего откроется страница просмотра выбранной карты сети.

5.7.2. Карта сети

Карта сети представляет собой граф, вершинами которого являются узлы сети, а ребра – связи между ними (рис. 114).

Карта сети

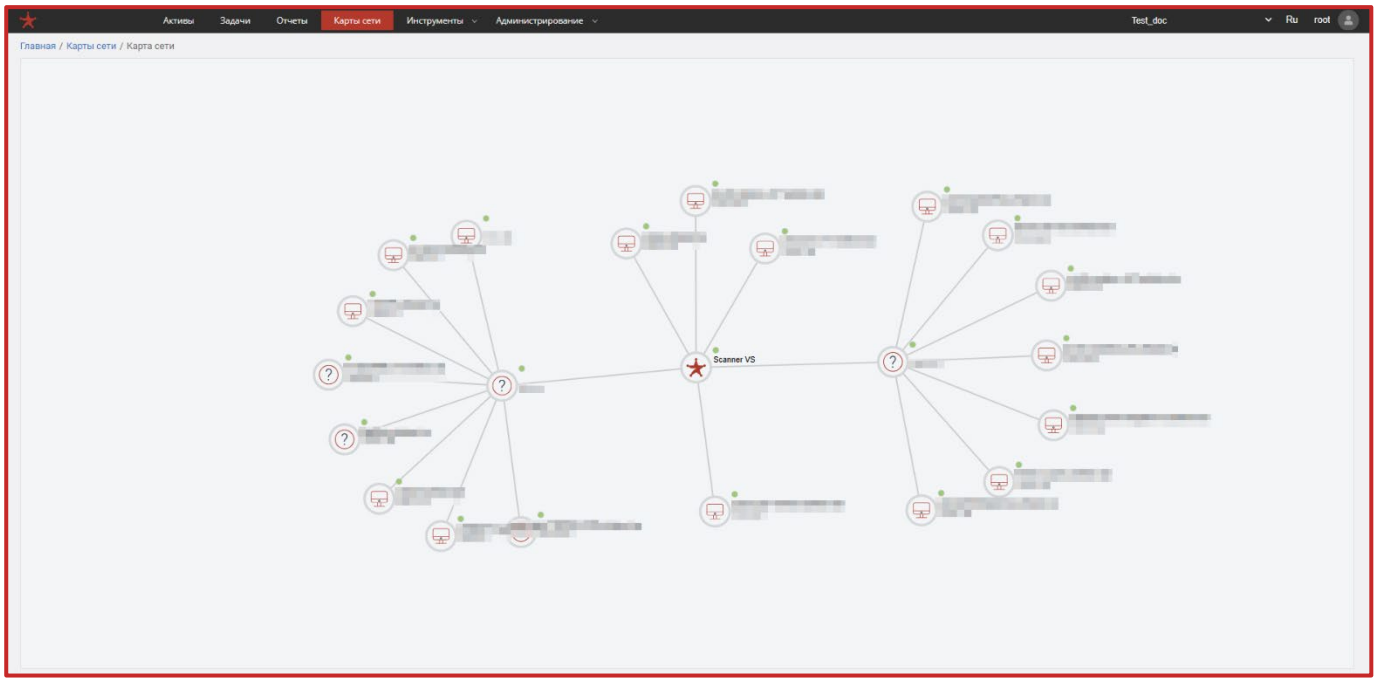


Рис. 114

Связи между узлами отображаются на карте на основе данных об активах и остальных узлах, полученных при исследовании сети. Если данные актива или узла изменились, то после сканирования карта обновится.

С помощью карты сети можно узнать:

– связи между узлами;

– отсутствие необходимых связей между узлами;

– проблемы архитектуры сети;

– постороннее оборудование, подключенное к внутренним сетям.

Примечание. Для отображения того или иного актива, при настройке параметров задачи «Исследовании сети», в которую он входит как цель сканирования, **обязательно должна быть включена** настройка «Трассировка для топологии».

В карте сети отображаются только те активы, что были получены в результате выполнения последней задачи «Исследование сети» с включенным параметром трассировки. Цвет рамки и заливки узла сети указывает на самый высокий уровень критичности уязвимостей среди всех выявленных для данного актива в процессе выполнения задачи «Поиск уязвимостей», в целях которой был указан рассматриваемый актив.

Цветовая гамма критичности найденных уязвимостей для узла сети описана в п. 5.5.5 настоящего документа.

5.7.3. Управление картой сети

Для управления картой сети в Сканер-ВС предусмотрено выполнение следующих операций:

– изменение взаимного расположения активов на карте сети;

– открытие параметров каждого узла для просмотра (рис. 115);

– переход к работе с конкретным активом из карты сети (нажатием в параметрах узла на кнопку «Подробнее», при этом произойдет переход в карточку актива (п. 5.4.5 настоящего документа);

– масштабирование рабочей области прокруткой колесика мыши;

– перемещение карты сети по рабочей области.

Примечание. Построение карты сети целесообразно для сети с числом активов не более 50. При большем числе активов исследуемой сети, карта получится малоинформативной и неудобной для работы.

Параметры узла

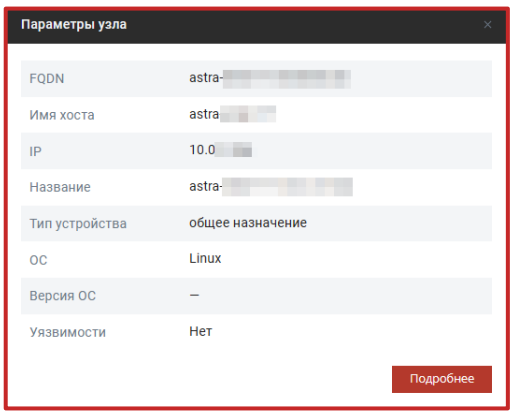


Рис. 115

Для изменения взаимного расположения необходимо нажать и зажать левую кнопку мыши на каком-либо узле карты и перетащить его на новое место. При этом карта сети будет автоматически перестраиваться в режиме реального времени.

Перемещение всей карты сети происходит аналогично изменению взаимного положения узлов сети. Однако, в данном случае необходимо нажать и зажать левую кнопку мыши в любом свободном месте рабочей области. Взаимное расположение узлов карты сети при этом изменяться не будет.

5.7.4. Редактирование карты сети

В Сканер-ВС предусмотрена функция редактирования ранее созданной карты сети. Для этого необходимо нажать на кнопку редактирования конкретной карты сети в таблице карт во вкладке «Карты сети» Сканер-ВС (рис. 112).

Страница редактирования карты сети аналогична странице создания новой карты сети. В рамках редактирования карты сети в Сканер-ВС предусмотрены следующие функции:

– изменение названия карты сети;

– добавление/удаление завершенных Сканер-ВС задач для построения карты сети.

Примечание. В результате добавления/удаления завершенных задач для построения карты сети изменится количество узлов исследуемой сети, отображаемых на карте сети.

После внесения изменений в настройки построения карты сети необходимо нажать на кнопку «Сохранить». После чего карта сети будет автоматически перестроена с учетом новых параметров.

5.7.5. Удаление карты сети

Для удаления созданной ранее карты сети необходимо нажать на кнопку удаления конкретной карты сети в таблице карт во вкладке «Карты сети» Сканер-ВС (рис. 112). После чего отобразится всплывающее окно подтверждения удаления, в котором для удаления карты сети необходимо нажать «Удалить», в противном случае – «Отменить».

В изделии предусмотрена функция удаления сразу нескольких карт сети. Для этого в таблице карт во вкладке «Карты сети» необходимо выбрать карты сети для удаления, после чего нажать на кнопку «Удалить», которая отобразится рядом с кнопкой «Добавить карту сети +».

5.8. Инструменты

Вкладка «Инструменты» предоставляет доступ к вспомогательным настройкам Сканер-ВС. Для раскрытия выпадающего списка «Инструменты» необходимо нажать на одноименную вкладку на панели навигации Сканер-ВС (рис. 116).

Раскрытие выпадающего списка «Инструменты»

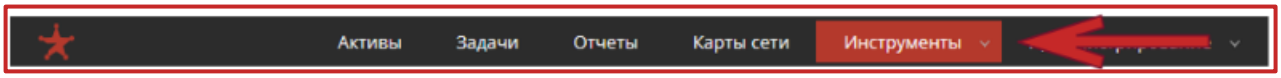


Рис. 116

При нажатии на выпадающий список «Инструменты» отобразится список доступных инструментов Сканер-ВС, где оператору предоставляются выбор для нажатия и открытия одной из следующих вкладок:

– «Теги»;
– «Словари»;
– «Проекты»;
– «База уязвимостей»;
– «Правила и шаблоны аудита»;
– «Скрипты»;
– «Пользовательские уязвимости».

5.8.1. Теги

После нажатия на вкладке «Теги» в Сканер-ВС отобразится меню «Теги» (рис. 117). Дополнительный инструмент «Теги» позволяет категорировать активы по какому-либо заданному пользователем критерию.

Меню «Теги» представляет собой таблицу со столбцами, содержащими следующую информацию о теге:

– «Название» – наименование тега, добавленного в Сканер-ВС;

– «Описание» – описание тега, добавленного в Сканер-ВС.

Меню теги

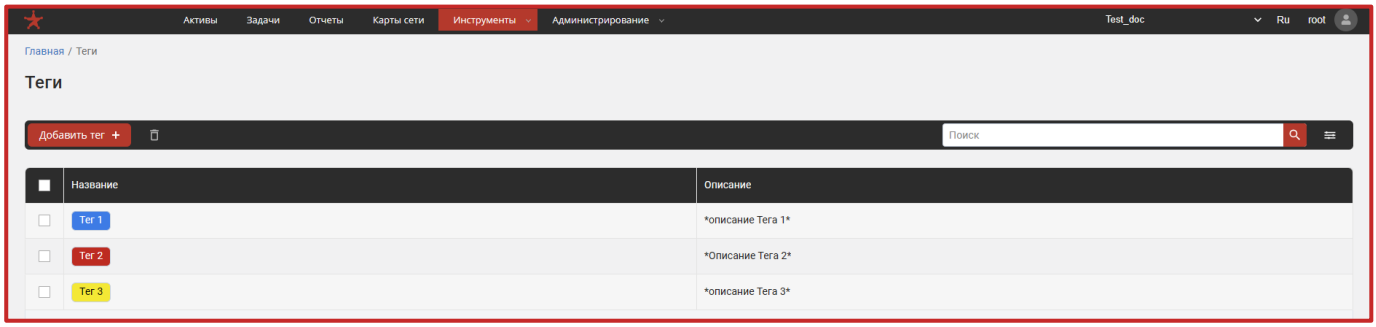


Рис. 117

5.8.1.1. Добавление тега

Для добавления нового пользовательского тега необходимо нажать на кнопку «Добавить тег +» в меню «Теги», после чего откроется окно создание тега (рис. 118).

Окно создания нового тега

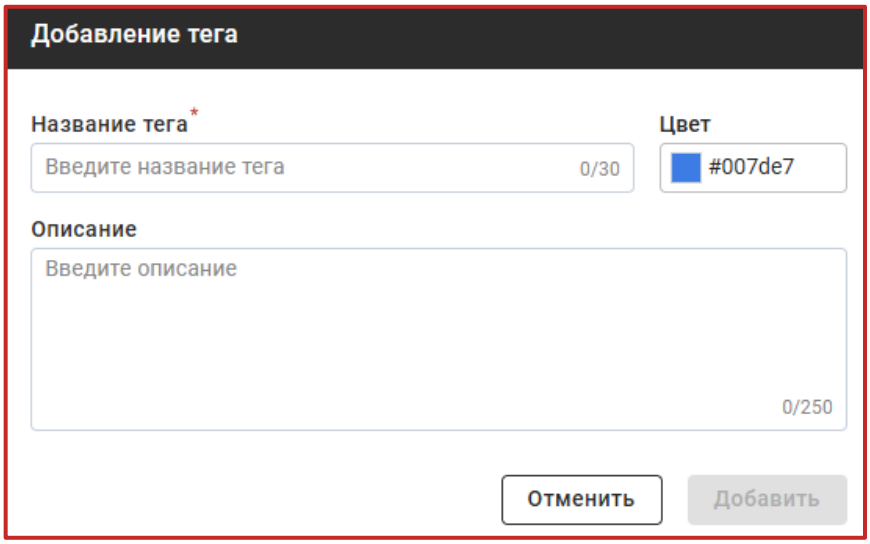


Рис. 118

Для создания нового тега необходимо заполнить поле «Название» (оно является обязательным для заполнения), выбрать цвет тега. Поле «Описание» заполнять не обязательно, однако, в случае большого количества добавленных в изделие пользовательских тегов, для более быстрой их идентификации рекомендуется заполнить данное поле.

Для выбора цвета тега необходимо нажать на поле «Цвет», после чего отобразится окно выбора цвета с помощью палитры цветов (см. рис. 119). Пользователь может выбрать абсолютно любой цвет для тега.

После ввода наименования тега в поле «Название» кнопка «Создать» станет активной. Для сохранения нового пользовательского тега необходимо нажать на кнопку «Создать», в противном случае – «Отменить».

Выбор цвета тега

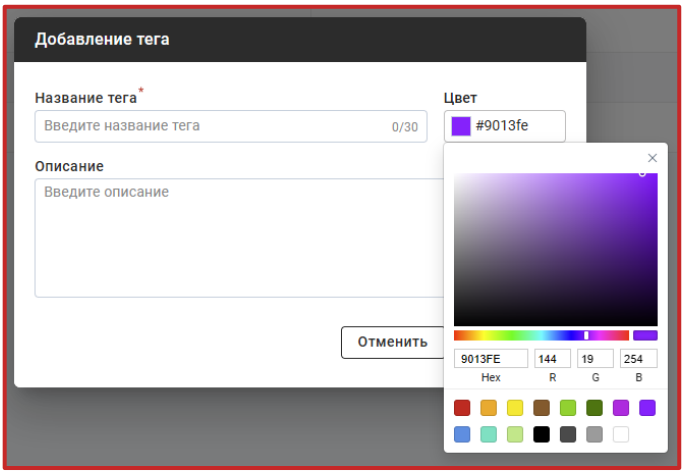


Рис. 119

5.8.1.2. Управление тегами

В Сканер-ВС предусмотрена возможность управления добавленными пользовательскими тегами. Для изменения параметров тега необходимо нажать в любом месте строки таблицы, отображаемой в меню «Теги», соответствующей тегу, информацию о котором необходимо изменить. После чего в Сканер-ВС отобразится окно редактирования тега.

Окно редактирования тега аналогично окну создания нового тега как внешне, так и функционально.

Для удаления необходимо выбрать теги, которые необходимо удалить, нажатием на пустой чекбокс « ☐ » рядом с их названиями. После чего в настройках отображения чекбокс станет активным « ☑ » рядом с названиями выбранных меток. После чего необходимо нажать на поле «Удалить» рядом с кнопкой «Добавить метку +».

При нажатии на поле «Удалить» отобразится всплывающее окно подтверждения, в котором необходимо нажать «Удалить» для удаления выбранных меток, в противном случае – нажать кнопку «Отменить».

5.8.2. Словари

После нажатия на вкладке «Словари» в Сканер-ВС отобразится меню «Словари» (рис. 120).

Меню «Словари»

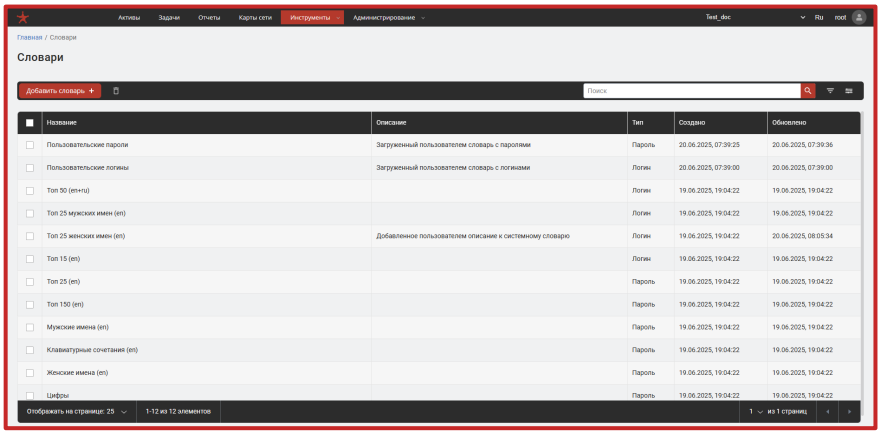


Рис. 120

Меню «Словари» является вспомогательным инструментом для настройки словарей, добавленных в Сканер-ВС. Словари используются при запуске задачи «Подбор паролей» (п. 5.5.6 настоящего документа). Данное меню представляет собой таблицу со следующими столбцами:

– название – наименование словаря, которое указывается при его создании;

– описание – краткое описание словаря, которое задается по усмотрению пользователя в момент создания словаря;

– тип – тип словаря, указывает на тип данных, которые содержаться в словаре (его назначение);

– создано – информация о дате и времени создания словаря;

– обновлено – информация о дате и времени проведения последней операции над словарем.

5.8.2.1. Карточка словаря

Для просмотра карточки конкретного словаря необходимо нажать на название этого словаря. После нажатия на название словаря отобразится карточка словаря, изображенная на рис. 121.

Карточка словаря

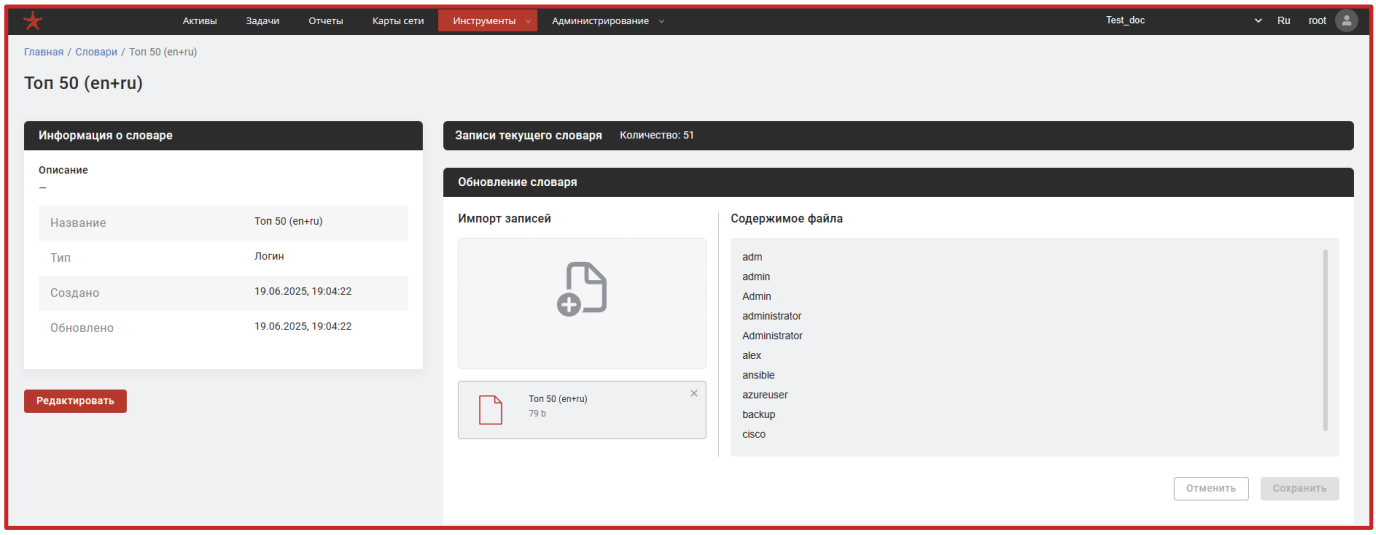


Рис. 121

В карточке словаря отображается следующая информация о нем:

– информационное поле «Записи текущего словаря» (отражает общее количество записей словаря);

– блок «Информация о словаре», который отображает следующие информационные строки:

а) «Описание»;

б) «Название»;

в) «Тип» – тип словаря (логин, пароль);

г) «Создано» – дата и время создания;

д) «Обновлено».

– кнопка «Редактировать»;

– блок «Обновление словаря», который содержит следующие элементы:

а) «Импорт записей»;

б) «Содержимое файла».

– кнопка «Отменить»;

– кнопка «Сохранить».

Для редактирования информации о словаре необходимо нажать на кнопку «Редактировать» в левом нижнем углу страницы.

Изделие предоставляет возможность изменить название, тип и описание редактируемого словаря. Для этого необходимо заполнить соответствующие поля в открывшемся окне редактирования словаря (рис. 122).

Окно редактирования словаря

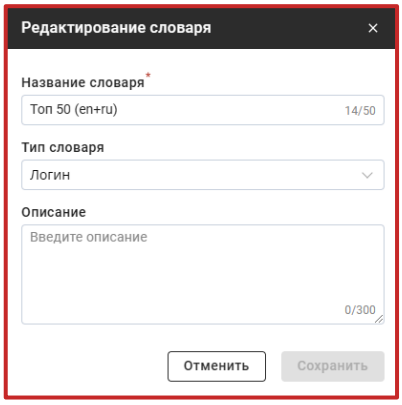


Рис. 122

После внесения необходимых изменений в окне редактирования словаря необходимо нажать кнопку «Сохранить» для того, чтобы изменения вступили в силу, в противном случае – нажать кнопку «Отменить».

Сканер-ВС предоставляет возможность просмотра записей словаря. Записи словаря отображаются в поле «Содержимое файла» блока «Обновление словаря» (рис. 123).

Блок «Обновление словаря

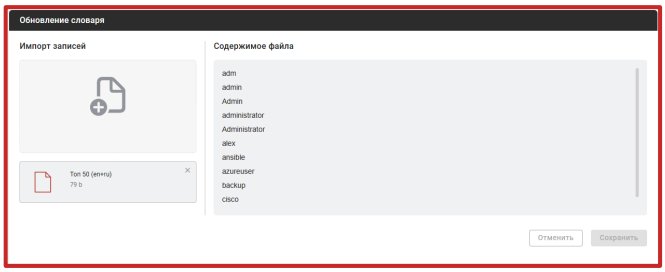


Рис. 123

Сканер-ВС отображает первые 10 записей загруженного словаря.

В левой части блока «Обновление словаря» отображается загруженный на данный момент файл **в формате txt**, содержащий записи данного словаря (поле «Импорт записей»). Для обновления словаря необходимо нажать на крестик в правом верхнем углу отображения загруженного файла. После чего поле «Импорт записей» примет следующий вид (рис. 124).

Поле «Импорт записей» после удаления загруженного файла

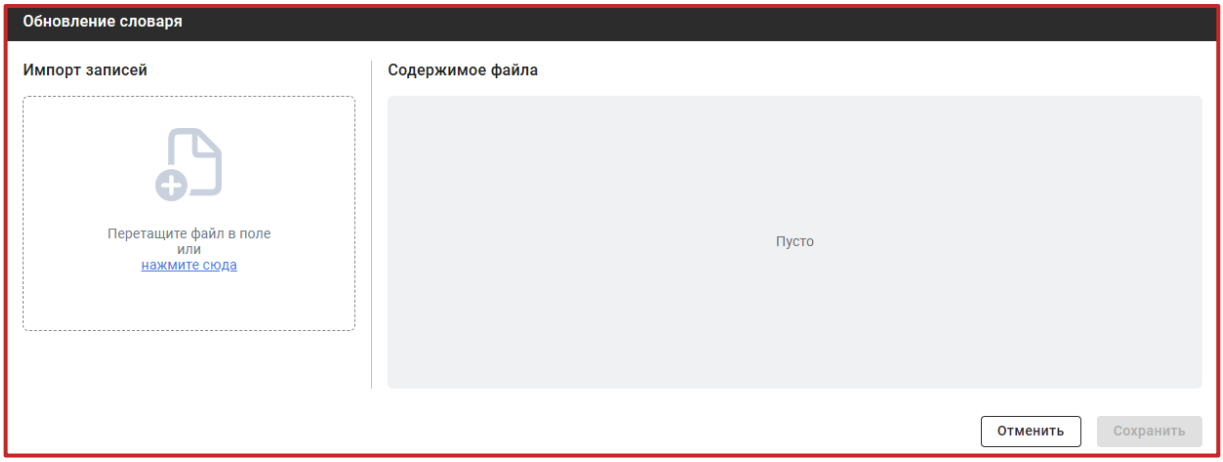


Рис. 124

После удаления существующего файла с записями словаря необходимо загрузить новый (обновленный) файл. Сделать это можно, перетащив файл с записями словаря в поле отображения загружаемого файла или нажатием на надпись «нажмите сюда». При нажатии на надпись «нажмите сюда» открывается стандартное окно выбора файла для загрузки.

После внесения изменений необходимо нажать на кнопку «Сохранить», которая станет доступной, для подтверждения этих изменений, в противном случае – нажать на кнопку «Отменить», после чего словарь вернется к своему состоянию до внесения изменений.

5.8.2.2. Добавление словаря

Для того, чтобы создать новый словарь необходимо нажать на кнопку «Добавить словарь +» в меню «Словари», после чего откроется окно создания словаря (рис. 125).

Окно создания словаря

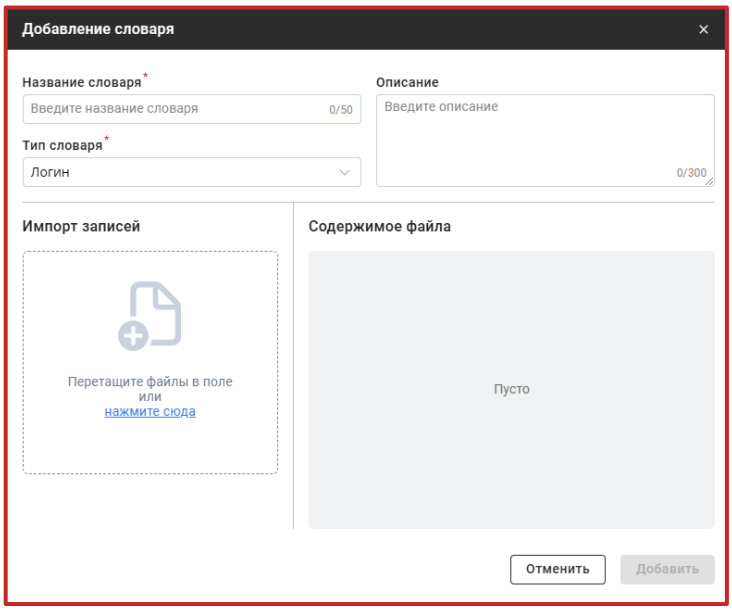


Рис. 125

При создании словаря необходимо указать его наименование в поле «Название», назначение в поле «Тип словаря». Поле «Описание» заполняется при необходимости. В случае большого количества словарей рекомендуется заполнять данное поле для упрощения последующей идентификации словарей.

В изделии предусмотрена возможность импорта записей в словарь из файла. Добавление записей словаря происходит аналогично обновлению, описанному ранее. После добавления файла с записями словаря в поле «Содержимое файла» отобразятся строчки, содержащиеся в загруженном файле записей словаря.

После настройки нового словаря необходимо нажать на кнопку «Добавить», которая станет доступной. После чего созданный словарь отобразится в таблице словарей (рис. 120).

5.8.3. Проекты

Инструмент Сканер-ВС «Проекты» описан в п. 5.3 настоящего документа.

5.8.4. База уязвимостей

5.8.4.1. Общее описание

После нажатия на вкладке «База уязвимостей» в Сканер-ВС отобразится страница «База уязвимостей» (рис. 126).

Страница «База уязвимостей»

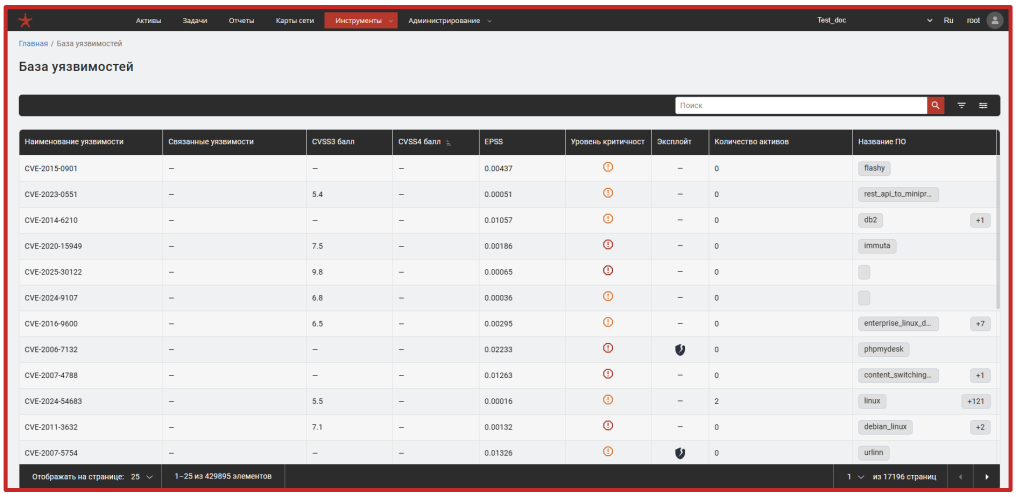


Рис. 126

Базы уязвимостей предоставляет доступ ко всем обновленным уязвимостям из NIST NVD (National Vulnerability Database), БДУ ФСТЭК России и базы вендоров. Пользователь может легко искать, фильтровать и просматривать каждую уязвимость для получения подробной информации в виде карточек уязвимостей.

Каждая карточка уязвимости содержит не только основные сведения, но также включает таблицу со связанными активами, на которых была обнаружена данная уязвимость. Это помогает оператору понять, какие активы подвержены риску из-за конкретной уязвимости, и принять необходимые меры для защиты.

На странице «Базы уязвимостей» в информационной таблице существует возможность фильтровать представленную информацию по представленным в заголовке таблицы категориям, а также по названию конкретного ПО, наличию рекомендаций, наличию эксплойтов и наличию **опасного** эксплойта (CISA KEV).

Сервис обеспечивает удобный и информативный интерфейс для работы с уязвимостями, что также поможет оператору эффективно управлять безопасностью своих систем.

5.8.4.2. Карточка уязвимости

Для просмотра карточки конкретной уязвимости необходимо нажать на название интересующей уязвимости. После нажатия на название уязвимости отобразится карточка этой уязвимости (рис. 127).

Страница «Карточка уязвимости»

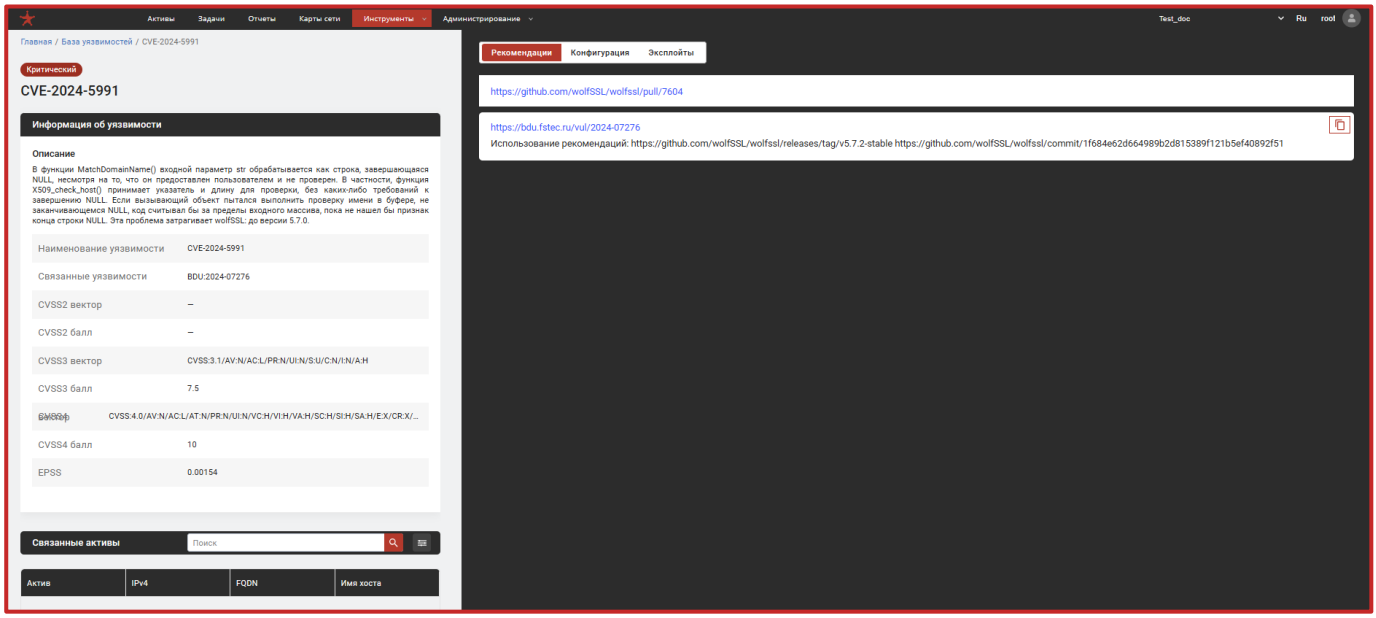


Рис. 127

В блоке «Информация об уязвимости» представлена общая информация о выбранной уязвимости, а в блоке «Связанные активы» пользователь может увидеть активы, которые связаны с текущей уязвимостью (рис. 127).

Также блоки и элементы страницы «Карточка уязвимости» подробно описаны в п. 5.4.5.6 настоящего документа.

5.8.5. Правила и шаблоны аудита

5.8.5.1. Общее описание

После нажатия на вкладке «Правила и шаблоны аудита» в Сканер-ВС отобразится страница «Правила и шаблоны аудита» (рис. 128 и 129).

Страница «Правила аудита»

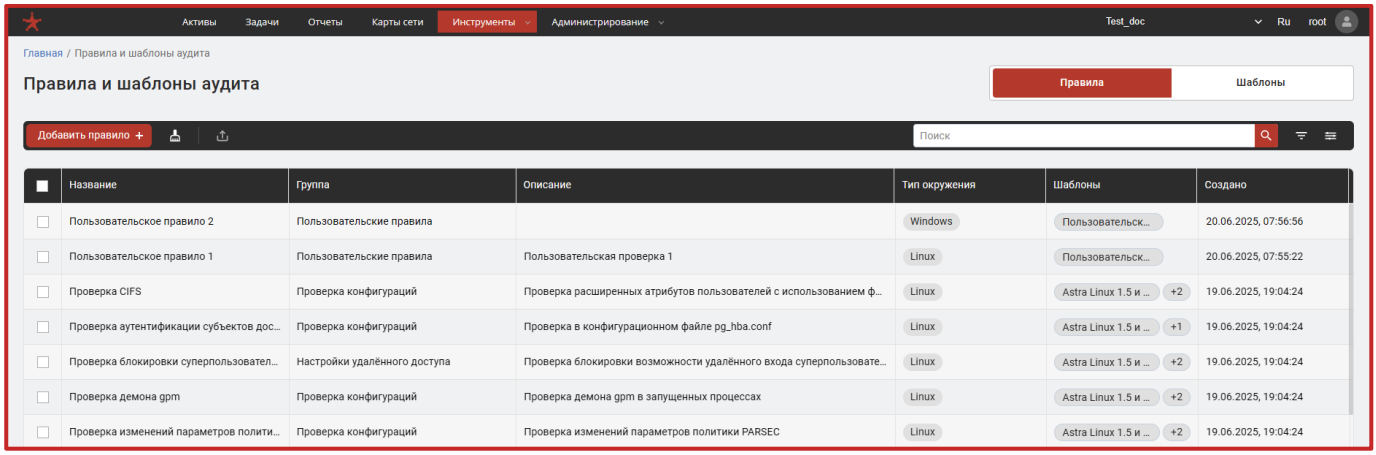


Рис. 128

Страница «Шаблоны аудита»

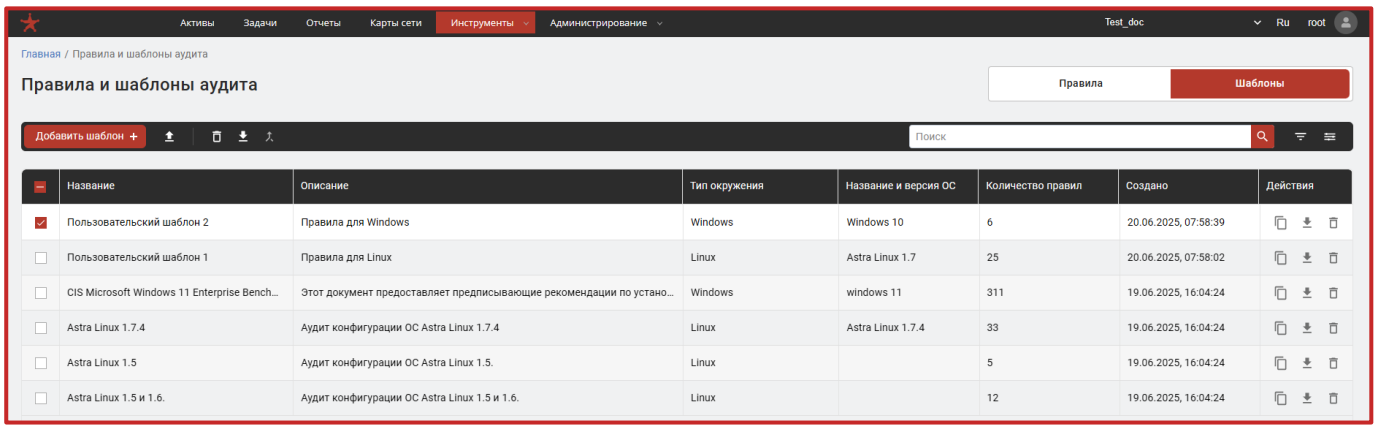


Рис. 129

На странице в правом верхнем углу присутствуют кнопки «Правила» и «Шаблоны», которые позволяют переключать страницу на просмотр, добавление и изменение правил и шаблонов изделия.

Инструмент «Правила и шаблоны аудита» предоставляет возможность оператору эффективно управлять правилами и шаблонами аудита для различных сетевых устройств. Он предоставляет функционал импорта и экспорта шаблонов аудита, а также возможность создания, редактирования и тестирования отдельных правил аудита конфигураций.

База шаблонов и правил позволяет оператору эффективно проверить целевую систему в задаче «Аудит конфигурации» (см. п. 5.5.7 настоящего документа) на соответствие различным правилам и параметрам безопасности, а также стандартам безопасности. Путем создания шаблонов из предварительно установленных правил аудита конфигураций можно обеспечить оптимальный уровень безопасности в сетевых устройствах.

В таблице «Правила и шаблоны аудита» в столбце «Действия» пользователь может дублировать, импортировать и удалять выбранные в таблице элементы.

5.8.5.2. Добавление нового шаблона

Шаблон можно импортировать в изделие, нажав иконку «⬆» (рис. 130) или создать новый шаблон аудита вручную.

Импорт шаблона аудита

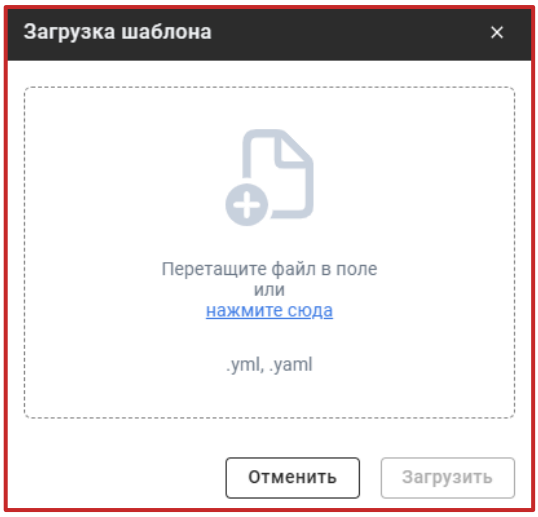


Рис. 130

Для добавления нового шаблона вручную необходимо нажать справа страницы кнопку «Шаблоны» и далее нажать на кнопку «Добавить шаблон +» после чего откроется страница «Новый шаблон» (рис. 131).

Страница «Новый шаблон»

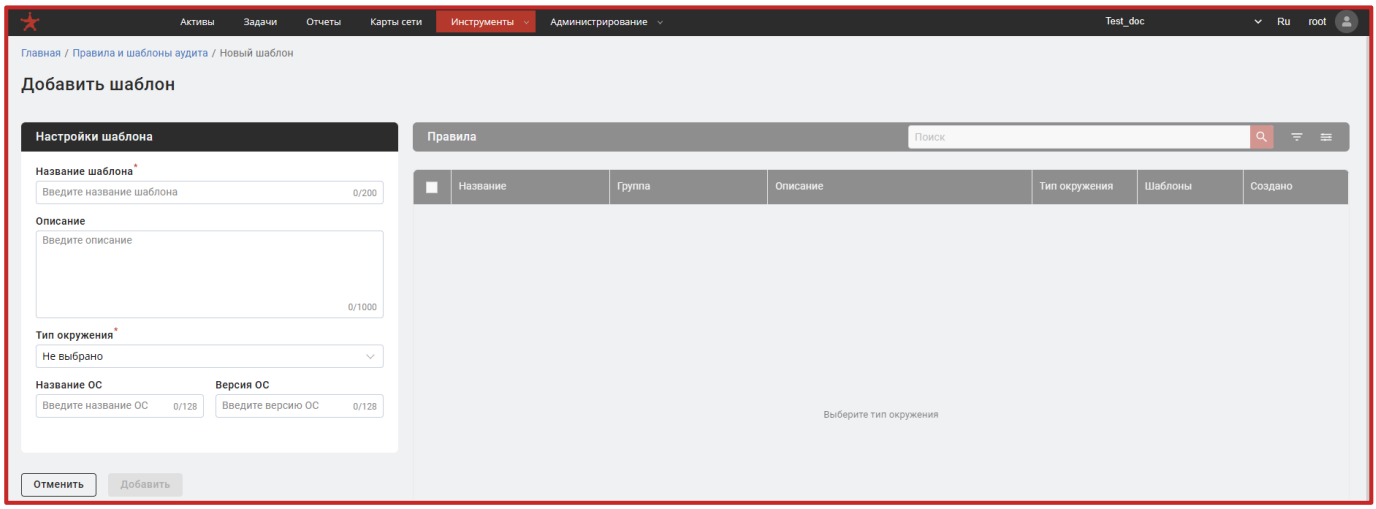


Рис. 131

Страница «Новый шаблон» содержит следующие доступные для настройки блоки:

– «Информация о шаблоне»;

– «Правила».

В блоке «Информация о шаблоне» рекомендуется заполнять все доступные поля для более подробной информации о шаблоне и удобства пользования в дальнейшем.

В блоке «Правила» отражаются доступные для выбора и добавления в шаблон правила аудита. **При создании шаблона вручную необходимо обязательно выбрать хотя бы одно правило.**

По завершению настроек нового шаблона для его сохранения необходимо нажать кнопку «Создать». Для отмены введенных данных и создания нового шаблона необходимо нажать кнопку «Отменить».

На странице «Правила и шаблоны аудита» после создания шаблона можно будет его выбрать и посмотреть страницу с описанием этого шаблона и входящих в него правил (рис. 132).

Пример просмотра страницы выбранного шаблона аудита

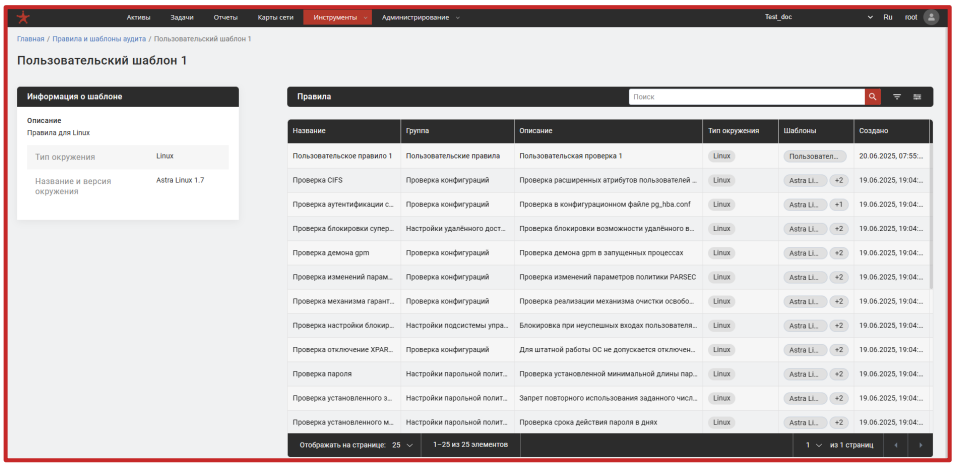


Рис. 132

5.8.5.3. Добавление нового правила

При необходимости пользователь может создать новое правило вручную, нажав справа страницы кнопку «Правила» и далее нажав кнопку «Добавить правило +» (рис. 133).

Пример заполненной страницы «Новое правило»

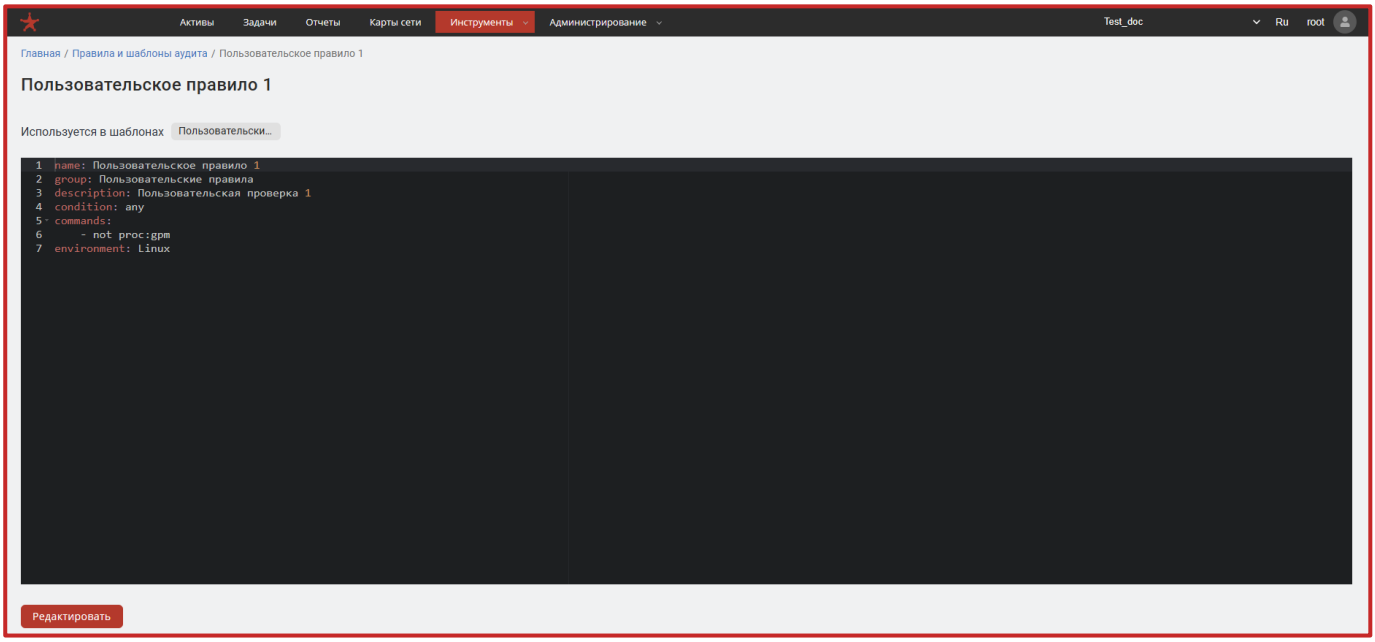


Рис. 133

Каждое правило описывается следующими полями:

– commands – список команд. Каждая команда представляет собой строку определенного вида;

– condition – условие. Описывает, как должны агрегироваться результаты команд;

– description – текстовое поле, содержащее общее описание назначения правила. Уточняет, какие настройки проверяются, что должна выполнять команда и за что отвечают соответствующие параметры в конфигурации. Может также в себя включать текстовые рекомендации по безопасным параметрам конфигурации;

– group – заполняется пользователем и используется для логической группировки правил. Например, аутентификация и авторизация, управление пользователями, аудит и логирование, удалённый доступ, сетевые протоколы, файловая система и права доступа;

– before_commands – список команд, которые выполняются перед основными командами правила. Используется для настройки окружения перед выполнением проверки. Наиболее актуально для роутеров, где может потребоваться переход в нужный режим CLI, но также может применяться в других окружениях, например, для установки переменных окружения или подготовки сессии.

Условие может иметь следующие значения:

– any – выполнять команды до первой с результатом PASSED;

– all – выполнять команды до первой с результатом NOT_PASSED или INVALID.

Команды могут проверять наличие файлов, директорий, элементов в xml-документах, разделов и значений реестра, запущенных процессов, рекурсивно проверять наличие файлов внутри директорий. Когда дело доходит до проверки содержимого, команды могут проверять содержимое файлов, вывод команд и значения разделов реестра, рекурсивно проверять содержимое файлов внутри директорий.

Абстрактно, команда начинается с цели и ее типа. За целью следует описание проверки. Проверки делятся на две категории: проверка наличия и проверка содержимого. Тип цели указан в таблице ниже, и этой целью может быть файл, директория, xml-документ, название процесса, команда или раздел реестра.

Команда завершается с одним из трех результатов:

– PASSED – команда выполнилась успешно. Например, проверялось наличие файла и файл был обнаружен;

– NOT_PASSED – команда выполнилась неуспешно. Например, проверялось наличие определенной строки в файле и строка не нашлась;

– INVALID – команда выполнилась некорректно. Например, на активе не оказалось необходимой для выполнения команды утилиты или было разорвано соединение с активом.

Примеры написания команд

Проверяет, что файл существует:

```
file:/proc/sys/net/ipv4/ip_forward
```

Проверяет, что содержимое файла соответствует всей строке:

```
file:/proc/sys/net/ipv4/ip_forward -> 1
```

Проверяет, что root единственный аккаунт с UID равным 0:

```
file:/etc/passwd -> !r:^# && !r:^root: && r:^\w+:\w+:0:
```

Проверяет, что директория существует:

```
dir:/etc/mysql
```

Проверяет, что директория содержит файлы:

```
dir:/home -> ^.mysql_history$
```

Проверяет, что атрибут элемента xml-документа равен 1:

```
xml:C:\ProgramData\Security Code\Secret Net Studio\Client\Control
Center\DefaultTemplatesSettings.xml ->
//Template[Nodes/Node[@path='TemplateInfo' and
a[@name='name']]]/Nodes/Node[@path='Basic']/Node[@path=
'GinaMode']/a[@name='value']/@value -> 1
```

Проверяет, что процесс существует:

```
proc:avahi-daemon
```

Проверяет конфигурацию sshd на предмет максимального количества попыток аутентификации:

```
cmd:sshd -T -> !r:^\s*maxauthtries\s+4\s*$
```

Проверяет значение ключа в разделе реестра:

```
reg:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
Netlogon\Parameters -> MaximumPasswordAge -> 0
```

Более подробное описание синтаксиса написания правил указано в подсказке на странице «Новое правила», которую можно раскрыть, нажав на кнопку « ⓘ » в верхней правой части страницы.

5.8.5.4. Тестирование правила перед добавлением в изделие

Если созданное оператором правило будет с ошибкой, тогда в задаче «Аудит конфигурации» оно не пройдет. На данном правиле появится серый статус «Невоспроизводимо». Для предотвращения данных ситуаций рекомендуется тестировать правила перед сохранением и добавлением их в изделие.

Для тестирования правила после написания необходимо выполнить следующее:

– на странице «Новое правило» (рис. 133), с записанным для добавления правилом, необходимо выбрать актив для проверки этого правила, нажав кнопку «Выбрать из списка активов»;

– нажать кнопку «Проверить» под окном для записи правила;

– дождаться результата проверки.

5.8.5.5. Возможные результаты проверки

Статусы в задаче «Аудит конфигурации» (результаты проверки правила) могут быть следующими:

– успешный (текст в результате проверки будет окрашен в зеленый цвет – см. рис. 134);

Успешный результат проверки

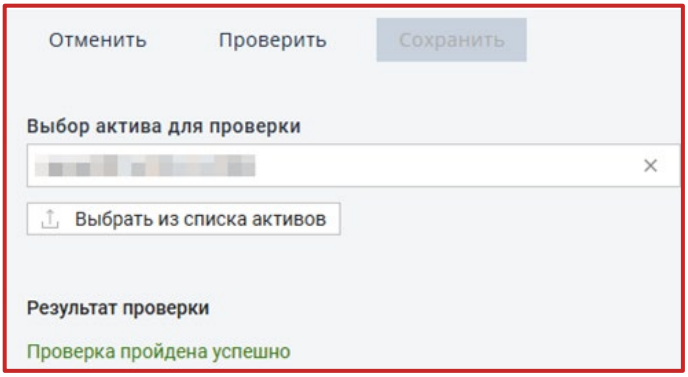


Рис. 134

– не успешный (правило не смогло запуститься на активе (см. рис. 141) или не прошло проверку (см. рис. 136). Текст в результате проверки будет окрашен в красный цвет);

Не успешный результат – правило не смогло запуститься на активе

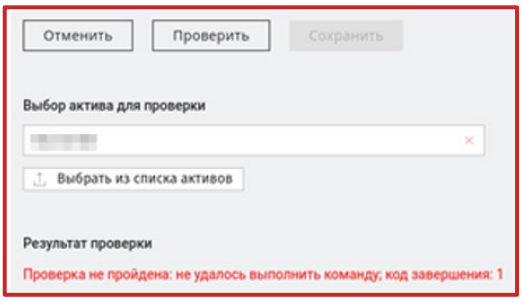


Рис. 135

Не успешный результат – правило не прошло проверку

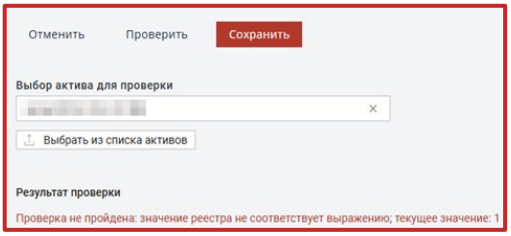


Рис. 136

– невоспроизводимое (правило не смогло воспроизвестись т. к. не подходит под тип окружения выбранного актива (см. рис. 137). Текст в результате проверки будет окрашен в серый цвет);

Не успешный результат – невоспроизводимое правило

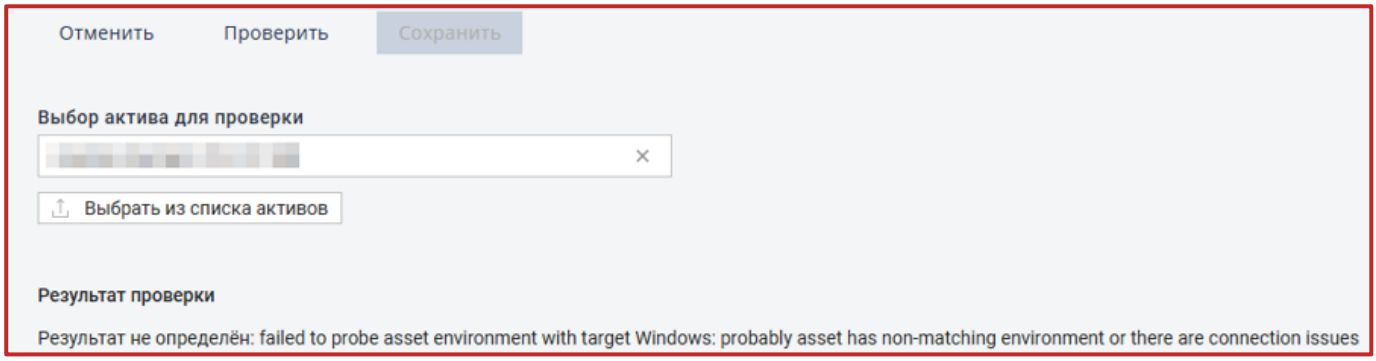


Рис. 137

5.8.5.6. Добавление решающего правила для задачи «Аудит конфигурации»

Для выполнения задачи «Аудит конфигурации» Сканер-ВС использует встроенную базу решающих правил. Данная база правил обновляется вместе с обновлением изделия. В случае необходимости внесения нового решающего правила, администратор Сканер-ВС может обратиться в службу поддержки для последующего уточнения необходимых параметров и решающего правила. После получения информации от администратора Сканер-ВС разработчиком будет проведен соответствующий анализ предоставленных данных и, в случае подтверждения необходимости нового решающего правила, оно будет добавлено в базу решающих правил и передано эксплуатирующей организации с очередным обновлением.

5.8.6. Скрипты

5.8.6.1. Общее описание

После нажатия на вкладке «Скрипты» в Сканер-ВС отобразится страница «Скрипты» (рис. 138).

Страница «Скрипты»

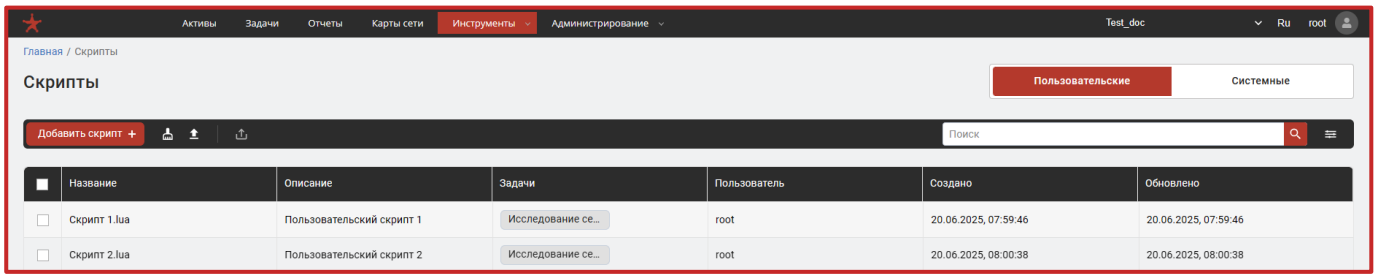


Рис. 138

Инструмент «Скрипты» предоставляет возможность оператору проводить и автоматизировать расширенный процесс анализа сети и получения более полного представления безопасности активов. Он предоставляет функционал импорта / экспорта пользовательских и экспорта системных скриптов для различных сетевых устройств, а также написания отдельных пользовательских скриптов и их валидация на языке «Lua».

На странице «Скрипты» отображаются добавленные ранее оператором скрипты в виде таблицы. Таблица со скриптами позволяет взаимодействовать с ними следующим образом: добавлять новые, импортировать или удалять.

Кнопка «Удалить неиспользуемые» позволит оператору удалить все скрипты, которые не задействованы в задачах – в столбце «Задачи» в строке выбранного пользовательского скрипта должен быть прочерк.

При нажатии на выбранный скрипт откроется страница для его полного отображения и редактирования.

На странице «Скрипты» в правом верхнем углу также доступны следующие кнопки:

– «Пользовательские» – кнопка переключит пользователя на страницу с таблицей пользовательских скриптов, добавленных оператором;

– «Системные» – кнопка переключит пользователя на страницу с таблицей системных скриптов, добавленных ранее производителем изделия (рис. 139).

Страница с таблицей системных скриптов

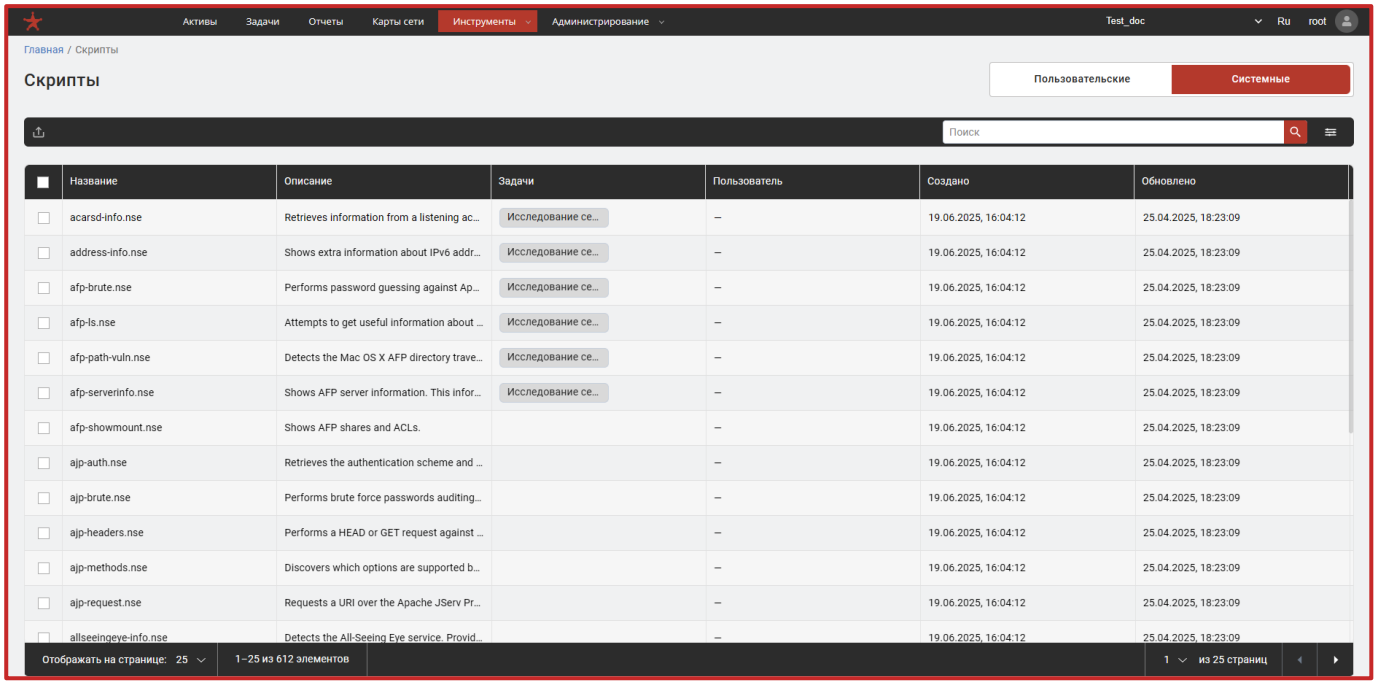


Рис. 139

5.8.6.2. Добавление нового пользовательского скрипта

Для добавления нового пользовательского скрипта необходимо нажать справа страницы кнопку «Пользовательские» и далее нажать на кнопку «Добавить скрипт +» после чего совершится переход на страницу «Добавить скрипт» (рис. 140).

Страница «Добавить скрипт»

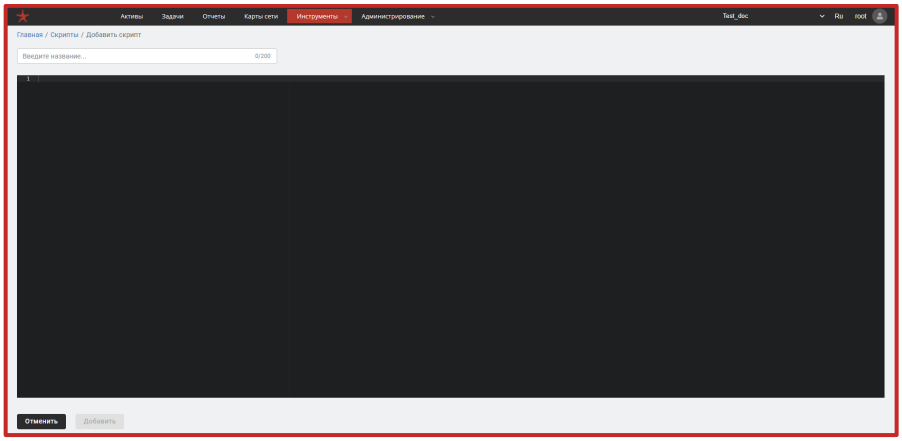


Рис. 140

Для добавления нового пользовательского скрипта необходимо следующее:

– ввести название будущего скрипта в поле для ввода с надписью «Введите название…»;

– в черное поле для ввода необходимо вписать требуемый скрипт на языке «Lua»;

– нажать кнопку «Сохранить» для сохранения и добавления нового скрипта.

5.8.7. Пользовательские уязвимости

5.8.7.1. Общее описание

После нажатия на вкладке «Пользовательские уязвимости» в Сканер-ВС отобразится страница «Пользовательские уязвимости» (рис. 141).

Страница «Пользовательские уязвимости»

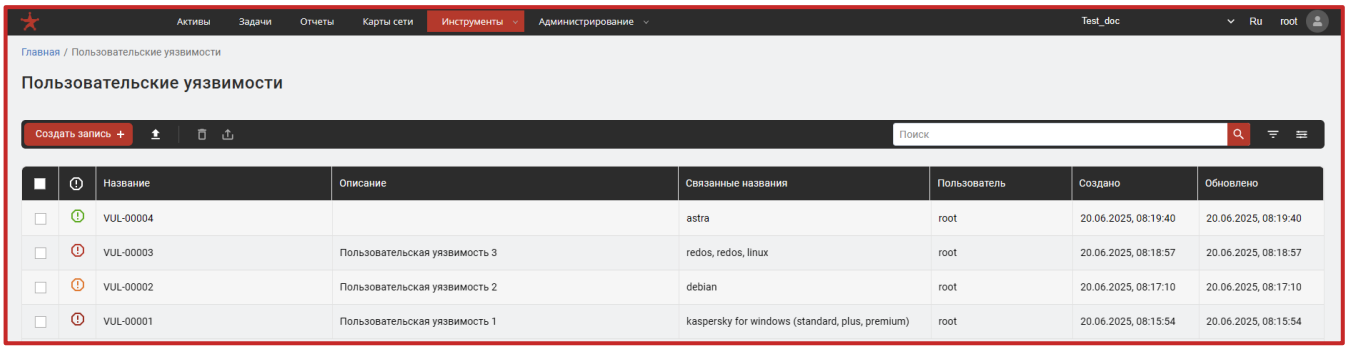


Рис. 141

Инструмент «Пользовательские уязвимости» предоставляет возможность оператору задать описание уязвимостей для более глубокого и широкого понимания потенциальных проблем безопасности.

Добавленные пользовательские уязвимости пользователь может удалить, импортировать или экспортировать, выбрав нужные записи в таблице.

Главные преимущества использования данной функции в Сканер-ВС включают в себя:

– специфичность уязвимостей – описания пользовательских уязвимостей могут содержать информацию о специфических сценариях использования, которые могут быть уникальны для конкретного приложения или среды. Это помогает идентифицировать и анализировать уязвимости, которые могут быть упущены, если использовать только описание от вендора;

– дополнительные детали и контекст – пользовательские описания уязвимостей могут включать дополнительные детали, примеры эксплойтов, технические детали и контекст специфических проблем безопасности. Это обеспечивает более глубокое понимание уязвимости и помогает лучше подготовиться к угрозам;

– независимость от вендоров – использование пользовательских описаний уязвимостей позволяет независимо оценивать безопасность приложений и систем, не полагаясь исключительно на информацию от вендоров. Это позволяет получать дополнительную точку зрения и обеспечивает большую гибкость при анализе уязвимостей.

Примечание. При использовании пользовательских описаний следует учитывать возможные риски, такие как недостоверность информации и ограниченный охват. Это подчеркивает важность тщательного анализа и проверки происхождения информации для выявления достоверности данных.

Использование функции «Пользовательская уязвимость» (далее – ПУ) как дополнение к вендорским может значительно обогатить процесс поиска уязвимостей, обеспечивая более глубокое понимание и широкий охват потенциальных уязвимостей.

Для создания новой записи пользовательской уязвимости необходимо воспользоваться конструктором пользовательских уязвимостей.

5.8.7.2. Конструктор пользовательских уязвимостей

Для создания новой записи пользовательской уязвимости необходимо нажать кнопку «Создать запись +», чтобы перейти к конструктору ПУ (рис. 142).

Конструктор пользовательских уязвимостей

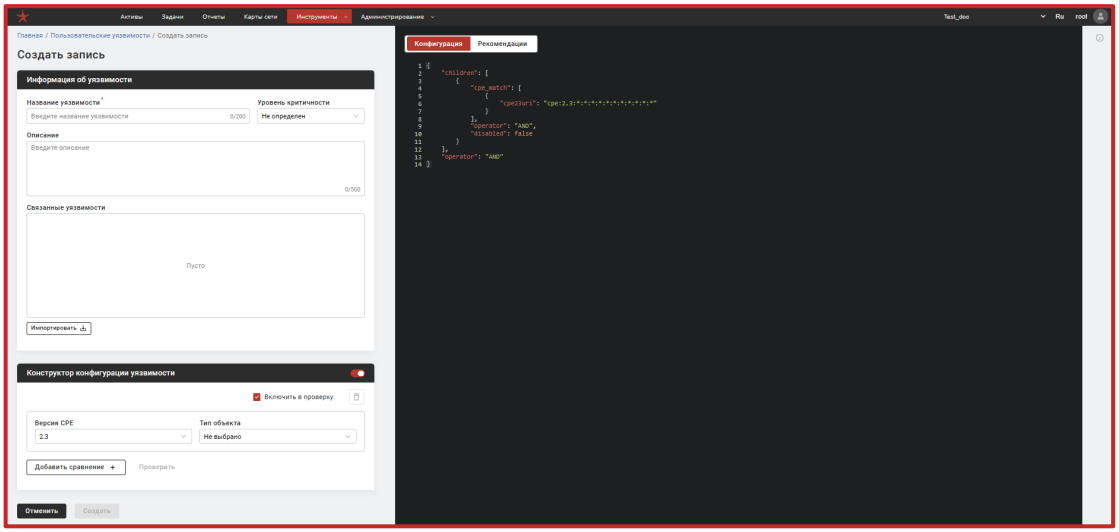


Рис. 142

Описание уязвимости добавляется в формате json в правой части страницы во вкладке «Конфигурация».

«Конфигурация уязвимости» – это основная часть записи об уязвимости, где содержатся все детали и характеристики уязвимости. В конфигурации уязвимости следует указать структуру CPE в формате json.

Для получения более подробной информации о правилах заполнения описания уязвимости с помощью вкладки «Конфигурация» необходимо нажать кнопку « ⓘ », что позволит воспользоваться подсказкой в правой части окна (см. рис. 143). Для закрытия подсказки необходимо еще раз нажать на кнопку « ⓘ ».

Подсказка вкладки «Конфигурация»

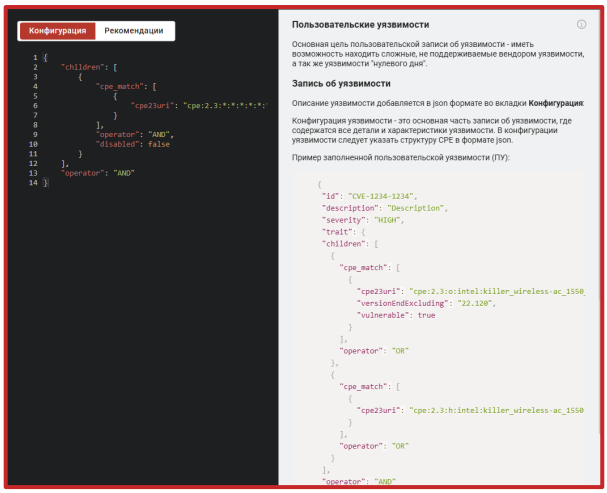


Рис. 143

Помимо написания json-конфигурации пользователь также может создать описание для ПУ через «Конструктор описания уязвимости». Данная возможность необходима для упрощения работы, снижения сложности написания конфигурации и тестирования текущей конфигурации ПУ через поиск уязвимостей на выбранном активе.

Конструктор пользовательских уязвимостей содержит следующие функциональные блоки:

– «Информация об уязвимости» – предназначен для внесения общей информации о ПУ;

– «Конструктор конфигурации уязвимости» – предназначен для создания и редактирования json-файла во вкладке «Конфигурация» через пользовательский интерфейс Сканер-ВС.

5.8.7.2.1. Блок «Информация об уязвимости»

Блок «Информация об уязвимости» (см. рис. 144) содержит следующие элементы:

– поле «Название уязвимости» – предназначено для ввода наименования ПУ и является обязательным для заполнения;

– выпадающий список «Уровень критичности» – предназначен для выбора уровня критичности уязвимости и дальнейшей приоритезации ПУ;

– поле «Описание» – предназначено для ввода подробной информации о ПУ;

– поле «Связанные уязвимости» и кнопка «Импортировать» – предназначены для создания связи между создаваемой ПУ и другими уязвимостями, выбранными оператором. Для добавления в список связанных уязвимостей необходимо нажать кнопку «Импортировать». Далее откроется таблица «Импорт из уязвимостей», в которой пользователь сможет выбрать необходимые уязвимости для создания связи между ними. После чего выбранные названия уязвимостей добавятся в поле «Связанные уязвимости». Для удаления одной или нескольких уязвимостей из поля «Связанные уязвимости» необходимо справа от наименования уязвимости нажать кнопку « X ».

Блок «Информация об уязвимости»

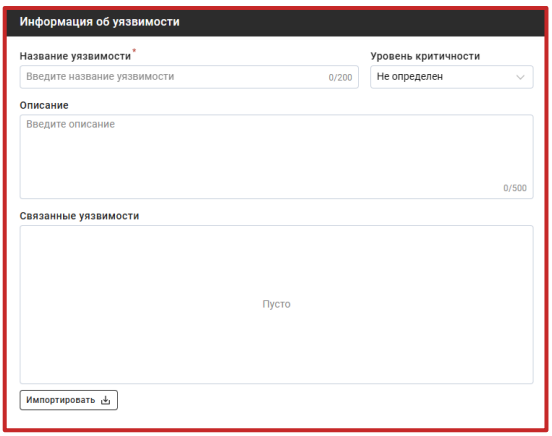


Рис. 144

5.8.7.2.2. Блок «Конструктор конфигурации уязвимости»

Для добавления конфигурации с помощью конструктора, а также дальнейшего отслеживания синхронных изменений конструктора и json-конфигурации необходимо активировать блок «Конструктор конфигурации уязвимости» (см. рис. 145).

Блок «Конструктор конфигурации уязвимости»

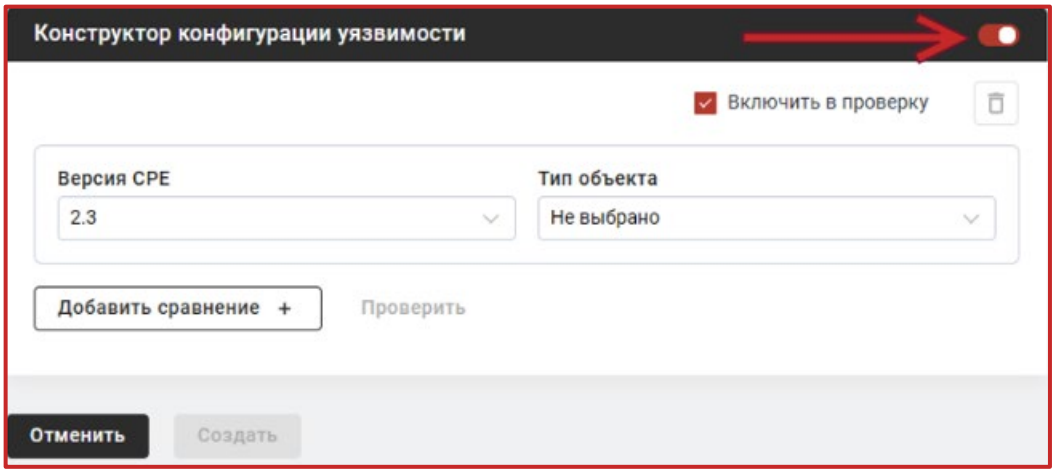


Рис. 145

Примечание. При ручном вводе конфигурации уязвимости необходимо указывать только параметры уязвимости, которые в стандарте описания CPE указываются в ключе «trait».

Далее необходимо выбрать версию стандарта CPE (2.2 или 2.3) и тип объекта (операционная система или программное обеспечение), после чего появятся дополнительные поля для выбора способа проверки (см. рис. 146). В данных полях необходимо указать название ПО или ОС, используя контекстный поиск. Далее следует выбрать один из доступных операторов и указать версию (или несколько версий) продукта. Внутри блока можно добавлять неограниченное количество условий с тем же набором полей с помощью кнопки «Добавить условие +» (рис. 147). По умолчанию между условиями json-конфигурации всегда будет пользователь «AND».

Дополнительные поля конструктора

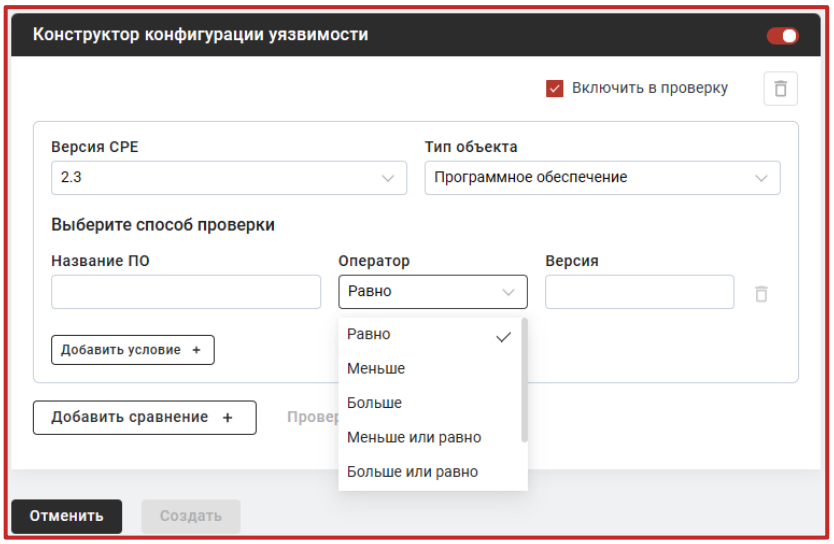


Рис. 146

Кнопка «Добавить условие»

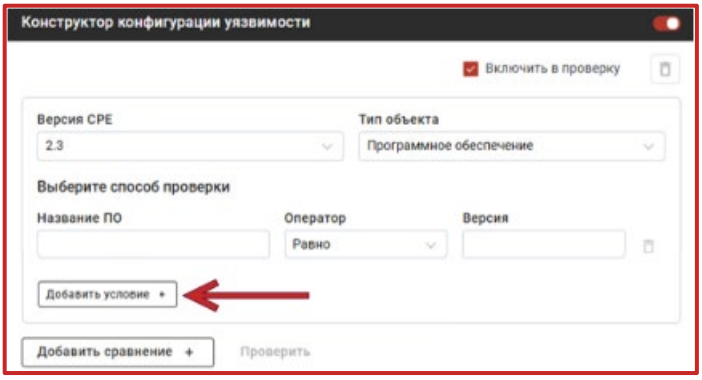


Рис. 147

Для добавления нового блока необходимо нажать кнопку «Добавить сравнение +» (рис. 148). Для всех новых блоков предусмотрена возможность выбора логического пользователя (рис. 149). Оператор «И» необходимо выбрать, если требуется одновременное выполнение всех условий каждого блока, пользователь «ИЛИ», если достаточным является выполнение условий хотя бы одного блока.

Примечание. В конце массива объектов json-конфигурации появляется параметр «operator», по умолчанию принимающий значение «AND» (рис. 150). Для смены логического пользователя необходимо отключить конструктор конфигурации уязвимости и вручную изменить значение на «OR».

Кнопка «Добавить сравнение +»

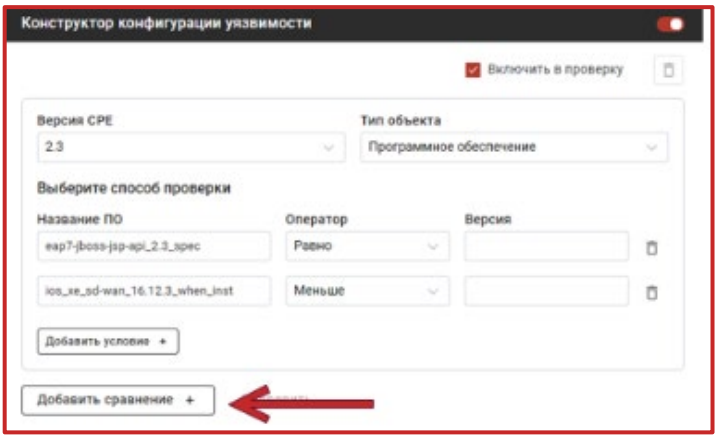


Рис. 148

Выбор логического пользователя

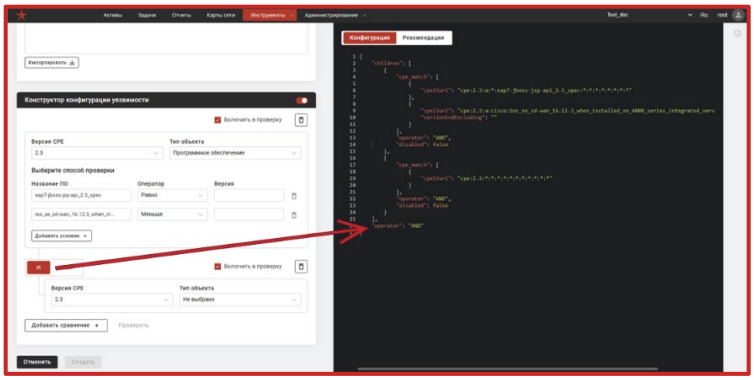


Рис. 149

Пример json-конфигурации

Рис. 150

После добавления в конфигурацию уязвимости объектов и способов проверки станет активной кнопка «Проверить», при нажатии на которую откроется поле «Выбор актива для проверки» (рис. 151). Далее необходимо нажать кнопку «Выбрать из списка активов», после чего откроется окно «Импорт активов», содержащее список доступных для проверки активов.

Примечание. Для исключения объектов пользовательской уязвимости из проверки, необходимо отключить чекбокс «Включить в проверку» (рис. 152)

Кнопка «Проверить»

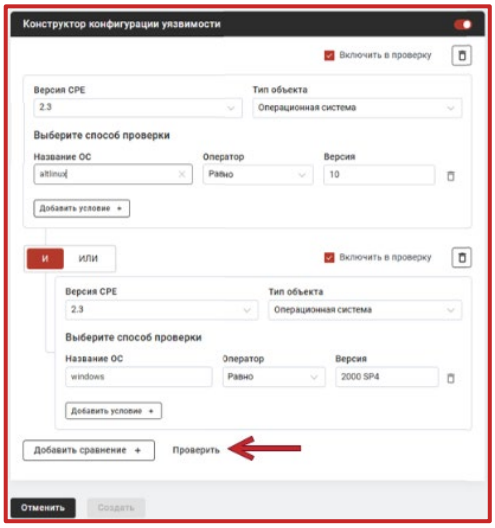


Рис. 151

Чекбокс «Включить в проверку»

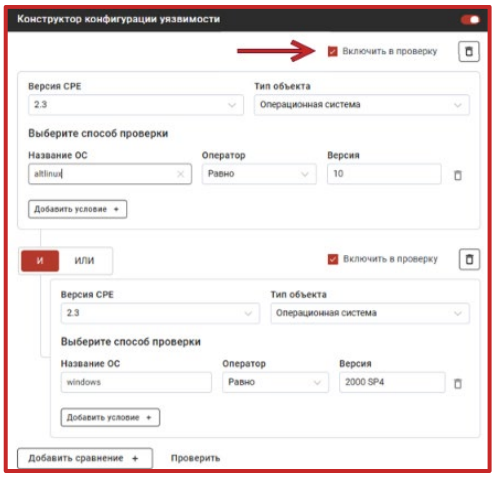


Рис. 152

5.8.7.3. Карточка пользовательской уязвимости

После проведения задачи «Поиск уязвимостей» с выбранным пунктом «Использовать пользовательскую базу уязвимостей» (см. п. 5.5.5.2 настоящего документа) оператору будет доступна к просмотру карточка ПУ (рис. 153).

Пример карточки пользовательской уязвимости

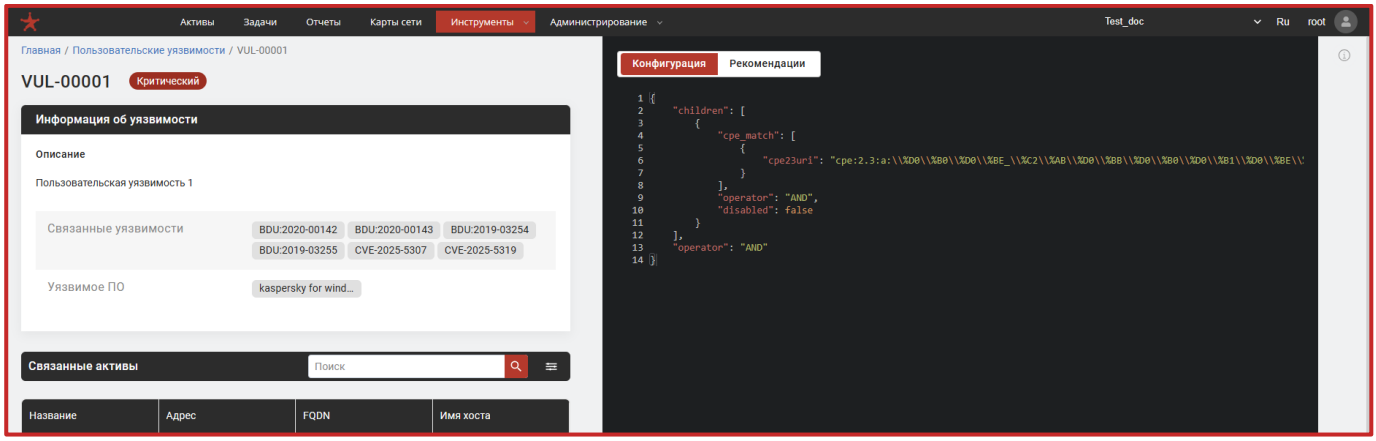


Рис. 153

5.8.7.4. Просмотр удаленных пользовательских уязвимостей

Во вкладке «Пользовательские уязвимости» можно удалить описание ранее созданных уязвимостей, сделав их недоступными для проведения последующих задач «Поиск уязвимостей» с опцией «Использовать пользовательскую базу уязвимостей».

Если ранее были проведены задачи с базой ПУ, содержащей удаленные записи, у пользователя будет возможность просмотреть карточку удаленной ПУ в результатах выполненных задач. Такая карточка ПУ будет содержать метку «Архив», в таблице всех ПУ (Инструменты/Пользовательские уязвимости) данные записи будут удалены и не видны пользователю.

5.9. Администрирование

Вкладка «Администрирование» предоставляет доступ к вспомогательным настройкам Сканер-ВС. Для раскрытия выпадающего списка «Администрирование» необходимо нажать на одноименную вкладку на панели навигации Сканер-ВС (рис. 154).

Раскрытие выпадающего списка «Администрирование»

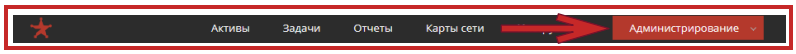


Рис. 154

При нажатии на выпадающий список «Администрирование» отобразится список доступных инструментов Сканер-ВС, где оператору предоставляются выбор для нажатия и открытия одной из следующих вкладок:

– «Пользователи»;

– «Секреты и подключения»;

– «Обновления».

Вкладка «Администрирование» доступна для просмотра операторам с любыми правами доступа, но **управление инструментами данной вкладки доступно только оператору с правами доступа «Администратор»**.

5.9.1. Пользователи

5.9.1.1. Общее описание

После нажатия на вкладке «Пользователи» в Сканер-ВС отобразится страница «Пользователи» (рис. 155).

Данная функция применяется для хранения данных авторизации пользователей в Сканер-ВС.

Страница «Пользователи»

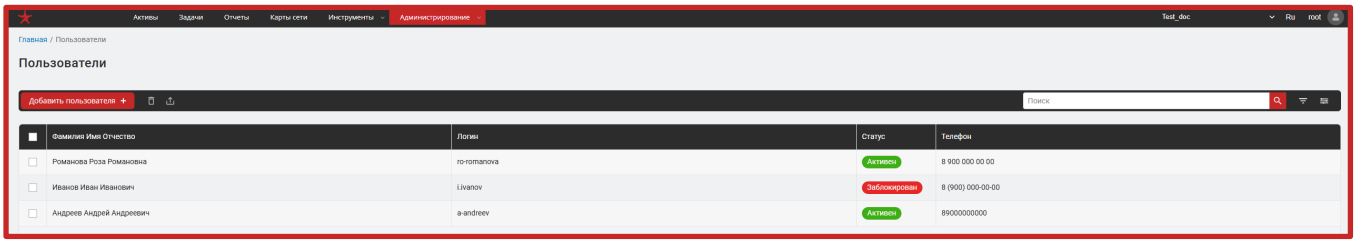


Рис. 155

Вкладка «Пользователи» применяется для администрирования Сканер-ВС. С помощью данной вкладки можно выполнять следующие функции администрирования:

– добавление нового пользователя (пользователя) Сканер-ВС;

– редактирование информации о существующем пользователе Сканер-ВС;

– редактирование аутентификационной информации пользователя;

– удаление пользователя Сканер-ВС.

Вкладка «Пользователи» представляет собой таблицу с описанием параметров учетных записей пользователей, а именно:

– «ФИО» – Фамилия, Имя, Отчество;

– «Логин»;

– «Статус»;

– «Телефон».

В Сканер-ВС предусмотрена возможность экспорта данных из таблицы пользователей. Для экспорта данных в файл необходимо нажать на иконку «⬆» после выбора строк, которые необходимо загрузить в файл.

5.9.1.2. Добавление нового пользователя

Для добавления нового пользователя в Сканер-ВС необходимо нажать на кнопку «Добавить пользователя +» (рис. 156).

Страница «Новый пользователь»

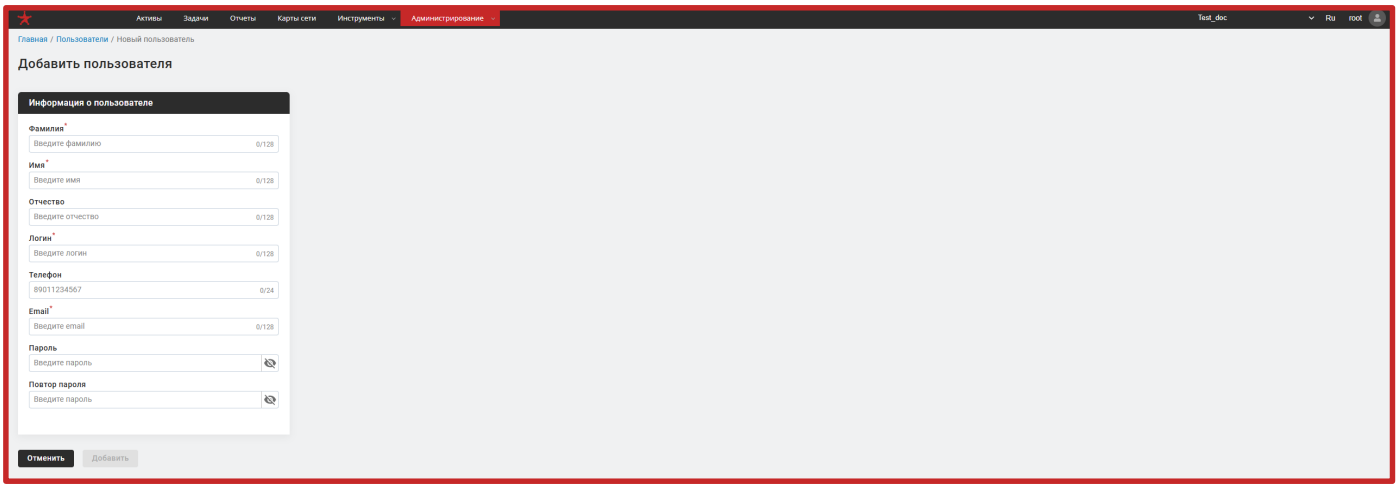


Рис. 156

Чтобы добавить нового пользователя в Сканер-ВС необходимо заполнить соответствующие поля в блоке «Данные о пользователе» и нажать кнопку «Сохранить».

Примечание. Кнопка «Сохранить» по умолчанию не активна и становится активной в тот момент, когда пользователь Сканер-ВС с ролью «Администратор» **заполнит все обязательные поля** (рис. 156).

В Сканер-ВС предусмотрена проверка на уникальность добавляемого пользователя. Таким образом, поля «Логин» и «Email» должны содержать уникальные данные для каждого добавляемого пользователя. Иначе в Сканер-ВС появится сообщение «duplicate error» и кнопка «Сохранить» не станет доступной пока в описанных полях не будут указаны уникальные данные.

Для достаточной защищенности паролей операторов Сканер-ВС рекомендуется задавать пароли, отвечающие следующим критериям:

– пароль должен содержать латинские буквы обоих регистров: как заглавные (A-Z), так и строчные (a-z);

– в пароле обязательно должна присутствовать хотя бы одна цифра (0-9);

– пароль должен содержать минимум один специальный символ, например: !, @, #, $, %, ^, &, *, и т. д.;

– минимальная длина пароля – не менее 9 символов;

– рекомендуется избегать последовательностей одинаковых символов подряд;

– запрещается использовать пробелы и управляющие символы;

– рекомендуется не использовать легко угадываемые слова, такие как «password», «123456», имя пользователя и т.д.

В Сканер-ВС предусмотрена настройка сложности задаваемого пароля для аутентификации операторов, которая подробна описана в документе НПЕШ.00606-01 91-1 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Руководство администратора. Часть 2».

5.9.1.3. Удаление пользователя

Для удаления одного или нескольких пользователей необходимо выбрать пользователей для последующего удаления путем нажатия на пустой чекбокс «☐» рядом с именем необходимого пользователя. После чего в настройках отображения появится активный чекбокс «☑» рядом с именем выбранного пользователя.

После выбора пользователей, которых необходимо удалить, рядом с кнопкой «Добавить пользователя +» отобразится кнопка «Удалить» являющаяся по умолчанию скрытой и подтвердить удаление в отобразившемся окне подтверждения.

5.9.1.4. Редактирование информации о пользователе

Для редактирования информации о пользователе Сканер-ВС необходимо перейти в окно редактирования информации о пользователе, для чего необходимо кликнуть на имя пользователя, информацию о котором необходимо изменить. После чего откроется окно редактирования пользователя идентичное окну добавления нового пользователя, в котором необходимо изменить интересующую информацию о пользователе и нажать кнопку «Сохранить».

Редактирование информации о пользователе Сканер-ВС осуществляется путем внесения изменений в карточку пользователя. Для перехода к карточке пользователя необходимо нажать на выбранной строке таблицы с необходимым пользователем (рис. 155). После чего произойдет переход к карточке информации о выбранном пользователе (рис. 157).

Карточка информации о пользователе

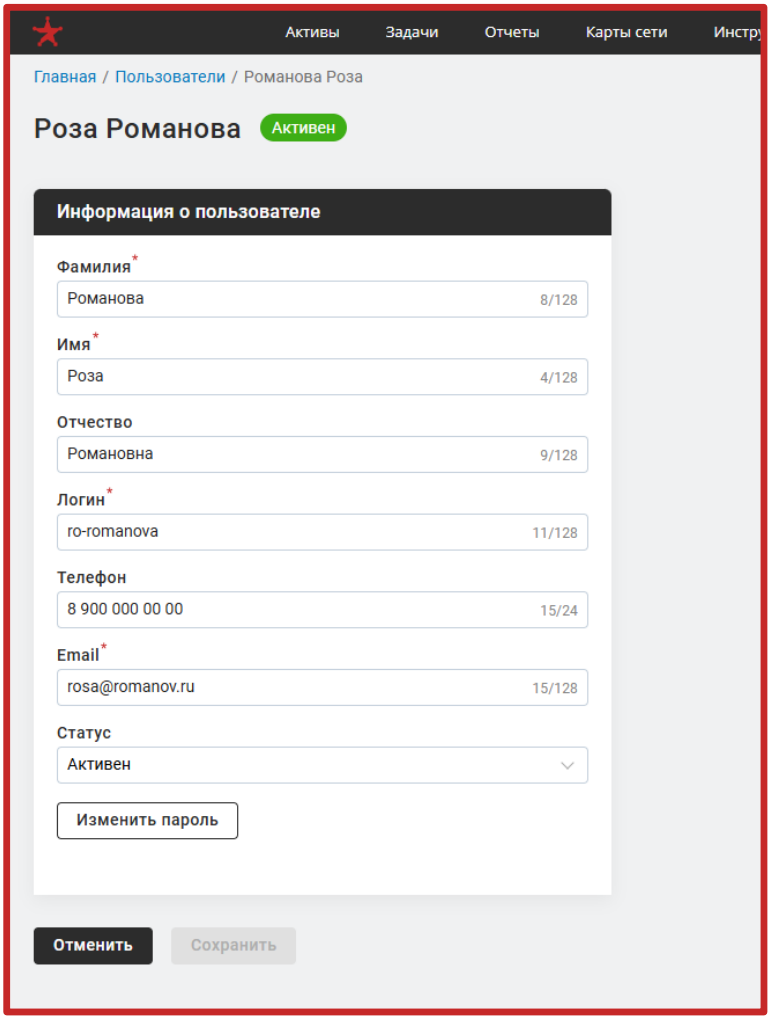


Рис. 157

Для смены пароля пользователя Сканер-ВС необходимо нажать на надпись «Изменить пароль». После чего отобразится окно смены пароля пользователя (рис. 158).

Окно смены пароля пользователя

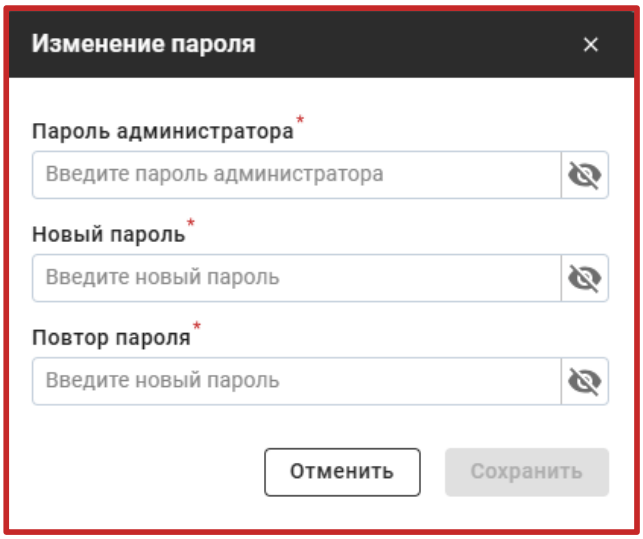


Рис. 158

Для смены пароля пользователя необходимо ввести текущий пароль от учетной записи пользователя Сканер-ВС с ролью «Администратор» и дважды ввести новый пароль пользователя. После чего нажать на кнопку «Сохранить», которая станет активной после заполнения всех полей.

Критерии достаточной защищенности паролей можно подробно рассмотреть в п. 5.9.1.2 настоящего документа и в НПЕШ.00606-01 91-1 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Руководство администратора. Часть 2».

Для отмены смены пароля пользователя необходимо нажать на красный крестик в правом верхнем углу окна смены пароля.

После внесения изменений в карточку информации о пользователе необходимо нажать на кнопку «Сохранить» чтобы подтвердить внесенные изменения. Данная кнопка по умолчанию неактивна. Она становится активной в тот момент, когда вносится какое-либо изменение в любое из полей карточки пользователя.

5.9.2. Секреты и подключения

После нажатия на вкладке «Секреты и подключения» в Сканер-ВС по умолчанию отобразится страница «Подключения» (рис. 159). Данная функция «Секреты и подключения» предназначена для централизованного управления учетными данными (логины, пароли, ключи) и настройки безопасного доступа к активам (серверам, сетевым устройствам). Она позволяет создавать, хранить и обновлять секреты, а также настраивать правила подключения к активам с указанием протоколов, портов и привязкой к секретам.

Страница «Подключения»

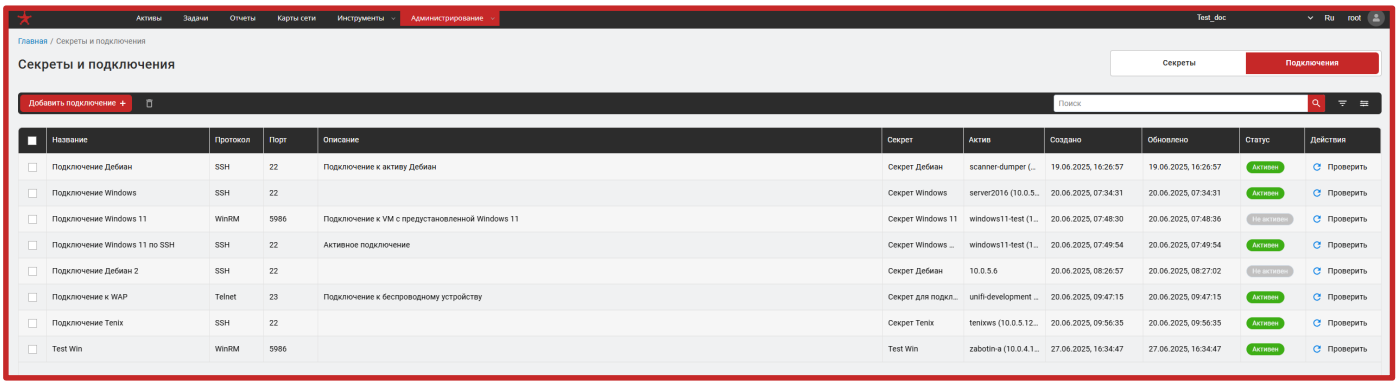


Рис. 159

При нажатии в верхнем правом углу кнопки «Секреты» отобразится страница «Секреты» (рис. 160). Чтобы вернуться на страницу «Подключения» необходимо будет снова нажать кнопку «Подключения» (рис. 161).

Страница «Секреты»

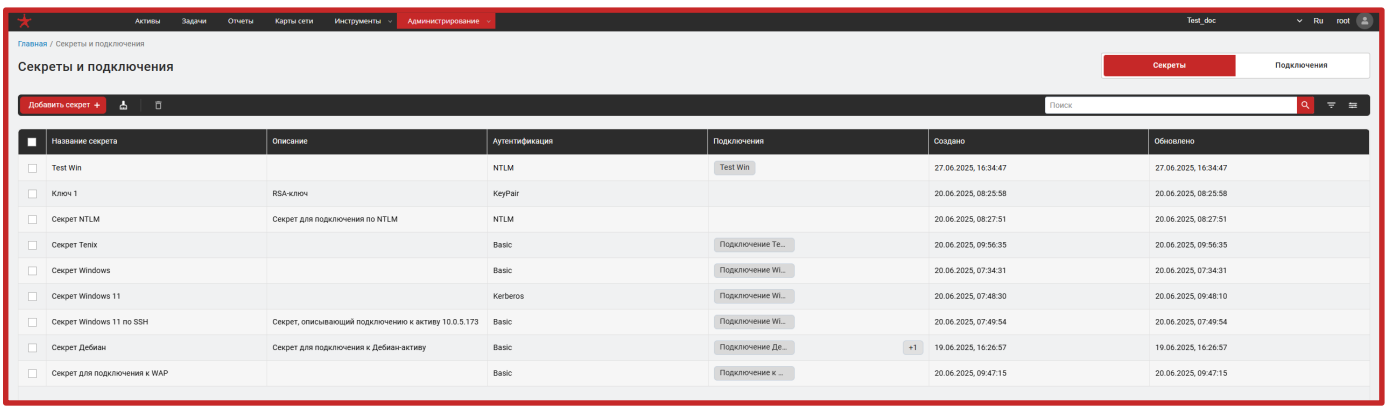


Рис. 160

Кнопки переключения страниц «Секреты» и «Подключения»

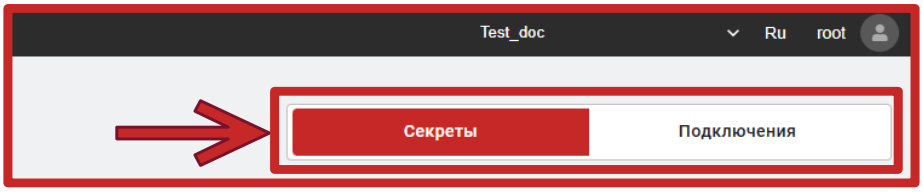


Рис. 161

5.9.2.1. Страница «Подключения»

5.9.2.1.1. Общая информация

После нажатия на строку «Секреты и подключения» в разделе «Администрирование» откроется страница «Подключения» вкладки «Секреты и подключения» (рис. 159). Данная функция позволяет задавать настройки подключения секретов для каждого актива исследуемой сети для дальнейшего проведения задач «Инвентаризация» и «Аудит конфигурации», что обеспечивает автоматизацию процессов без необходимости ручного ввода конфиденциальных данных.

Данная страница представляет собой таблицу, содержащую все добавленные в проект подключения и предоставляет следующую информацию:

– «Название» – название подключения;

– «Протокол» – информация об используемом в подключении протоколе обмена информацией;

– «Порт» – порт протокола;

– «Описание» – описание подключения, задаваемое оператором;

– «Секрет» – секрет, связанный с подключением;

– «Актив» – актив, для которого создается подключение;

– «Создано» – дата и время создания;

– «Обновлено» – дата и время обновления;

– «Статус» – информация о статусе подключения;

– «Действия» – позволяет выполнить проверку подключения.

5.9.2.1.2. Добавление нового подключения

Для добавления нового подключения необходимо нажать на кнопку «Добавить подключение», после чего откроется окно для ввода параметров создаваемого подключения (рис. 162).

Окно «Добавить подключение»

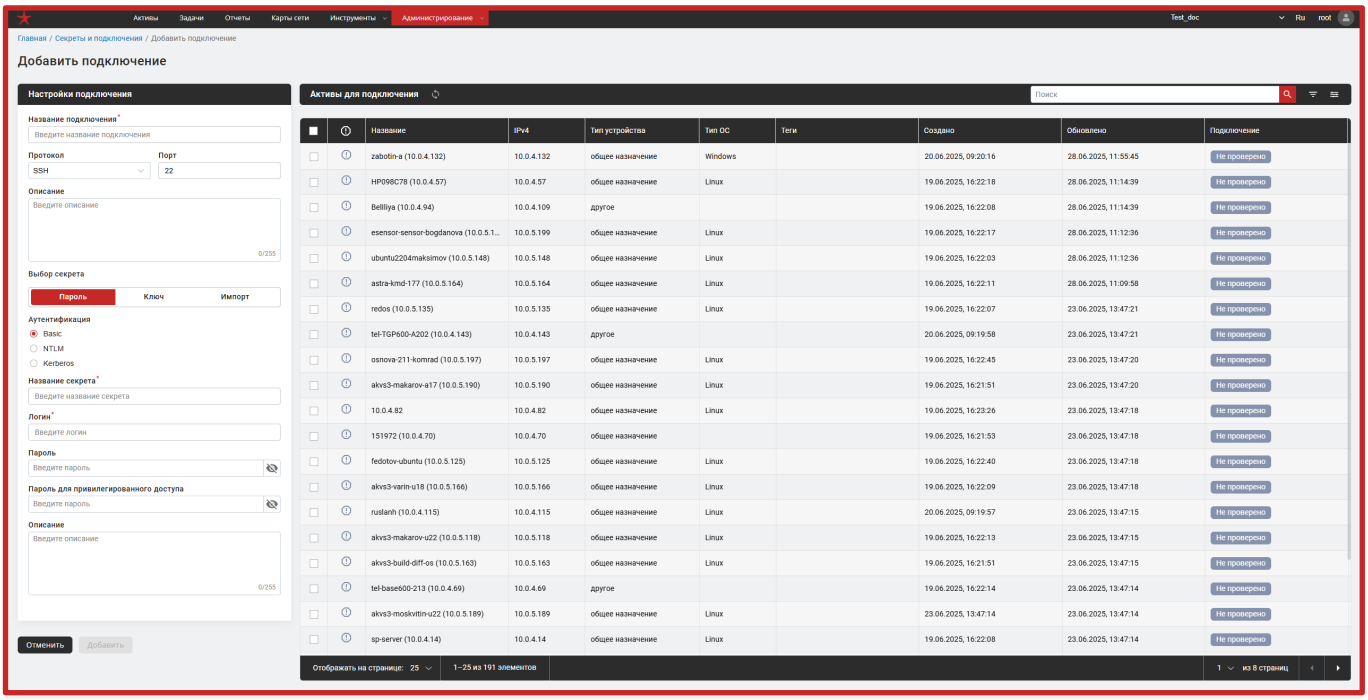


Рис. 162

В окне «Настройки подключения» необходимо ввести название подключения, выбрать протокол (SSH, WinRM, TELNET) и актив для подключения. Далее необходимо создать (с помощью методов «Пароль» или «Ключ», описанных в п. 5.9.2.2.2) или импортировать ранее созданный секрет.

Примечание. Протоколы SSH и WinRM используются для проведения задач «Инвентаризация» и «Аудит конфигурации».

ВАЖНО! При создании секрета типа «Пароль» в окне «Настройки подключения» после выбора типов аутентификации «NTML» или «Kerberos» появятся дополнительные поля «FQDN» и «Область (realm)», которые необходимо заполнить в соответствии со всплывающими подсказками (рис. 163).

После внесения всех настроек необходимо нажать кнопку «Добавить», в результате чего новое подключение появится на странице «Подключения».

В случае редактирования существующего подключения кнопка «Добавить» изменится на кнопку «Сохранить».

Дополнительные поля окна «Настройки подключения»

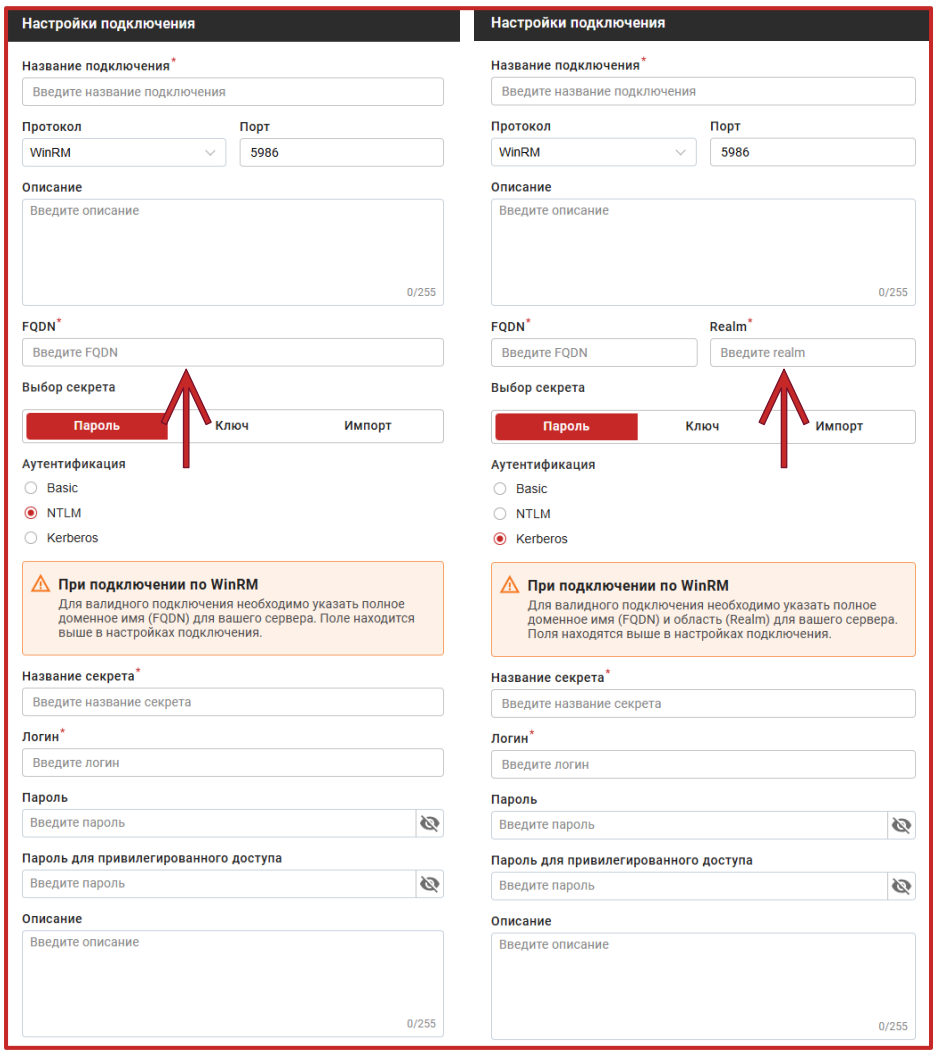


Рис. 163

В Сканер-ВС предусмотрена функция проверки подключения. Для проверки настраиваемого подключения необходимо нажать на кнопку «Проверить подключение». Проверка подключения может пройти успешно или завершиться ошибкой. В обоих случаях подключение можно сохранить, нажав кнопку «Добавить». Кнопка «Проверить подключение» будет присутствовать над кнопкой «Отменить» внизу страницы и доступна в случае создания или редактирования подключения для 1 актива.

Также в изделии предусмотрена функция одновременной проверки подключений сразу для нескольких активах. Для проверки подключения сразу на нескольких активах необходимо выбрать интересующие активы в таблице в правой части окна настройки подключения, после чего нажать кнопку «⟳».

Кнопка «⟳» (одновременная проверка подключений) и таблица «Активы для подключения» доступна только на этапах создания подключения и создания секрета (Администрирование → Секреты и подключения).

Примечание. При одновременном создании подключения к нескольким активам Сканер-ВС создает отдельные записи подключений для каждого из выбранных активов.

После нажатия на кнопку «⟳» справа от нее отобразится кнопка «■», позволяющая остановить процесс проведения одновременной проверки подключений.

5.9.2.1.3. Удаление и редактирование подключений

Для удаления необходимо выбрать одно или несколько подключений, после чего нажать на кнопку «🗑», которая станет активной.

Для редактирования необходимо кликнуть в любом месте строки подключения, после чего отобразится карточка подключения (рис. 164). Далее необходимо нажать кнопку «Редактировать», внести изменения и нажать «Сохранить».

Карточка подключения

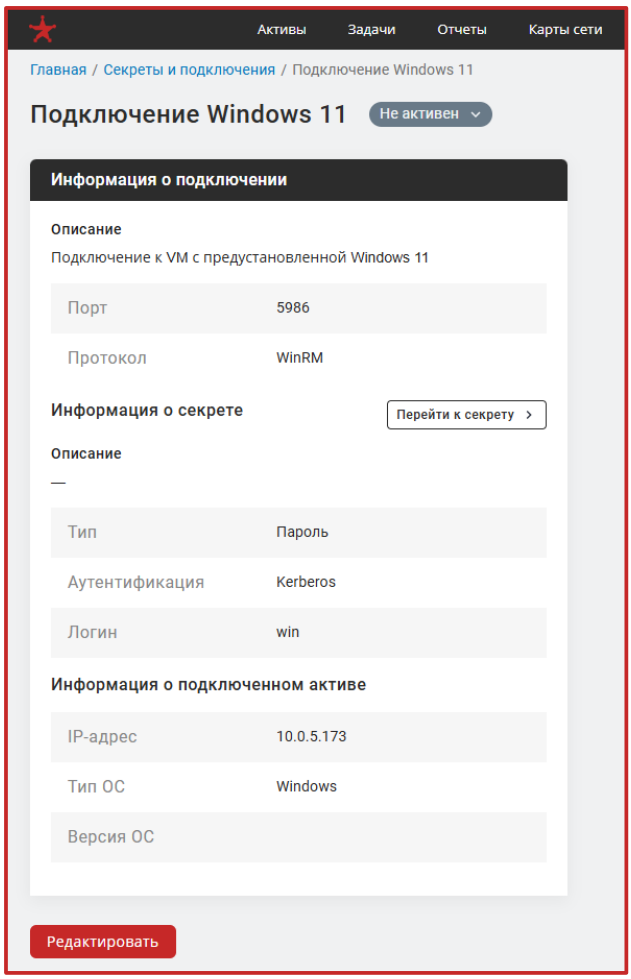


Рис. 164

5.9.2.2. Страница «Секреты»

5.9.2.2.1. Общее описание

После нажатия на кнопку «Секреты» на вкладке «Секреты и подключения» откроется страница «Секреты» (рис. 160). Данная функция позволяет создавать и хранить пароли (или ключи) авторизации административных учетных записей, назначать их на активы исследуемой сети и настраивать для каждого актива подключения для дальнейшего проведения задач «Инвентаризация» и «Аудит конфигурации».

Страница «Секреты» представляет собой таблицу со списком добавленных в проект секретов и содержит следующую информацию:

– «Название секрета»;

– «Описание» – краткое описание секрета, задаваемое оператором;

– «Аутентификация» – тип аутентификации, для которого используется секрет;

– «Подключение» – связанные с секретом сетевые настройки актива;

– «Создано» – дата и время создания секрета;

– «Обновлено» – дата и время обновления секрета.

5.9.2.2.2. Создание нового секрета

Для создания нового секрета на странице «Секреты» необходимо нажать на кнопку «Добавить секрет +», после чего откроется окно добавления секрета с возможность создания подключения для текущего секрета.

В Сканер-ВС предусмотрено два типа секретов (рис. 165):

– «Пароль» – создание секрета с помощью логина и пароля;

– «Ключ» – создание секрета на основе сгенерированного или импортированного ключа.

Вкладки «Пароль» и «Ключ»

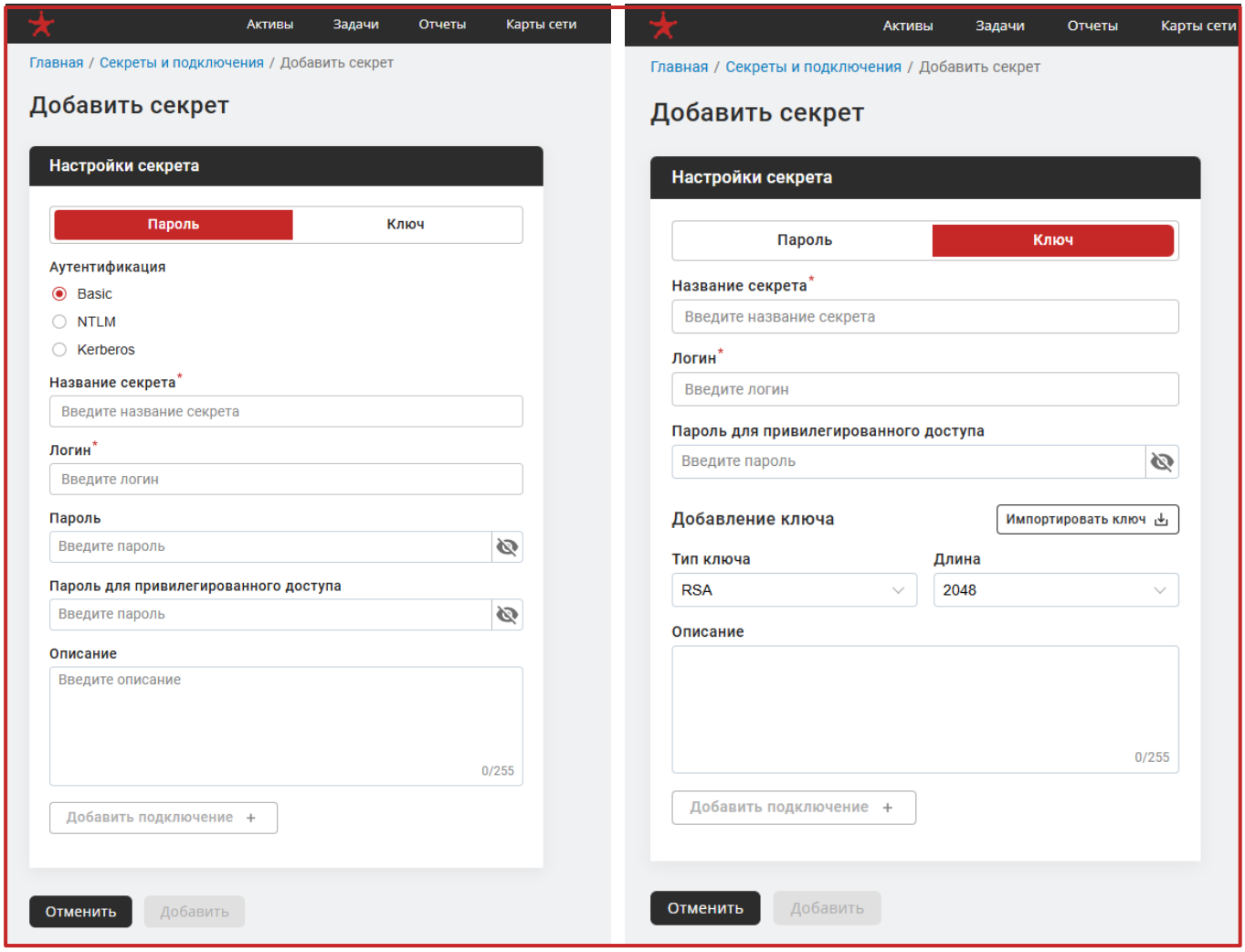


Рис. 165

При создании секрета «Пароль» необходимо выбрать протокол аутентификации (Basic, NTML или Kerberos), заполнить обязательные поля «Название секрета» и «Логин». При необходимости далее заполнить поля «Пароль» и/или «Пароль для привилегированного доступа» для учетной записи секрета.

Пароль для привилегированного доступа необходим для выполнения команд с правами администратора (например, через `sudo` для проведения аудита конфигурации или инвентаризации программных пакетов), и изменения чувствительной информации такой как логин и пароль. После чего нажать на кнопку «Добавить», которая станет активной.

При создании секрета «Ключ» необходимо заполнить обязательные поля «Название секрета», «Логин» и/или необязательное поле «Пароль для привилегированного доступа», а также выбрать тип ключа:

– «RSA» – генерируемое по алгоритму RSA число определенной длины (2048, 3072, 4096 бит);

– «ECDSA» – генерируемая по алгоритму ECDSA эллиптическая кривая с определенной длиной ключа (256, 384, 521 бит);

– «ED25519» – генерируемая по алгоритму ed25519 эллиптическая кривая, отличие от ECDSA в используемых при генерации кривых.

Для импорта уже существующего ключа необходимо нажать на кнопку «Импортировать ключ» (см. рис. 166) и перетащить файл в открывшееся окно импорта (рис. 167).

Примечание. При переключении в режим импорта обязательным файлом (.pem) является только приватный ключ.

Кнопка «Импортировать ключ»

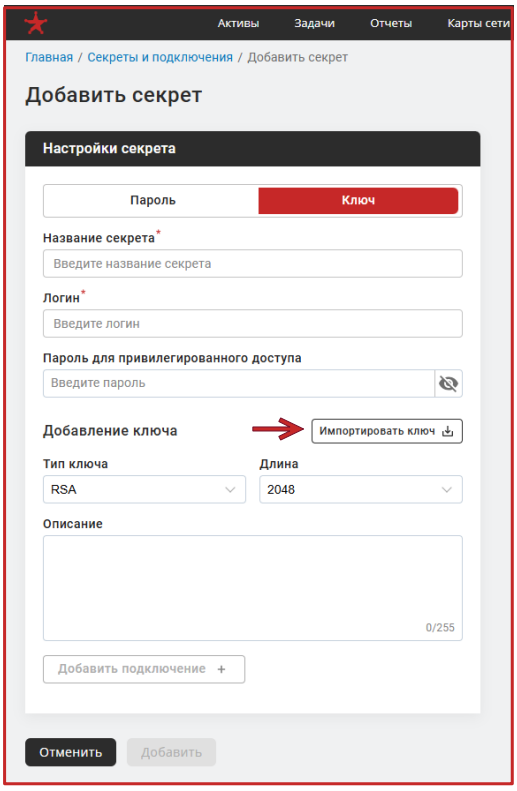


Рис. 166

Окно «Импорт приватного ключа»

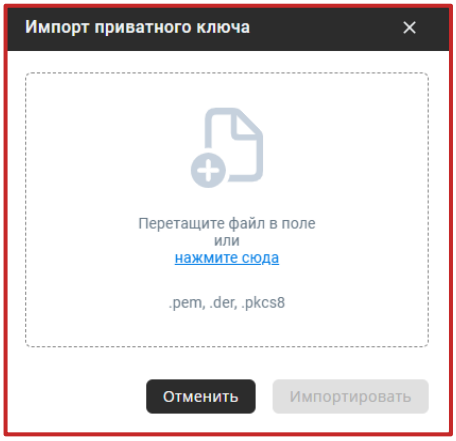


Рис. 167

В окне создания секрета предусмотрена возможность добавления подключения к текущему секрету. После нажатия на кнопку «Добавить подключение +» (рис. 168), откроется окно настройки подключения (рис. 162) (подробное описание настройки подключений приведено в п. 5.9.2.1).

Кнопка «Добавить подключение +»

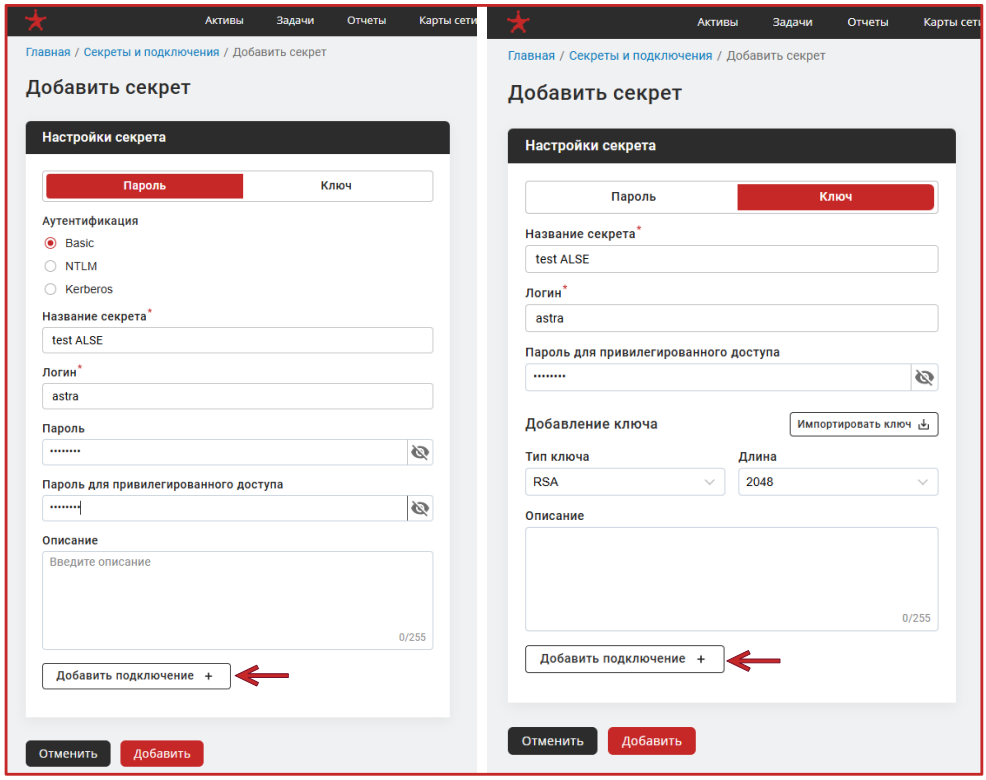


Рис. 168

5.9.2.2.3. Удаление и редактирование секретов

Для удаления неиспользуемых секретов нужно нажать на кнопку «» (Удалить неиспользуемые). Для удаления одного или нескольких секретов из списка необходимо выбрать нужные секреты и нажать на иконку «» (рис. 169).

Удаление секретов

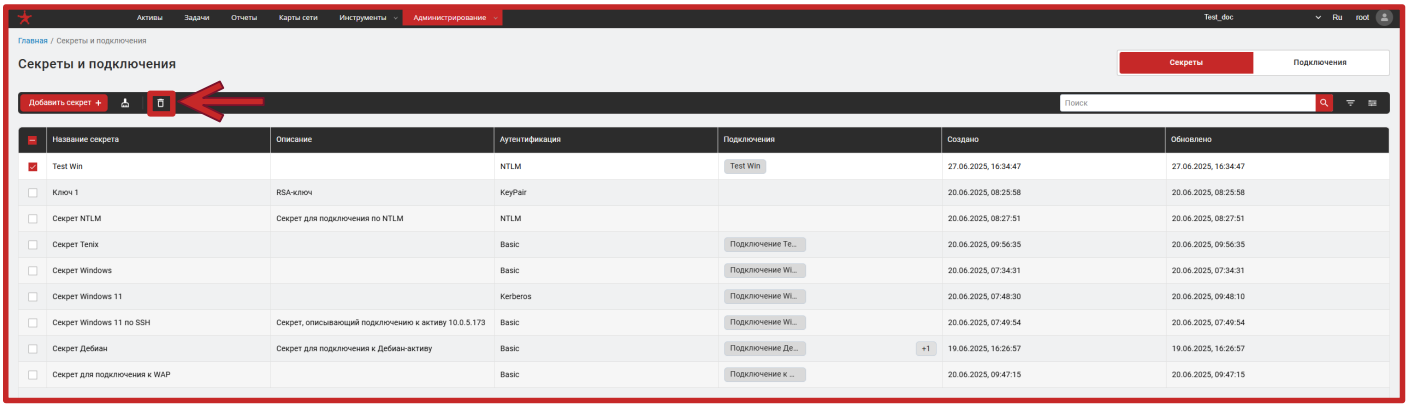


Рис. 169

Для редактирования информации о секрете необходимо перейти в карточку секрета, кликнув на соответствующую строку в списке (рис. 170).

Карточка секрета

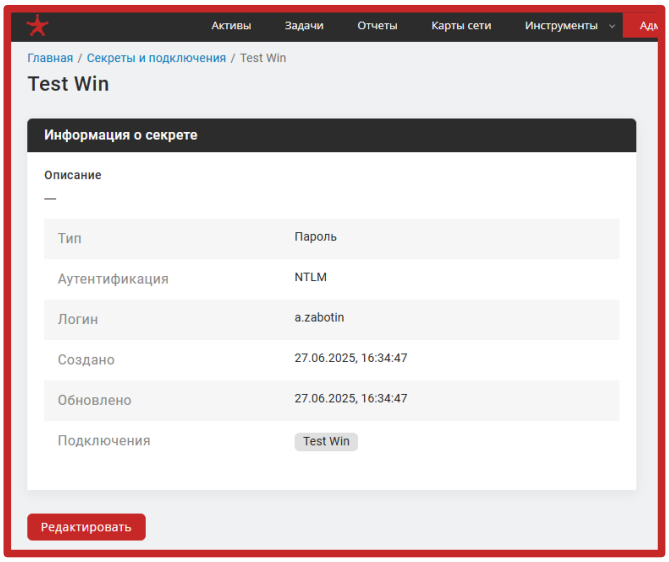


Рис. 170

Для редактирования информации о секрете необходимо нажать на кнопку «Редактировать». После чего отобразится окно редактирования секрета (рис. 171).

Окно редактирования секрета

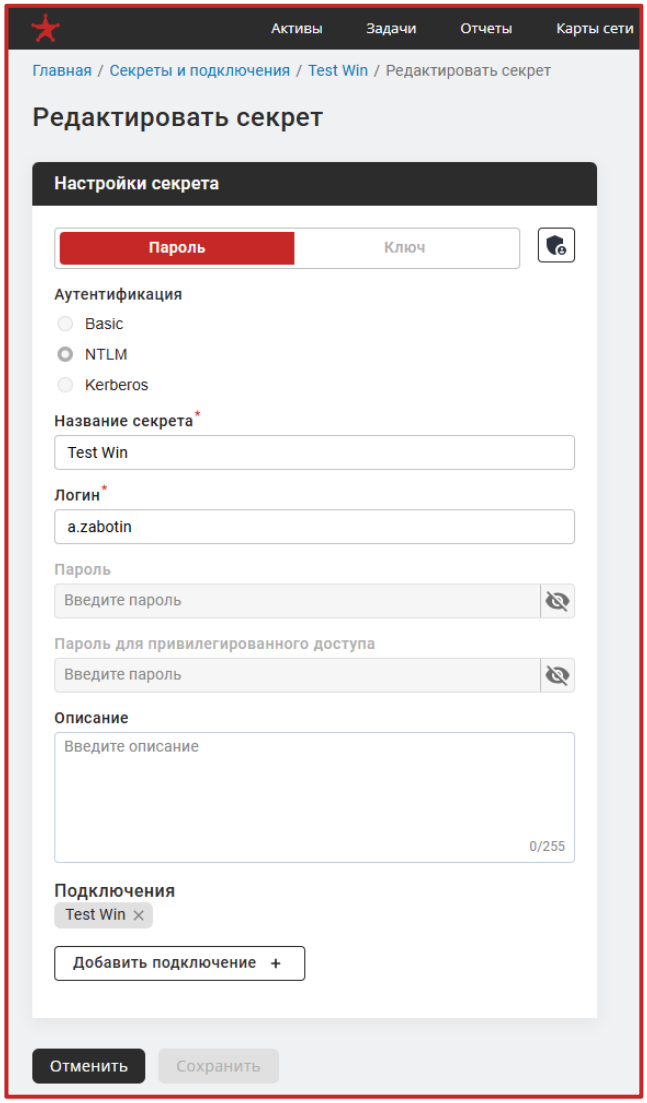


Рис. 171

Иконка « » (кнопка «Перейти в режим редактирования чувствительной информации») предназначена для подтверждения доступа к данным паролем привилегированного доступа (установленным ранее при создании секрета). После этого будут доступны все поля для редактирования информации на странице.

Остальные поля редактируются или заполняются аналогично описанному в п. 5.9.2.2.2 настоящего документа.

После внесения любого изменения в карточке секрета необходимо нажать на кнопку «Сохранить», которая станет активной. После чего в таблице, отображаемой на странице «Секреты» появится новая информация о секрете, который был отредактирован.

5.9.3. Обновления

Для лучшей защиты сети необходимы актуальные базы данных уязвимостей. Пользователю Сканер-ВС доступна функция просмотра информации об установленной версии базы данных уязвимостей.

После нажатия на вкладке «Обновления» в разделе «Администрирование» отобразится страница «Центр обновлений», предоставляющая информацию об истории скачивания обновлений (рис. 172).

Центр обновлений

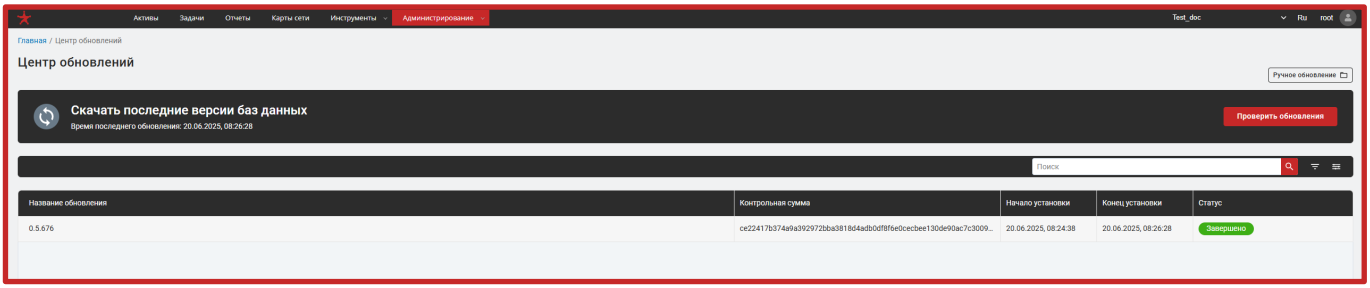


Рис. 172

На данной странице отображена таблица с историей обновления баз данных уязвимостей Сканер-ВС. Данная таблица содержит следующие столбцы:

– название обновления, в столбце отображается название обновления;

– контрольная сумма, в столбце отображается контрольная сумма файлов завершенного обновления базы данных;

– начало установки, в столбце указывается дата и время начала установки обновления баз данных уязвимостей;

– конец установки, в столбце указывается дата и время окончания установки обновления баз данных уязвимостей;

– статус, в столбце указывается статус выполнения обновления из следующих вариантов: завершено – обновление завершено без ошибок, активно – обновление в процессе установки, отменено – обновление было отменено оператором в ходе проведения скачивания и установки обновления, ошибка – обновление завершено по причине обнаружения какой-либо ошибки.

Область над таблицей с историей обновления баз данных уязвимостей предназначена для управления записями в таблице и ручным обновлением. В этой области предусмотрен поиск по записям, управление фильтрами и управление отображением столбцов.

5.9.3.1. Установка ручного обновления

Для ручной установки обновлений Сканер-ВС необходимо над полем с временем последнего обновления в правом углу страницы (рис. 172) нажать кнопку «Ручное обновление».

После нажатия на кнопку «Ручное обновление» в Сканер-ВС отобразится всплывающее окно для загрузки файла, содержащего обновления баз данных уязвимостей (рис. 173).

Окно «Ручное обновление»

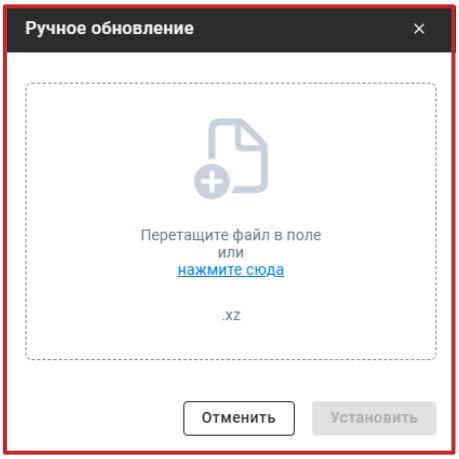


Рис. 173

Для ручной установки обновления необходимо перетащить необходимые файлы в соответствующее поле в окне «Ручное обновление» либо нажать левой кнопкой мыши по надписи «нажмите сюда», после чего откроется стандартный менеджер файлов, в котором необходимо выбрать нужные файлы обновления.

После добавления файла для установки обновления Сканер-ВС проверяет добавленный файл на целостность.

После успешного прохождения файлом обновления проверки он будет отображен в соответствующем поле окна «Ручное обновление», а кнопка «Установить» станет активной. Для перехода к установке обновлений необходимо нажать кнопку «Установить». В случае, если добавляемый файл не прошел проверку на целостность Сканер-ВС отобразить сообщение об ошибке «Файл поврежден».

В случае возникновения ошибки при загрузке файла для обновления рекомендуется повторить попытку. При повторной ошибке в ходе загрузке файла обновления рекомендуется заново скачать файл обновлений из официального источника и повторить попытку. Если загрузка файла закончится с ошибкой снова, то рекомендуется обратиться к своему администратору или в техническую поддержку предприятия-поставщика.

При нажатии на кнопку «Установить» произойдет возврат к странице «Центр обновлений», а в таблице (рис. 172) отобразится статус загрузки обновления.

Запуск обновления может завершиться следующими вариантами:

– начнется установка обновления;

– обнаружением ошибки:

а) отображается сообщение «Не удалось установить обновление;

б) отображается сообщение «Данное обновление уже устанавливалось».

В случае **а)** рекомендуется повторить попытку установки обновления, при повторном завершении обновления баз данных уязвимостей с ошибкой рекомендуется обратиться к своему администратору или в техническую поддержку предприятия-поставщика.

В случае **б)** нет необходимости предпринимать какие-либо действия. Сообщение «Данное обновление уже устанавливалось» говорит о том, что файл, который был загружен для установки обновления уже не актуален в силу того, что данные обновления уже были установлены в Сканер-ВС. Пользователю необходимо нажать кнопку «Понятно» после чего произойдет возврат в интерфейс центра обновлений Сканер-ВС.

5.9.4. Загрузка лицензии

В Сканер-ВС доступна функция управления лицензией.

После нажатия на вкладке «Загрузка лицензии» в разделе «Администрирование» отобразится окно «Центр обновлений», предоставляющая информацию об истории скачивания обновлений (рис. 174)

Окно «Загрузка лицензии»

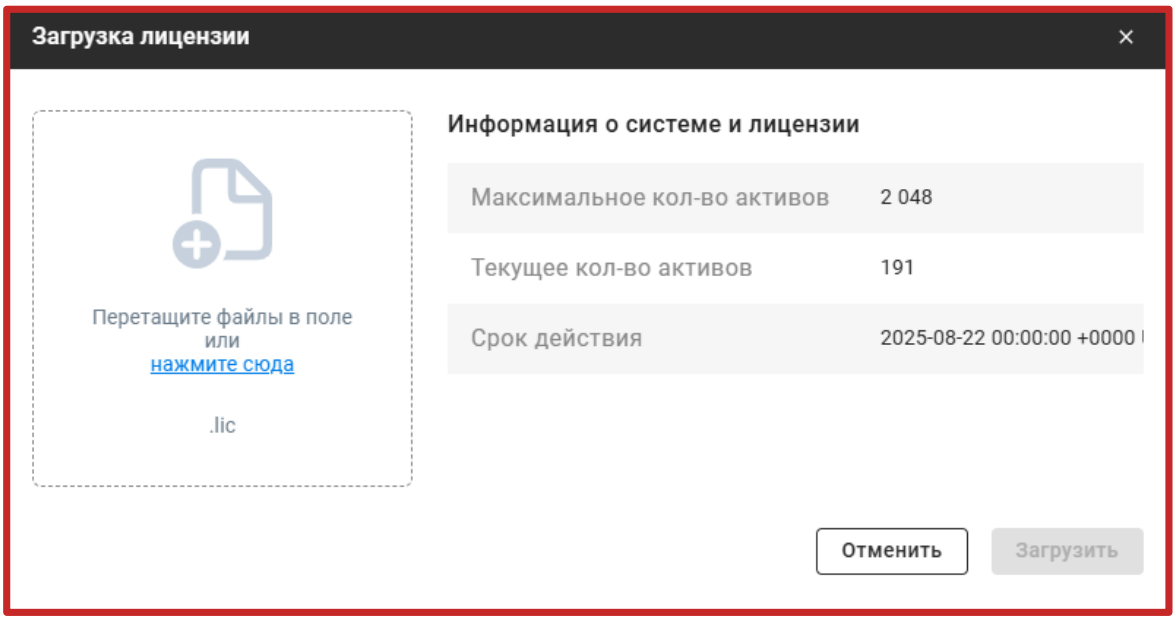


Рис. 174

Для загрузки лицензии необходимо перетащить файл лицензии в соответствующее поле в окне «Загрузка лицензии» либо нажать левой кнопкой мыши по надписи «нажмите сюда», после чего откроется стандартный менеджер файлов, в котором необходимо выбрать нужный файл лицензии.

После добавления файла лицензии Сканер-ВС проверяет добавленный файл на валидность.

После успешного прохождения файлом лицензии проверки информация о сроке действия лицензии и количестве доступных активов будет отображена в соответствующих полях окна «Загрузка лицензии», а кнопка «Загрузить» станет активной (рис. 175). Для загрузки новой лицензии необходимо нажать кнопку «Загрузить». В случае, если добавляемый файл не прошел проверку на валидность Сканер-ВС отобразить сообщение об ошибке «Ошибка: невалидный файл» (рис. 176).

Добавление валидного файла лицензии

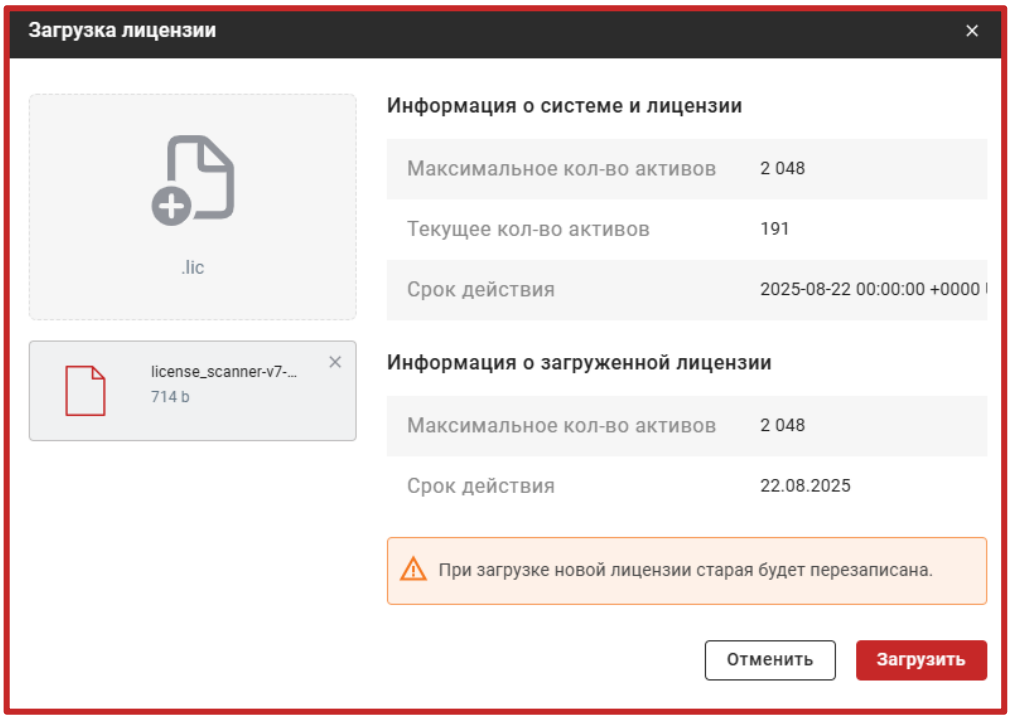


Рис. 175

Добавление невалидного файла лицензии

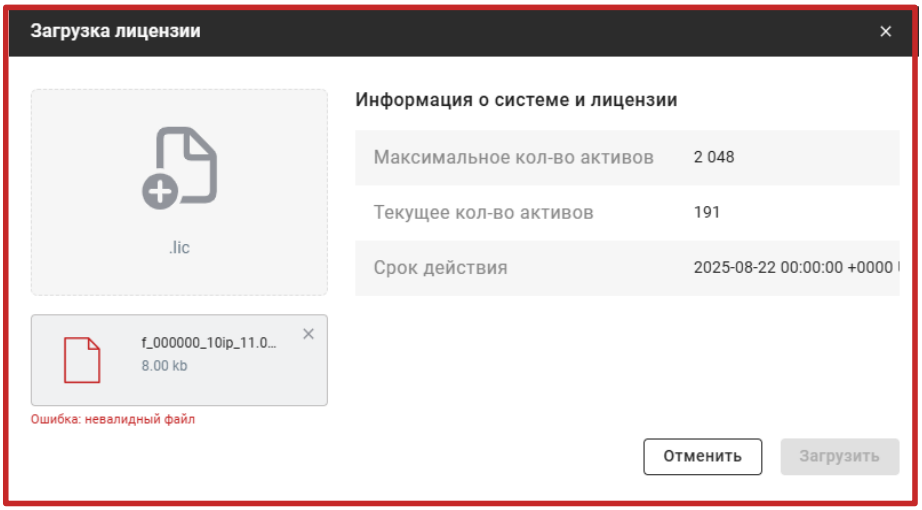


Рис. 176

Также, Сканер-ВС проверяет срок действия лицензии при добавлении нового файла лицензии и, в случае добавления просроченной лицензии отображает сообщение об ошибке: «Срок действия лицензии истек» (рис. 177).

Добавление файла лицензии с истекшим сроком действия

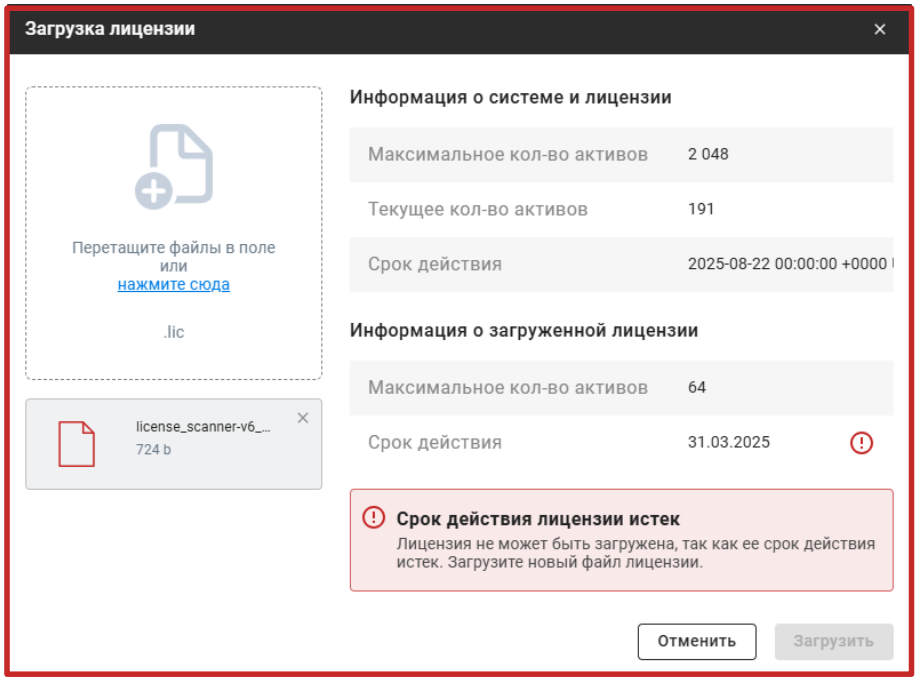


Рис. 177

6. Компонент «Инспектор» версии 3

Компонент «Инспектор» из состава ПК «Сканер-ВС» обеспечивает:

– формирование и контроль дискреционных и мандатных полномочий доступа пользователей (локальных и доменных) к выбранным сетевым папкам и объектам файловой системы ОС семейства Windows, в том числе с учетом настроек СЗИ Secret Net Studio, СЗИ Secret Net Studio-C, СЗИ Secret Net 7, СЗИ НСД Dallas Lock 8.0-K, СЗИ НСД Dallas Lock 8.0 C;

– формирование и контроль дискреционных и мандатных полномочий доступа локальных пользователей к выбранным объектам файловой системы ОС специального назначения «Astra Linux Special Edition»;

– поиск остаточной информации на машинных носителях информации, а также определение директории файла с найденной информацией;

– тестирование механизмов очистки оперативной памяти ОС семейства Microsoft Windows, ОС специального назначения «Astra Linux Special Edition» и запоминающих устройств рабочей станции;

– контрольное суммирование заданных файлов, папок, подпапок, съемных носителей и накопителей на жестких магнитных дисках.;

– инвентаризацию программных и аппаратных средств;

– контроль работоспособности антивирусного ПО на основе использования EICAR Test File.

Компонент «Инспектор» эксплуатируется в среде под управлением ОС специального назначения «Astra Linux Special Edition»: 1.4, 1.5, 1.6 и ОС семейства Microsoft Windows: 7, 8.1, 10.

6.1. Запуск компонента

Для начала работы с компонентом «Инспектор» необходимо подключить носитель ПК «Сканер-ВС» к рабочей станции и запустить исполняемый файл inspector.exe, расположенный в корневом каталоге носителя.

После запуска откроется окно активации лицензии (рис. 178).

Окно активации лицензии

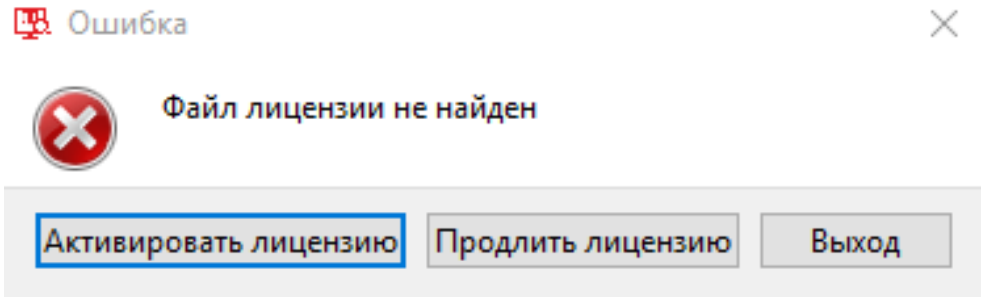


Рис. 178

Для активации необходимо нажать кнопку «Активировать лицензию» и выбрать файл с лицензией (с расширением «.lic»).

Далее откроется окно с информацией об успешной активации лицензии (рис. 179).

Окно с информацией об успешной активации лицензии

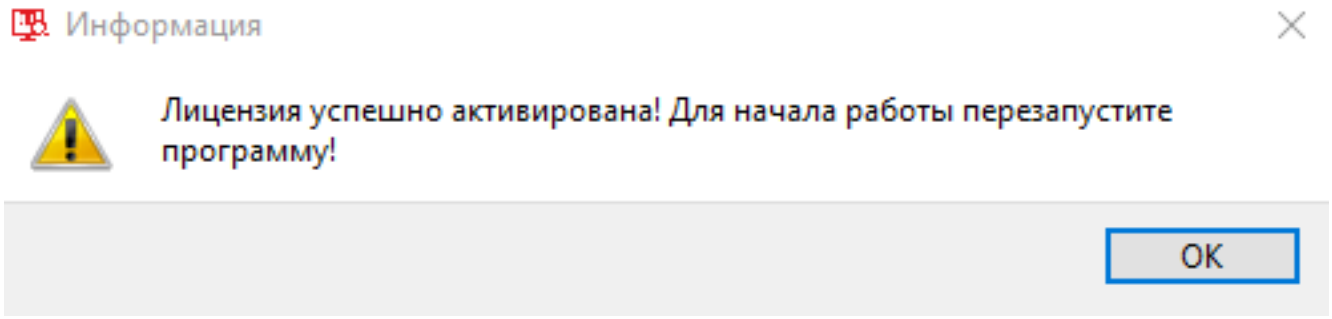


Рис. 179

Далее необходимо повторно запустить компонент «Инспектор».

После запуска откроется стартовое окно компонента «Инспектор» (рис. 180).

Стартовое окно

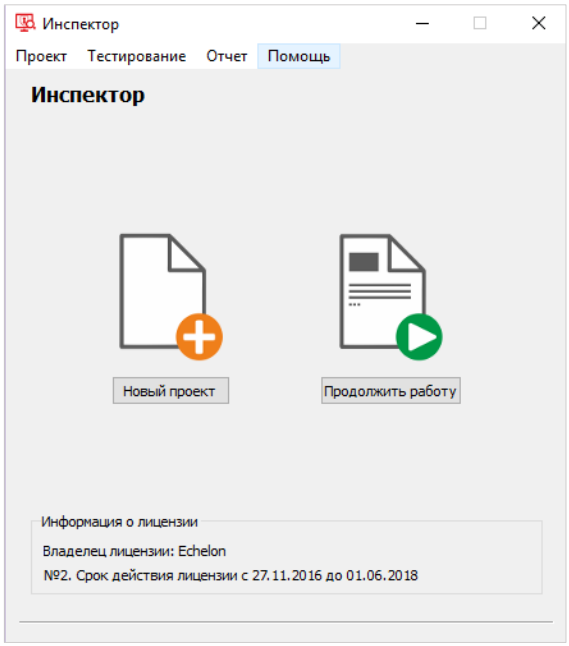


Рис. 180

После запуска Оператору необходимо создать новый проект или выбрать проект из ранее созданных (рис. 180).

Для того, чтобы продолжить работу с ранее созданным проектом необходимо нажать кнопку «Продолжить работу» и в открывшемся окне выбрать сохраненный проект (рис. 181).

Сохраненный проект

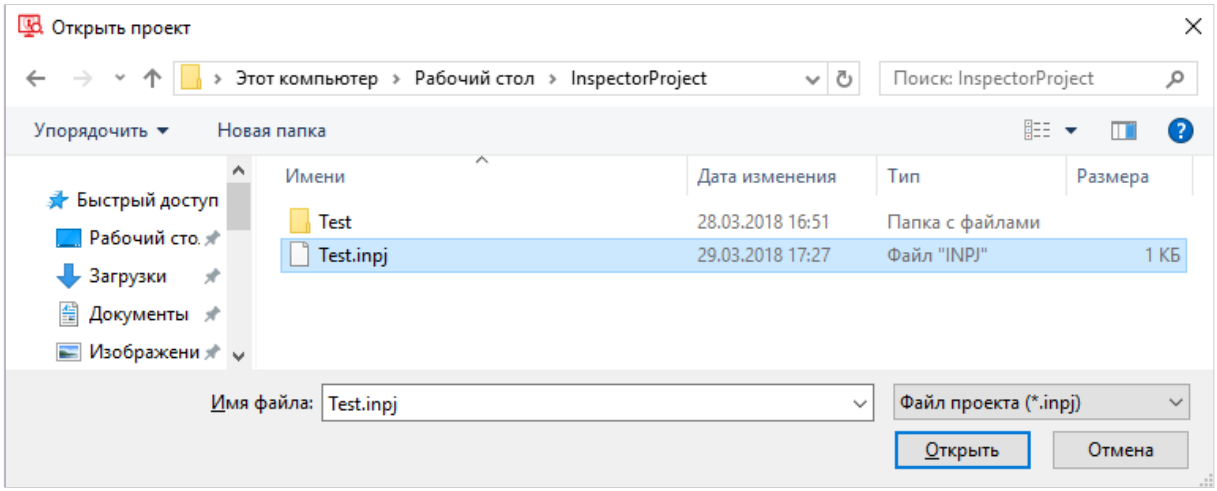


Рис. 181

Для создания нового проекта необходимо нажать кнопку «Новый проект». В открывшемся окне (рис. 182) необходимо указать следующие параметры:

– имя проекта (поле «Имя»);

– расположение файла проекта (поле «Расположение»);

– наименование организации (поле «Организация»).

Далее необходимо нажать кнопку «Завершить». Если создавать проект не требуется, нужно нажать кнопку «Отмена».

Примечание. Папка, указанная в поле «Расположение», будет использоваться для хранения отчетов.

Ввод параметров нового проекта

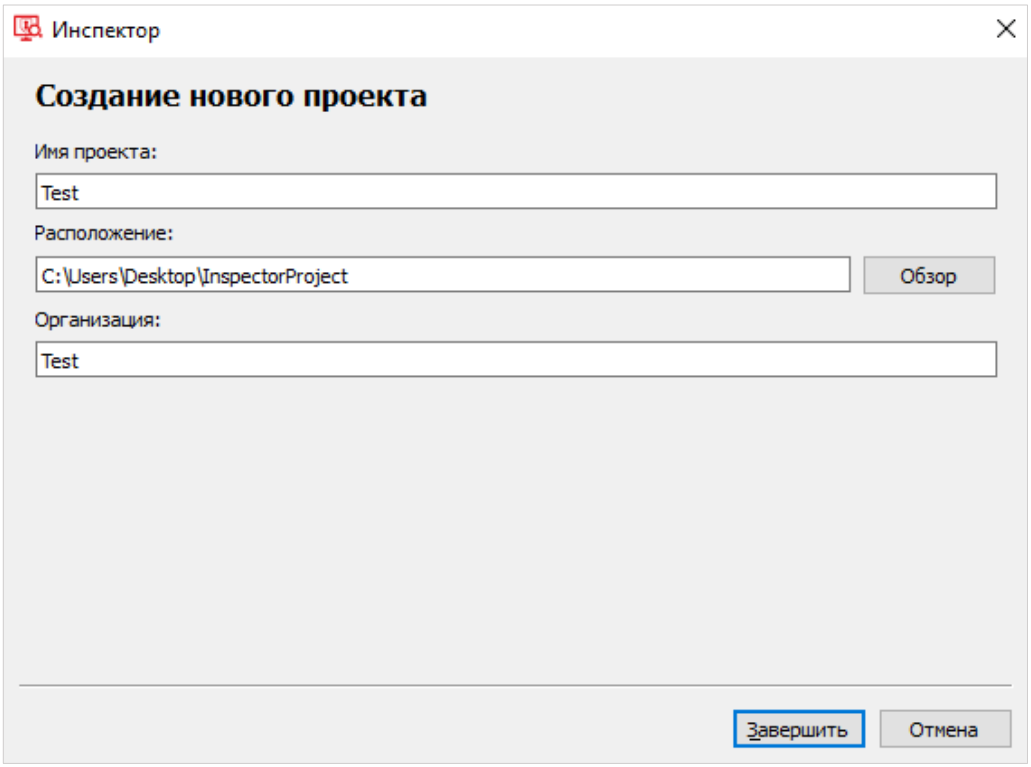


Рис. 182

После нажатия кнопки «Завершить» по указанному адресу будет автоматически создана папка с конфигурациями проекта, содержащая файл проекта с расширением «.inpj» (рис. Рис. 183), и откроется рабочее окно компонента «Инспектор» (рис. 184).

Папка проекта

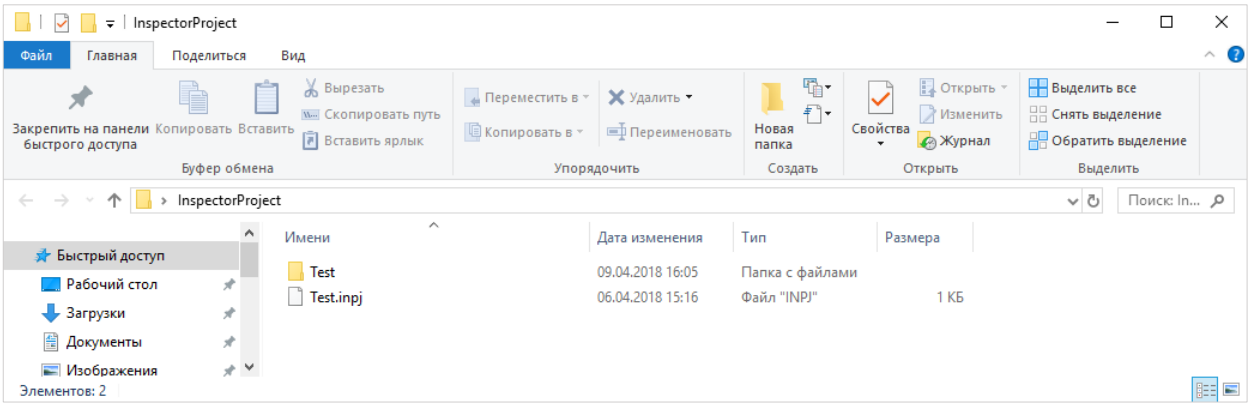


Рис. 183

Рабочее окно

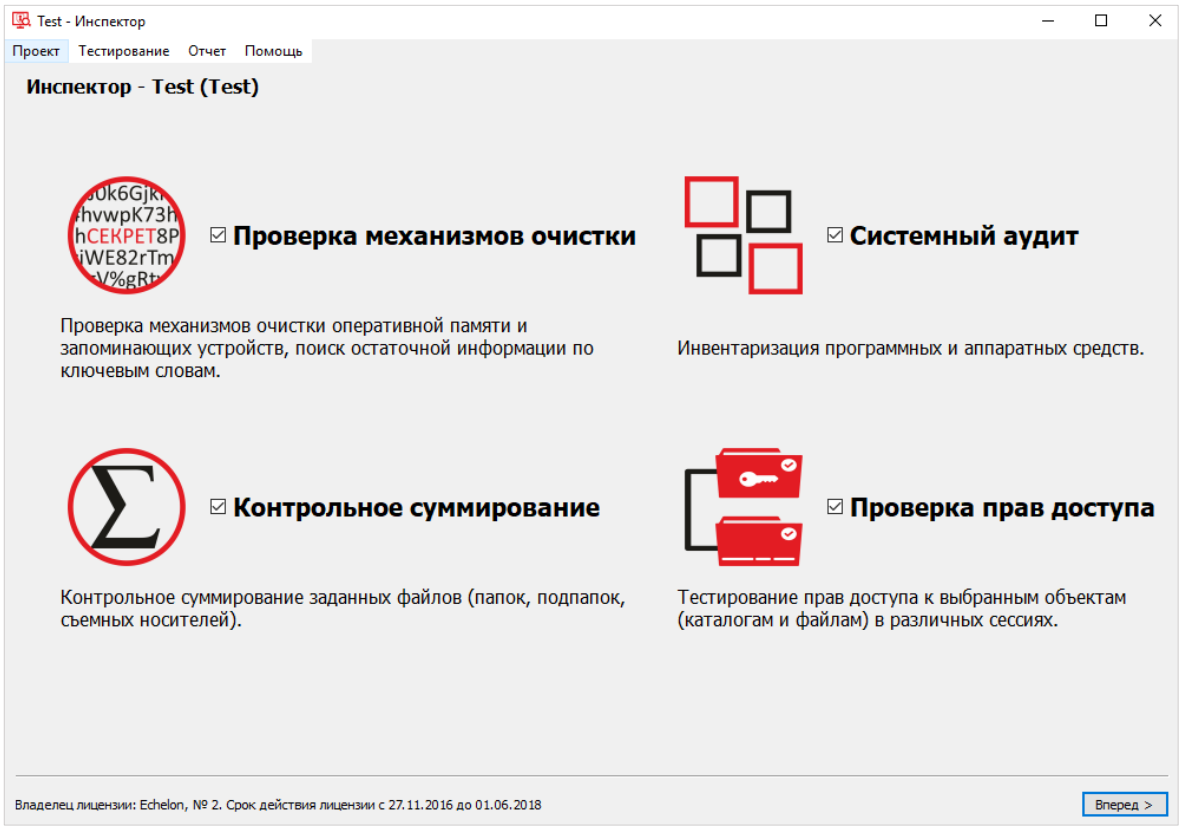


Рис. 184

В рабочем окне (рис. 184) перечислены инструменты компонента «Инспектор»:

– проверка механизмов очистки;

– системный аудит;

– контрольное суммирование;

– проверка прав доступа.

У каждого инструмента есть пиктограмма, название и краткое описание с перечнем решаемых задач. Выбор каждого инструмента отмечается галочкой рядом с названием (также галочка выставляется и убирается нажатием на пиктограмму или название инструмента).

Меню компонента «Инспектор», расположенное в левом верхнем углу окна, состоит из следующих элементов:

– «Проект» дает доступ к управлению проектами: сохранение, создание и открытие проектов, а также выход из программы (рис. 185);

Подменю «Проект»

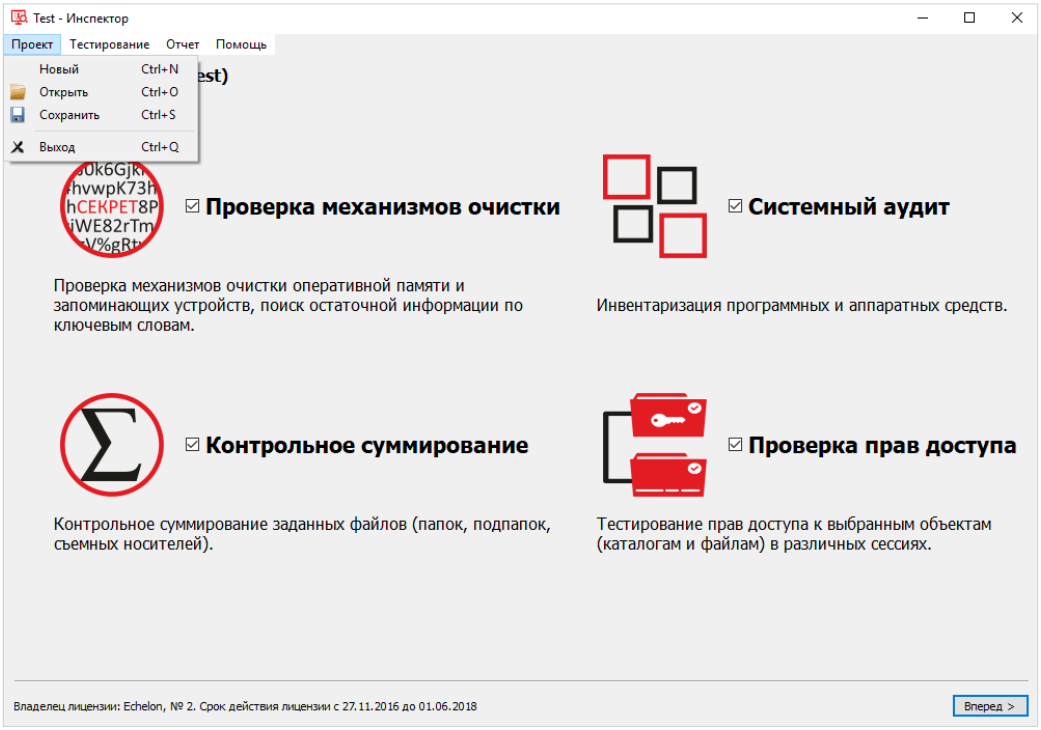


Рис. 185

– «Тестирование» содержит инструменты: «Проверка прав доступа», «Проверка механизма очистки памяти», «Тестирование антивируса» (рис. 186);

Подменю «Тестирование»

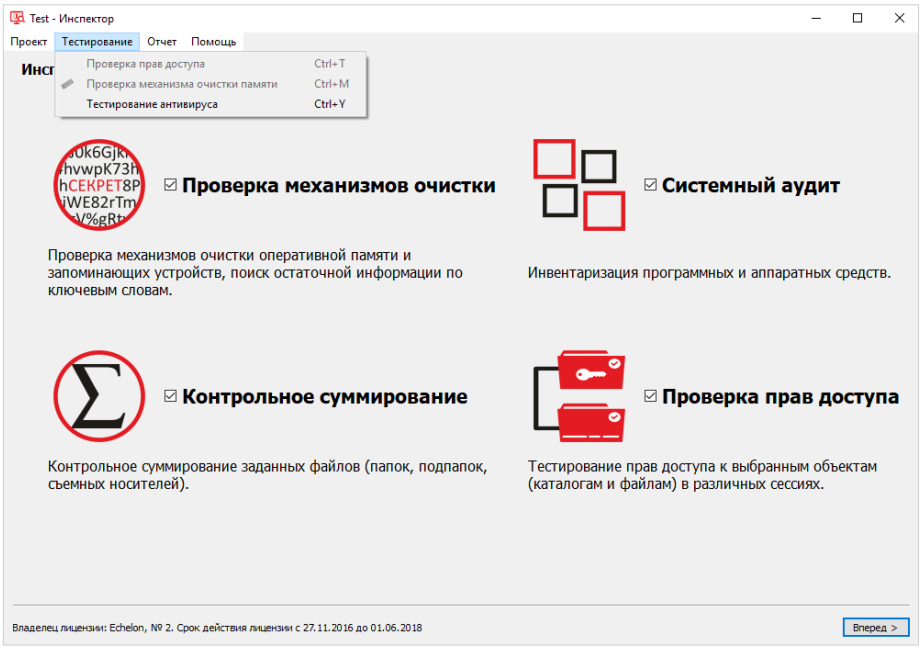


Рис. 186

– «Отчет» открывает отчеты, которые были созданы ранее, и содержит инструмент сравнения отчетов (рис. 187);

Подменю «Отчет»

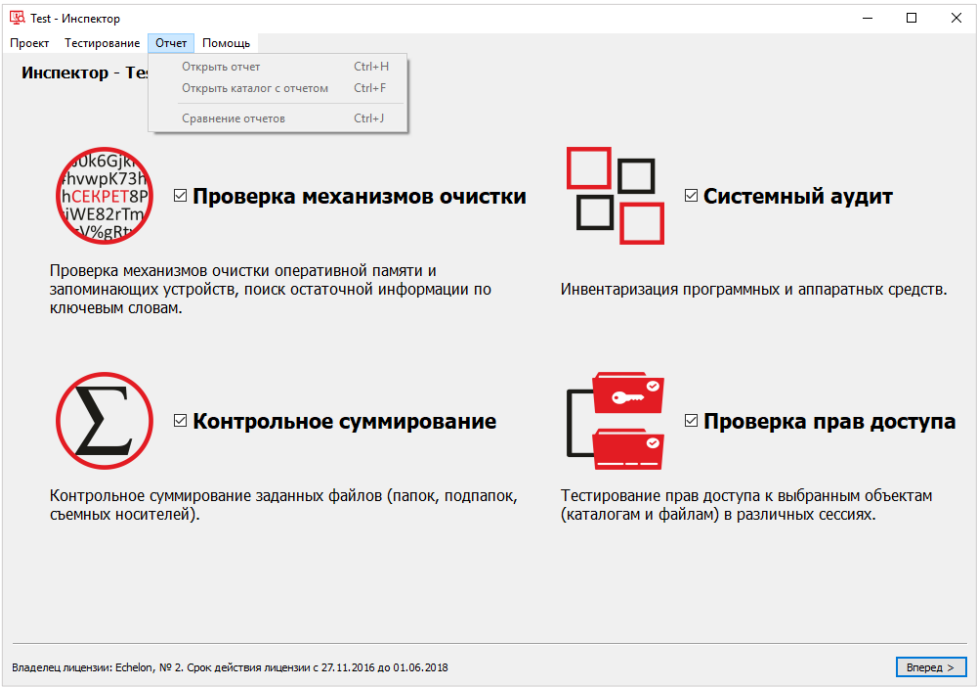


Рис. 187

– «Помощь» (рис. 188) открывает окно с информацией о версии, лицензии и ее продлении (кнопка «Продлить лицензию») (рис. 189).

Подменю «Помощь»

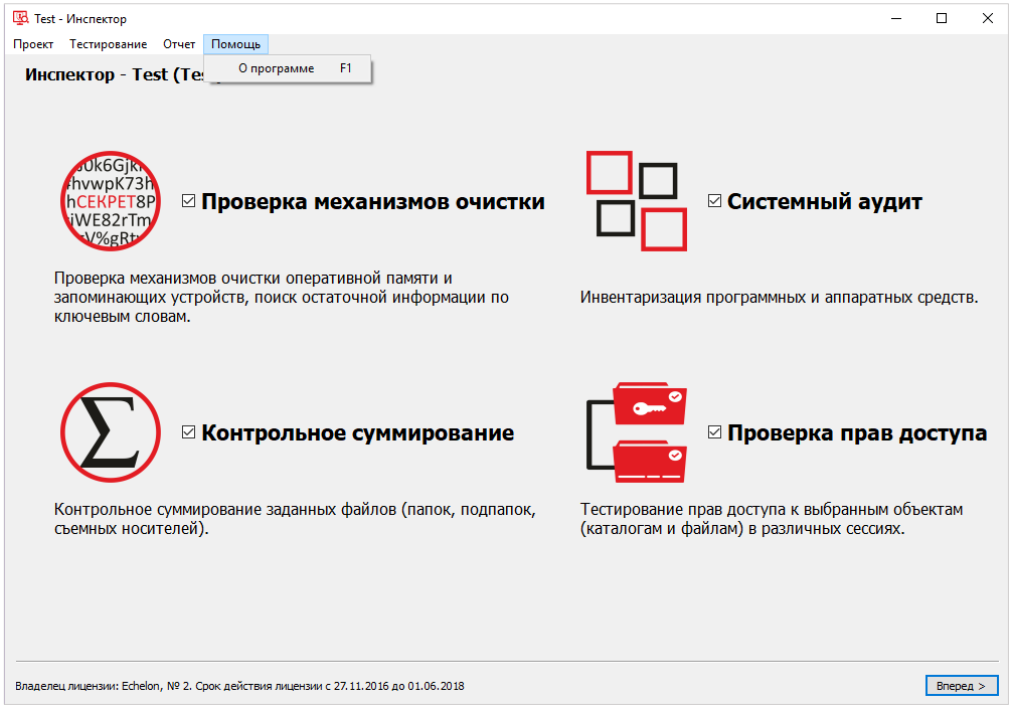


Рис. 188

Окно с информацией о лицензии

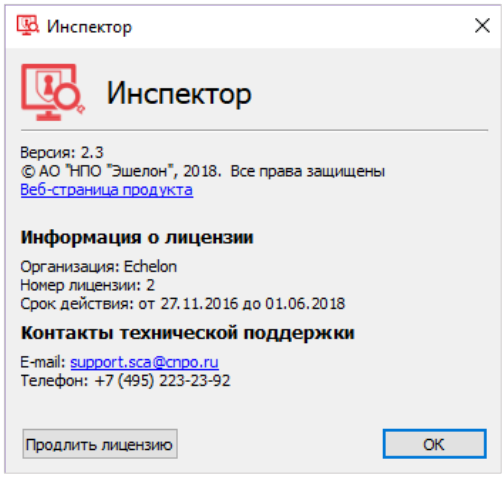


Рис. 189

Примечание. Комбинации клавиш для клавиатурного режима работы с компонентом представлены в приложении.

6.2. Работа с компонентом «Инспектор» в режиме замкнутой программной среды ОС Astra Linux

Механизм замкнутой программной среды (ЗПС) ОС Astra Linux позволяет ограничить доступ Операторов к исполняемым файлам только теми программами, у которых есть цифровая подпись.

6.2.1. Запуск ЗПС на ОС Astra Linux 1.5

Перед запуском ЗПС необходимо поместить ключ «zao_npo_echelon_pub_key.gpg» в каталог:

```
/ etc / digsig / keys
```

Далее в файле «/ etc / digsig / digsig_initramfs.conf» необходимо установить следующие параметры (рис. 190):

```
DIGSIG_ENFORCE=1
DIGSIG_LOAD_KEYS=1
```

Установленные параметры для запуска ЗПС

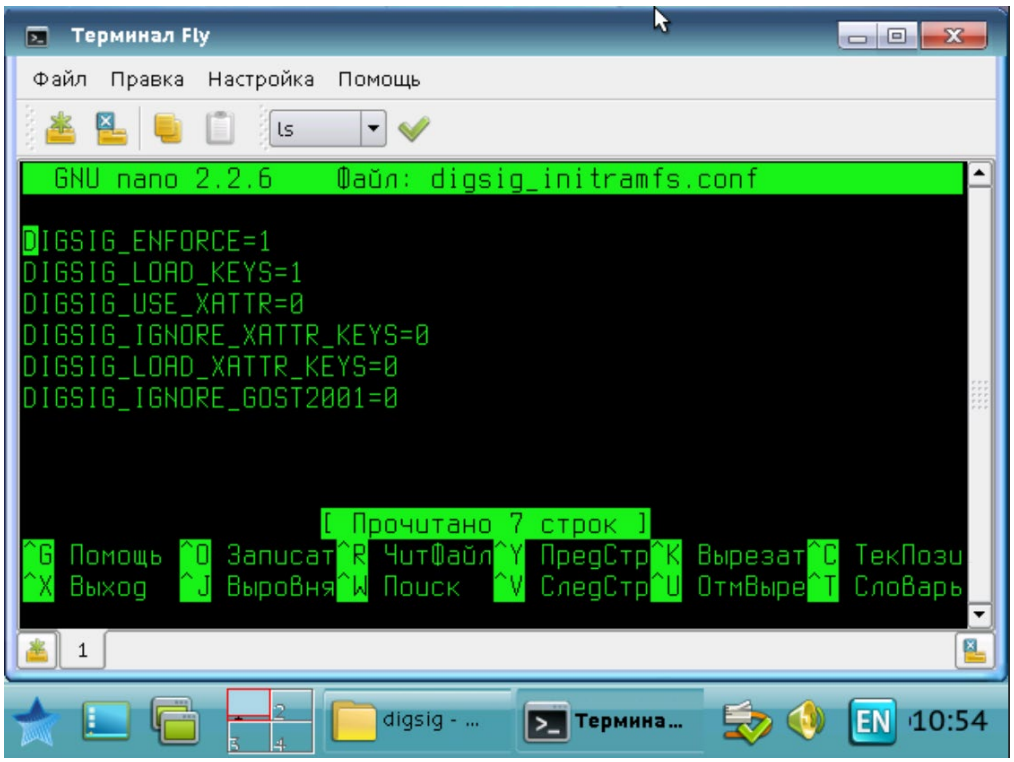


Рис. 190

Далее необходимо закрыть файл «digsig_initramfs.conf» и сохранить изменения, после чего, нужно ввести команду `update-initramfs -u -k all` и выполнить перезагрузку (рис. 191).

Ввод команды для запуска ЗПС

```
root@astra:/etc/digsig# update-initramfs -u -k all
update-initramfs: Generating /boot/initrd.img-4.2.0-23-pax
update-initramfs: Generating /boot/initrd.img-4.2.0-23-gener
ic
root@astra:/etc/digsig#
```

Рис. 191

После перезагрузки, ОС Astra Linux 1.5 будет работать в режиме ЗПС.

6.2.2. Запуск ЗПС на ОС Astra Linux 1.6

Перед запуском ЗПС необходимо поместить ключ «zao_npo_echelon_pub_key.gpg» в каталог:

```
/ etc / digsig / keys
```

Для запуска ЗПС на ОС Astra Linux 1.6 необходимо перейти в панель управления (рис. 192).

Путь к панели управления

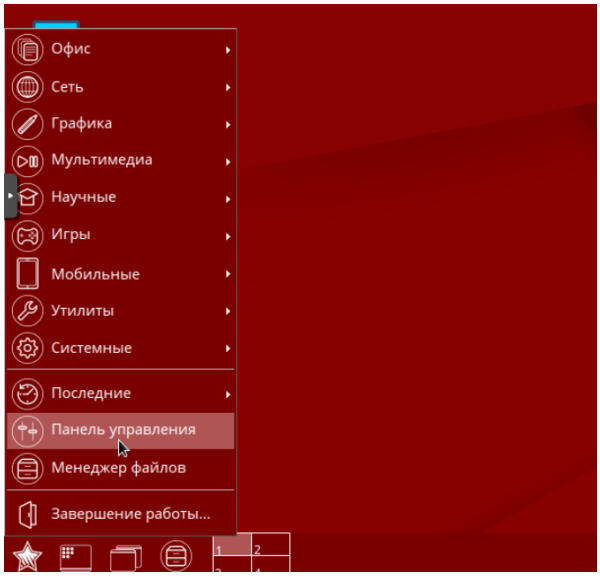


Рис. 192

Далее необходимо открыть вкладку «Безопасность» и открыть программу «Политика безопасности» (рис. 193).

Вкладка «Безопасность»

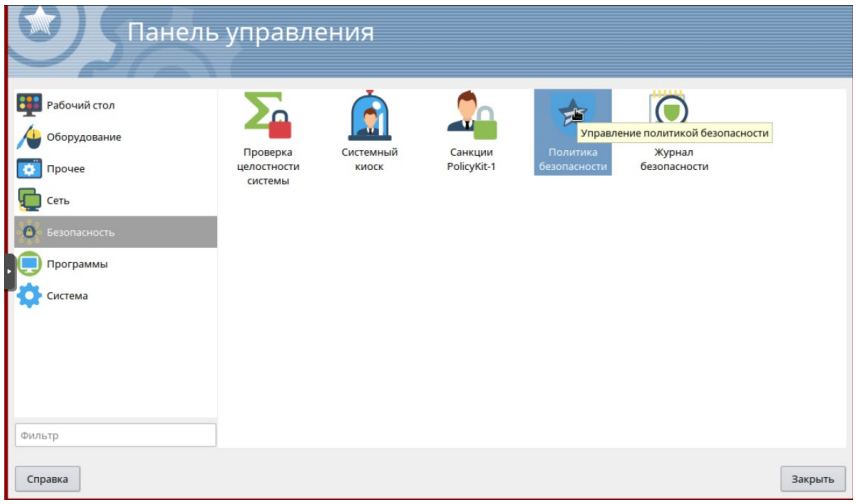


Рис. 193

После запуска программы «Политика безопасности» нужно перейти во вкладку «Замкнутая программная среда» и выбрать пункт «Включить» в окне контроля исполняемых файлов (рис. Рис. 194).

Включение ЗПС

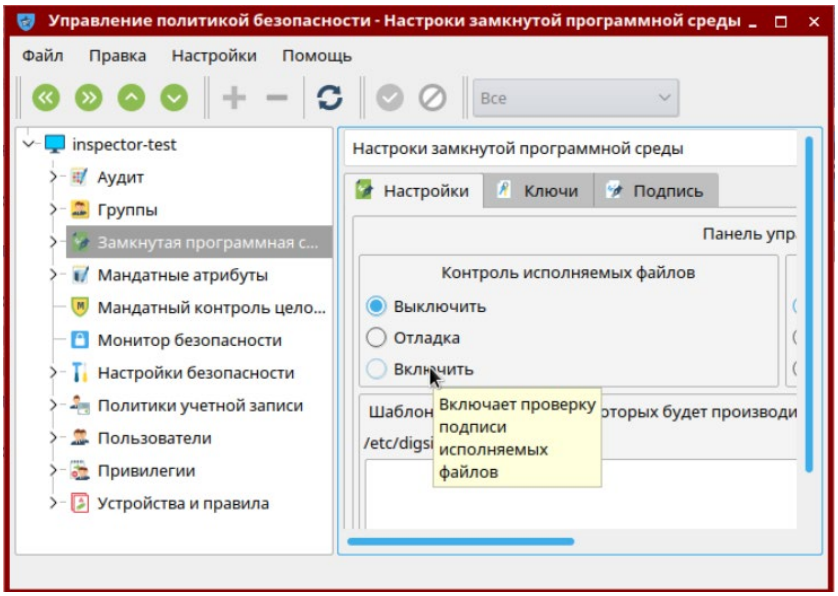


Рис. 194

Далее необходимо в меню выбрать пункт «Правка» и нажать «Применить» (рис. 195).

Применение настроек

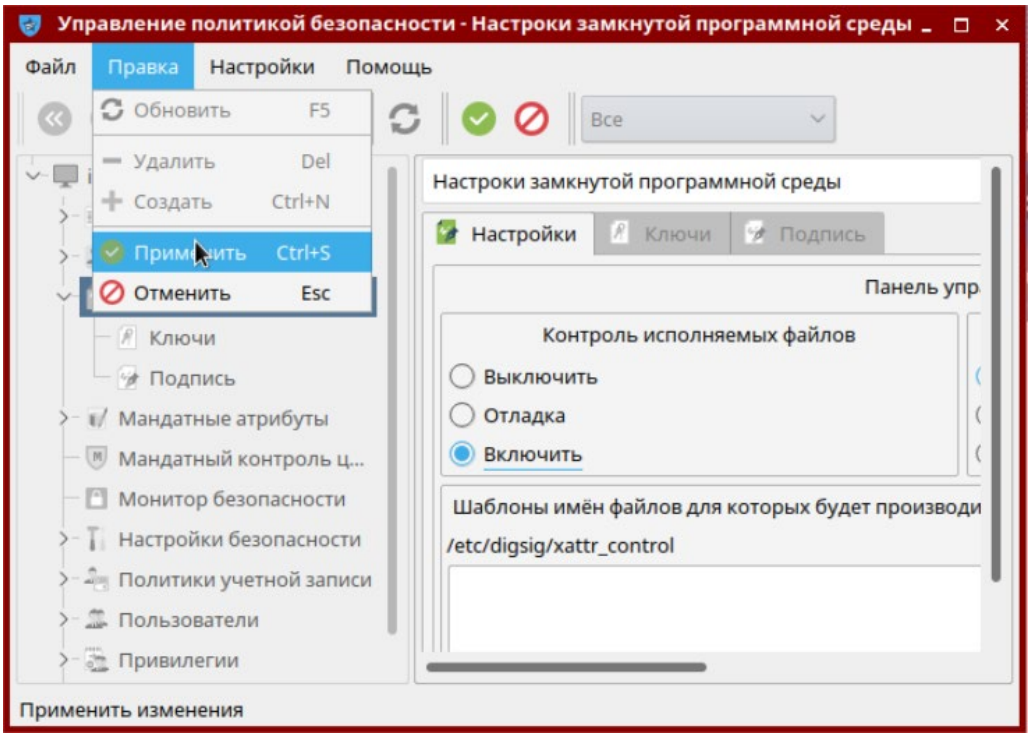


Рис. 195

После нажатия кнопки «Применить» появится сообщение с предупреждением о запуске ЗПС (рис. 196). Нужно нажать «Да» и дождаться перезагрузки, после чего ОС Astra Linux 1.6 будет работать в режиме ЗПС.

Сообщение с предупреждением о запуске ЗПС

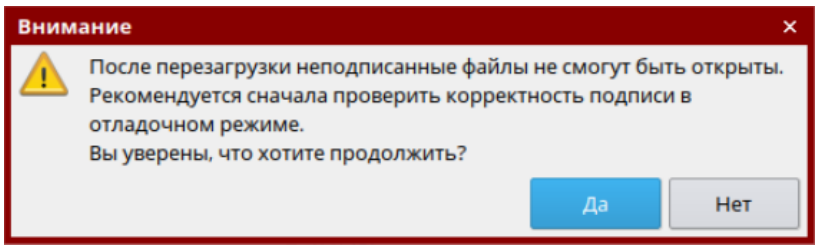


Рис. 196

6.3. Работа с инструментами

В рамках одного проекта для проведения тестирования можно выбрать один, несколько или все инструменты компонента «Инспектор». Работа инструментов может занимать довольно продолжительное время и зависит от параметров: объема накопителя, выбранного для поиска остаточной информации, количества файлов, выбранных для проведения контрольного суммирования, алгоритма контрольного суммирования и пр.

6.3.1. Проверка механизмов очистки

Для запуска инструмента проверки механизмов очистки необходимо установить соответствующую галочку, нажав на пиктограмму инструмента или на его название, и нажать кнопку «Вперед» (рис. 184). Откроется рабочее окно инструмента «Проверка механизмов очистки» (рис. 197).

Инструмент «Проверка механизмов очистки»

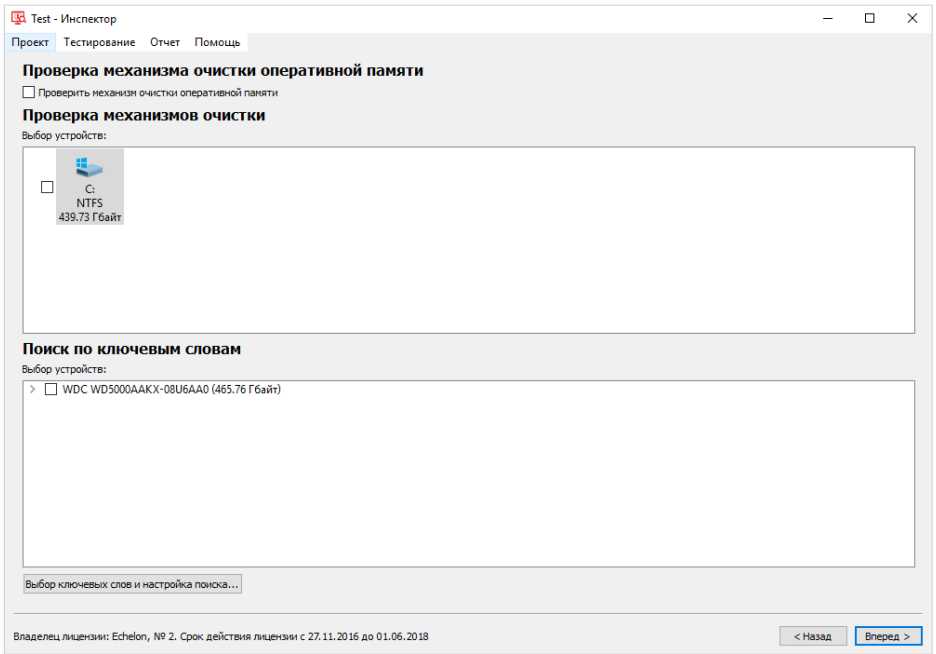


Рис. 197

Инструмент «Проверка механизмов очистки» (рис. 197) предназначен для проверки эффективности работы средств гарантированного уничтожения информации, осуществляющих оперативное удаление данных на рабочих станциях, и решает следующие задачи:

– проверка механизма очистки оперативной памяти;

– проверка механизмов очистки устройств;

– поиск по ключевым словам.

6.3.1.1. Проверка механизма очистки оперативной памяти

Для запуска нужно поставить галочку в квадратном поле рядом с «Проверить механизм очистки оперативной памяти» (рис. 198) и нажать кнопку «Вперед». Откроется новое окно с информацией о настройках проекта (рис. 199). Для начала проверки необходимо нажать кнопку «Вперед».

Примечание. Функция проверки механизма очистки оперативной памяти доступна для ядер: 4.2.0-23-generic, 4.2.0-23-pax, 3.16.0-16-generic, 3.16.0-16-pax.

Проверка механизма очистки оперативной памяти

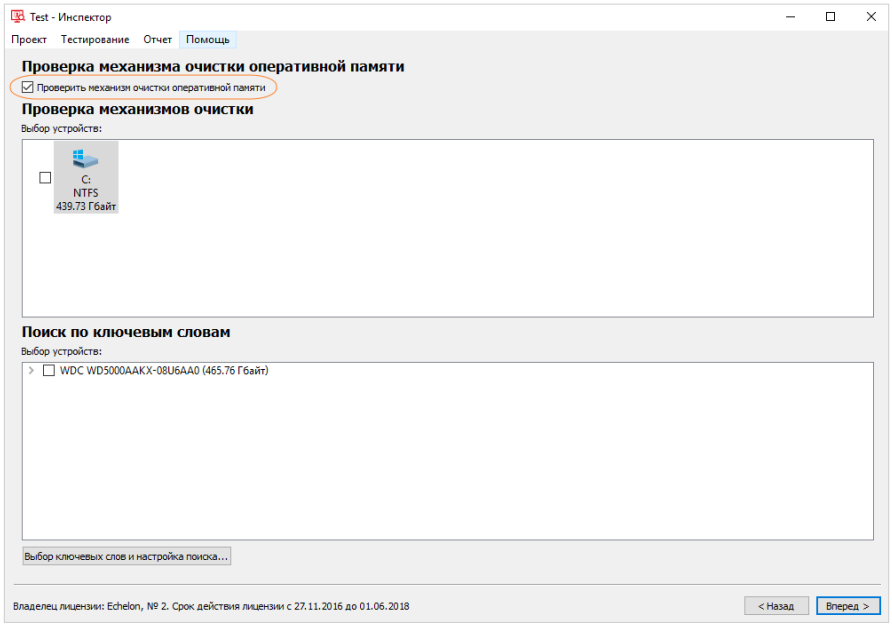


Рис. 198

Информация о проекте

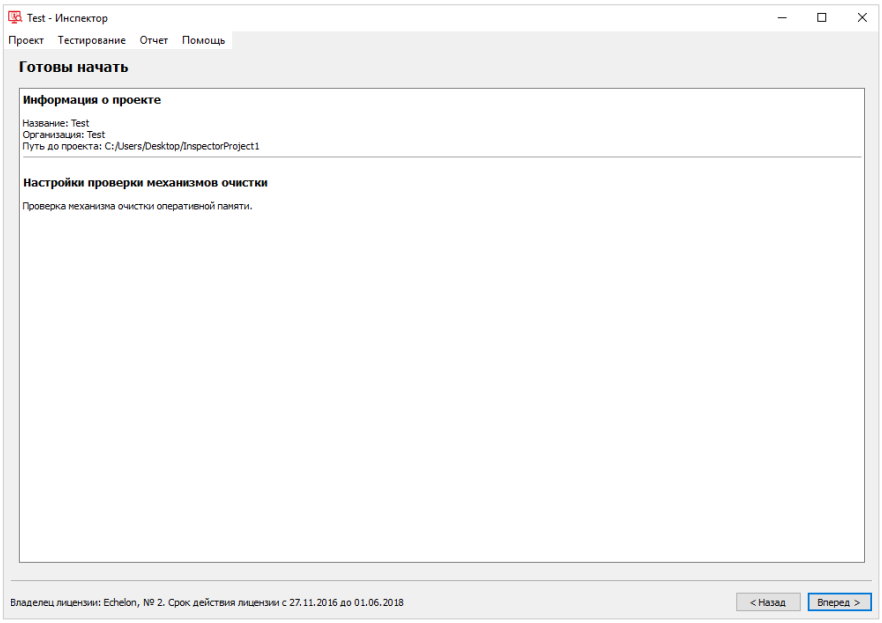


Рис. 199

В открывшемся окне (рис. 200) будет представлена информация о ходе выполнения проверки.

Ход выполнения проверки

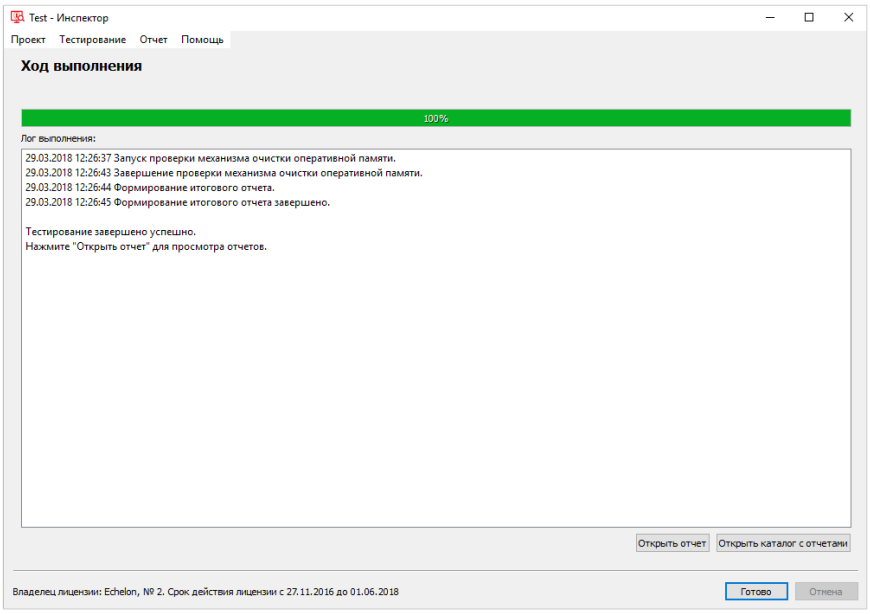


Рис. 200

После успешного завершения тестирования необходимо выбрать в подменю «Тестирование» пункт «Проверка механизма очистки памяти» (рис. 201).

Подменю «Тестирование»

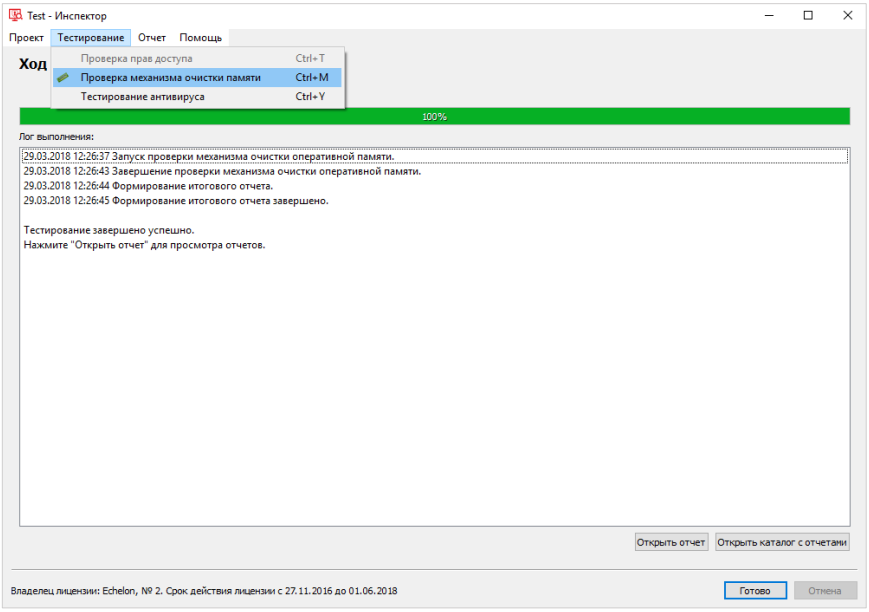


Рис. 201

В появившемся окне необходимо нажать кнопку «Начать проверку» (рис. 202).

Проверка механизма очистки оперативной памяти

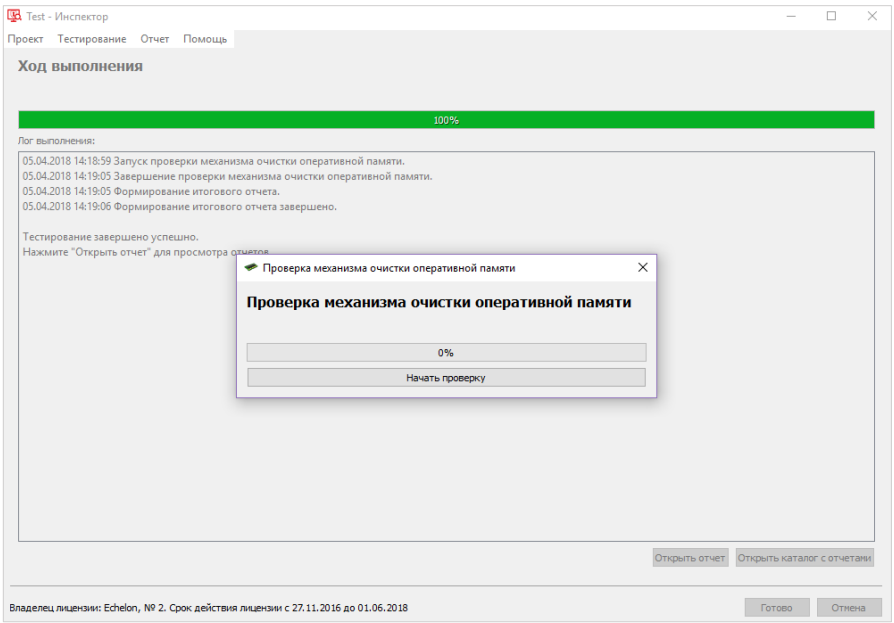


Рис. 202

По завершению проверки появится соответствующее сообщение (рис. 203). Далее нужно нажать кнопку «ОК».

Сообщение об окончании тестирования

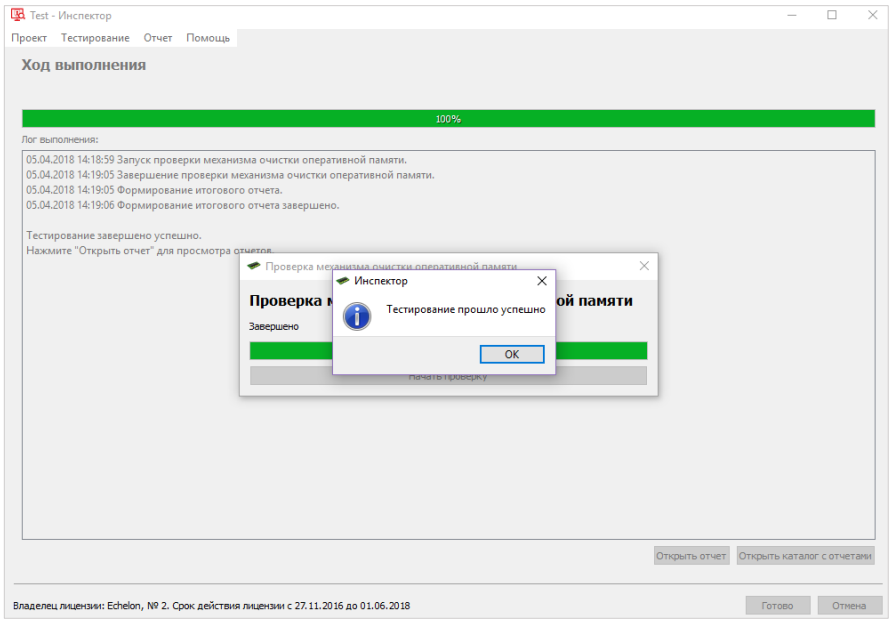


Рис. 203

Для просмотра отчета о проверке механизма очистки оперативной памяти нужно нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 6.3.5).

Для возврата к списку инструментов нужно нажать кнопку «Готово».

6.3.1.2. Проверка механизмов очистки устройств

Для запуска нужно отметить галочкой устройство в поле «Выбор устройств» рабочего окна инструмента и нажать кнопку «Вперед» (рис. 204).

Примечание. В среде функционирования под управлением ОС специального назначения «Astra Linux Special Edition» доступна функция проверки механизмов очистки для устройств с файловыми системами: ext2, ext3, ext4, vfat.

Проверка механизмов очистки устройств

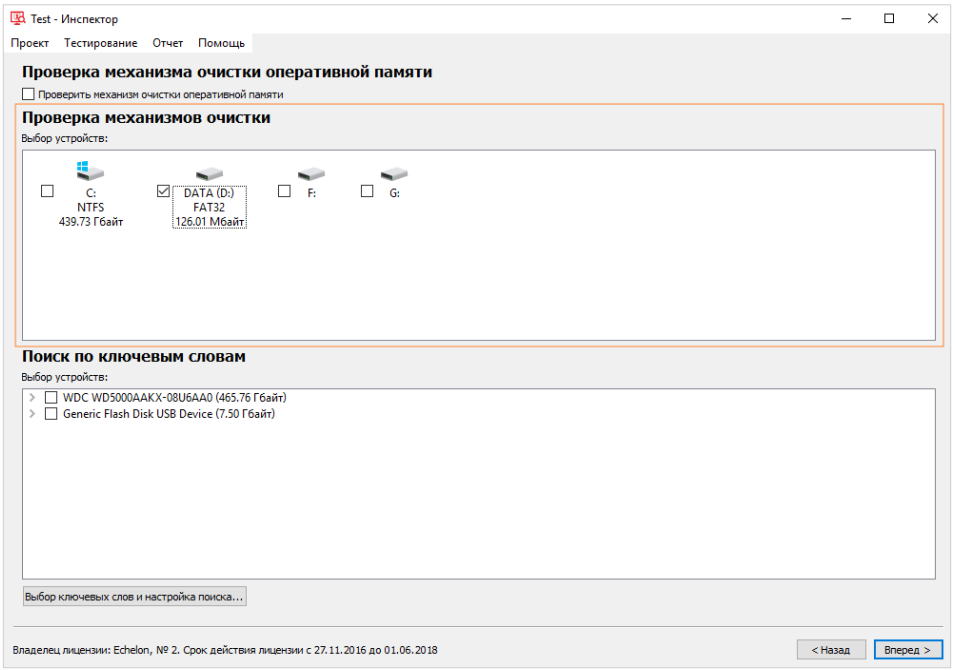


Рис. 204

Откроется новое окно с информацией о проекте и настройках проверки (рис. 205). В случае обнаружения ошибки в настройках проверки необходимо нажать кнопку «Назад» и скорректировать настройки. Если все данные верны, для начала проверки нужно нажать кнопку «Вперед».

Информация о проекте

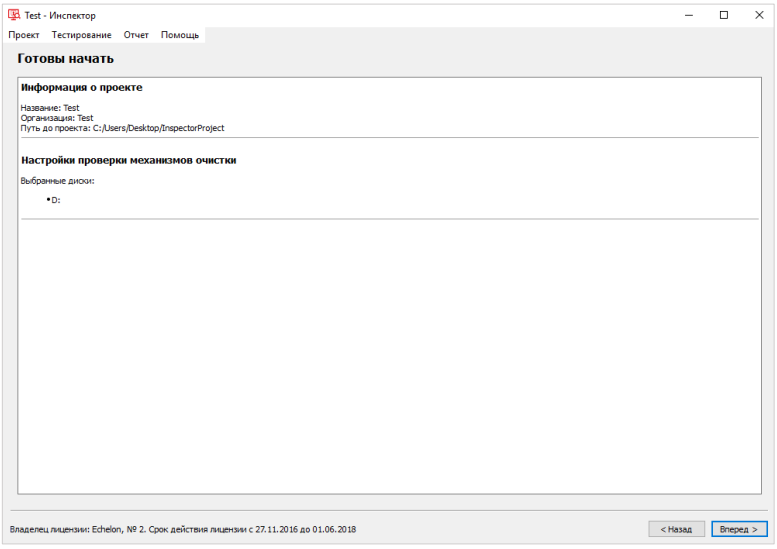


Рис. 205

В открывшемся окне (рис. 206) будет представлена информация о ходе выполнения проверки.

Ход выполнения проверки

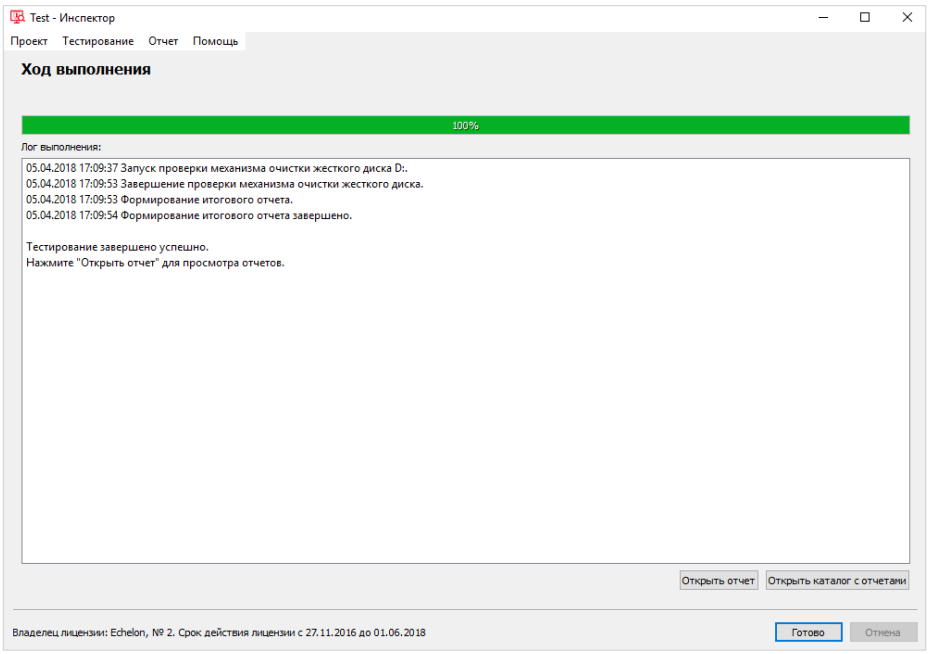


Рис. 206

После завершения проверки для просмотра отчета необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 6.3.5).

Для возврата к списку инструментов нужно нажать кнопку «Готово».

6.3.1.3. Поиск по ключевым словам

Для запуска нужно отметить галочкой устройство в прямоугольном поле и нажать кнопку «Выбор ключевых слов и настройка поиска» (рис. 207).

Поиск по ключевым словам

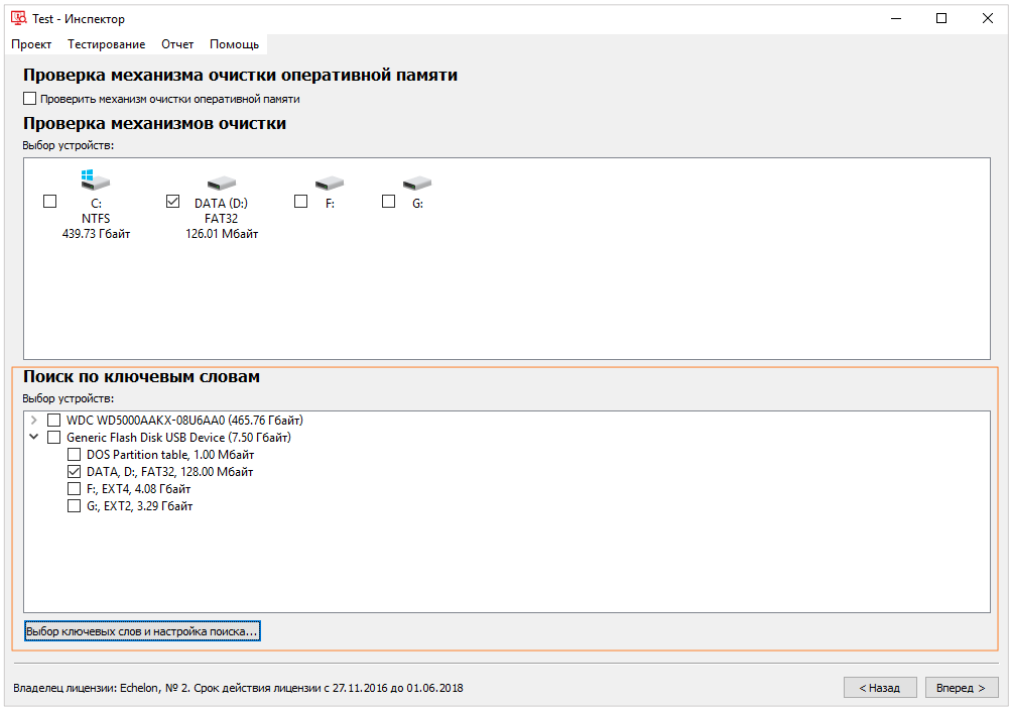


Рис. 207

В открывшемся окне «Выбор ключевых слов и настройка поиска» необходимо указать ключевые слова для поиска остаточной информации (рис. 208).

Указать слова для поиска можно двумя способами:

– вручную. В поле «Фраза» нужно ввести слова или словосочетания и нажать кнопку «Добавить»;

– импортировать. Для импорта необходимо загрузить заранее подготовленный список ключевых слов в формате TXT и кодировке UTF-8 с помощью кнопки «Импортировать из словаря».

Дополнительно можно указать:

– кодировку и типы документов;

– учет регистра при проверке;

– определение пути до файлов, содержащих ключевые слова;

– ограничение области поиска. Значения ограничения выбранного раздела округляются до чисел кратных 4096. При этом начальное значение округляется в меньшую сторону, а конечное значение в большую.

В отчете будет отражена позиция начала документа (файла) относительно раздела диска, в котором найдено ключевое слово.

Действуют следующие ограничения:

– документ должен располагаться непрерывно;

– размер документа не должен превышать 10 Мбайт;

– документ должен конвертироваться в текстовый формат (время на конвертацию ограничено тайм-аутом);

– максимальная длина слова для поиска – 100 символов;

– максимальное количество слов для поиска – 100 слов;

– одно ключевое слово может быть найдено не более 1000 раз.

После ввода слова для поиска необходимо нажать «ОК», а затем «Вперед».

Выбор ключевых слов и настройка поиска

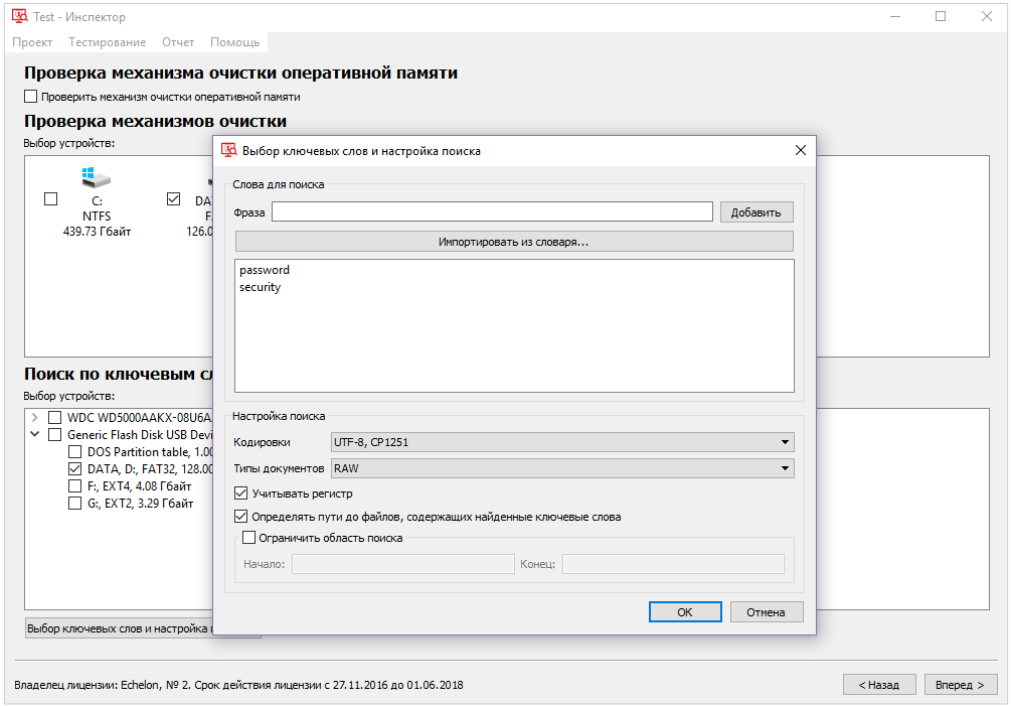


Рис. 208

Откроется новое окно с информацией о проекте и настройках проверки (рис. 209). В случае обнаружения ошибки в настройках проверки необходимо нажать кнопку «Назад» и скорректировать настройки. Для начала проверки нужно нажать кнопку «Вперед».

Параметры тестирования

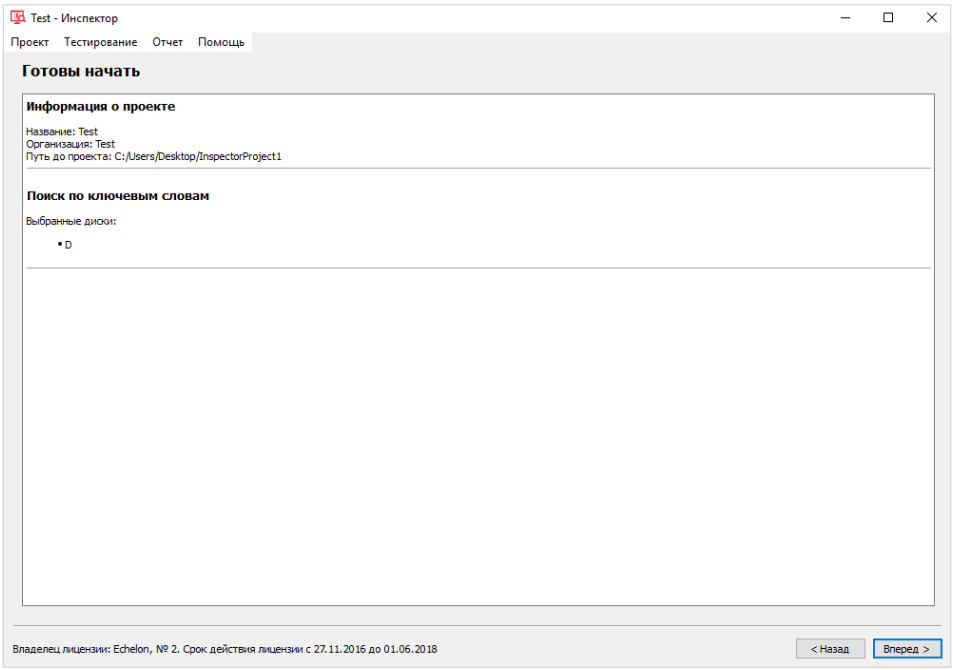


Рис. 209

В открывшемся окне (рис. 210) будет представлена информация о ходе выполнения проверки.

Ход выполнения проверки

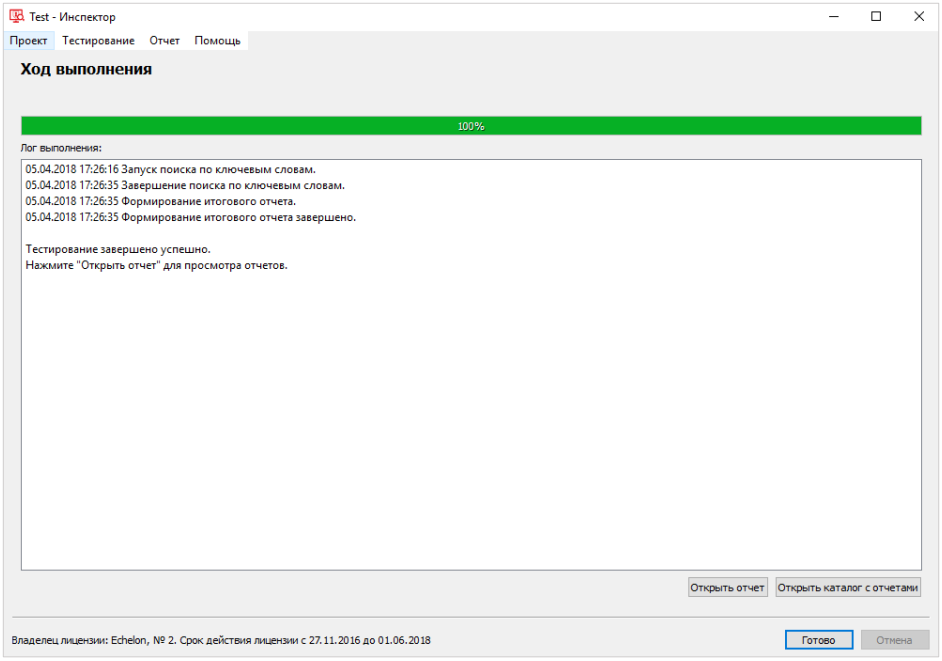


Рис. 210

После завершения проверки для просмотра отчета нужно нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 6.3.5).

Для возврата к списку инструментов нужно нажать кнопку «Готово».

6.3.2. Контрольное суммирование

Инструмент контрольного суммирования предназначен для контроля целостности выбранных файлов и каталогов по заданным алгоритмам.

Для запуска инструмента «Контрольное суммирование» необходимо установить соответствующую галочку, нажав на пиктограмму инструмента или на его название, и нажать кнопку «Вперед». Рабочее окно инструмента «Контрольное суммирование» представлено на рисунке (рис. 211).

Рабочее окно инструмента «Контрольное суммирование»

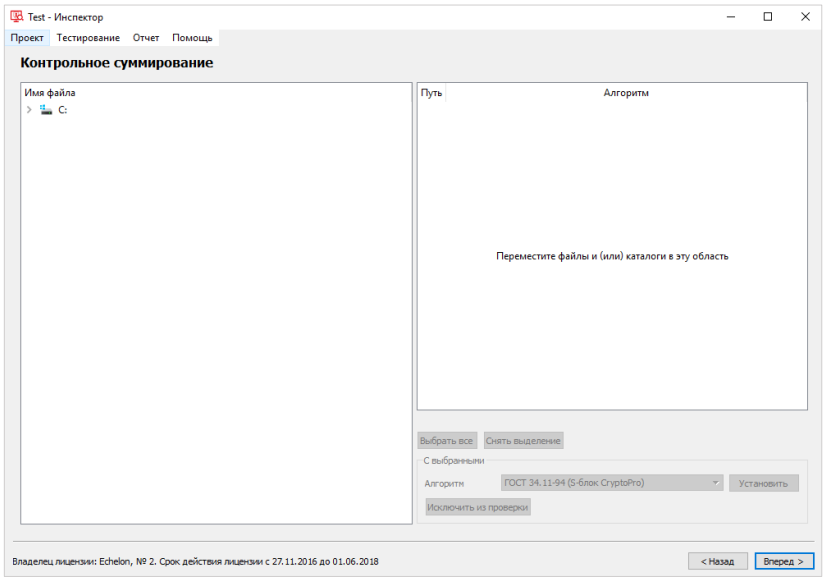


Рис. 211

Рабочее окно инструмента контрольного суммирования разделено на две области. Слева – дерево каталогов для выбора объектов для контрольного суммирования, а справа – настройки для каждого выбранного объекта (путь, алгоритм).

Чтобы начать процесс контрольного суммирования необходимо двойным нажатием левой кнопки мыши добавить интересующие объекты в область настроек (рис. 212).

Выбор объектов и алгоритмов для контрольного суммирования

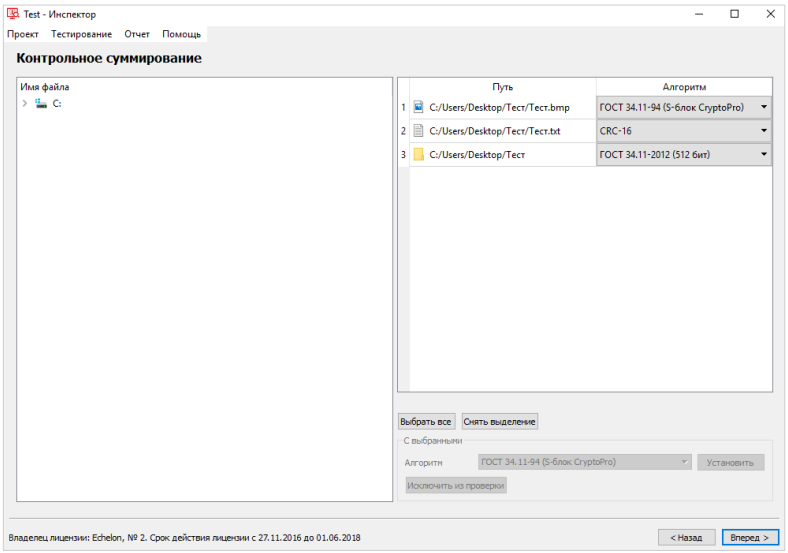


Рис. 212

Для удаления объектов из области настроек необходимо выбрать объект нажатием левой кнопки и нажать «Исключить из проверки» или нажать на клавиатуре клавишу «Delete».

После того как объекты добавлены, можно скорректировать настройки контрольного суммирования (рис. 212), выбрав из выпадающего списка поддерживаемых алгоритмов необходимый алгоритм.

Алгоритм контрольного суммирования можно настроить для каждого файла отдельно или задать один алгоритм для всех файлов с помощью меню в нижнем правом углу. Для выбора одного алгоритма для всех объектов суммирования необходимо нажать кнопку «Выбрать все». Далее, из выпадающего списка алгоритмов нужно выбрать нужный и нажать кнопку «Установить».

После установки всех настроек нужно нажать кнопку «Вперед».

Примечание. Если нажать кнопку «Вперед», не выбрав объект для контрольного суммирования, появится соответствующая всплывающая подсказка.

Откроется новое окно с информацией о настройках проекта (рис. 213). В случае обнаружения ошибки в настройках контрольного суммирования необходимо нажать кнопку «Назад» и скорректировать настройки. Для начала суммирования нужно нажать кнопку «Вперед».

Информация о проекте

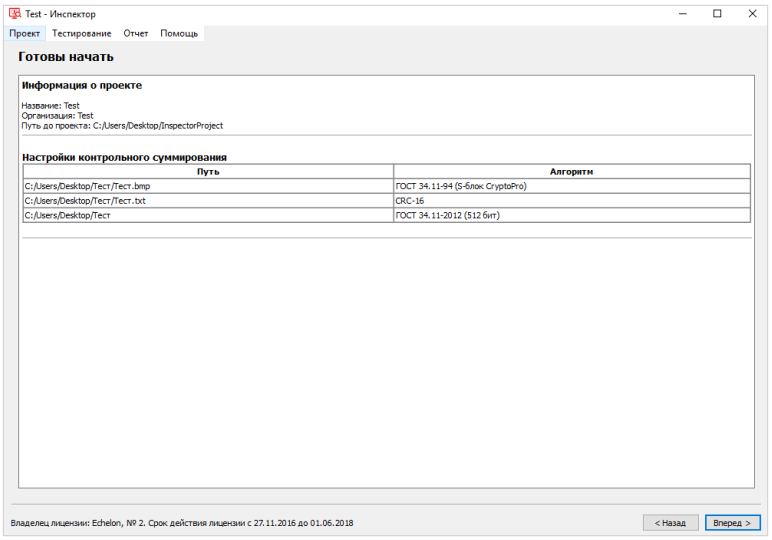


Рис. 213

В открывшемся окне (рис. 214) будет представлена информация о ходе выполнения проверки.

Ход выполнения контрольного суммирования

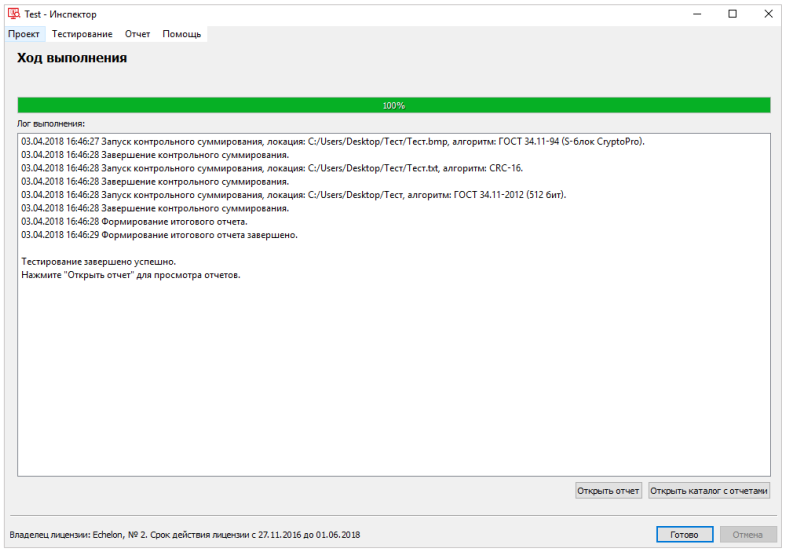


Рис. 214

После завершения проверки для просмотра отчета нужно нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 6.3.5).

Для возврата к списку инструментов нужно нажать кнопку «Готово».

6.3.3. Системный аудит

Для запуска инструмента «Системный аудит» необходимо установить соответствующую галочку, нажав на пиктограмму или название инструмента, и нажать кнопку «Вперед» (рис. 184). В открывшемся окне будет показана информация о проекте (рис. 215). Для начала проверки устройств и программного обеспечения нужно нажать кнопку «Вперед».

Информация о проекте

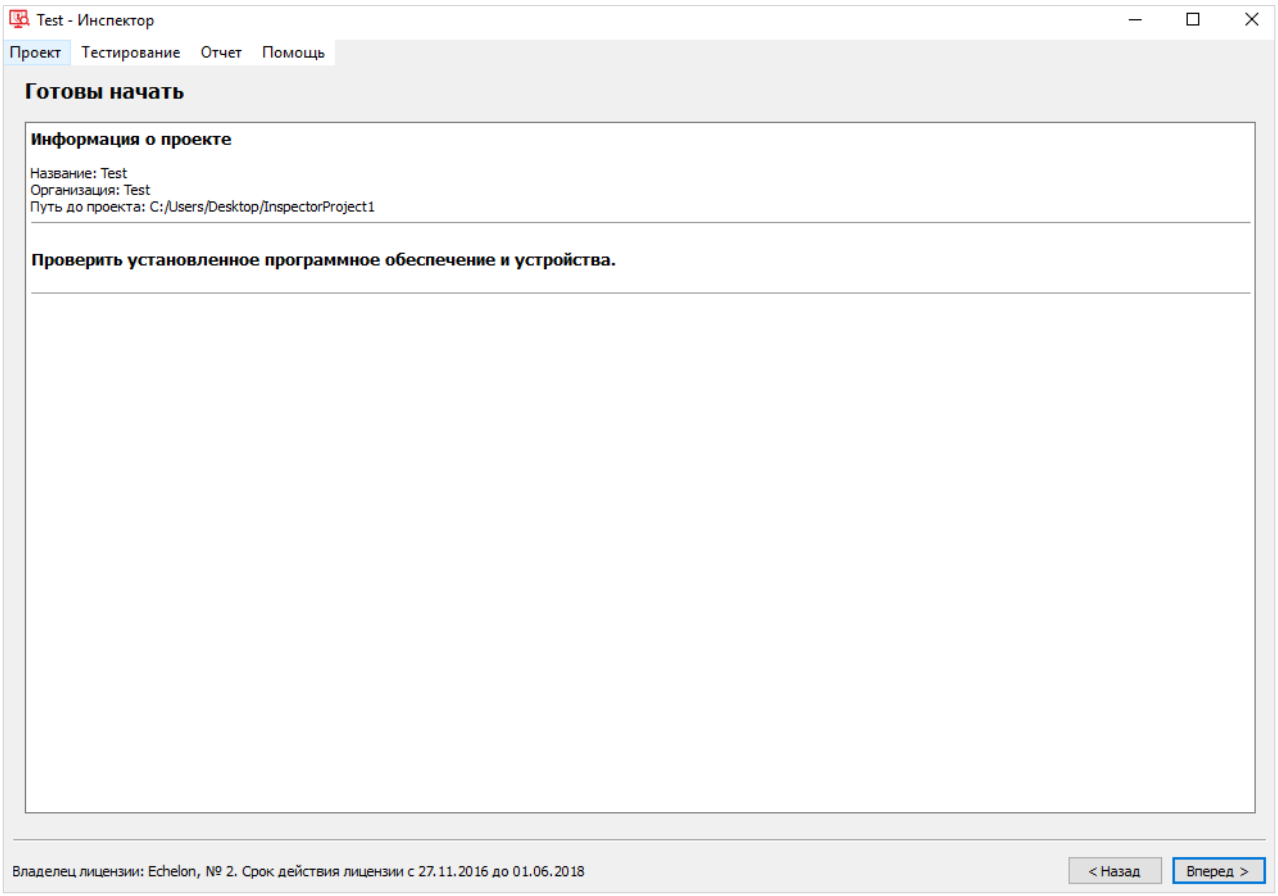


Рис. 215

В открывшемся окне будет представлена информация о ходе выполнения проверки (рис. 216).

Ход выполнения аудита

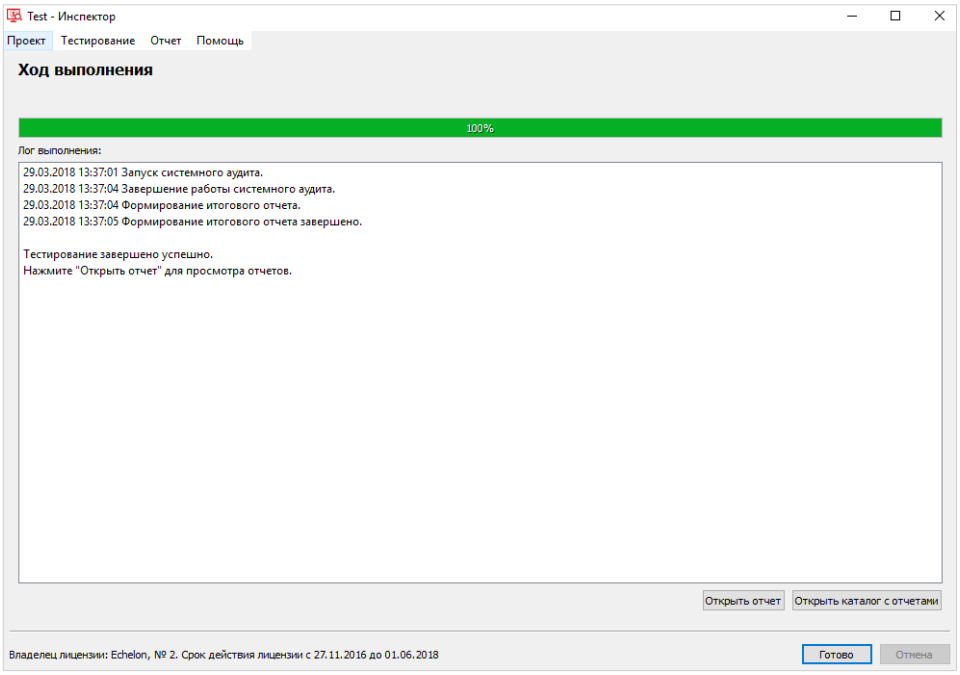


Рис. 216

После завершения проверки для просмотра отчета нужно нажать кнопку «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 6.3.5).

Для возврата к списку инструментов нужно нажать кнопку «Готово».

6.3.3.1. Тестирование антивируса

Для тестирования антивируса необходимо запустить инструмент «Тестирование антивируса» из подменю «Тестирование» (рис. 186).

Примечание. Функция тестирования антивируса не доступа в среде функционирования под управлением ОС специального назначения «Astra Linux Special Edition».

После запуска инструмента высветится сообщение о создании тестового файла (рис. 217). Необходимо нажать «ОК», чтобы открыть директорию с созданным тестовым файлом (рис. 217).

Тестирование антивируса

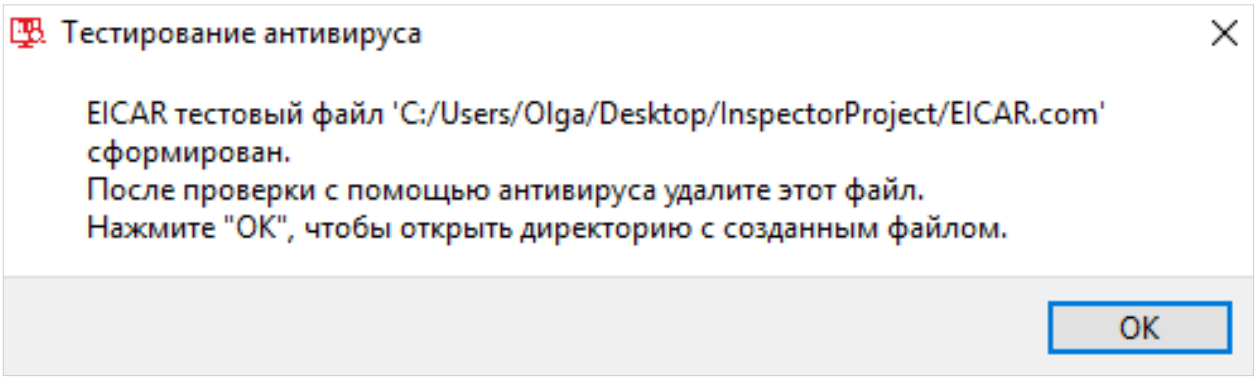


Рис. 217

После завершения проверки необходимо удалить тестовый файл, используя антивирусное ПО.

6.3.4. Проверка прав доступа

Для запуска инструмента «Проверка прав доступа» необходимо установить соответствующую галочку нажатием на пиктограмму или название инструмента, и нажать «Вперед» (рис. 184). Откроется рабочее окно инструмента «Проверка прав доступа» компонента «Инспектор» (рис. 218).

Рабочее окно инструмента разделено на четыре области. В верхней части рабочего окна расположены слева направо области: дерево каталогов, перечень проверяемых файлов и (или) каталогов, список пользователей. В нижней части рабочего окна расположена область модели доступа. По умолчанию на основании ресурсов и настроек проверяемой рабочей станции заполнены области: дерево каталогов и список пользователей.

Рабочее окно

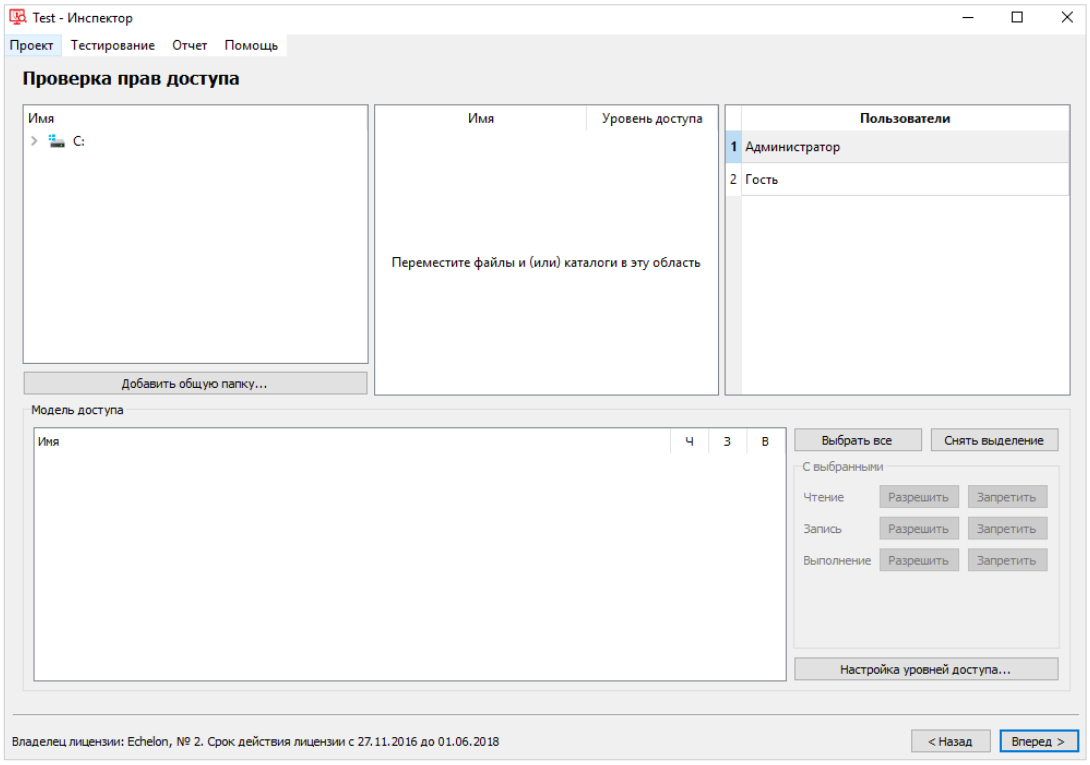


Рис. 218

По умолчанию реализованы 3 уровня доступа (сессии): 0 - Несекретная, 1 - Секретная, 2 - Совершенно секретная. Для изменения (удаления и / или добавления новых) уровней (сессий) необходимо нажать кнопку «Настройка уровней доступа». В открывшемся окне нужно переименовать сессии по умолчанию и / или удалить выделенные с помощью кнопки «Удалить выбранные», и / или добавить новые с помощью кнопки «Добавить». Максимально можно создать двадцать уровней (сессий).

Примечание. Изменить уровни доступа необходимо до выбора проверяемых объектов.

Для добавления каталога в перечень проверяемых необходимо найти его в дереве каталогов и переместить в соответствующее поле (уровень доступа секретности по умолчанию – 0: Несекретная), одновременно с этим в таблице прав доступа появятся текущие права для текущего пользователя (чтение (Ч), запись (З), выполнение (В)) (рис. 219).

Список каталогов в перечне проверяемых объектов

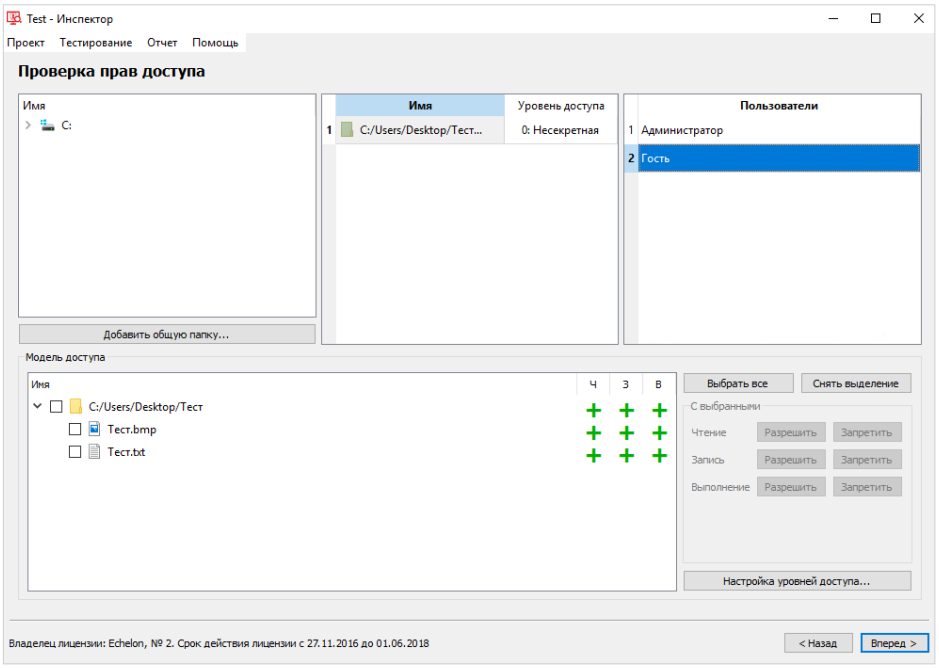


Рис. 219

Также добавить объекты можно с помощью двойного клика левой кнопкой мыши. Для удаления каталога из перечня проверяемых необходимо выделить его и нажать на клавиатуре клавишу «Delete».

В перечне проверяемых каталогов можно установить уровень доступа, для которого строится модель. Смена сессии происходит нажатием левой кнопкой мыши на ячейку столбца «Уровень доступа». Одновременно можно построить несколько моделей доступа (для различных файлов и пользователей в различных сессиях).

Примечание. Если нажать «Вперед», не добавив объект для тестирования прав, появится соответствующая всплывающая подсказка.

Если для какого-либо пользователя проверка прав не нужна, его можно удалить из списка, выделив его и нажав на клавишу «Delete». Для восстановления списка пользователей по умолчанию нужно нажать правой кнопкой мыши в области списка пользователей, вызвав контекстное меню, и выбрать «Загрузить пользователей из ОС» (рис. 220).

Чтобы добавить пользователя из домена, необходимо нажать правой кнопкой мыши в области списка пользователей, вызвав контекстное меню, и выбрать пункт «Добавить» (рис. 220). В открывшемся окне (рис. 221) укажите имя пользователя и домен, нажмите кнопку «ОК». Чтобы добавить локального пользователя в окне «Добавление пользователя» необходимо указать его имя и нажать кнопку «ОК» (рис. 221).

Обновление списка пользователей

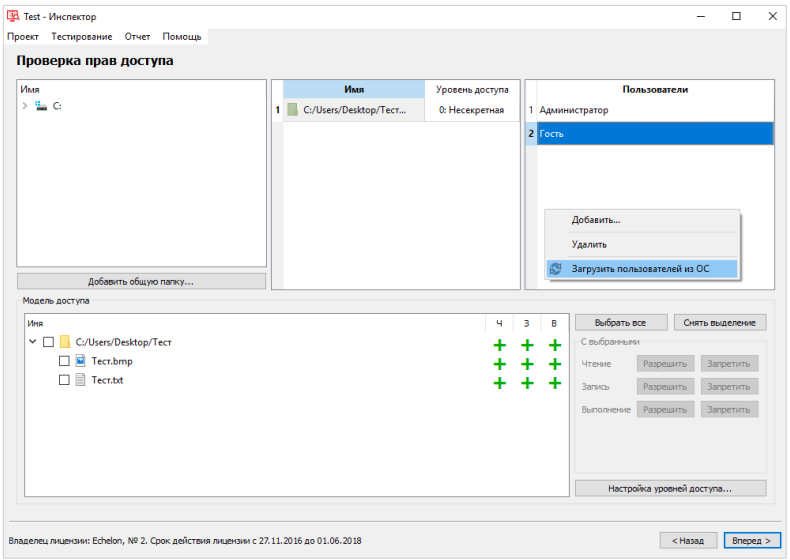


Рис. 220

Добавление пользователя

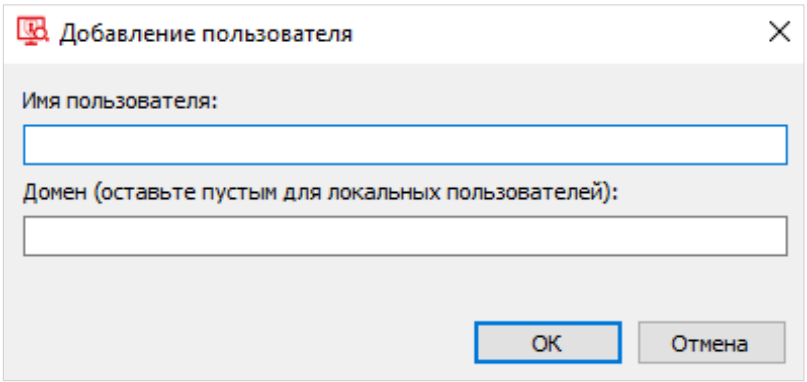


Рис. 221

6.3.4.1. Построение модели прав доступа

Построение модели прав доступа происходит путем редактирования в перечне проверяемых объектов прав доступа пользователей к файлам и каталогам рабочей станции. Это осуществляется путем нажатия кнопок «Разрешить» и «Запретить» напротив соответствующего права доступа, выделенного галочкой объекта. Также изменять права доступа пользователя можно в области «Модель доступа», нажимая на «+» и «-».

В нижнем правом углу окна расположена панель для редактирования прав доступа всех выбранных объектов. Чтобы отметить все файлы всех каталогов нужно нажать «Выбрать все», чтобы отменить выбор всех файлов нужно нажать «Снять выделение». Далее с помощью кнопок «Разрешить / Запретить» необходимо установить права доступа для всех отмеченных файлов.

6.3.4.2. Тестирование прав доступа

Для тестирования прав доступа после построения модели прав доступа необходимо нажать кнопку «Вперед» (рис. 220).

Откроется новое окно с информацией о настройках проекта (рис. 222). В случае обнаружения ошибки в настройках тестирования необходимо нажать кнопку «Назад» и скорректировать настройки. Если все данные верны, для начала тестирования нужно нажать кнопку «Вперед».

Информация о проекте

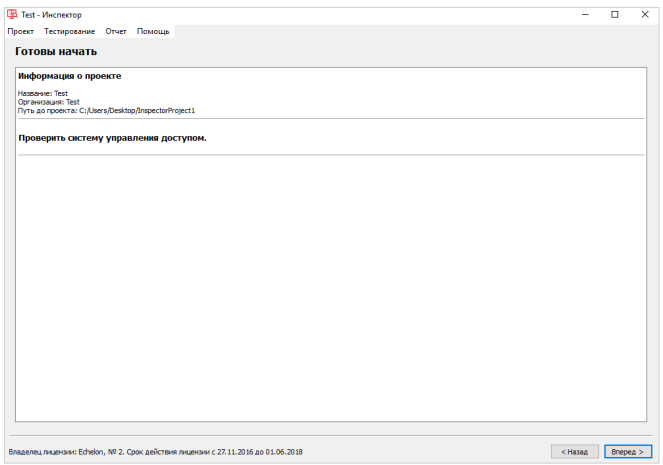


Рис. 222

В открывшемся окне будет представлена информация о ходе выполнения проверки (рис. 223).

Ход выполнения проверки

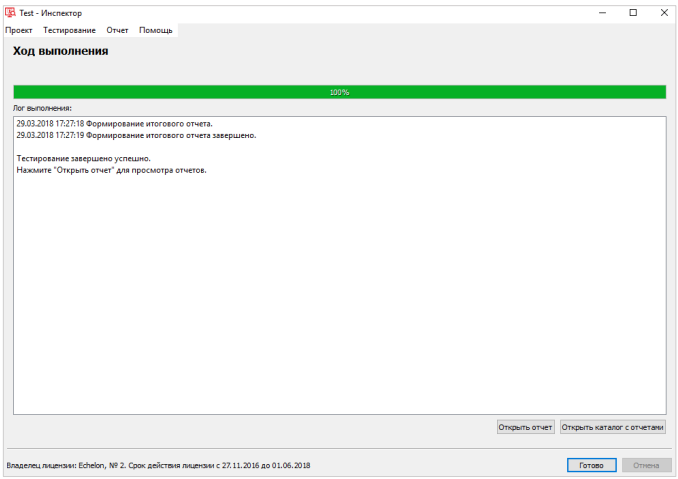


Рис. 223

После завершения тестирования необходимо запустить инструмент «Проверка прав доступа» для проверки прав доступа пользователей в различных сессиях к выбранным каталогам и файлам.

Для запуска инструмент необходимо выбрать в меню «Тестирование» инструмент «Проверка прав доступа» (рис. 224).

Подменю «Тестирование»

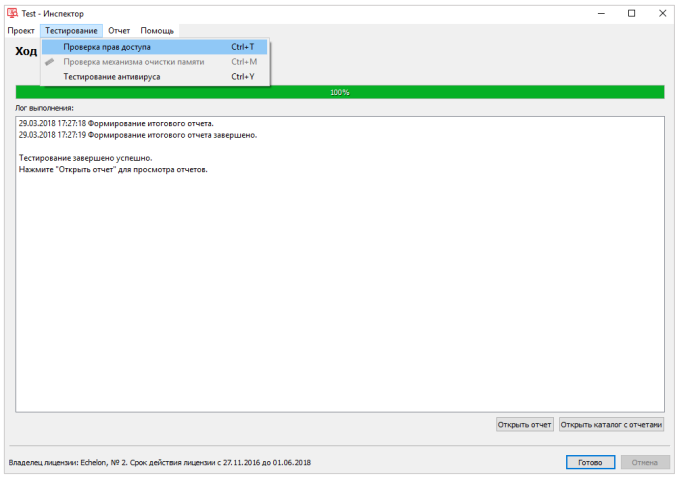


Рис. 224

В открывшемся окне необходимо указать текущий уровень сессии (рис. 225).

Выбор уровня сессии и пользователя для проведения проверки

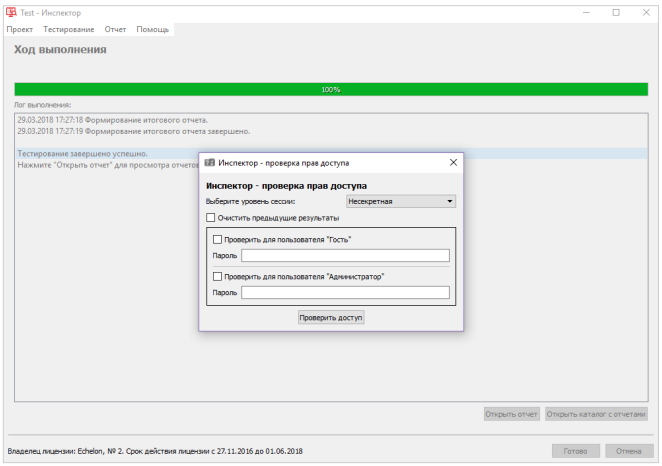


Рис. 225

В режиме «Несекретно» возможно провести проверку для всех пользователей. Для этого нужно поставить галочку в квадратное поле рядом с именем одного или нескольких пользователей, ввести пароль и нажать кнопку «Проверить доступ» (рис. 226).

Выбор пользователей для проверки прав доступа в несекретной сессии

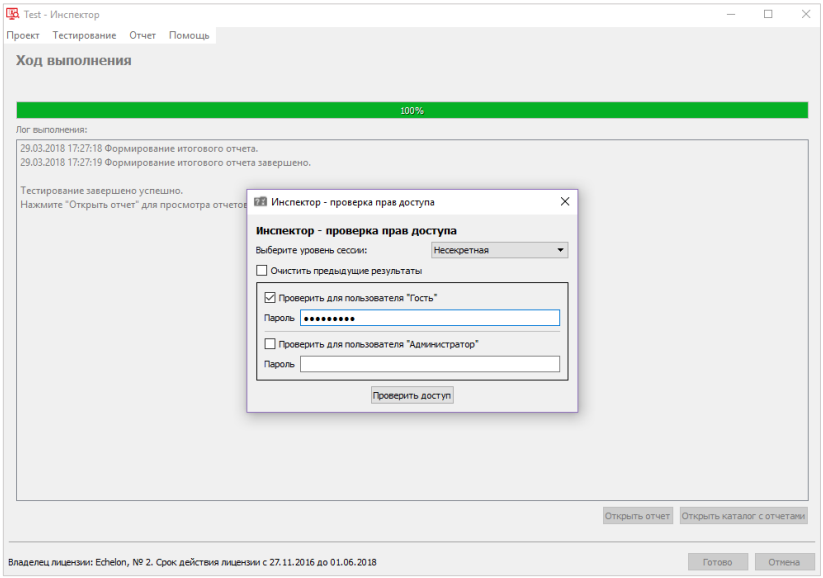


Рис. 226

После проведения тестирования появится соответствующее сообщение (рис. 227).

Сообщение

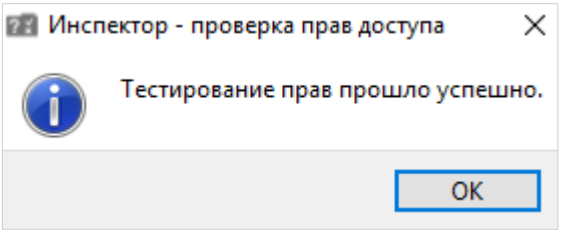


Рис. 227

После завершения проверки для просмотра отчета необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 6.3.5).

Для возврата к списку инструментов необходимо нажать кнопку «Готово».

6.3.4.3. Тестирование прав доступа к общим папкам

Для запуска инструмента «Проверка прав доступа» необходимо установить соответствующую галочку нажатием на пиктограмму или название инструмента и нажать «Вперед» (рис. 184). Откроется рабочее окно инструмента «Проверка прав доступа» компонента «Инспектор» (рис. 218).

Примечание. Функция тестирования прав доступа к общей папке недоступна, если установлено СЗИ Secret Net, а также в среде функционирования под управлением ОС специального назначения «Astra Linux Special Edition».

Для добавления сетевой папки в перечень проверяемых необходимо нажать кнопку «Добавить общую папку» (рис. 228).

Рабочее окно

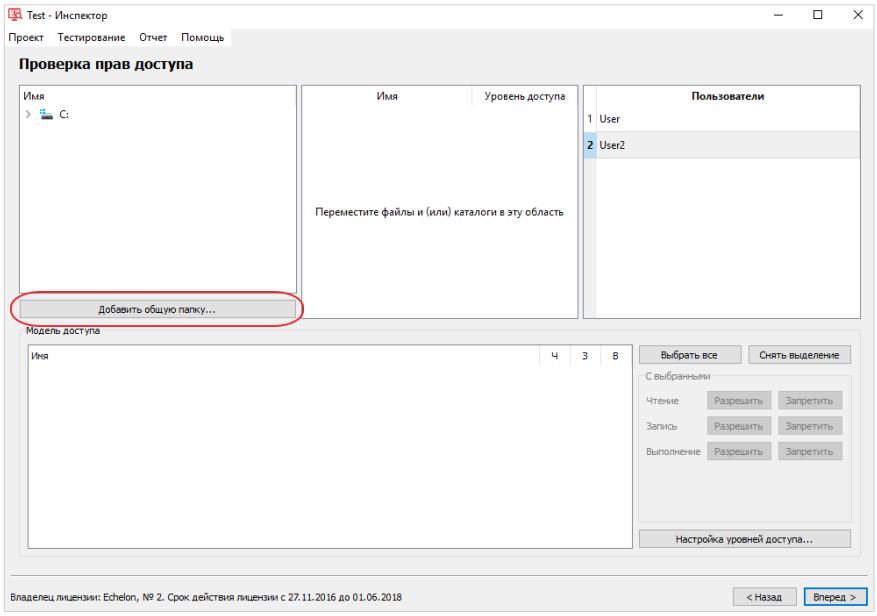


Рис. 228

В открывшемся окне (рис. 229) нужно указать путь и нажать кнопку «OK».

Добавление общей папки

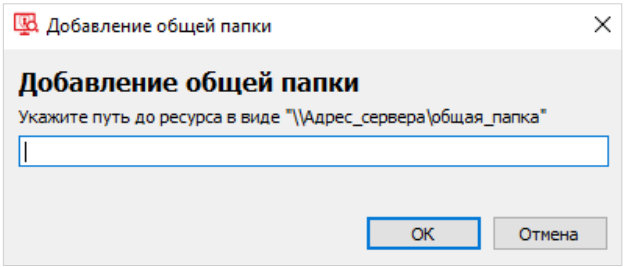


Рис. 229

Если появится окно авторизации, то необходимо ввести логин и пароль пользователя (рис. 230).

Ввод сетевых учетных данных

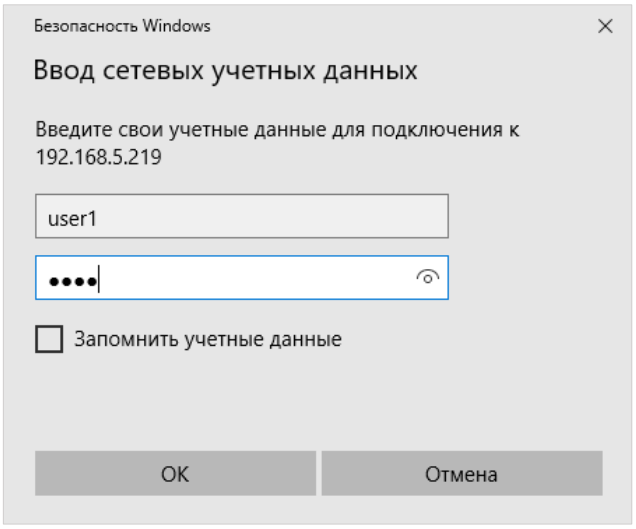


Рис. 230

Для запуска тестирования нужно нажать кнопку «Вперед». (рис. 231).

Проверка прав доступа

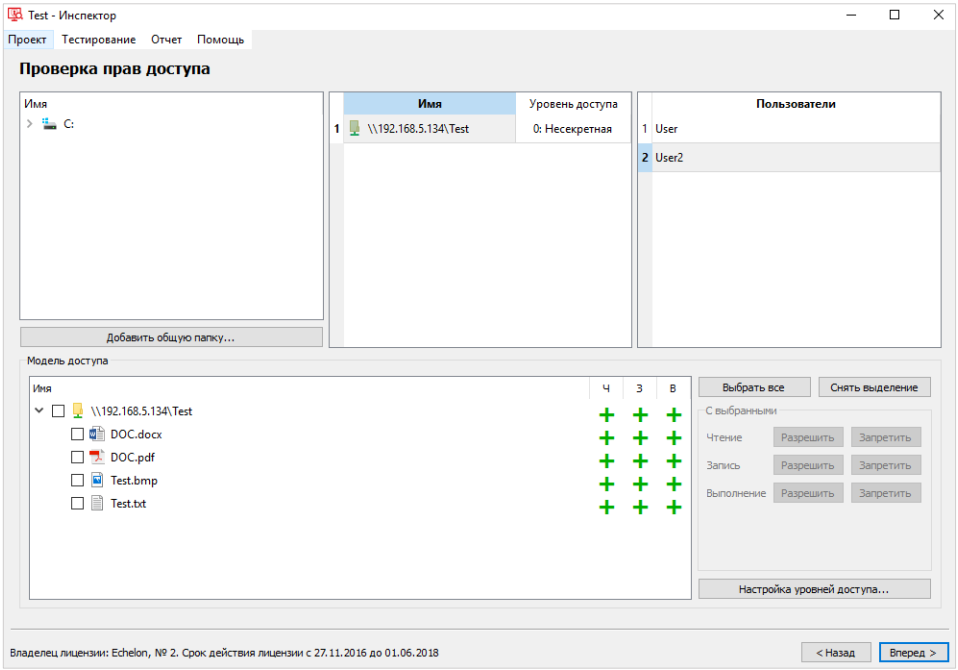


Рис. 231

В открывшемся окне будет представлена информация о проекте. Для начала тестирования необходимо нажать кнопку «Вперед» (рис. 232).

Информация о проекте

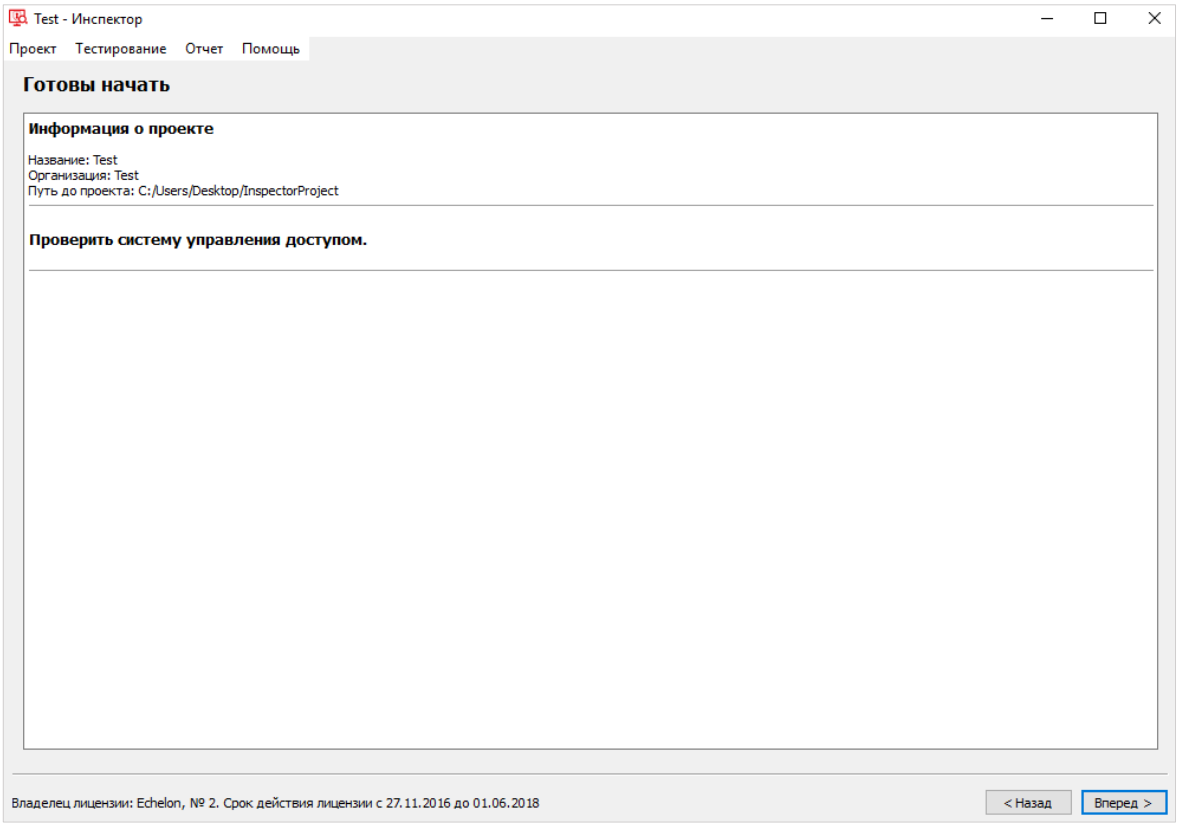


Рис. 232

После завершения тестирования необходимо запустить инструмент «Проверка прав доступа» для проверки прав доступа пользователей в различных сессиях к выбранным каталогам и файлам.

Для запуска инструмент необходимо выбрать в подменю «Тестирование» параметр «Проверка прав доступа» (рис. 233).

Запуск инструмента

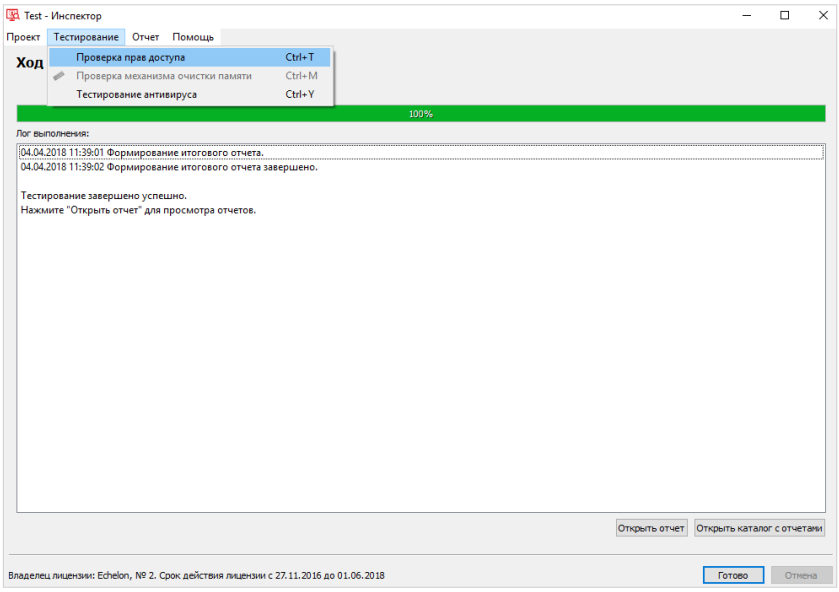


Рис. 233

В открывшемся окне нужно указать уровень сессии, пользователей, для которых необходимо провести проверку и нажать кнопку «Проверить доступ» (рис. 234).

Настройка тестирования прав доступа

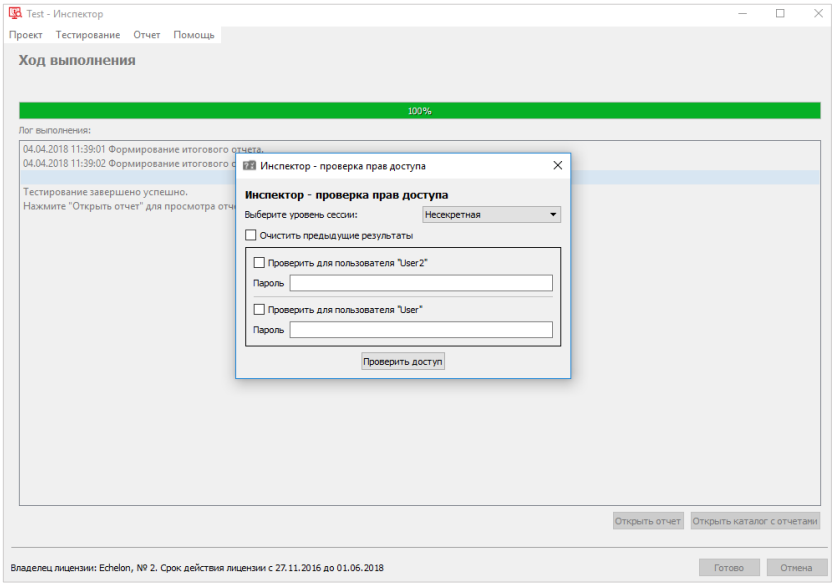


Рис. 234

Ели проверка прав сетевой папки осуществляется для доменных пользователей, причем компьютер с данной сетевой папкой также находится в этом домене, то после ввода пароля и нажатия кнопки «Проверить доступ» проверка пройдет автоматически, дополнительно вводить логин и пароль не требуется.

Ели проверка прав к сетевой папке осуществляется для пользователей, которые находятся не в одном домене или вообще не находятся в каком-либо домене, то после ввода пароля для любого из локальных пользователей и нажатия кнопки «Проверить доступ» высветятся окна консоли и авторизации. В окне авторизации необходимо ввести логин и пароль пользователя удаленного узла, (где расположена данная сетевая папка) для которого проверяется доступ к данной сетевой папке и нажать «ОК».

После успешной проверки прав доступа появится соответствующее сообщение (рис. 227).

После завершения проверки для просмотра отчета необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (рис. 233) (подробнее см. пп. 6.3.5).

6.3.4.4. Тестирование прав доступа с установленным СЗИ Dallas Lock

Для запуска инструмента «Проверка прав доступа» необходимо установить соответствующую галочку нажатием на пиктограмму или название инструмента и нажать «Вперед» (рис. 184). Откроется рабочее окно инструмента «Проверка прав доступа» компонента «Инспектор» (рис. 218).

Примечание. Функция тестирования прав доступа с установленным СЗИ Dallas Lock недоступна в среде функционирования под управлением ОС специального назначения «Astra Linux Special Edition».

Далее необходимо выполнить настройку для проверки прав доступа и нажать кнопку «Вперед» (рис. 235).

Запуск проверки прав доступа

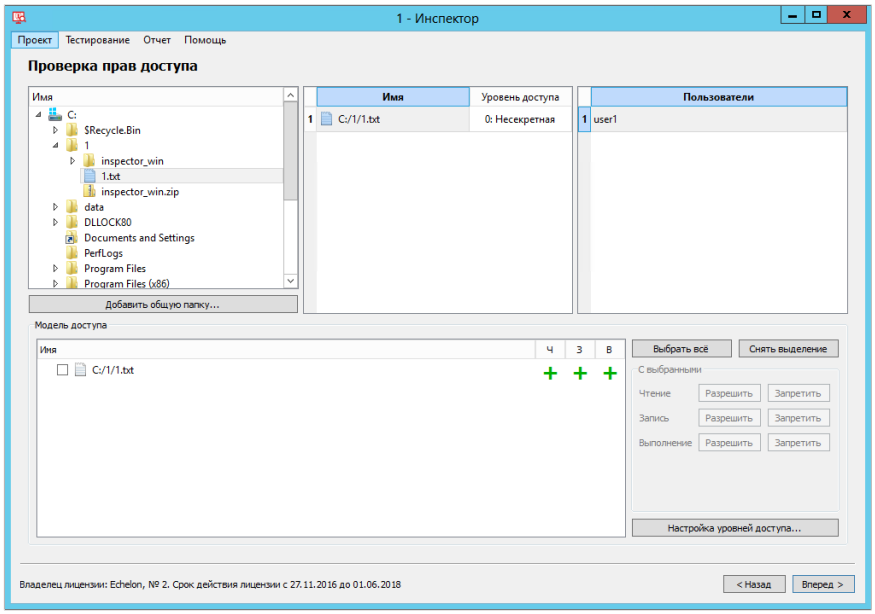


Рис. 235

В окне с информацией о тестировании нужно нажать кнопку «Вперед» (рис. 236).

Информация о проекте

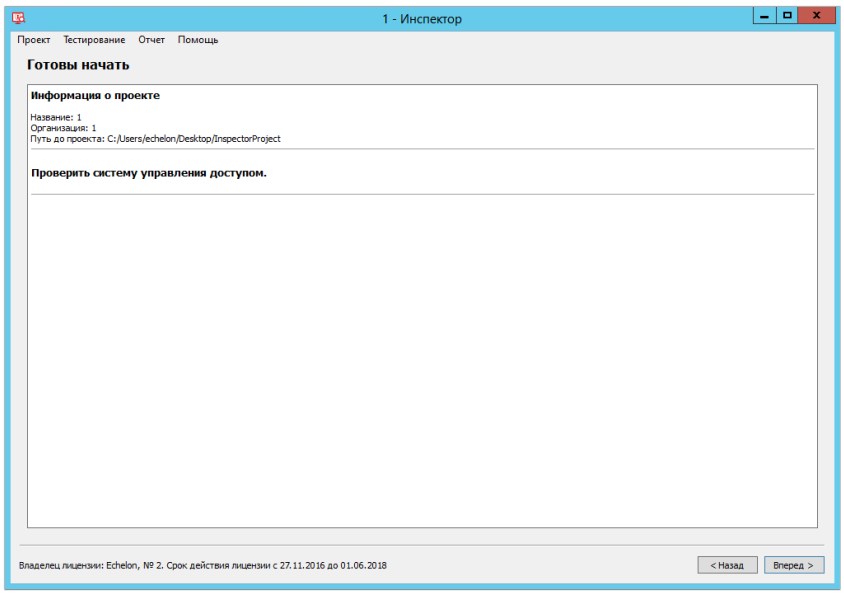


Рис. 236

После завершения тестирования необходимо запустить инструмент «Проверка прав доступа» для проверки прав доступа пользователей в различных сессиях к выбранным каталогам и файлам.

Для запуска инструмент необходимо выбрать в подменю «Тестирование» параметр «Проверка прав доступа» (рис. 237).

Запуск инструмента

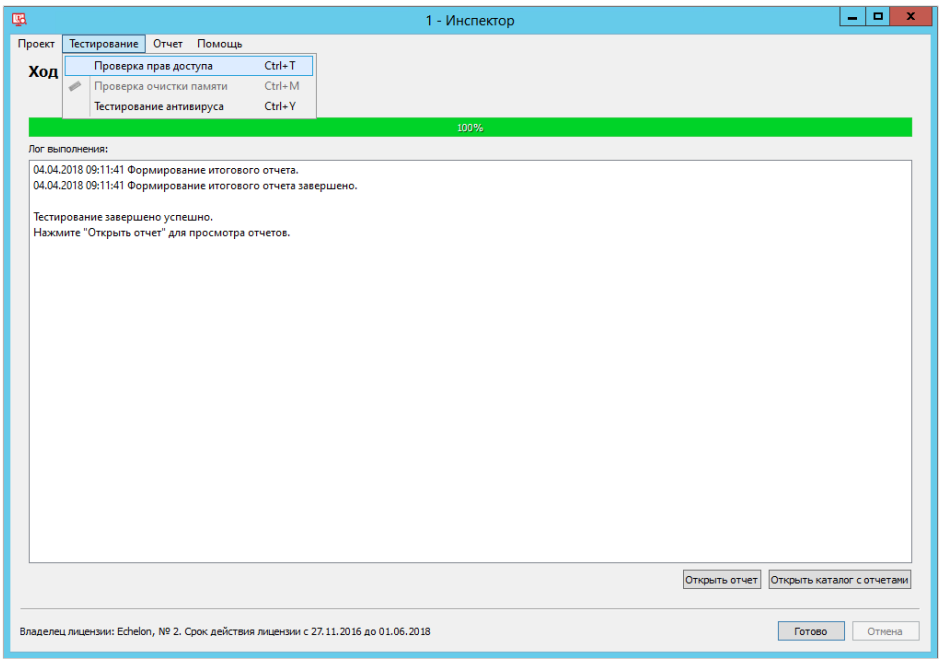


Рис. 237

В открывшемся окне нужно отметить галочкой «Использовать файл конфигурации Dallas Lock» и указать путь к файлу конфигурации, пользователей, для которых необходимо провести проверку, и нажать кнопку «Проверить доступ» (рис. 238).

Для создания (сохранения) файла конфигурации Dallas Lock воспользуйтесь в подменю «Конфигурация» параметром «Сохранить конфигурацию» СЗИ НСД Dallas Lock (подробнее см. в эксплуатационной документации на СЗИ НСД Dallas Lock).

Настройка тестирования прав доступа

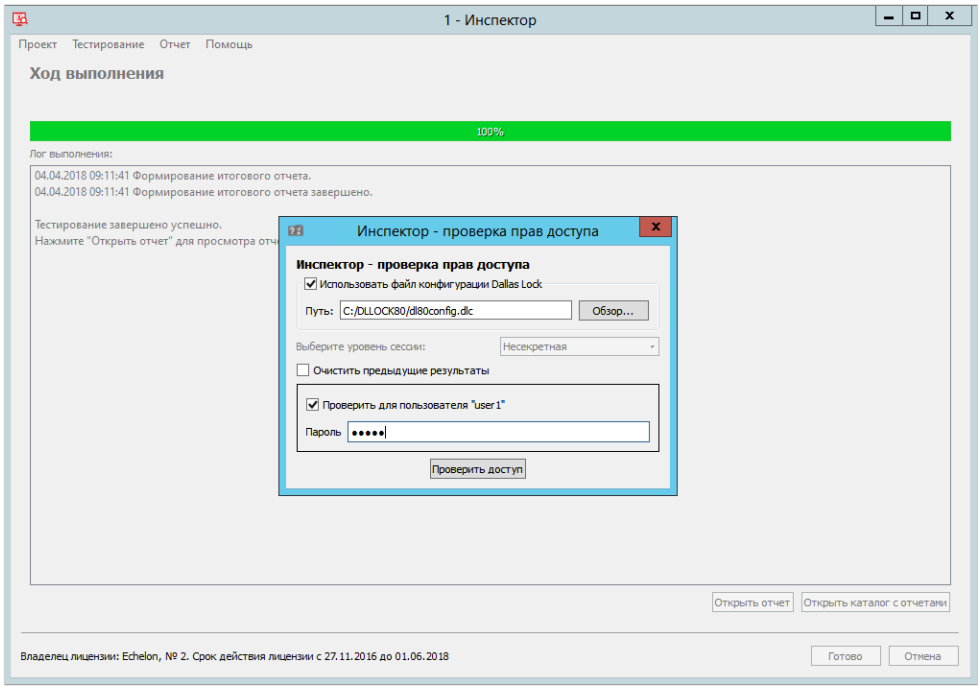


Рис. 238

После успешной проверки прав доступа появится соответствующее сообщение (рис. 227).

После завершения проверки для просмотра отчета необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (рис. 237).

6.3.4.5. Тестирование прав доступа с установленным СЗИ Secret Net

Для запуска инструмента «Проверка прав доступа необходимо» установить соответствующую галочку нажатием на пиктограмму или название инструмента и нажать «Вперед» (рис. 184). Откроется рабочее окно инструмента «Проверка прав доступа» компонента «Инспектор» (рис. 218).

Примечание. Функция тестирования прав доступа с установленным СЗИ Secret Net недоступна в среде функционирования под управлением ОС специального назначения «Astra Linux Special Edition».

Далее необходимо выполнить необходимые настройки для проверки прав доступа и нажать кнопку «Вперед» (рис. 239).

Запуск проверки прав доступа

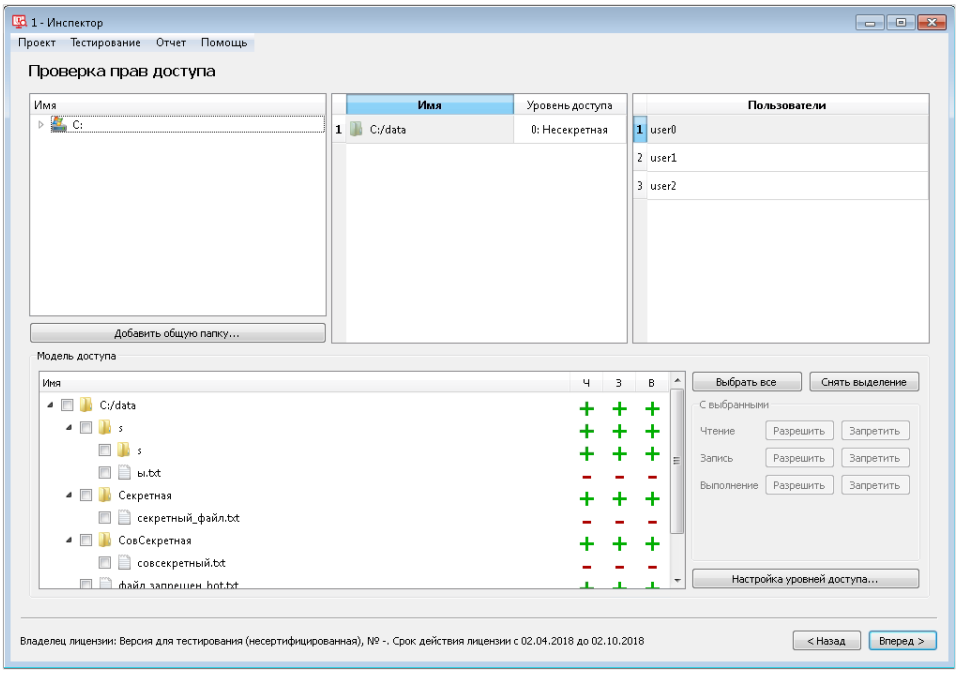


Рис. 239

В окне с информацией о тестировании необходимо нажать кнопку «Вперед» (рис. 240).

Информация о проекте

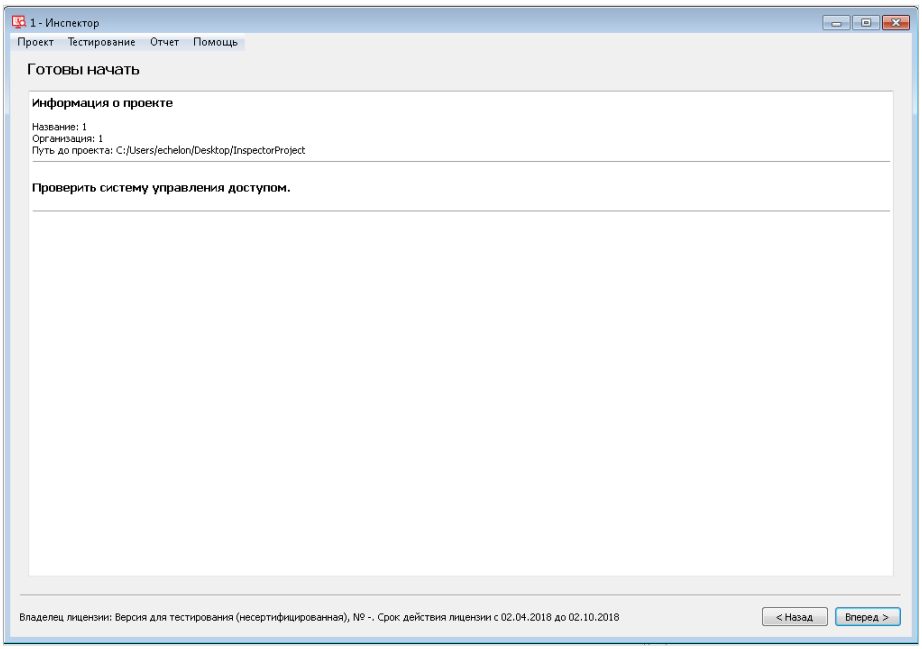


Рис. 240

После завершения тестирования необходимо запустить инструмент «Проверка прав доступа» для проверки прав доступа пользователей в различных сессиях к выбранным каталогам и файлам.

Для запуска инструмент необходимо выбрать в подменю «Тестирование» параметр «Проверка прав доступа».

В открывшемся окне нужно выбрать пользователей, для которых необходимо провести проверку, указать для них пароли и нажать кнопку «Проверить доступ» (рис. 241).

Примечание. В данном случае выбор сессии для проверки не требуется.

Настройка тестирования прав доступа

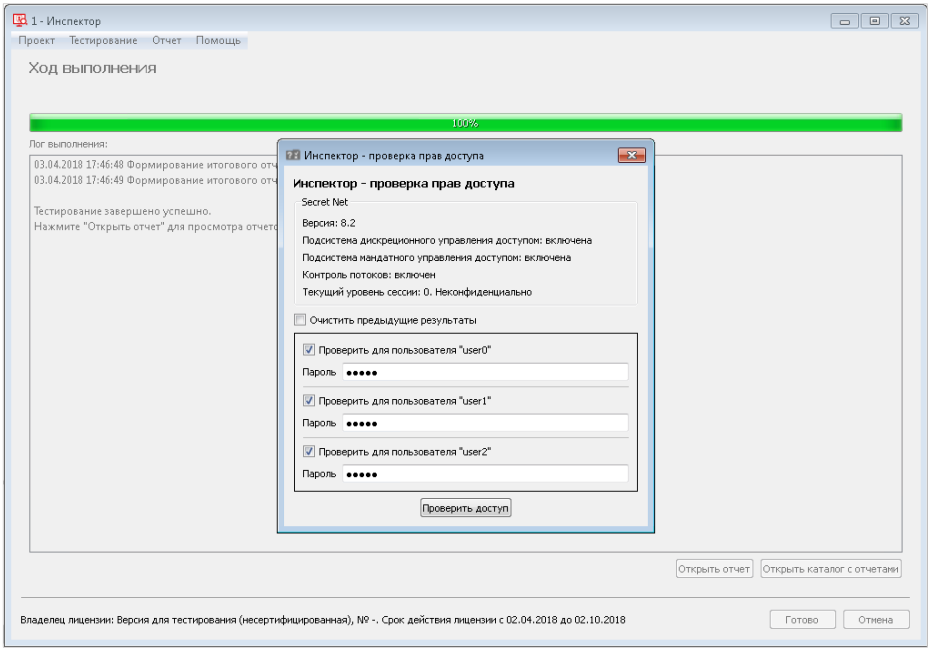


Рис. 241

После успешной проверки прав доступа появится соответствующее сообщение (рис. 227).

После завершения проверки для просмотра отчета необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (рис. 241).

6.3.5. Генерация отчетов

Итоговый отчет строится автоматически. Сгенерированный отчет разделен на вкладки с результатами работы каждого задействованного инструмента (рис. 242).

Общий вид отчета

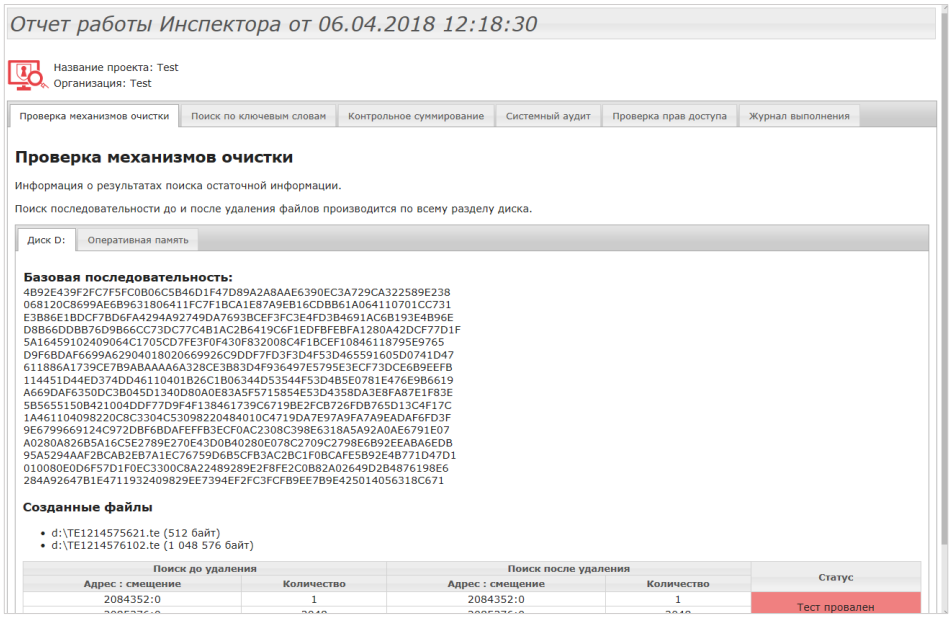


Рис. 242

6.3.5.1. Отчет инструмента «Проверка механизмов очистки»

Отчет инструмента «Проверка механизмов очистки» может состоять из вкладок «Проверка механизмов очистки» и / или «Поиск по ключевым словам». Вкладка «Проверка механизмов очистки» состоит из вкладок с данными о проверке устройств и / или с данными о проверке оперативной памяти (рис. 242).

В отчете о тестировании механизмов очистки устройства показана базовая последовательность, которая использовалась для тестирования. Под базовой последовательностью расположена таблица с данными о тестовых файлах и данными поиска. В столбце «Статус» показан итоговый результат тестирования (рис. 242).

Во вкладке «Оперативная память» содержится итоговый статус проверки механизмов очистки оперативной памяти (рис. 243).

Отчет проверки механизма очистки оперативной памяти

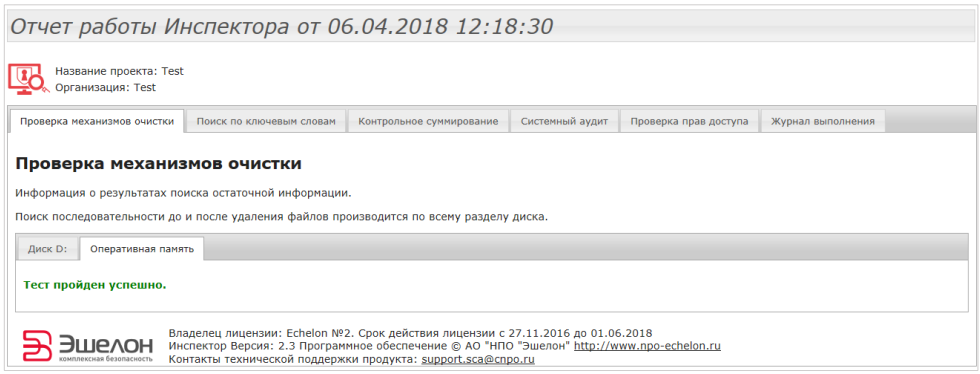


Рис. 243

Во вкладке «Поиск по ключевым словам» представлены параметры поиска и его результаты. Результаты оформлены в виде таблицы со столбцами: номер, найденное ключевое слово, кодировка, тип, локация и смещение (рис. 244).

Отчет поиска по ключевым словам

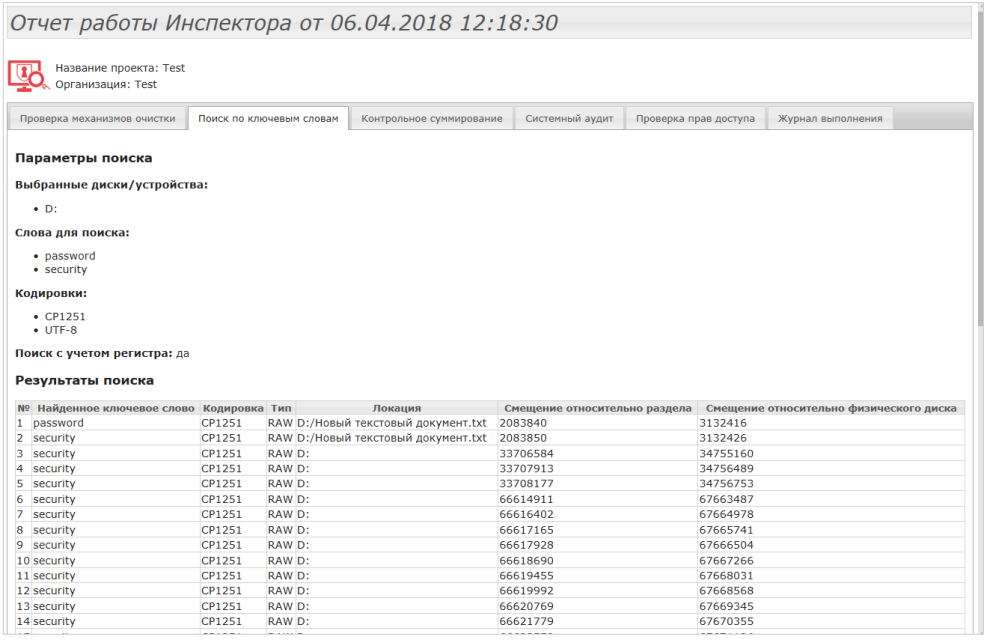


Рис. 244

6.3.5.2. Отчет инструмента «Контрольное суммирование»

Результаты контрольного суммирования оформлены в виде таблицы, где указаны порядковый номер, имя файла, его размер, время создания и изменения, алгоритм подсчета и контрольная сумма файла. (рис. 245).

Отчет о контрольном суммировании

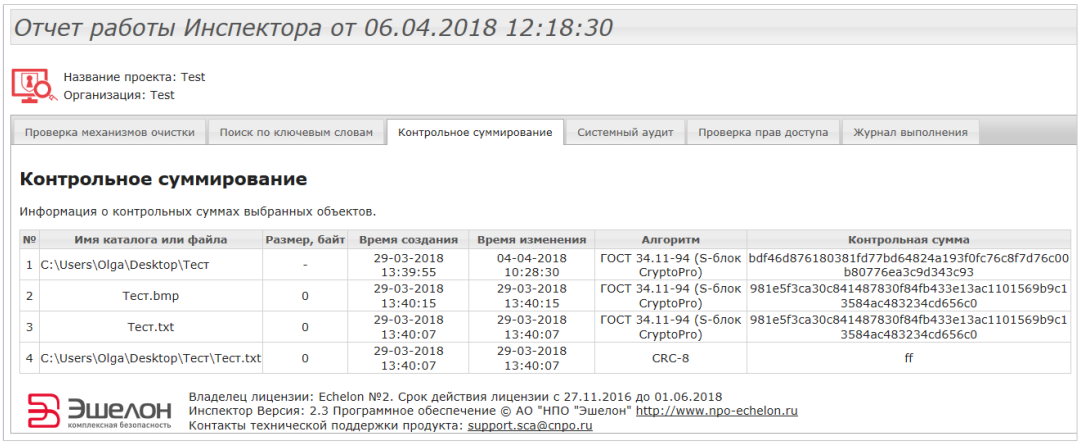
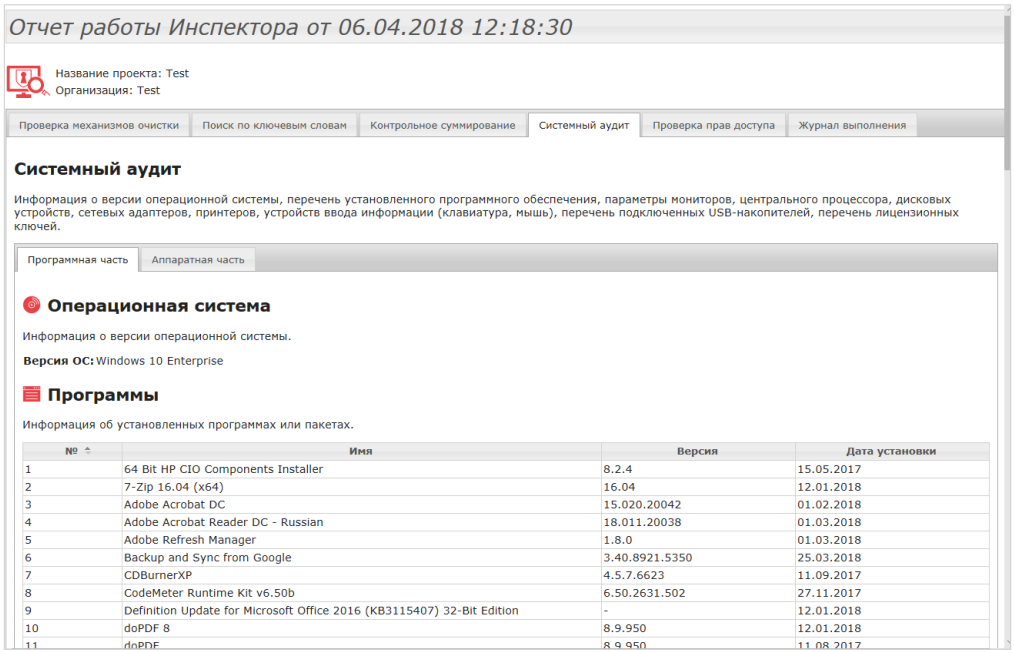


Рис. 245

6.3.5.3. Отчет инструмента «Системный аудит»

Отчет оформлен в виде таблиц и состоит из двух вкладок «Программная часть» и «Аппаратная часть» (рис. 246). Во вкладке «Программная часть» перечислены версия операционной системы, информация об установленных программах и пакетах, лицензионные номера установленных продуктов (рис. 246).

Отчет с результатами аудита рабочей станции



№	Имя	Версия	Дата установки
1	64 Bit HP CIO Components Installer	8.2.4	15.05.2017
2	7-Zip 16.04 (x64)	16.04	12.01.2018
3	Adobe Acrobat DC	15.020.20042	01.02.2018
4	Adobe Acrobat Reader DC - Russian	18.011.20038	01.03.2018
5	Adobe Refresh Manager	1.8.0	01.03.2018
6	Backup and Sync from Google	3.40.8921.5350	25.03.2018
7	CDBurnerXP	4.5.7.6623	11.09.2017
8	CodeMeter Runtime Kit v6.50b	6.50.2631.502	27.11.2017
9	Definition Update for Microsoft Office 2016 (KB3115407) 32-Bit Edition	-	12.01.2018
10	doPDF 8	8.9.950	12.01.2018
11	doPDF	8.9.950	11.08.2017

Рис. 246

Во вкладке «Аппаратная часть» перечислены данные о процессоре, дисковых устройствах, сетевых адаптерах, параметрах монитора, принтерах, устройствах ввода и USB-накопителях (рис. 247).

Примечание. Информация об USB-накопителе, который подключен к рабочей станции, содержится в таблице со статусом «Да» в графе «Подключен» (рис. 248).

Информация об аппаратной части рабочей станции

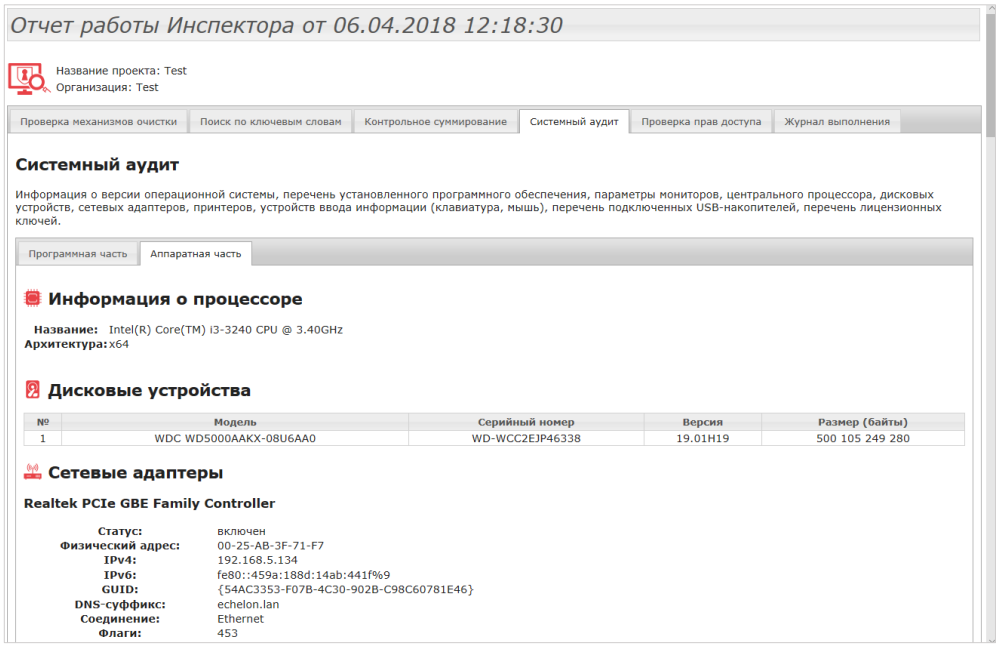


Рис. 247

Фрагмент отчета об аппаратной части рабочей станции

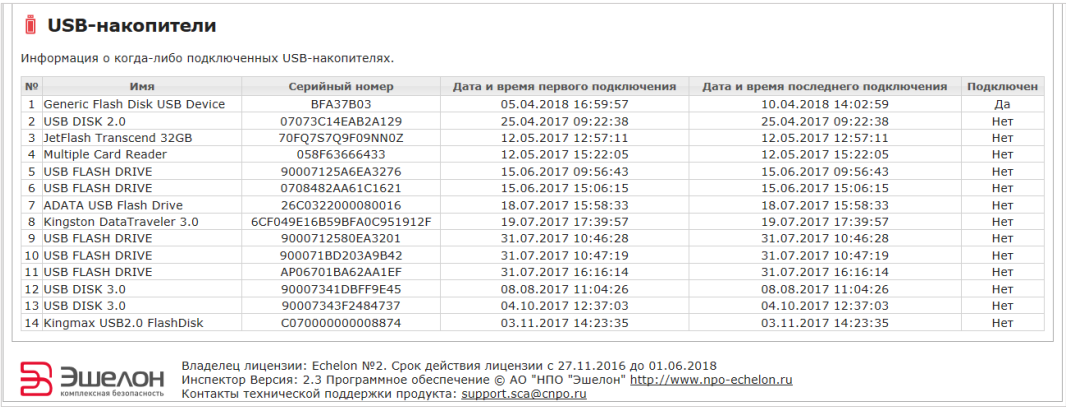


Рис. 248

6.3.5.4. Отчет инструмента «Проверка прав доступа»

Отчет состоит из вкладок, соответствующих уровням доступа, для которых проводилось тестирование. Результаты проверок отображаются в виде таблиц. На каждой вкладке каждому пользователю соответствует таблица (рис. 249).

Примечание. Если в процессе проверки прав доступа произошла ошибка (например, файл был удален), то в соответствующей ячейке будет знак «?».

Отчет с результатами проверки прав доступа

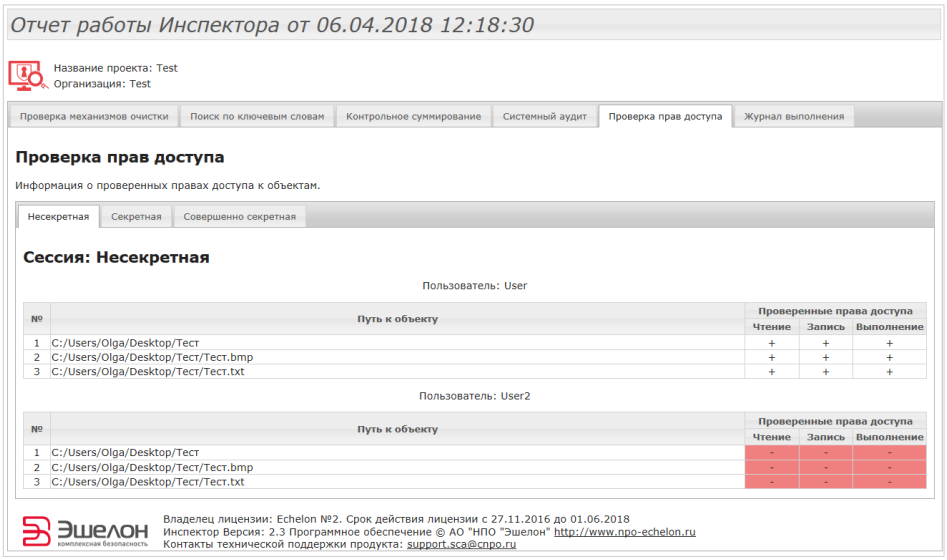


Рис. 249

6.3.5.5. Журналирование

Во вкладке «Журнал выполнения» содержится информация о ходе проведения тестирования (рис. 250).

Вкладка «Журнал выполнения»

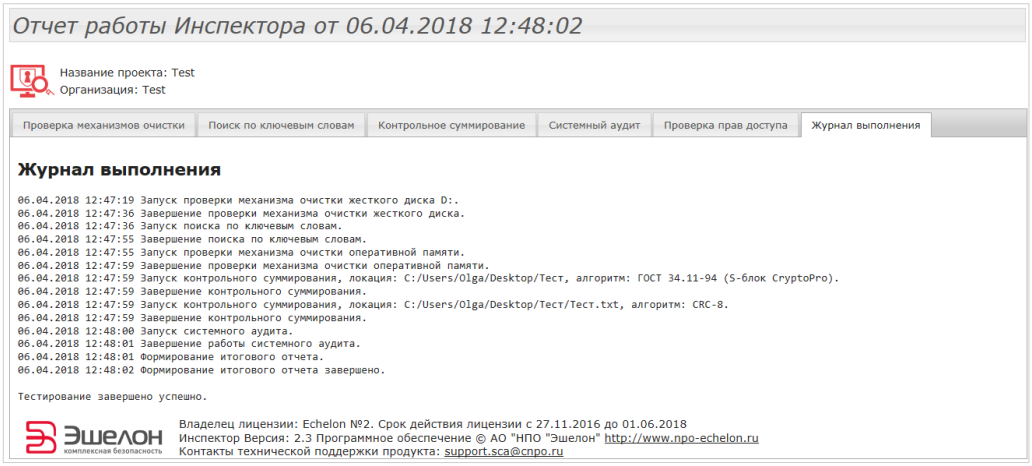


Рис. 250

6.3.5.6. Сравнение отчетов

В компоненте «Инспектор» реализована функция сравнения отчетов работы инструментов «Контрольное суммирование» и «Системный аудит».

Для сравнения отчетов необходимо выбрать в меню «Отчет» функцию «Сравнение отчетов» (см. рис. 187). Откроется окно «Инспектор – сравнение отчетов» (рис. 251).

Окно «Инспектор - сравнение отчетов»

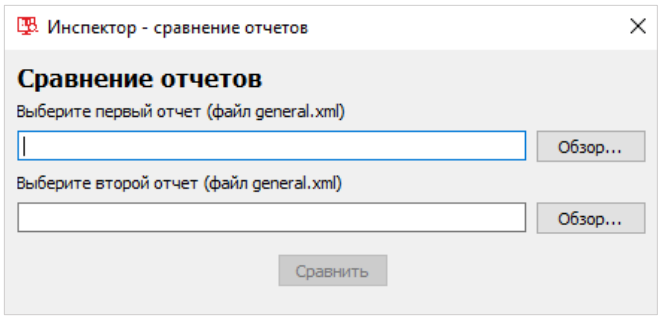


Рис. 251

Далее необходимо указать отчеты для сравнения и нажать кнопку «Сравнить» (рис. 252).

Выбор отчетов для сравнения

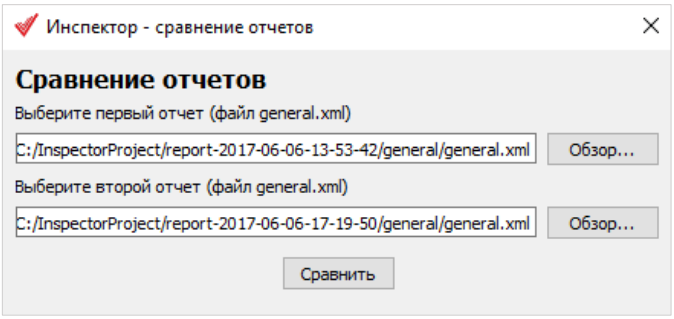


Рис. 252

В результате успешного сравнения отчетов откроется окно с соответствующим сообщением (рис. 253).

Сообщение

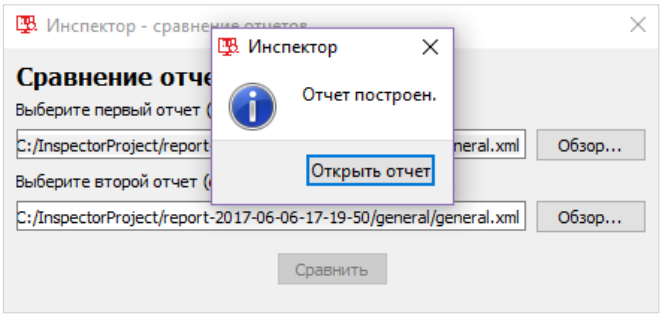


Рис. 253

После нажатия кнопки «Открыть отчет» (рис. 253) откроется отчет с результатами сравнения (рис.).

Сравнение отчетов

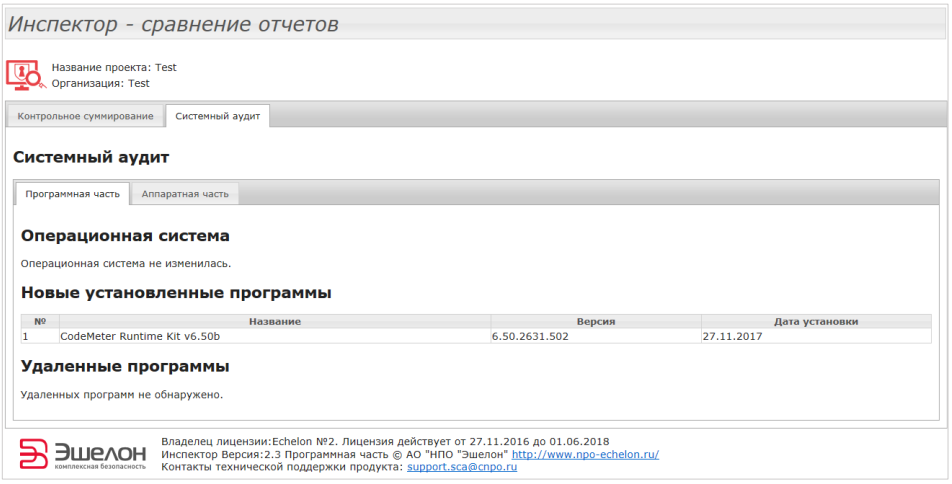


Рис. 254

6.4. Завершение работы

Для выхода из компонента «Инспектор» необходимо выбрать в подменю «Проект» параметр «Выход» либо нажать «Отмена» в любом из окон после завершения работы инструментов «Инспектора», либо нажать на «крестик» в верхнем правом углу рабочего окна.

7. Компонент «Инспектор» версии 4

Компонент «Инспектор» из состава ПК «Сканер-ВС» обеспечивает выполнение следующих функций:

– формирование и контроль дискреционных и мандатных полномочий доступа пользователей (локальных и доменных) к выбранным сетевым папкам и объектам файловой системы ОС специального назначения «Astra Linux Special Edition»;

– поиск остаточной информации на машинных носителях информации, а также определение директории файла с найденной информацией;

– тестирование механизмов очистки оперативной памяти ОС специального назначения «Astra Linux Special Edition» и запоминающих устройств рабочей станции;

– контрольное суммирование заданных файлов, папок, подпапок, съемных носителей и накопителей на жестких магнитных дисках;

– инвентаризацию программных и аппаратных средств.

Компонент «Инспектор» эксплуатируется в среде под управлением ОС специального назначения «Astra Linux Special Edition» 1.7.

7.1. Запуск компонента «Инспектор»

Для начала работы с компонентом «Инспектор» необходимо подключить носитель ПК «Сканер-ВС» к рабочей станции и запустить исполняемый файл inspector.exe, расположенный в корневом каталоге носителя.

После запуска откроется окно активации лицензии, изображенное на рис. 255.

Окно активации лицензии компонента «Инспектор»

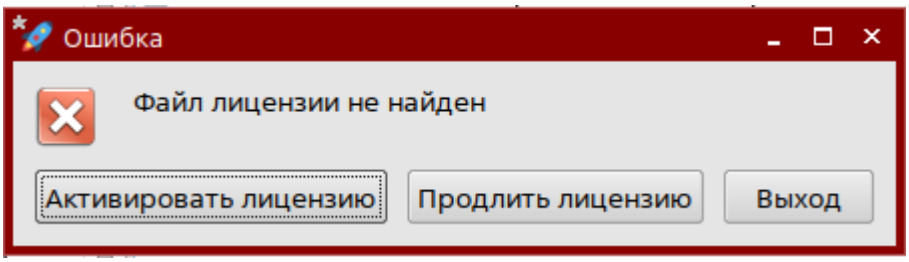


Рис. 255

Для активации необходимо нажать кнопку «Активировать лицензию» и выбрать файл с лицензией (с расширением «.lic»).

Далее откроется окно с информацией об успешной активации лицензии (рис. 256).

Окно с информацией об успешной активации лицензии

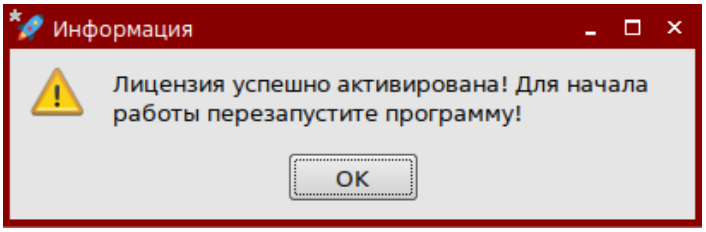


Рис. 256

Далее необходимо повторно запустить компонент «Инспектор».

После повторного запуска стартовое окно компонента «Инспектор» (рис. 257).

Стартовое окно компонента «Инспектор»

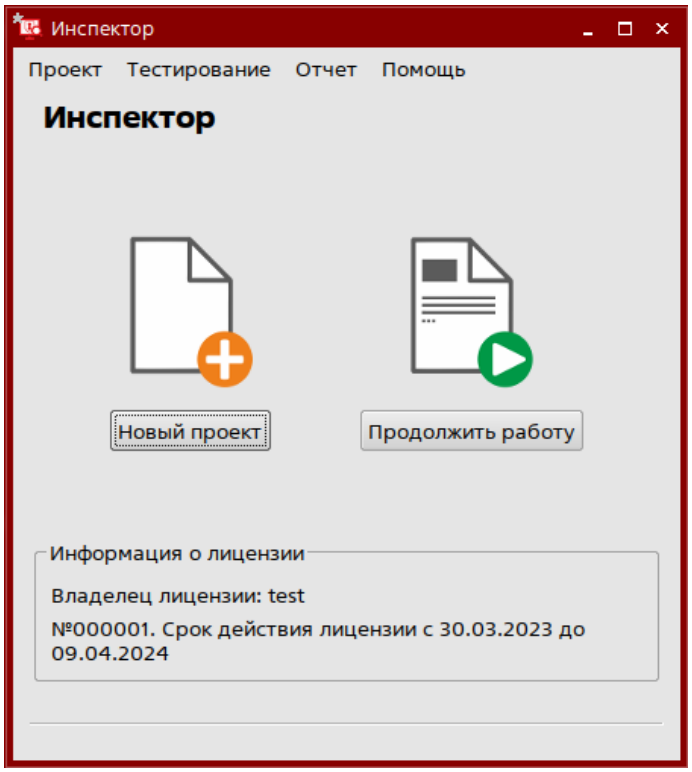


Рис. 257

После запуска необходимо создать новый проект или выбрать проект из ранее созданных (рис. 257). Для продолжения работы с ранее созданным проектом необходимо нажать кнопку «Продолжить работу» и в открывшемся окне выбрать сохраненный проект (рис. 258).

Выбор сохраненного проекта

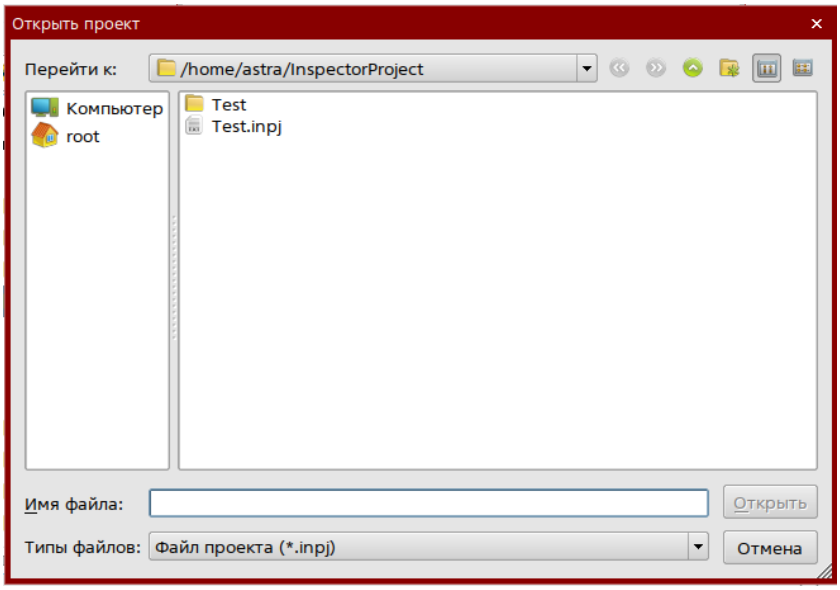


Рис. 258

Для создания нового проекта необходимо нажать кнопку «Новый проект». В открывшемся окне настройки нового проекта, изображенном на рис. 259, необходимо указать следующие параметры:

– имя проекта (поле «Имя»);

– расположение файла проекта (поле «Расположение»);

– наименование организации (поле «Организация»).

Для создания нового проекта после заполнения всех данных необходимо нажать кнопку «Завершить», в противном случае – кнопку «Отмена».

Примечание. Папка, указанная в поле «Расположение», будет использоваться для хранения отчетов по умолчанию.

Окно настройки нового проекта

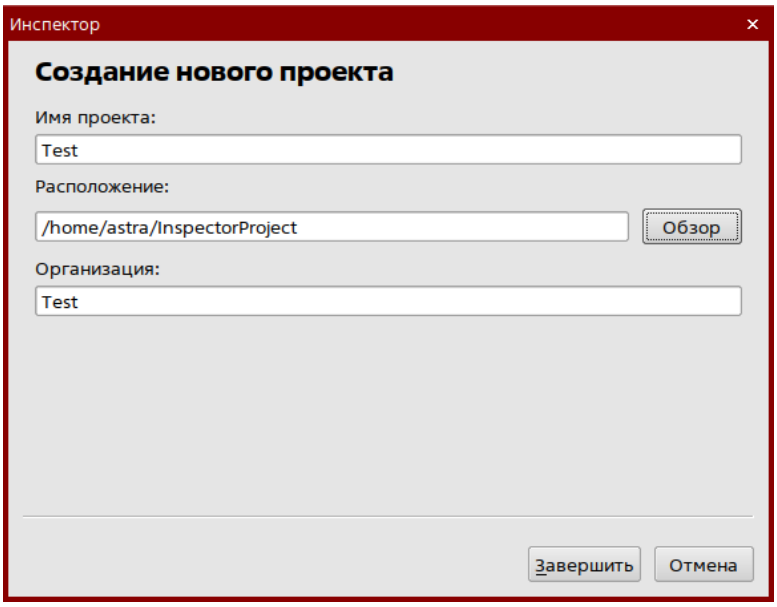


Рис. 259

После нажатия кнопки «Завершить» в указанной папке расположения будет автоматически создана папка с конфигурациями проекта, содержащая файл с расширением «.inpj», после чего откроется рабочее окно компонента «Инспектор», изображенное на рис. 260.

Рабочее окно компонента «Инспектор»

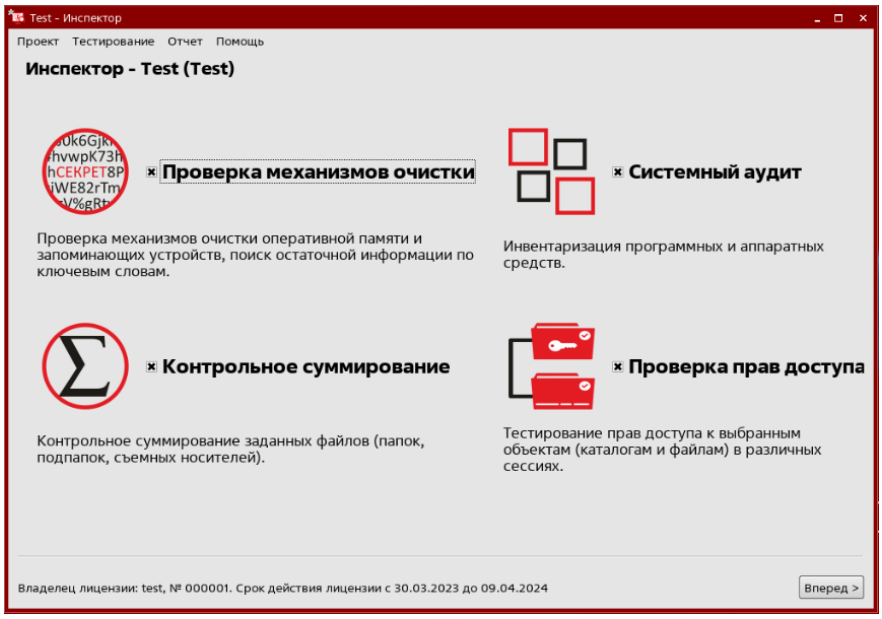


Рис. 260

Рабочее окно (рис. 260) предоставляет доступ к инструментам компонента «Инспектор», а именно:

– проверка механизмов очистки;

– системный аудит;

– контрольное суммирование;

– проверка прав доступа.

Каждый инструмент описывается своей пиктограммой, названием и кратким описанием с перечнем решаемых задач. Выбор каждого инструмента для текущего проекта отмечается галочкой рядом с названием (помимо чек-бокса, выбор инструмента также осуществляется нажатием на пиктограмму или название инструмента).

Меню компонента «Инспектор», расположенное в левом верхнем углу окна, состоит из следующих элементов:

– «Проект» дает доступ к управлению проектами: сохранение, создание и открытие проектов, а также выход из программы (рис. 261);

Подменю «Проект»

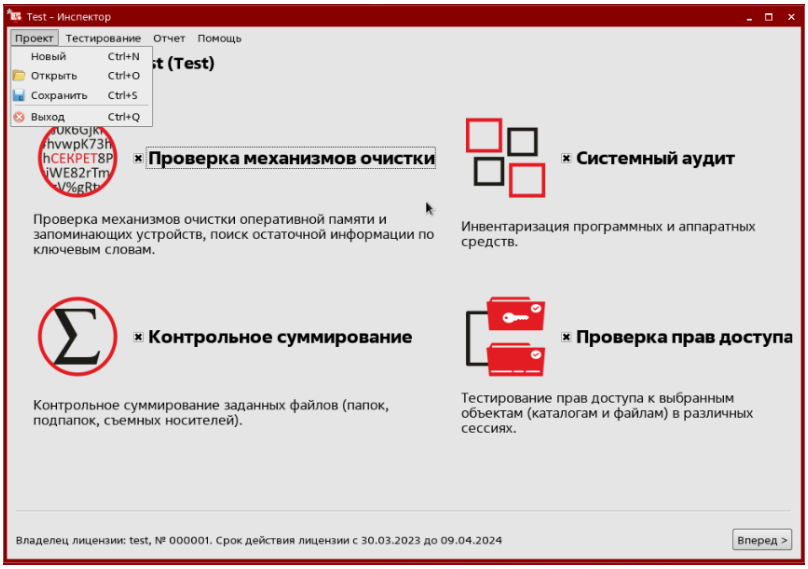


Рис. 261

– «Тестирование» содержит инструменты: «Проверка прав доступа», «Проверка механизма очистки памяти» (рис. 262);

Подменю «Тестирование»

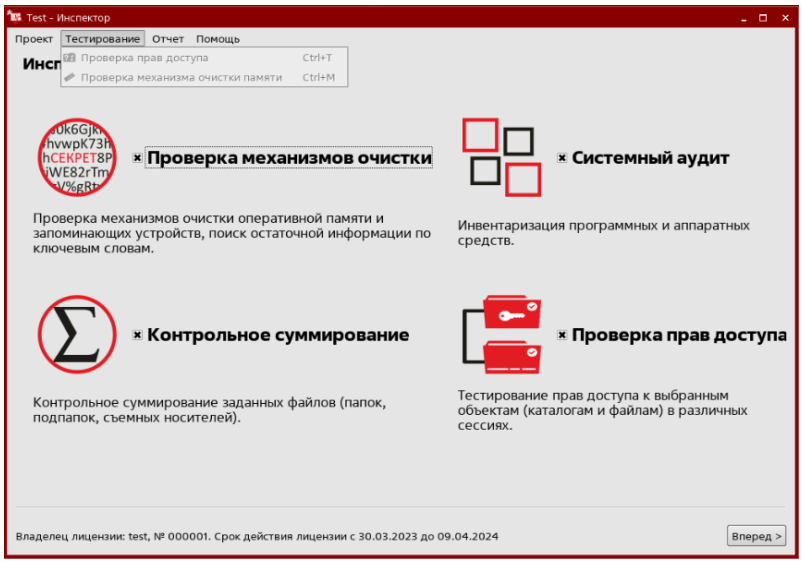


Рис. 262

– «Отчет» открывает отчеты, которые были созданы ранее и содержит инструмент сравнения отчетов (рис. 263);

Подменю «Отчет»

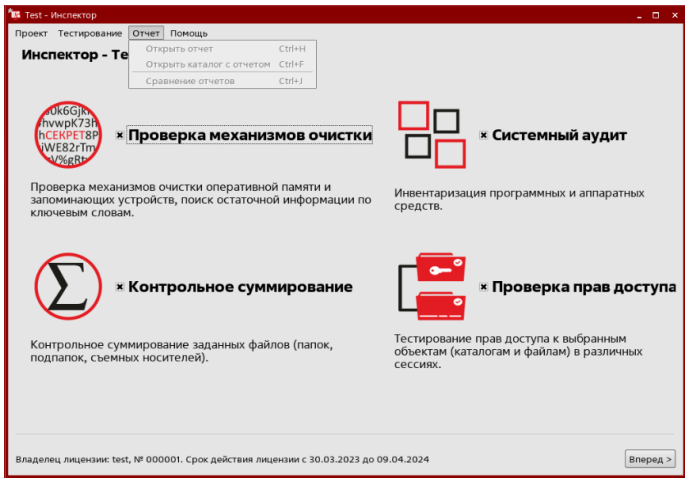


Рис. 263

– «Помощь» (рис.) открывает окно с информацией о версии, лицензии и ее продлении (кнопка «Продлить лицензию»). Данное окно изображено на рис. .

Подменю «Помощь»

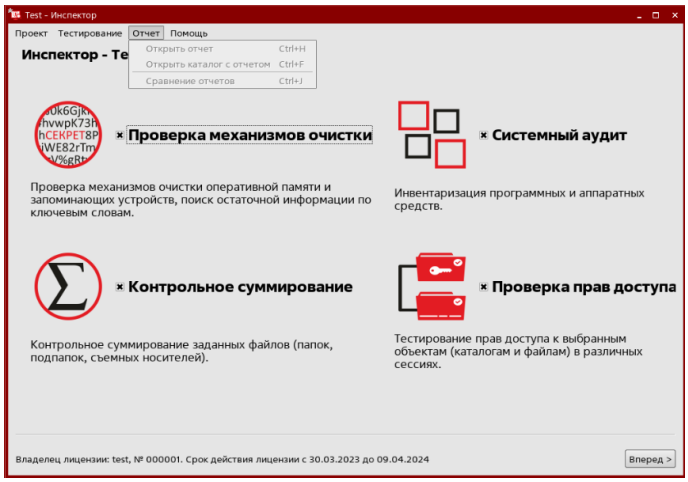


Рис. 264

Окно с информацией о лицензии

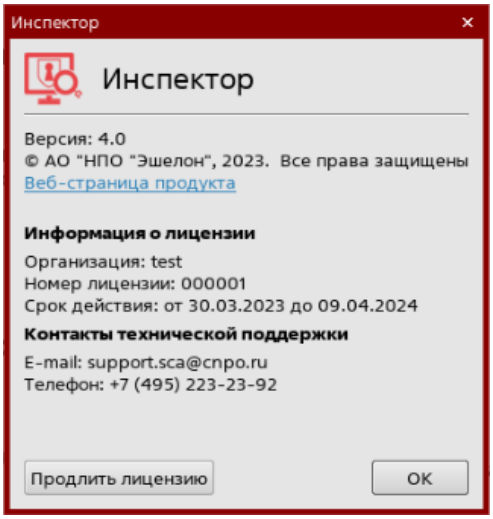


Рис. 265

Примечание. Комбинации клавиш для клавиатурного режима работы с компонентом «Инспектор» описаны в приложении Б настоящего руководства.

7.2. Работа с компонентом «Инспектор» в режиме замкнутой программной среды ОС Astra Linux

Механизм замкнутой программной среды (ЗПС) ОС Astra Linux позволяет ограничить доступ операторов к исполняемым файлам только теми программами, у которых есть цифровая подпись.

7.2.1. Запуск ЗПС на ОС Astra Linux 1.7

Перед запуском ЗПС необходимо поместить ключ «zao_npo_echelon_pub_key.gpg» в каталог «/etc/digsig/keys».

Для запуска ЗПС на ОС Astra Linux 1.7 необходимо перейти в панель управления (рис. 266).

Путь к панели управления

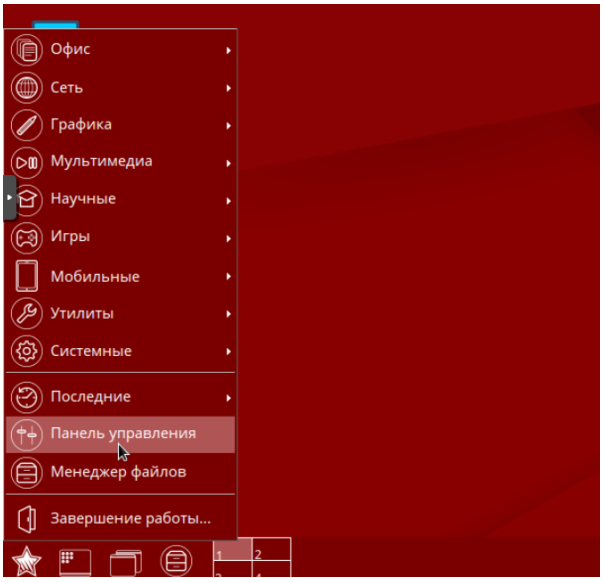


Рис. 266

Далее необходимо открыть вкладку «Безопасность» и открыть программу «Политика безопасности» (рис. 267).

Вкладка безопасность панели управления

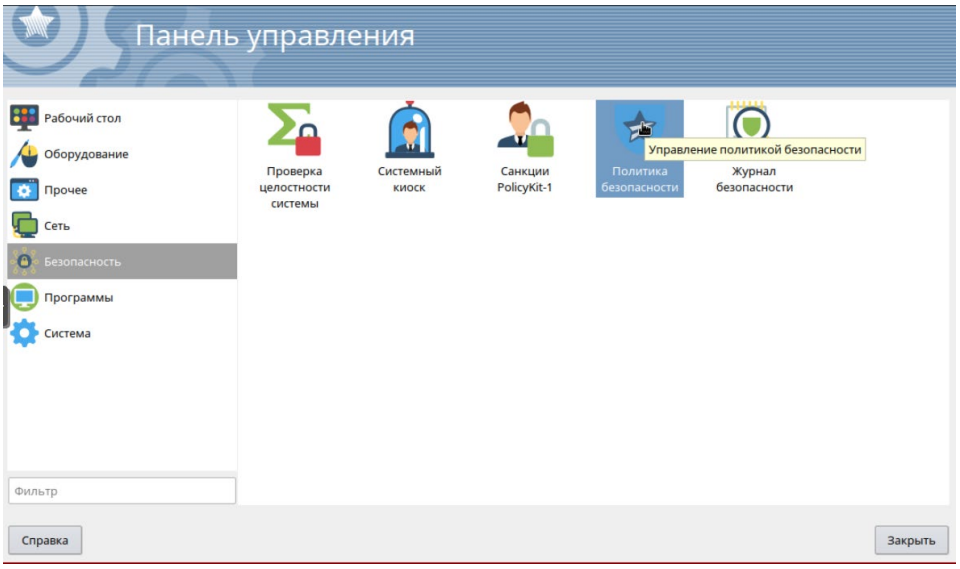


Рис. 267

После запуска программы «Политика безопасности» нужно перейти во вкладку «Замкнутая программная среда» и выбрать пункт «Включить» в окне контроля исполняемых файлов (рис. 268).

Включение ЗПС

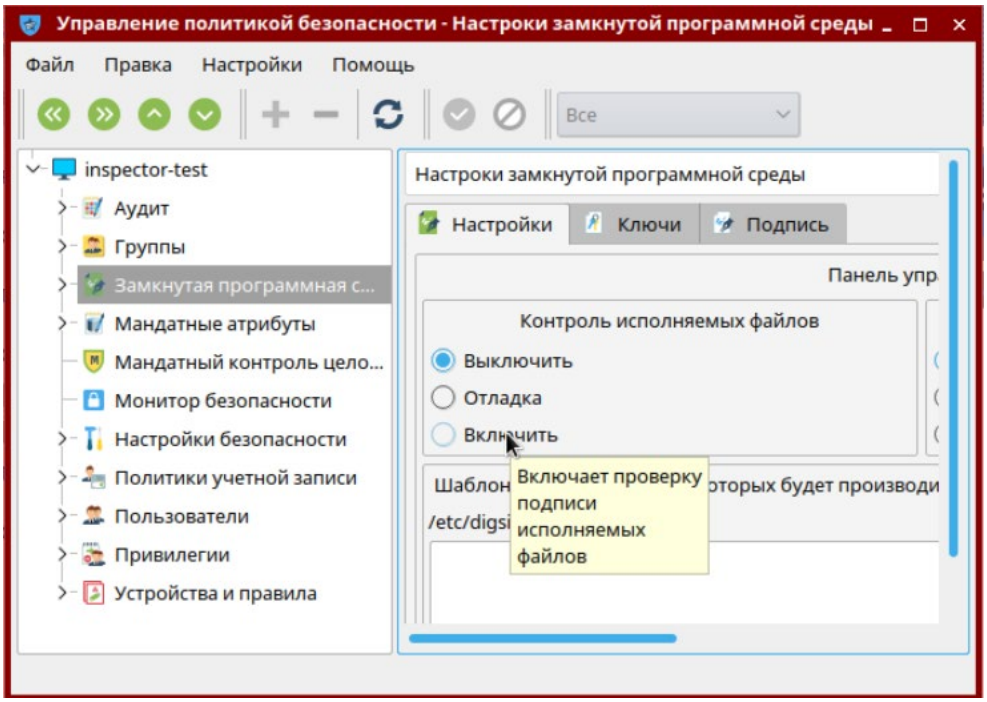


Рис. 268

Далее необходимо в меню выбрать пункт «Правка» и нажать «Применить» (рис. 269).

Применение настроек

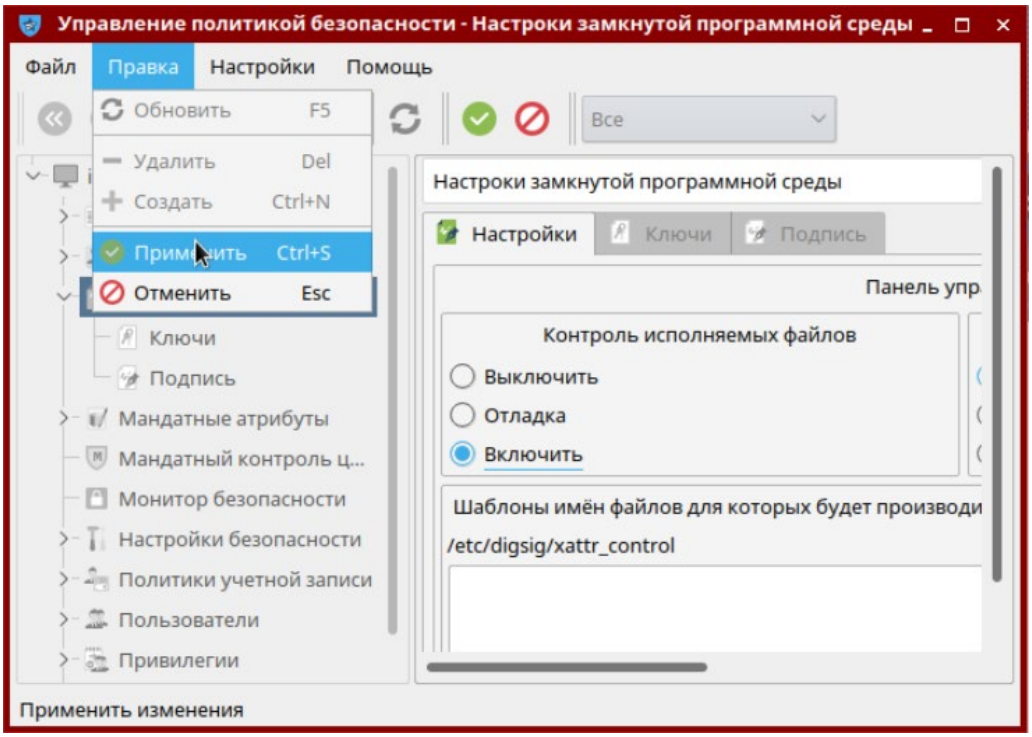


Рис. 269

После нажатия кнопки «Применить» появится сообщение с предупреждением о запуске ЗПС (рис. 270). Нужно нажать «Да» и дождаться перезагрузки, после чего ОС Astra Linux 1.7 будет работать в режиме ЗПС.

Сообщение с предупреждением о запуске ЗПС

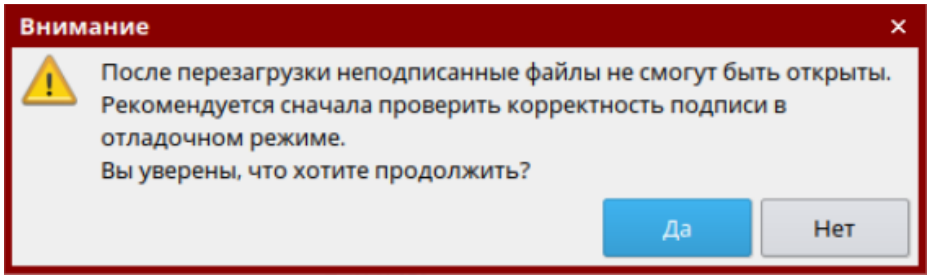


Рис. 270

7.3. Работа с инструментами

В рамках одного проекта для проведения тестирования можно выбрать один, несколько или все инструменты компонента «Инспектор». Работа инструментов может занимать довольно продолжительное время и зависит от параметров: объема накопителя, выбранного для поиска остаточной информации, количества файлов, выбранных для проведения контрольного суммирования, алгоритма контрольного суммирования и прочих факторов.

7.3.1. Проверка механизмов очистки

Для запуска инструмента проверки механизмов очистки необходимо установить соответствующую галочку, нажав на пиктограмму инструмента или на его название, и нажать кнопку «Вперед» (рис. 260). Откроется рабочее окно инструмента «Проверка механизмов очистки» (рис. 271).

Инструмент «Проверка механизмов очистки»

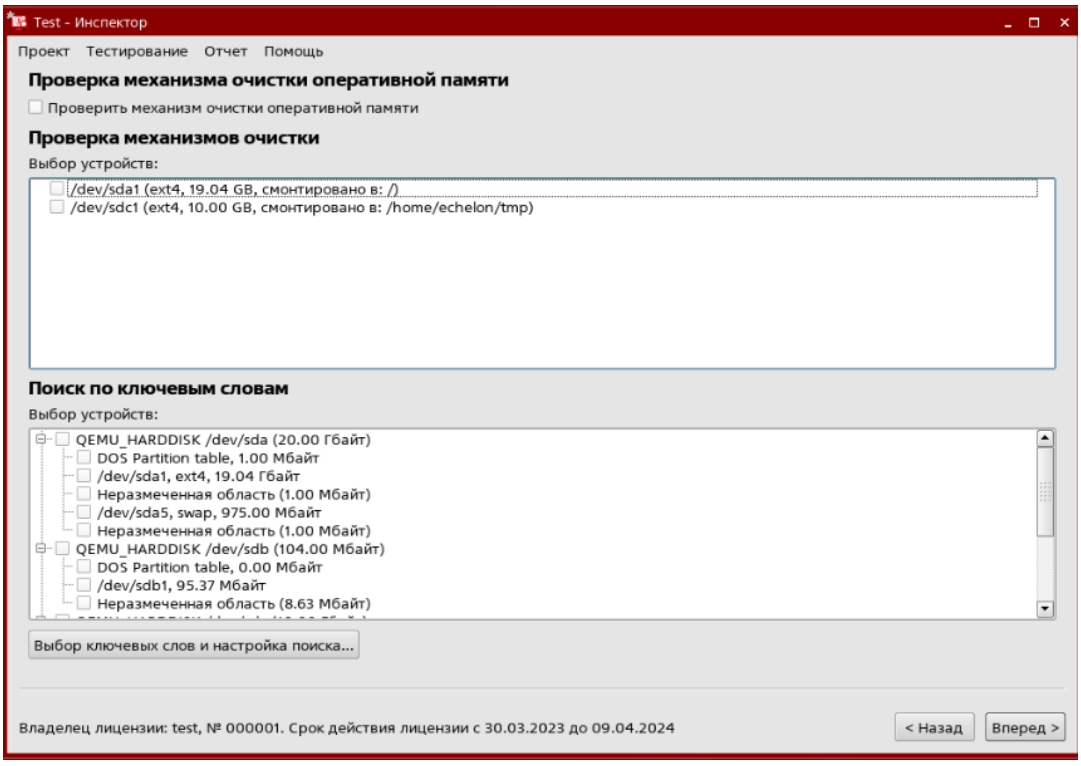


Рис. 271

Инструмент «Проверка механизмов очистки» (рис. 271) предназначен для проверки эффективности работы средств гарантированного уничтожения информации, осуществляющих оперативное удаление данных на рабочих станциях, и решает следующие задачи:

– проверка механизма очистки оперативной памяти;

– проверка механизмов очистки устройств;

– поиск по ключевым словам.

7.3.1.1. Проверка механизма очистки оперативной памяти

Для запуска нужно поставить галочку в квадратном поле рядом с «Проверить механизм очистки оперативной памяти» (рис. 272) и нажать кнопку «Вперед». Откроется новое окно с информацией о настройках проекта (рис. 273). Для начала проверки необходимо нажать кнопку «Вперед».

Примечание. Функция проверки механизма очистки оперативной памяти доступна для ядер: 4.2.0-23-generic, 4.2.0-23-pax, 3.16.0-16-generic, 3.16.0-16-pax.

Проверка механизма очистки оперативной памяти

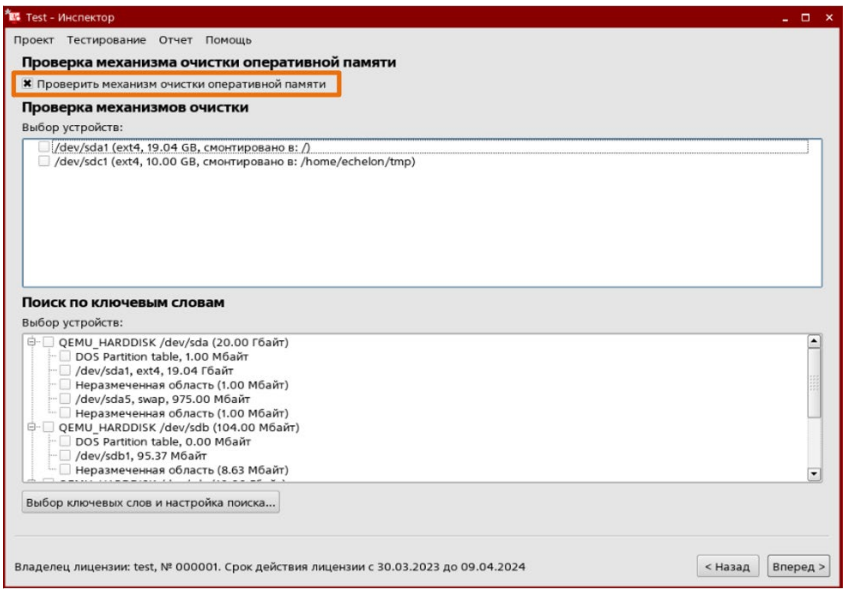


Рис. 272

Информация о проекте

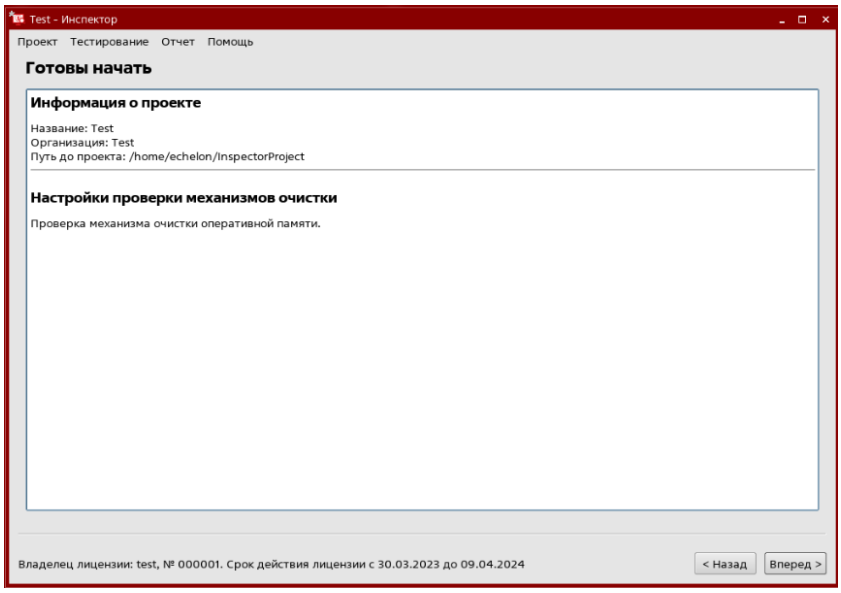


Рис. 273

В открывшемся окне (рис. 274) будет представлена информация о ходе выполнения проверки.

Ход выполнения проверки

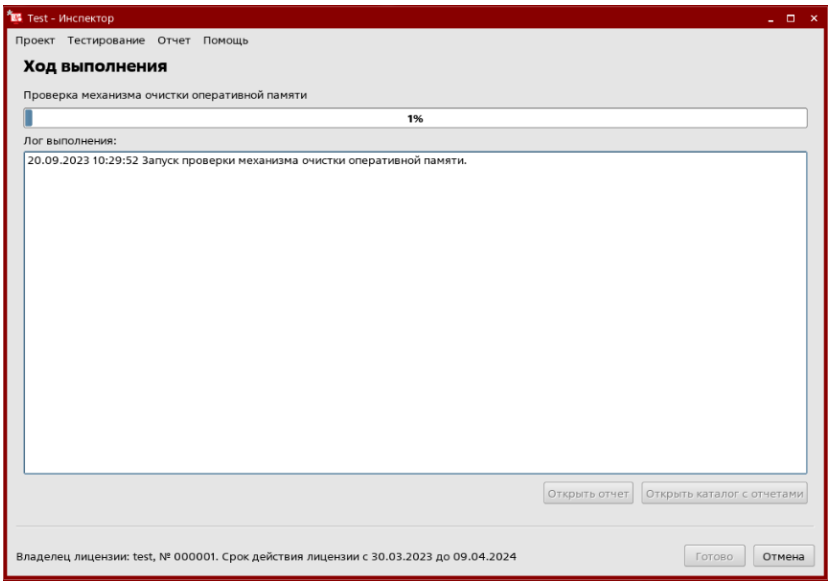


Рис. 274

После успешного завершения тестирования необходимо выбрать в подменю «Тестирование» пункт «Проверка механизма очистки памяти» (рис.).

Подменю «Тестирование»

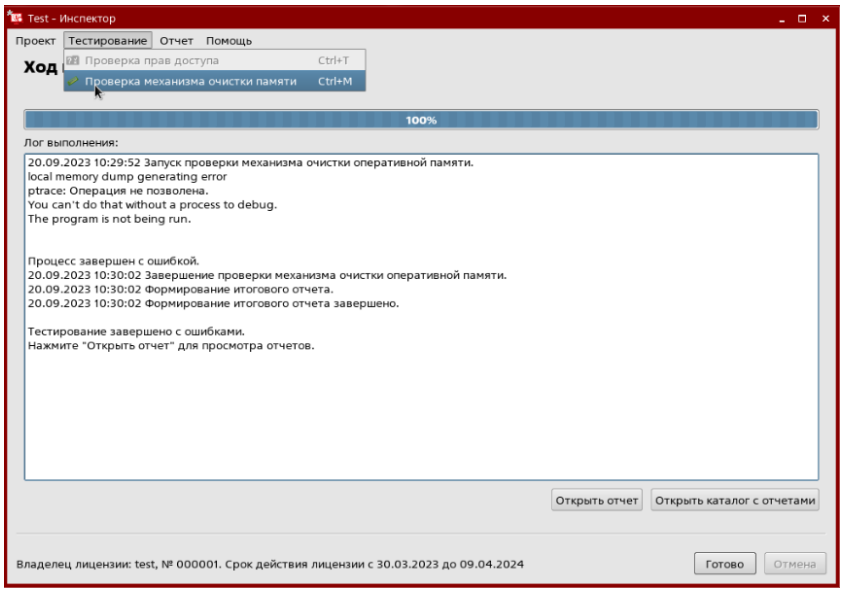


Рис. 275

В появившемся окне необходимо нажать кнопку «Начать проверку» (рис. 276).

Проверка механизма очистки оперативной памяти

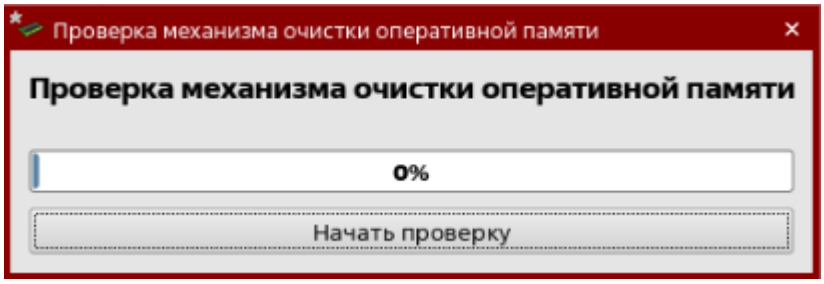


Рис. 276

По завершению проверки появится соответствующее сообщение. Далее нужно нажать кнопку «ОК».

Для просмотра отчета о проверке механизма очистки оперативной памяти нужно нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробное описание генерации отчетов приведено в п. 7.4 настоящего руководства).

Для возврата к списку инструментов необходимо нажать кнопку «Готово».

7.3.1.2. Проверка механизмов очистки устройств

Для запуска нужно отметить галочкой устройство в поле «Выбор устройств» рабочего окна инструмента и нажать кнопку «Вперед» (рис. 277).

Примечание. В среде функционирования под управлением ОС специального назначения «Astra Linux Special Edition» доступна функция проверки механизмов очистки для устройств с файловыми системами: ext2, ext3, ext4, vfat.

Проверка механизмов очистки устройств

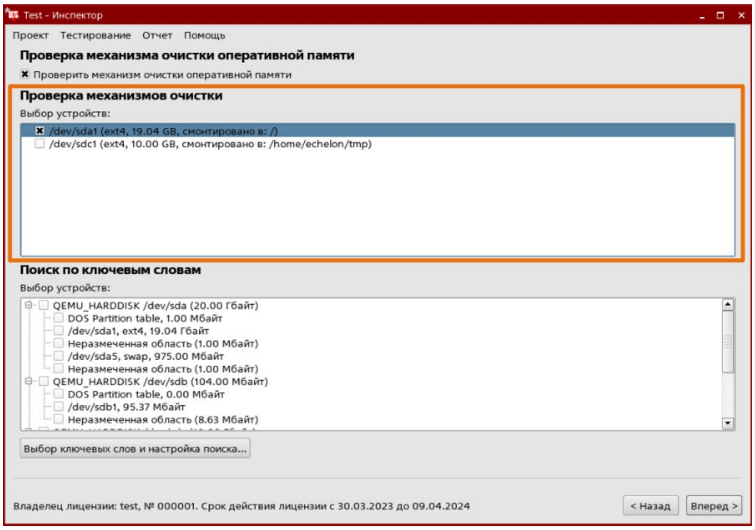


Рис. 277

Откроется новое окно с информацией о проекте и настройках проверки (рис. 278). В случае обнаружения ошибки в настройках проверки необходимо нажать кнопку «Назад» и скорректировать настройки. Если все данные верны, для начала проверки нужно нажать кнопку «Вперед».

Информация о проекте

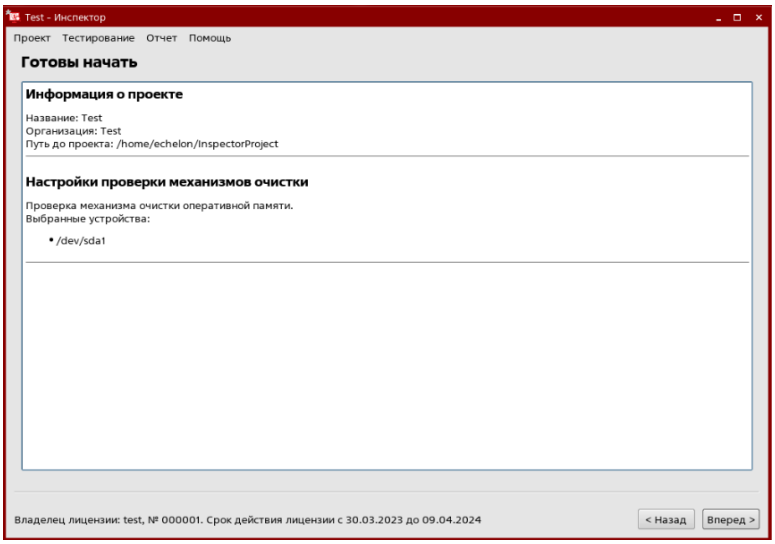


Рис. 278

В открывшемся окне (рис. 279) будет представлена информация о ходе выполнения проверки.

Ход выполнения проверки

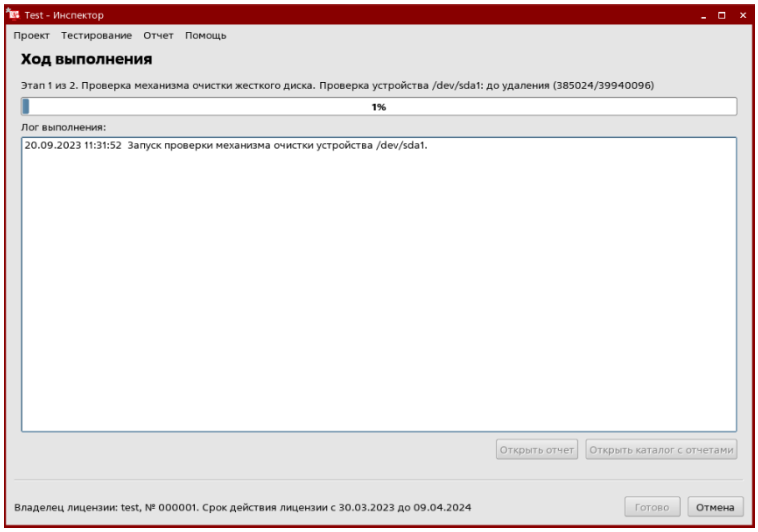


Рис. 279

После завершения проверки для просмотра отчета необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробное описание генерации отчетов приведено в п. 7.4 настоящего руководства).

Для возврата к списку инструментов нужно нажать кнопку «Готово».

7.3.1.3. Поиск по ключевым словам

Для запуска нужно отметить галочкой устройство в прямоугольном поле и нажать кнопку «Выбор ключевых слов и настройка поиска» (рис. 280).

Поиск по ключевым словам

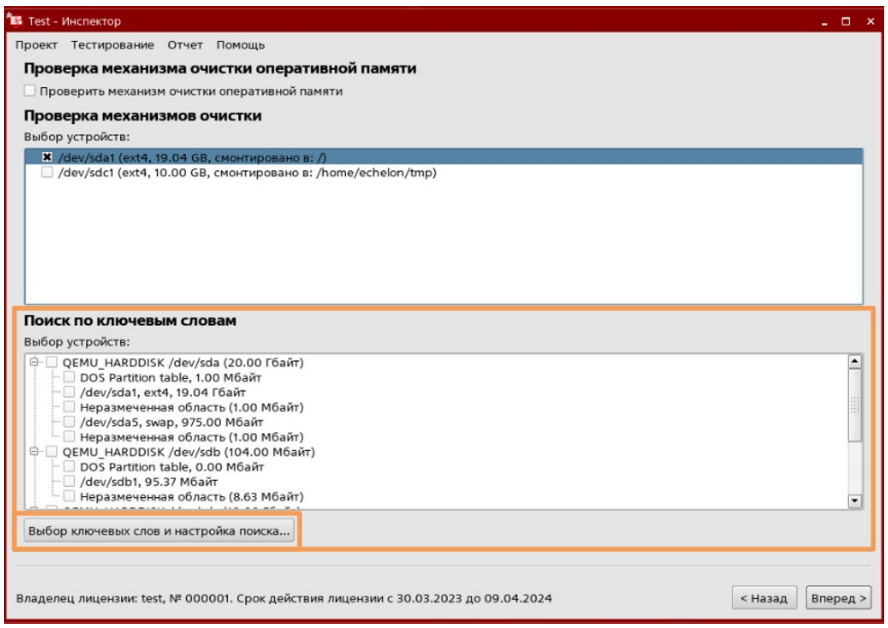


Рис. 280

В открывшемся окне «Выбор ключевых слов и настройка поиска» необходимо указать ключевые слова для поиска остаточной информации (рис. 281).

Указать слова для поиска можно двумя способами:

– вручную. В поле «Фраза» нужно ввести слова или словосочетания и нажать кнопку «Добавить»;

– импортировать. Для импорта необходимо загрузить заранее подготовленный список ключевых слов в формате TXT и кодировке UTF-8 с помощью кнопки «Импортировать из словаря».

Дополнительно можно указать:

– кодировку и типы документов;

– учет регистра при проверке;

– определение пути до файлов, содержащих ключевые слова;

– ограничение области поиска. Значения ограничения выбранного раздела округляются до чисел кратных 4096. При этом начальное значение округляется в меньшую сторону, а конечное значение в большую.

В отчете будет отражена позиция начала документа (файла) относительно раздела диска, в котором найдено ключевое слово.

Действуют следующие ограничения:

– документ должен располагаться непрерывно;

– размер документа не должен превышать 10 Мбайт;

– документ должен конвертироваться в текстовый формат (время на конвертацию ограничено тайм-аутом);

– максимальная длина слова для поиска – 100 символов;

– максимальное количество слов для поиска – 100 слов;

– одно ключевое слово может быть найдено не более 1000 раз.

После ввода слова для поиска необходимо нажать «ОК», а затем «Вперед».

Выбор ключевых слов и настройка поиска

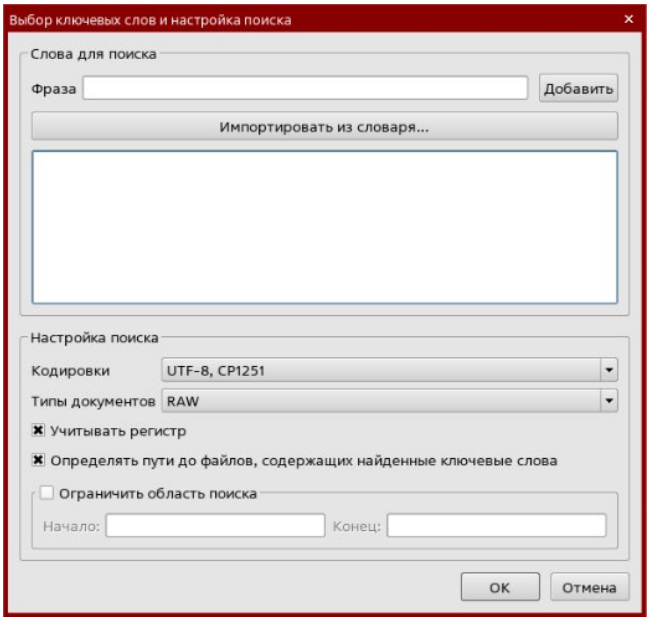


Рис. 281

Откроется новое окно с информацией о проекте и настройках проверки (рис. 282). В случае обнаружения ошибки в настройках проверки необходимо нажать кнопку «Назад» и скорректировать настройки. Для начала проверки нужно нажать кнопку «Вперед».

Информация о проекте

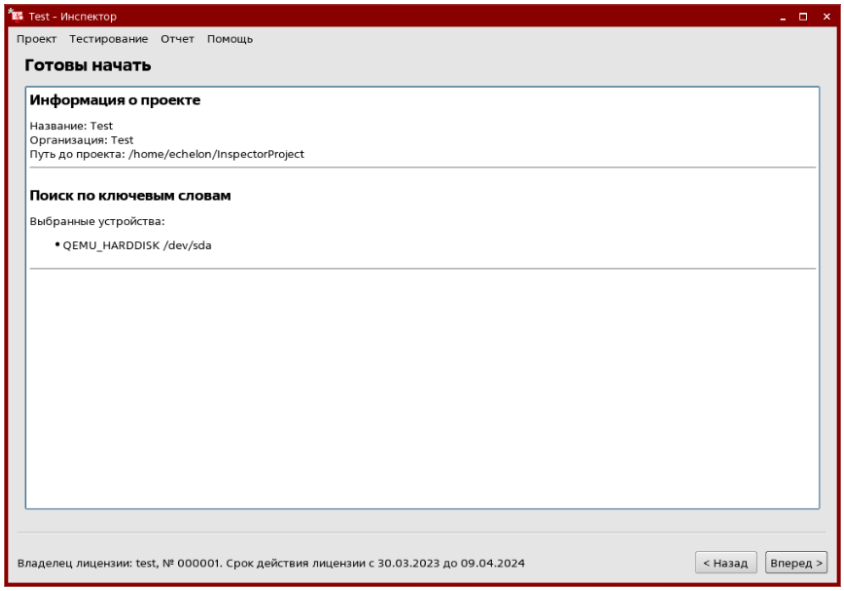


Рис. 282

В открывшемся окне (рис. 283) будет представлена информация о ходе выполнения проверки.

Ход выполнения проверки

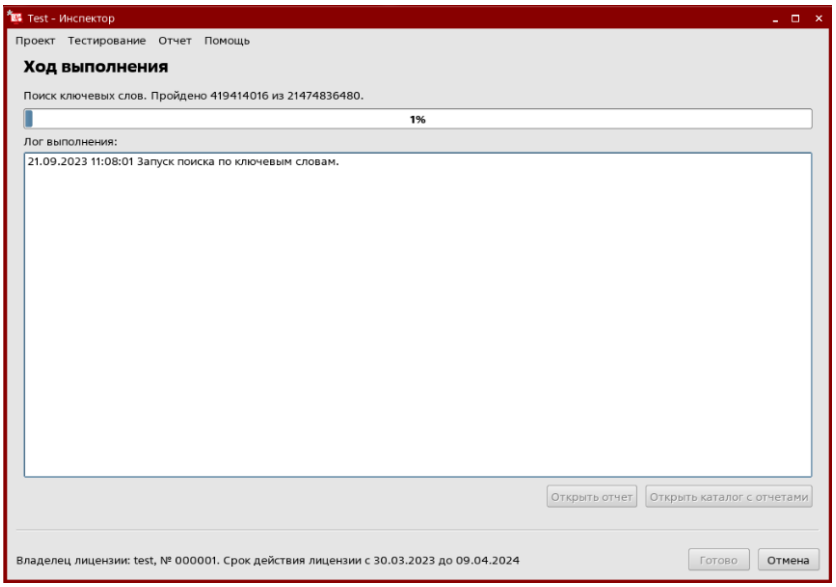


Рис. 283

После завершения проверки для просмотра отчета нужно нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробное описание генерации отчетов приведено в п. 7.4 настоящего руководства).

Для возврата к списку инструментов нужно нажать кнопку «Готово».

7.3.2. Контрольное суммирование

Инструмент контрольного суммирования предназначен для контроля целостности выбранных файлов и каталогов по заданным алгоритмам.

Для запуска инструмента «Контрольное суммирование» необходимо установить соответствующую галочку, нажав на пиктограмму инструмента или на его название, и нажать кнопку «Вперед». Рабочее окно инструмента «Контрольное суммирование» представлено на рисунке (рис. 284).

Рабочее окно инструмента «Контрольное суммирование»

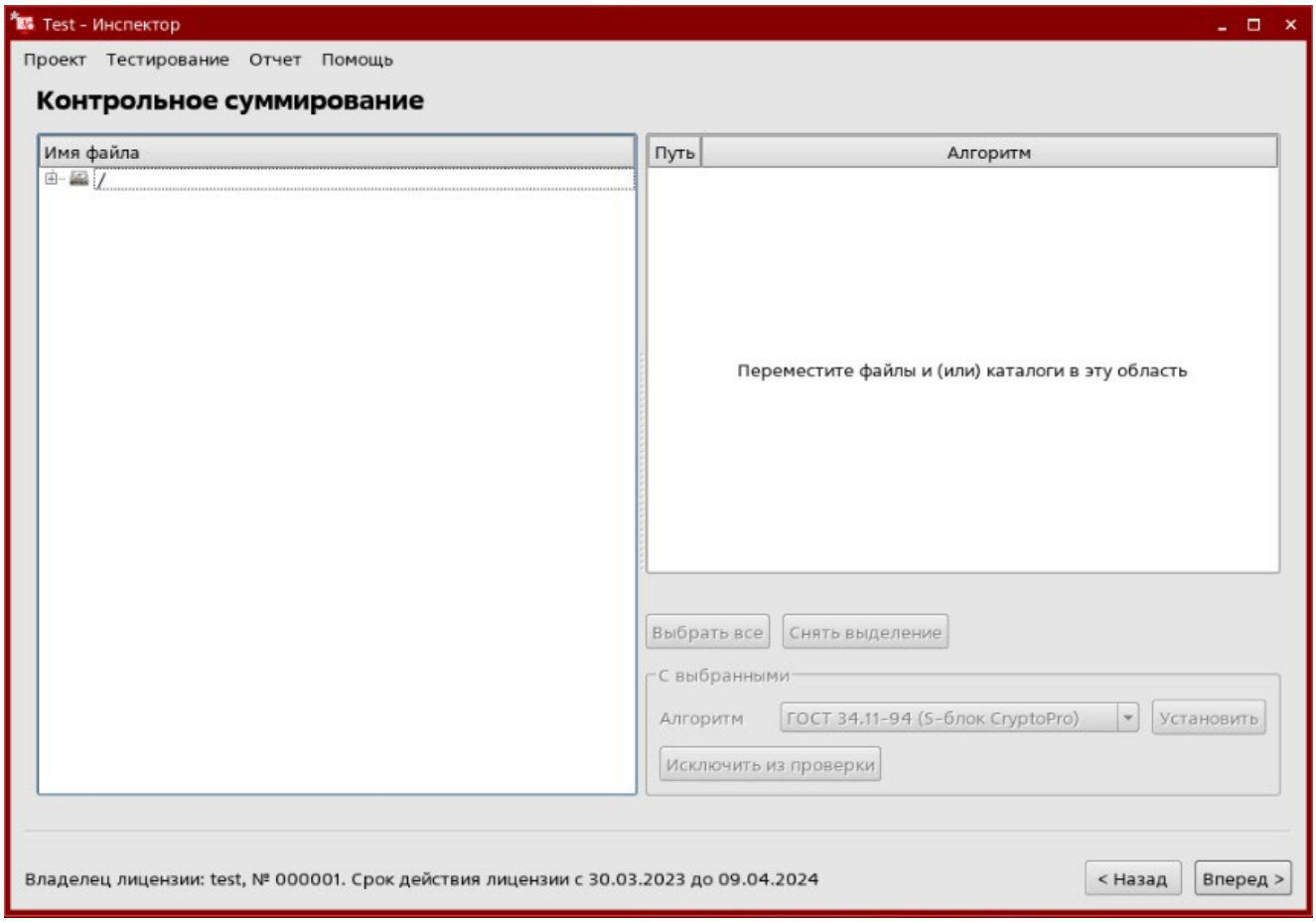


Рис. 284

Рабочее окно инструмента контрольного суммирования разделено на две области. Слева – дерево каталогов для выбора объектов для контрольного суммирования, а справа – настройки для каждого выбранного объекта (путь, алгоритм).

Чтобы начать процесс контрольного суммирования необходимо двойным нажатием левой кнопки мыши добавить интересующие объекты в область настроек (рис. 285).

Выбор объектов и алгоритмов для контрольного суммирования

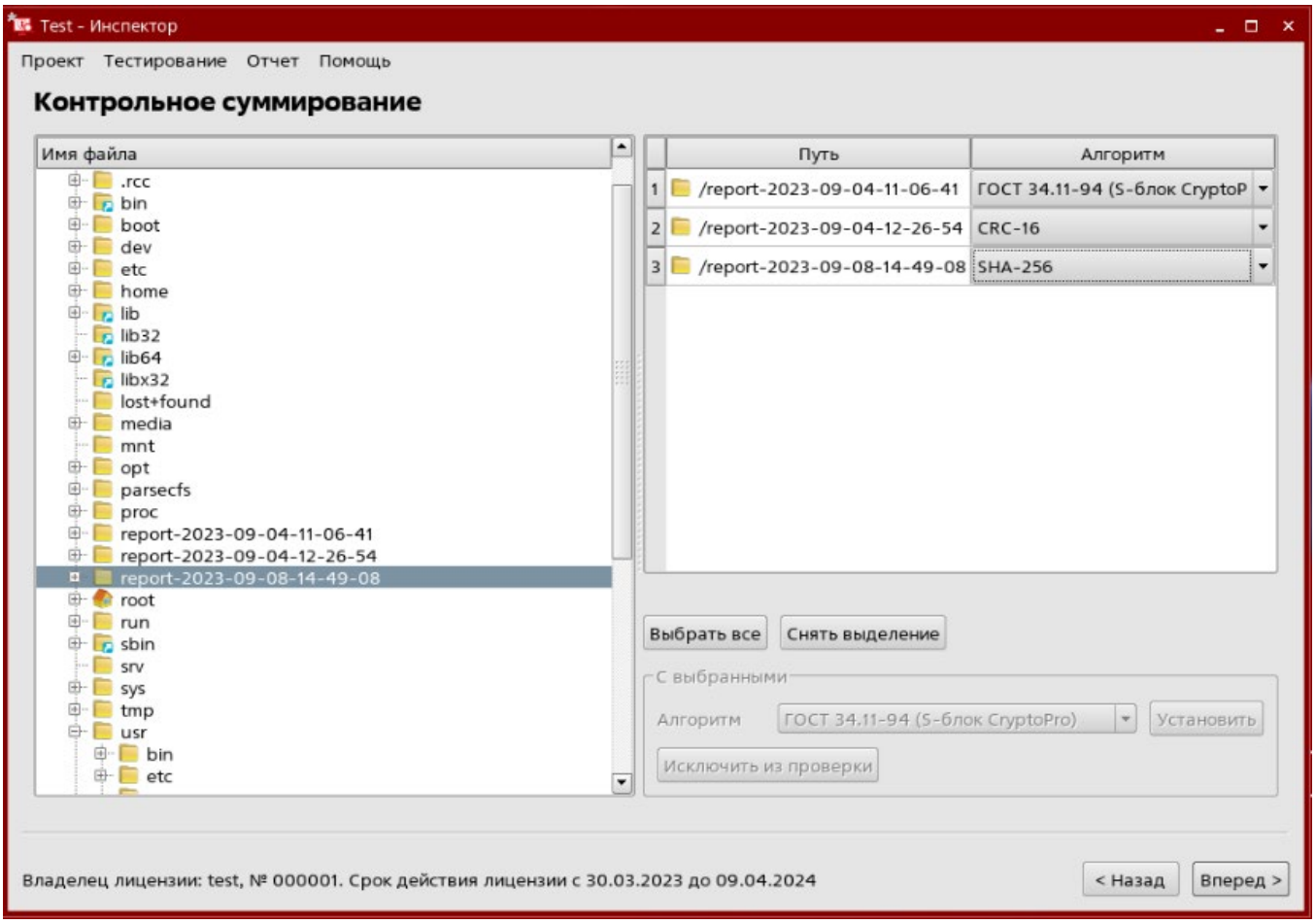


Рис. 285

Для удаления объектов из области настроек необходимо выбрать объект нажатием левой кнопки и нажать «Исключить из проверки» или нажать на клавиатуре клавишу «Delete».

После того как объекты добавлены, можно скорректировать настройки контрольного суммирования (рис. 285), выбрав из выпадающего списка поддерживаемых алгоритмов необходимый алгоритм.

Алгоритм контрольного суммирования можно настроить для каждого файла отдельно или задать один алгоритм для всех файлов с помощью меню в нижнем правом углу. Для выбора одного алгоритма для всех объектов суммирования необходимо нажать кнопку «Выбрать все». Далее, из выпадающего списка алгоритмов нужно выбрать нужный и нажать кнопку «Установить».

После установки всех настроек нужно нажать кнопку «Вперед».

Примечание. Если нажать кнопку «Вперед», не выбрав объект для контрольного суммирования, появится соответствующая всплывающая подсказка.

Откроется новое окно с информацией о настройках проекта (рис. 286). В случае обнаружения ошибки в настройках контрольного суммирования необходимо нажать кнопку «Назад» и скорректировать настройки. Для начала суммирования нужно нажать кнопку «Вперед».

Информация о проекте

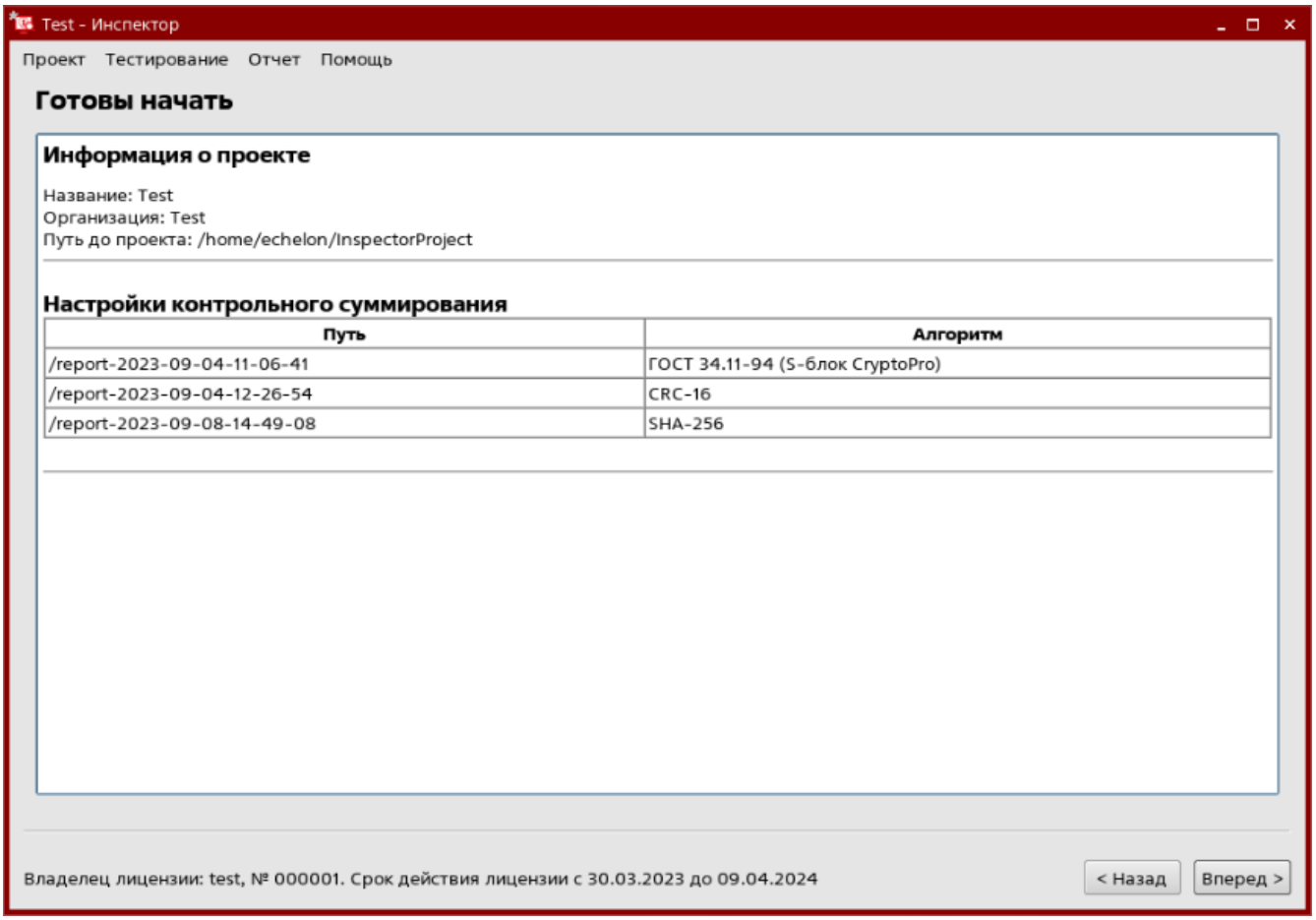


Рис. 286

В открывшемся окне (рис. 287) будет представлена информация о ходе выполнения проверки.

Ход выполнения проверки

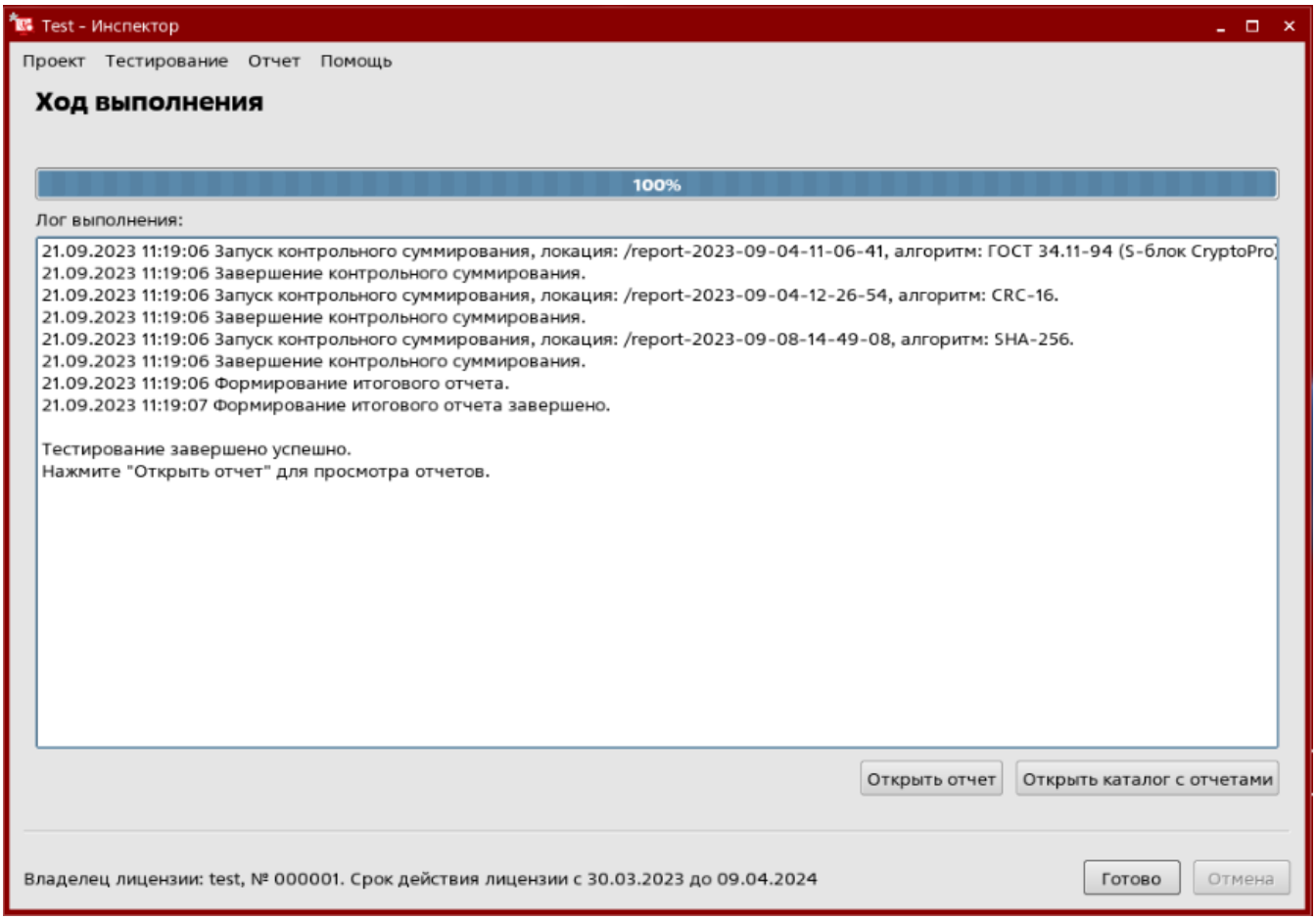


Рис. 287

После завершения проверки для просмотра отчета нужно нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробное описание генерации отчетов приведено в п. 7.4 настоящего руководства).

Для возврата к списку инструментов нужно нажать кнопку «Готово».

7.3.3. Системный аудит

Для запуска инструмента «Системный аудит» необходимо установить соответствующую галочку, нажав на пиктограмму или название инструмента, и нажать кнопку «Вперед» (рис. 260). В открывшемся окне будет показана информация о проекте (рис. 288). Для начала проверки устройств и программного обеспечения нужно нажать кнопку «Вперед».

Информация о проекте

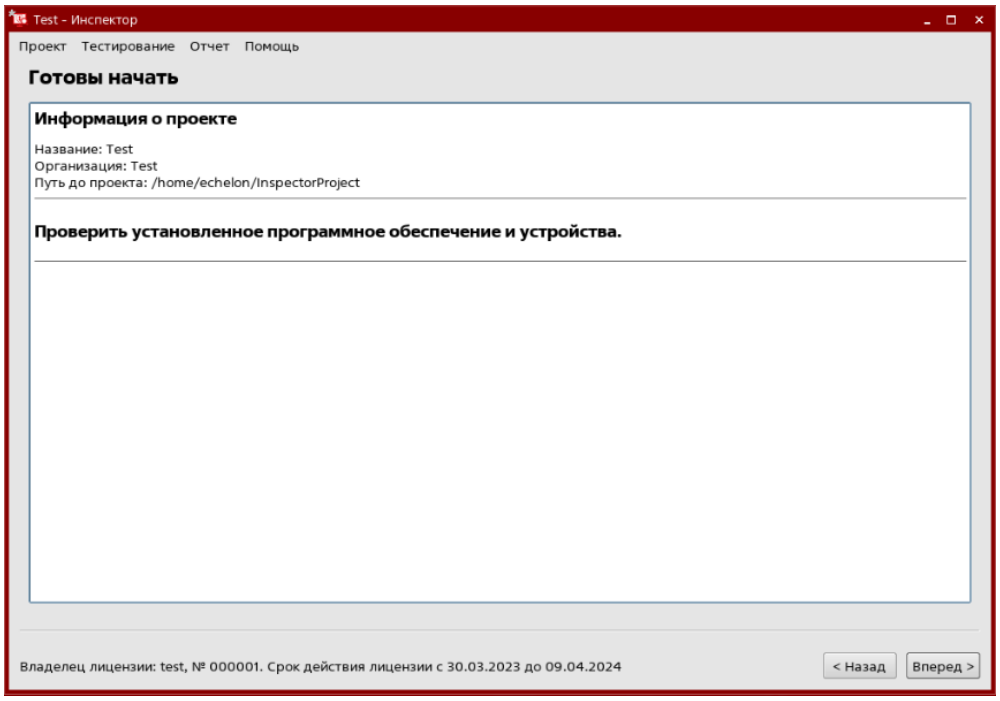


Рис. 288

В открывшемся окне будет представлена информация о ходе выполнения проверки (рис. 289).

Ход выполнения проверки

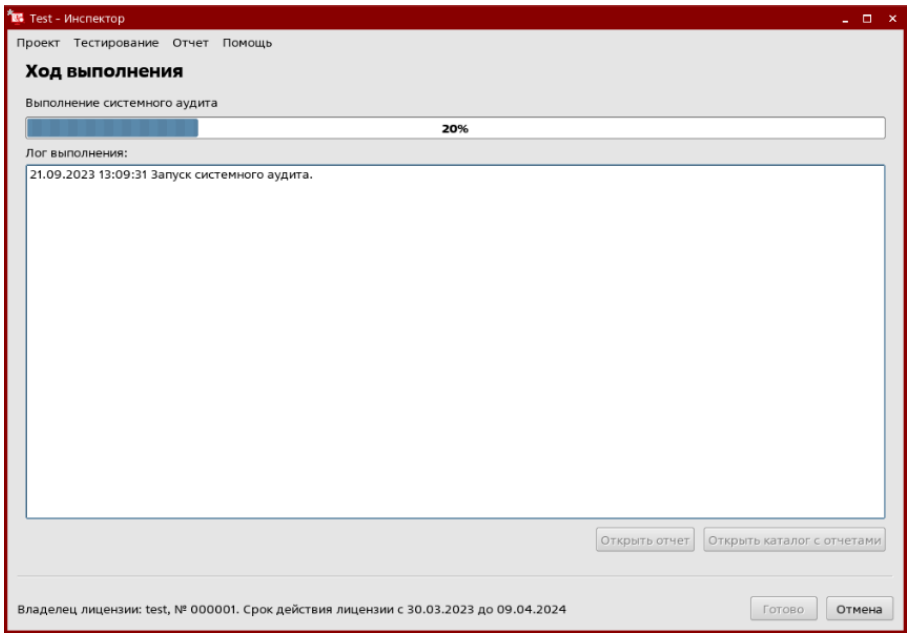


Рис. 289

После завершения проверки для просмотра отчета нужно нажать кнопку «Открыть отчет» или «Открыть каталог с отчетами» (подробное описание генерации отчетов приведено в п. 7.4 настоящего руководства).

Для возврата к списку инструментов нужно нажать кнопку «Готово».

7.3.4. Проверка прав доступа

Для запуска инструмента «Проверка прав доступа» необходимо установить соответствующую галочку нажатием на пиктограмму или название инструмента, и нажать «Вперед» (рис. 260). Откроется рабочее окно инструмента «Проверка прав доступа» компонента «Инспектор» (рис. 290).

Рабочее окно инструмента разделено на четыре области. В верхней части рабочего окна расположены слева направо области: дерево каталогов, перечень проверяемых файлов и (или) каталогов, список пользователей. В нижней части рабочего окна расположена область модели доступа. По умолчанию на основании ресурсов и настроек проверяемой рабочей станции заполнены области: дерево каталогов и список пользователей.

Рабочее окно инструмента «Проверка прав доступа»

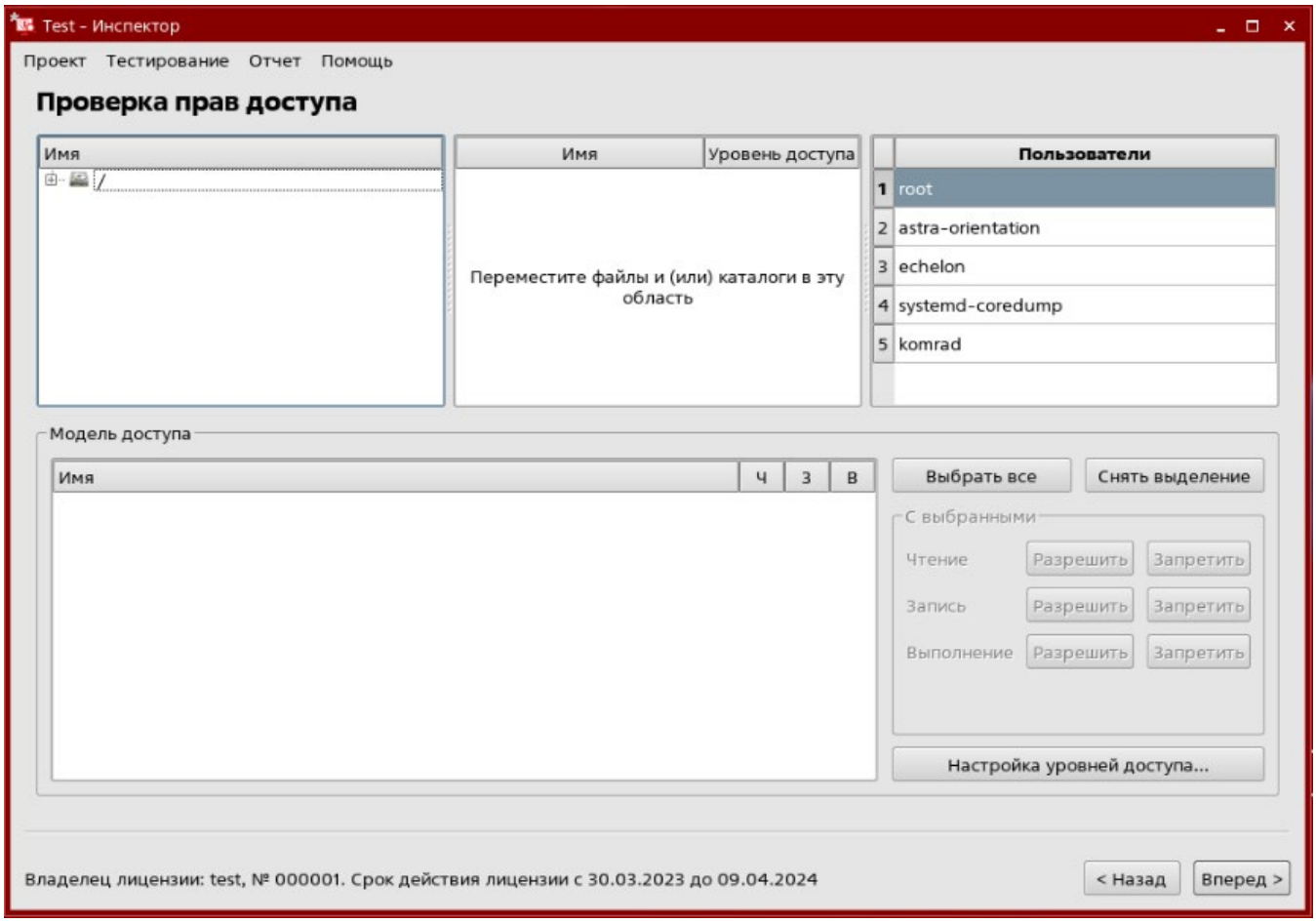


Рис. 290

Для изменения (удаления и / или добавления новых) уровней (сессий) необходимо нажать кнопку «Настройка уровней доступа». В открывшемся окне нужно переименовать сессии по умолчанию и / или удалить выделенные с помощью кнопки «Удалить выбранные», и / или добавить новые с помощью кнопки «Добавить» (рис. 291). Максимально можно создать двадцать уровней (сессий).

Примечание. Изменить уровни доступа необходимо до выбора проверяемых объектов.

Окно «Настройка уровней доступа»

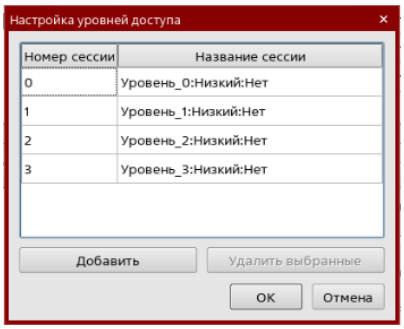


Рис. 291

Для добавления каталога в перечень проверяемых необходимо найти его в дереве каталогов и переместить в соответствующее поле (уровень доступа по умолчанию – 0), одновременно с этим в таблице прав доступа появятся текущие права для текущего пользователя (чтение (Ч), запись (З), выполнение (В)) (рис. 292).

Список каталогов в перечне проверяемых объектов

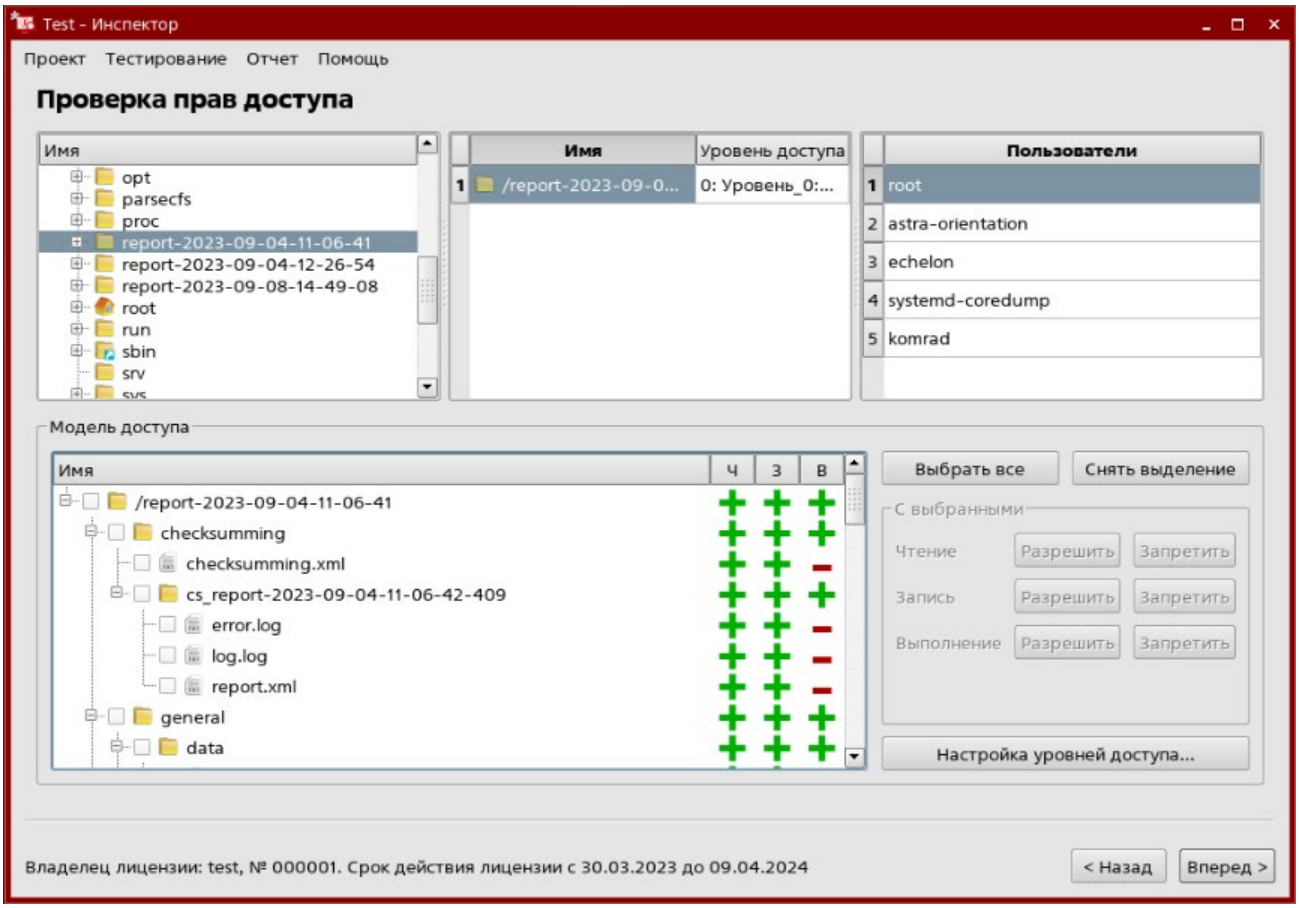


Рис. 292

Также добавить объекты можно с помощью двойного клика левой кнопкой мыши. Для удаления каталога из перечня проверяемых необходимо выделить его и нажать на клавиатуре клавишу «Delete».

В перечне проверяемых каталогов можно установить уровень доступа, для которого строится модель. Смена сессии происходит нажатием левой кнопкой мыши на ячейку столбца «Уровень доступа». Одновременно можно построить несколько моделей доступа (для различных файлов и пользователей в различных сессиях).

Примечание. Если нажать «Вперед», не добавив объект для тестирования прав, появится соответствующая всплывающая подсказка.

Если для какого-либо пользователя проверка прав не нужна, его можно удалить из списка, выделив его и нажав на клавишу «Delete». Для восстановления списка пользователей по умолчанию нужно нажать правой кнопкой мыши в области списка пользователей, вызвав контекстное меню, и выбрать «Загрузить пользователей из ОС» (рис. 293).

Чтобы добавить пользователя, необходимо нажать правой кнопкой мыши в области списка пользователей, вызвав контекстное меню, и выбрать пункт «Добавить» (рис. 293). В открывшемся окне (рис. 294) укажите имя пользователя и нажмите кнопку «ОК». Чтобы добавить пользователя в окне «Добавление пользователя» необходимо указать его имя и нажать кнопку «ОК» (рис. 294).

Обновление списка пользователей

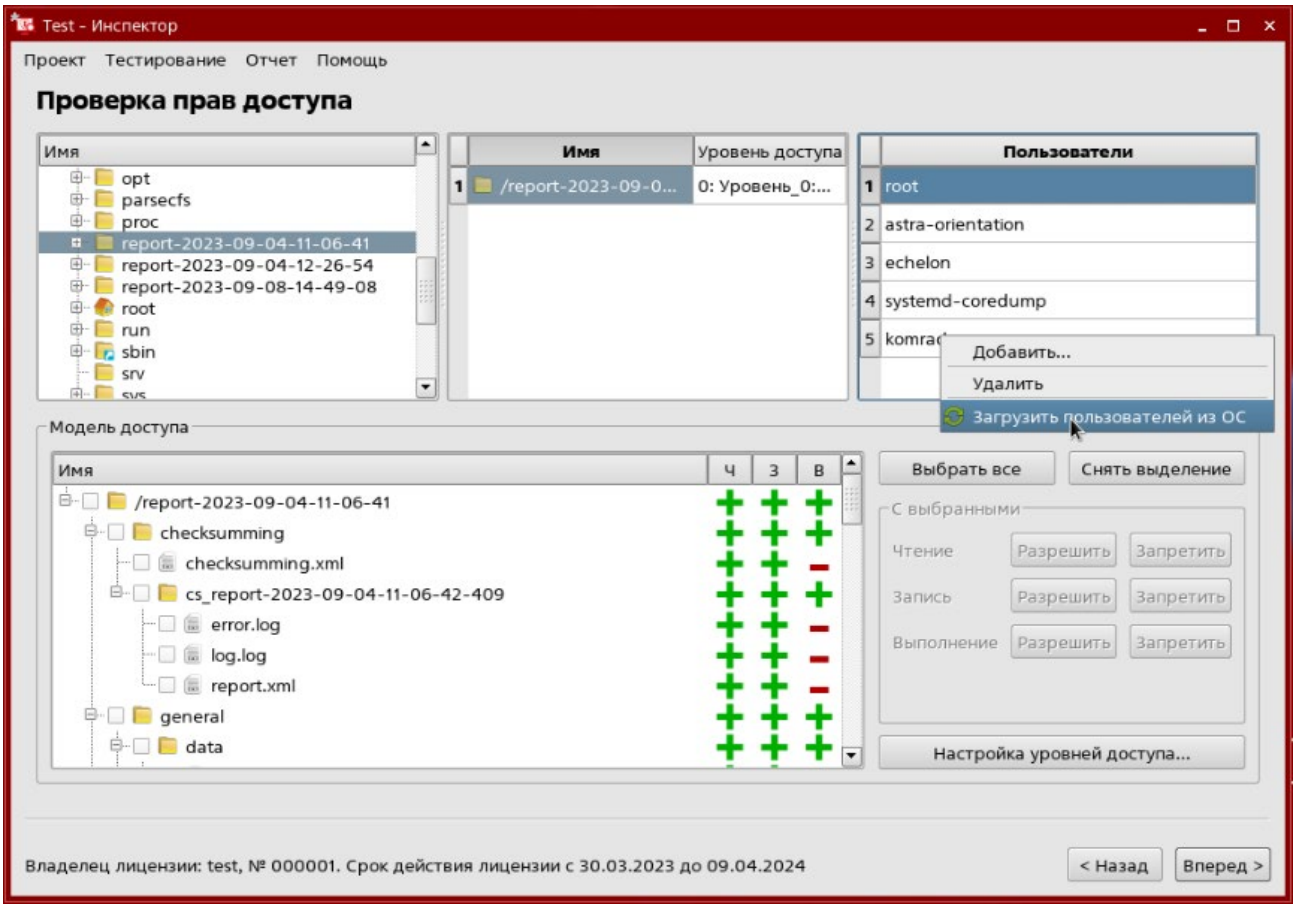


Рис. 293

Добавление пользователя

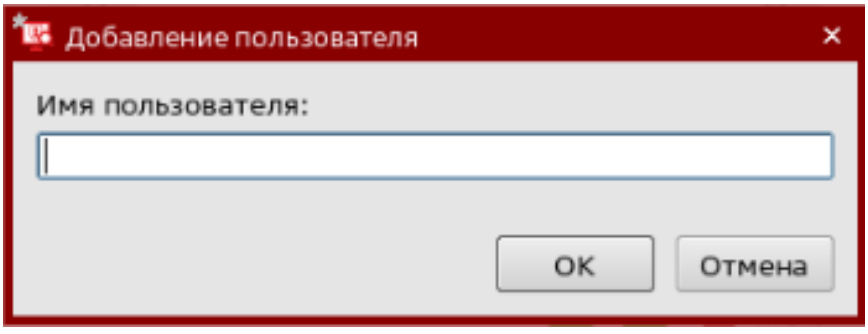


Рис. 294

7.3.4.1. Построение модели прав доступа

Построение модели прав доступа происходит путем редактирования в перечне проверяемых объектов прав доступа пользователей к файлам и каталогам рабочей станции. Это осуществляется путем нажатия кнопок «Разрешить» и «Запретить» напротив соответствующего права доступа, выделенного галочкой объекта. Также изменять права доступа пользователя можно в области «Модель доступа», нажимая на «+» и «-».

В нижнем правом углу окна расположена панель для редактирования прав доступа всех выбранных объектов. Чтобы отметить все файлы всех каталогов нужно нажать «Выбрать все», чтобы отменить выбор всех файлов нужно нажать «Снять выделение». Далее с помощью кнопок «Разрешить / Запретить» необходимо установить права доступа для всех отмеченных файлов.

7.3.4.2. Тестирование прав доступа

Для тестирования прав доступа после построения модели прав доступа необходимо нажать кнопку «Вперед» (рис. 293).

Откроется новое окно с информацией о настройках проекта (рис. 295). В случае обнаружения ошибки в настройках тестирования необходимо нажать кнопку «Назад» и скорректировать настройки. Если все данные верны, для начала тестирования нужно нажать кнопку «Вперед».

Информация о проекте

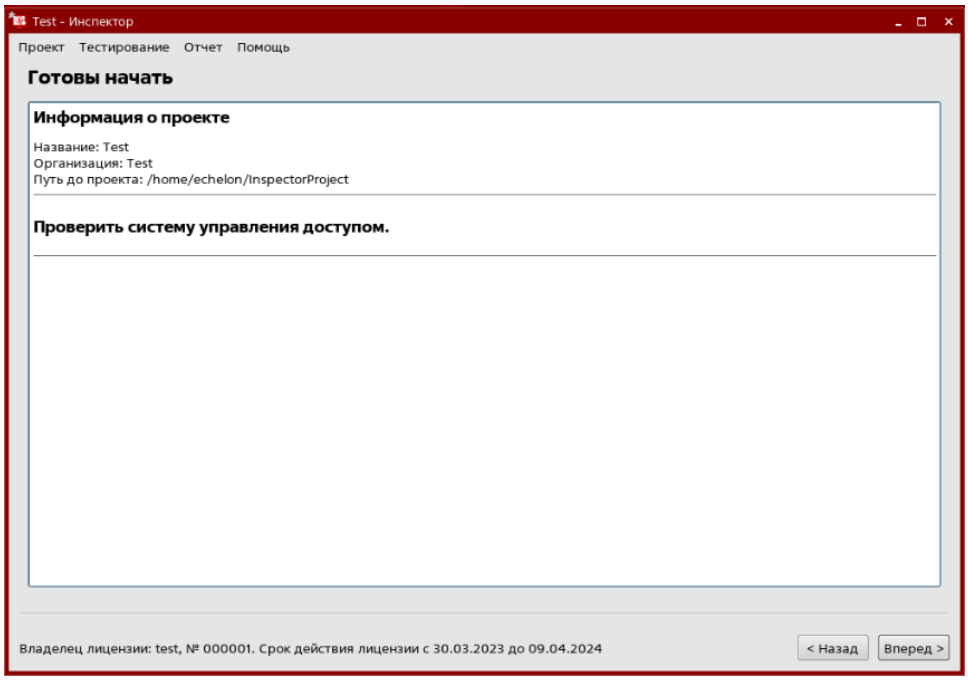


Рис. 295

В открывшемся окне будет представлена информация о ходе выполнения проверки (рис. 296).

Ход выполнения проверки

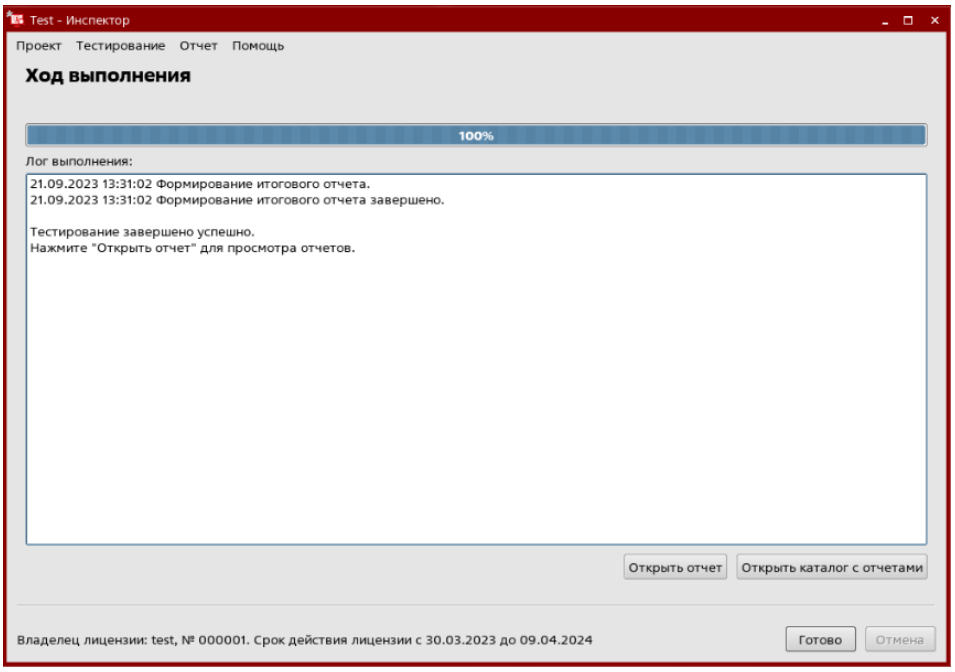


Рис. 296

После завершения тестирования необходимо запустить инструмент «Проверка прав доступа» для проверки прав доступа пользователей в различных сессиях к выбранным каталогам и файлам.

Для запуска инструмент необходимо выбрать в меню «Тестирование» инструмент «Проверка прав доступа» (рис. 297).

Подменю «Тестирование»

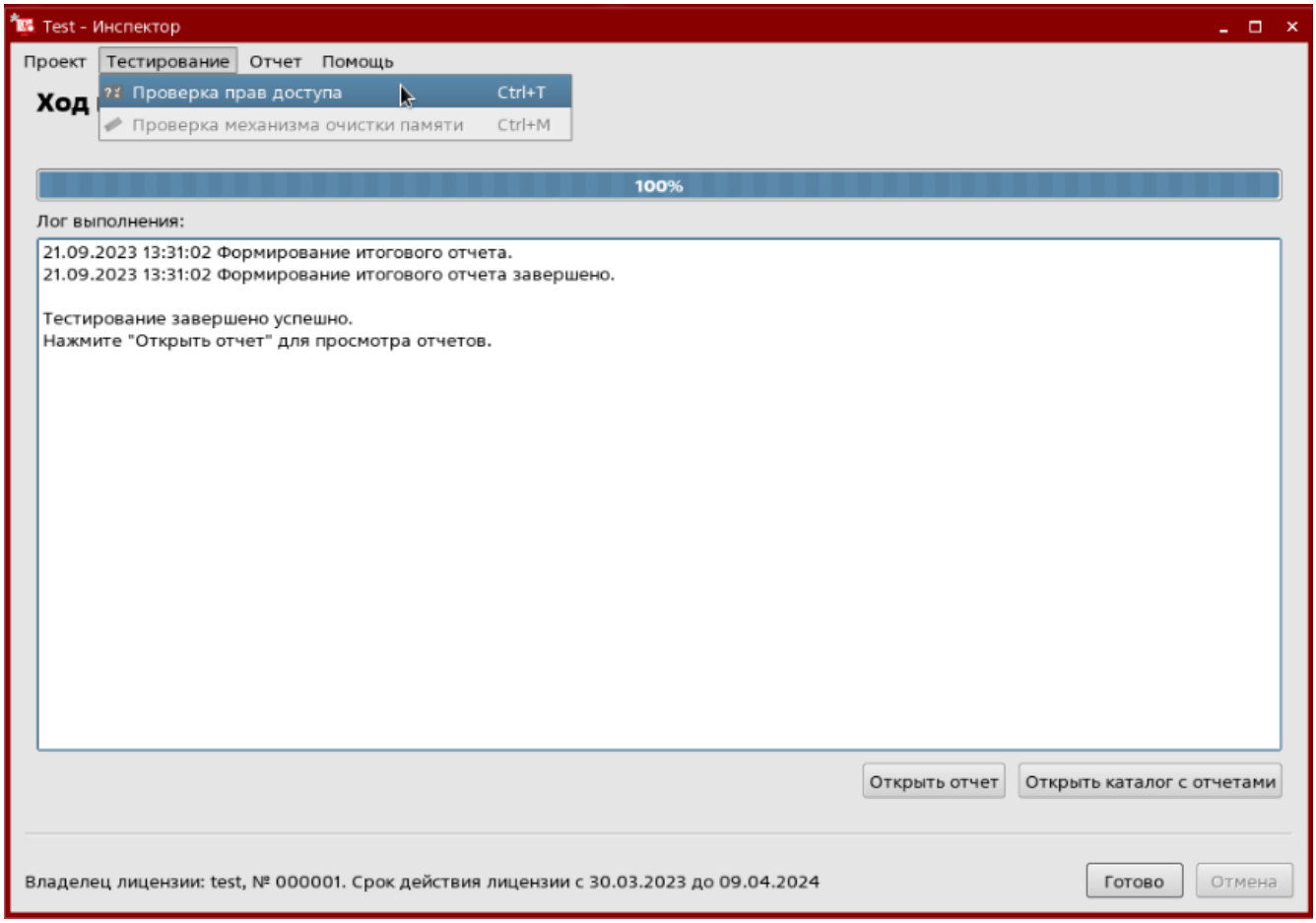


Рис. 297

В открывшемся окне необходимо указать текущий уровень сессии и пользователей для проведения проверки, после чего нажать кнопку «Проверить доступ» (рис. 298).

Выбор уровня сессии и пользователей для проверки

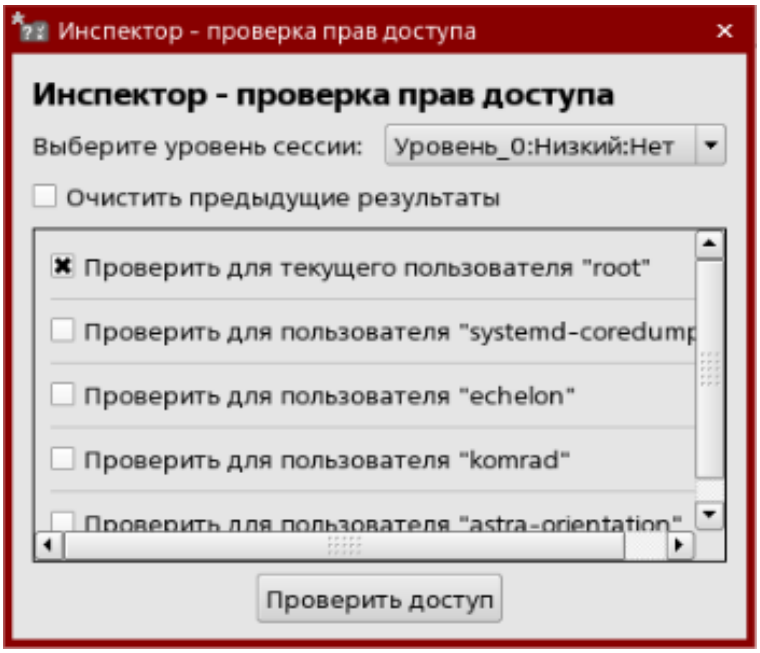


Рис. 298

После проведения тестирования появится соответствующее сообщение (рис. 299).

Сообщение

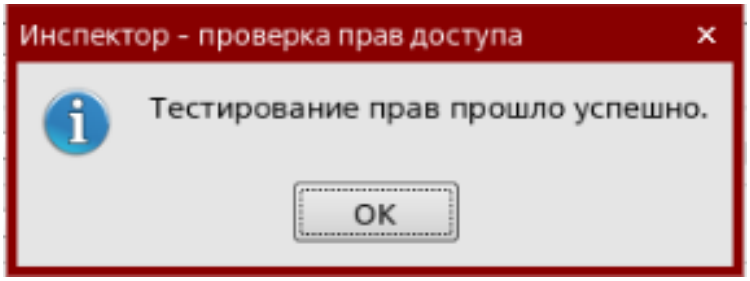


Рис. 299

Необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробное описание генерации отчетов приведено в п. 7.4 настоящего руководства).

Для возврата к списку инструментов необходимо нажать кнопку «Готово».

7.4. Отчеты

7.4.1. Генерация отчетов

Итоговый отчет строится автоматически. Сгенерированный отчет разделен на вкладки с результатами работы каждого задействованного инструмента (рис. 300).

Общий вид отчета

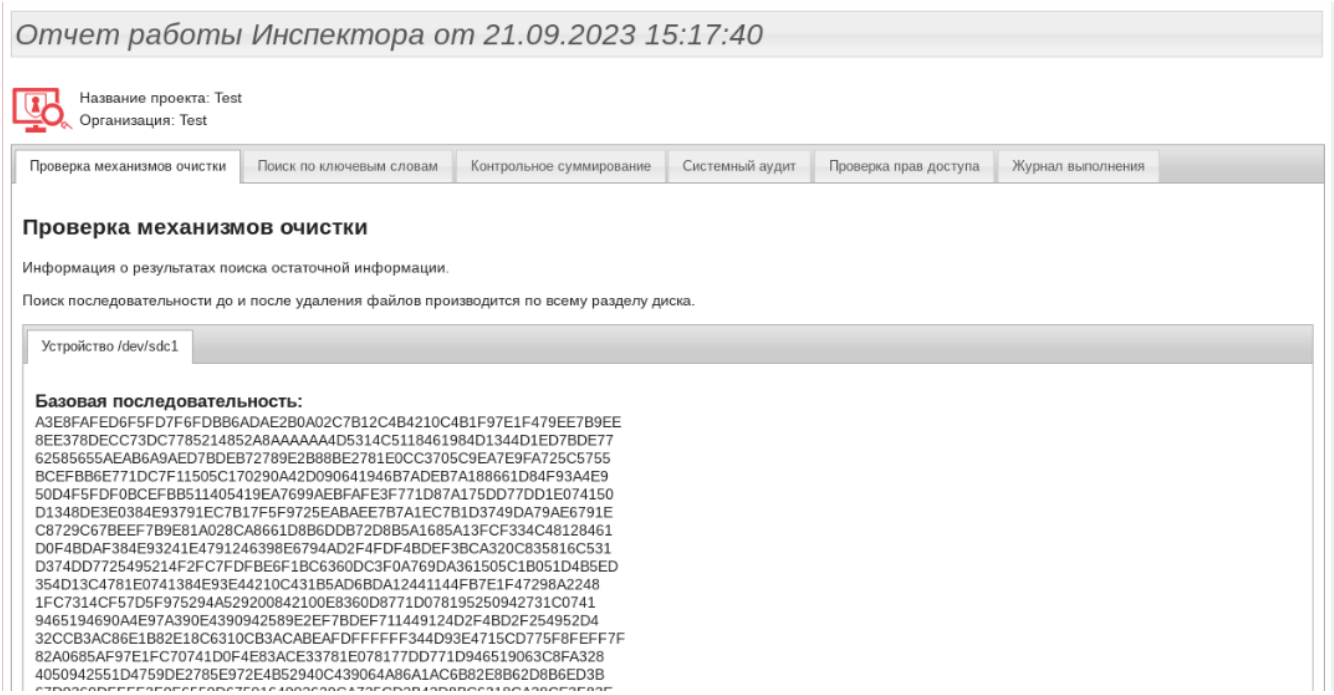


Рис. 300

7.4.1.1. Отчет инструмента «Проверка механизмов очистки»

Отчет инструмента «Проверка механизмов очистки» может состоять из вкладок «Проверка механизмов очистки» и / или «Поиск по ключевым словам». Вкладка «Проверка механизмов очистки» состоит из вкладок с данными о проверке устройств и / или с данными о проверке оперативной памяти (рис. 300).

В отчете о тестировании механизмов очистки устройства показана базовая последовательность, которая использовалась для тестирования. Под базовой последовательностью расположена таблица с данными о тестовых файлах и данными поиска. В столбце «Статус» показан итоговый результат тестирования (рис. 300).

Во вкладке «Оперативная память» (данная вкладка присутствует в итоговом отчете в том случае, если проводилась проверка механизма очистки оперативной памяти) содержится итоговый статус проверки механизмов очистки оперативной памяти.

Во вкладке «Поиск по ключевым словам» представлены параметры поиска и его результаты. Результаты оформлены в виде таблицы со столбцами: номер, найденное ключевое слово, кодировка, тип, локация и смещение (рис. 301).

Отчет поиска по ключевым словам

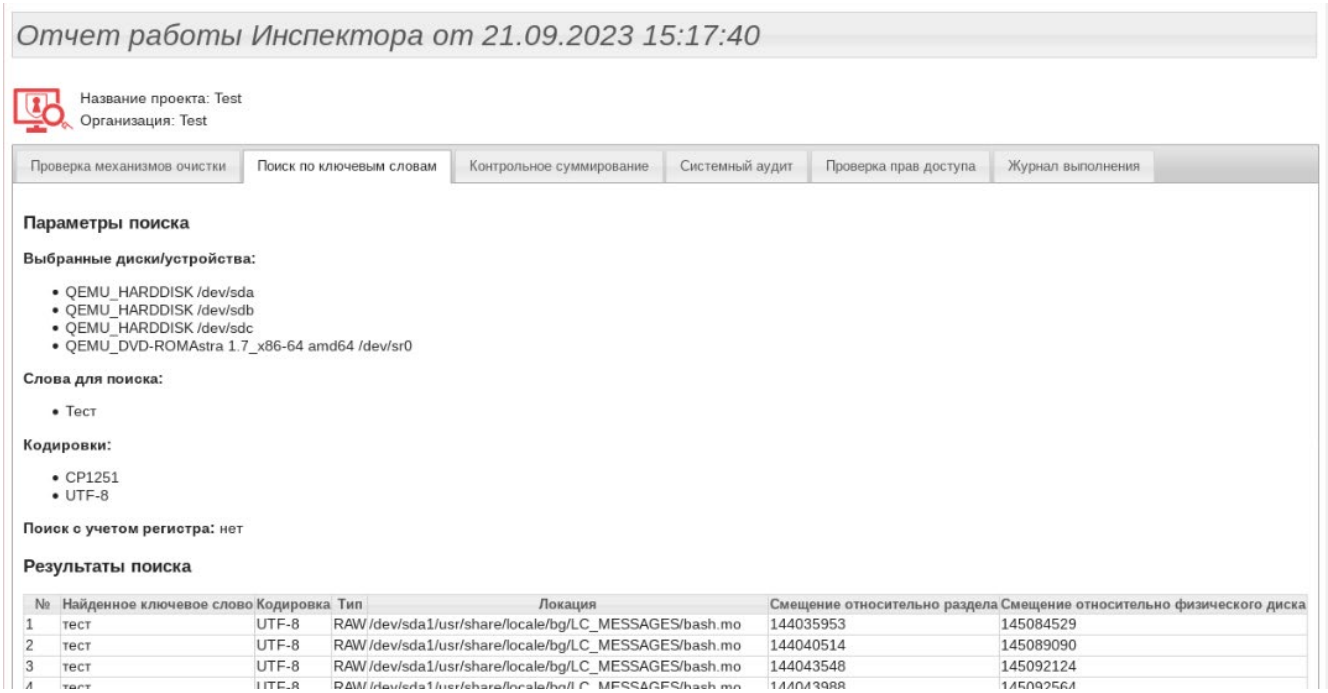


Рис. 301

7.4.1.2. Отчет инструмента «Контрольное суммирование»

Результаты контрольного суммирования оформлены в виде таблицы, где указаны порядковый номер, имя файла, его размер, время создания и изменения, алгоритм подсчета и контрольная сумма файла (рис. 302).

Отчет о контрольном суммировании

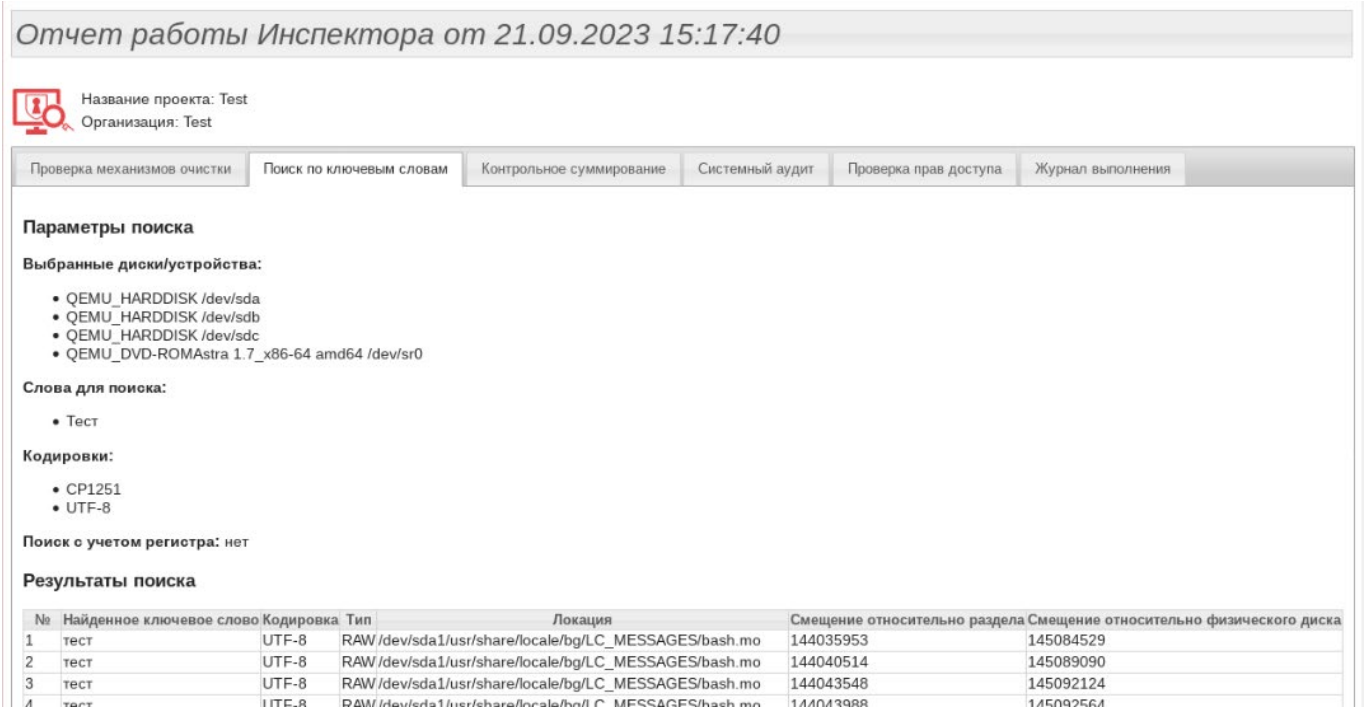


Рис. 302

7.4.1.3. Отчет инструмента «Системный аудит»

Отчет оформлен в виде таблиц и состоит из двух вкладок «Программная часть» и «Аппаратная часть» (рис. 303). Во вкладке «Программная часть» перечислены версия операционной системы, информация об установленных программах и пакетах, лицензионные номера установленных продуктов (рис. 303).

Отчет с результатами аудита рабочей станции

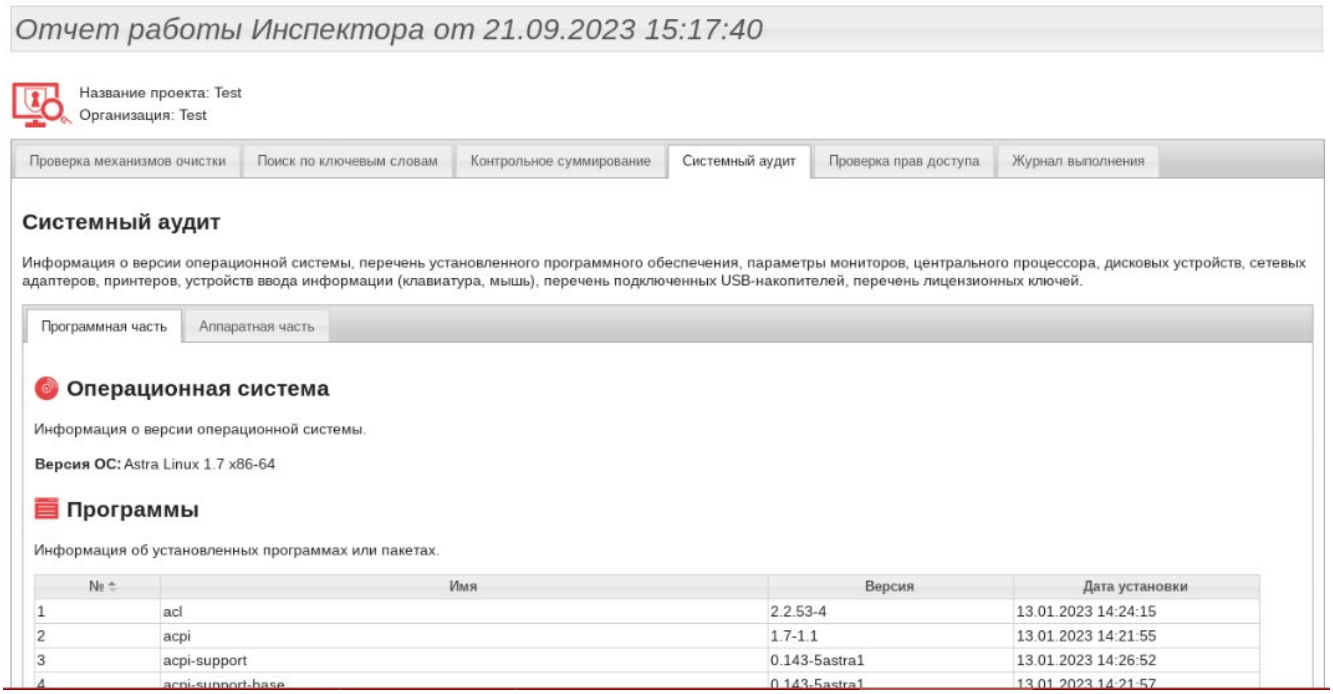


Рис. 303

Во вкладке «Аппаратная часть» перечислены данные о процессоре, дисковых устройствах, сетевых адаптерах, параметрах монитора, принтерах, устройствах ввода и USB-накопителях (рис. 304).

Информация об аппаратной части рабочей станции

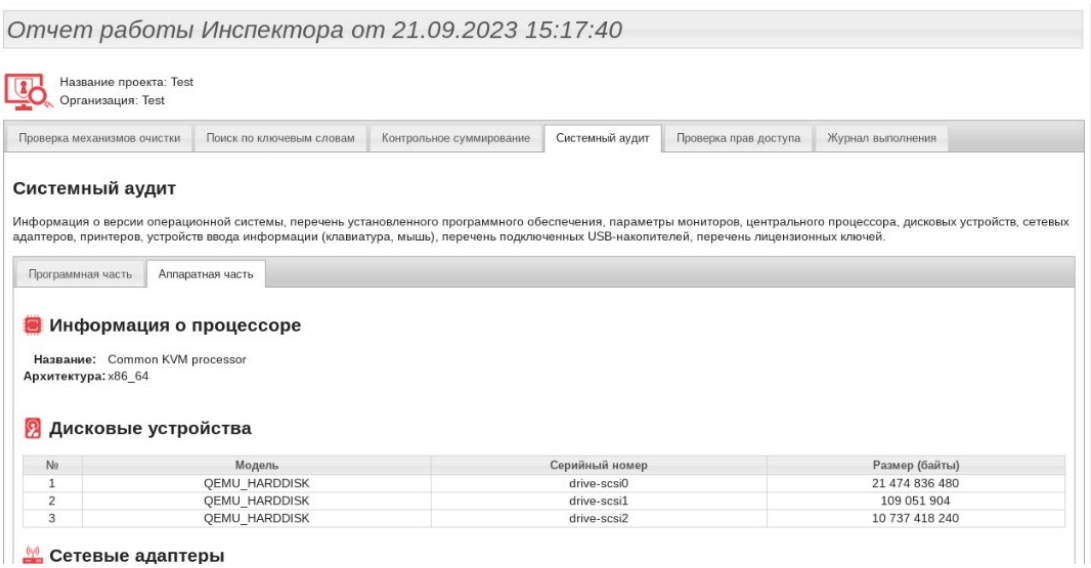


Рис. 304

7.4.1.4. Отчет инструмента «Проверка прав доступа»

Отчет состоит из вкладок, соответствующих уровням доступа, для которых проводилось тестирование. Результаты проверок отображаются в виде таблиц. На каждой вкладке каждому пользователю соответствует таблица.

Примечание. Если в процессе проверки прав доступа произошла ошибка (например, файл был удален), то в соответствующей ячейке будет знак «?».

7.4.1.5. Журналирование

Во вкладке «Журнал выполнения» содержится информация о ходе проведения тестирования (рис. 305).

Вкладка «Журнал выполнения»

Рис. 305

7.4.2. Сравнение отчетов

В компоненте «Инспектор» реализована функция сравнения отчетов работы инструментов «Контрольное суммирование» и «Системный аудит».

Для сравнения отчетов необходимо выбрать в меню «Отчет» функцию «Сравнение отчетов» (рис. 263). Откроется окно «Инспектор – сравнение отчетов» (рис. 306).

Окно «Инспектор – сравнение отчетов»

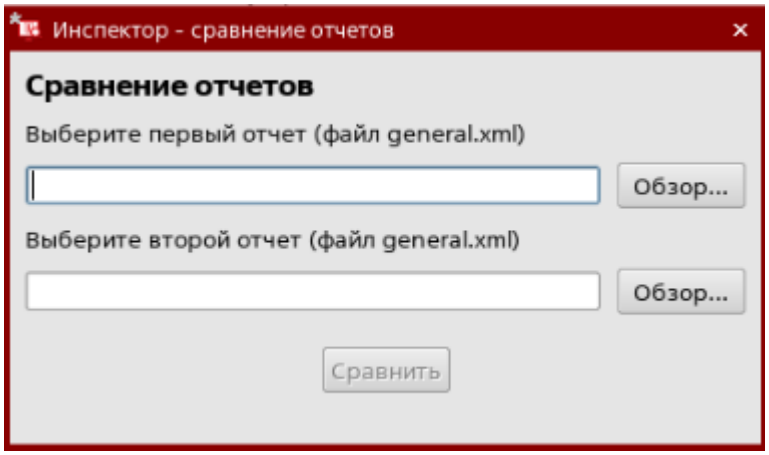


Рис. 306

Далее необходимо указать отчеты для сравнения и нажать кнопку «Сравнить» (рис. 307).

Выбор отчетов для сравнения

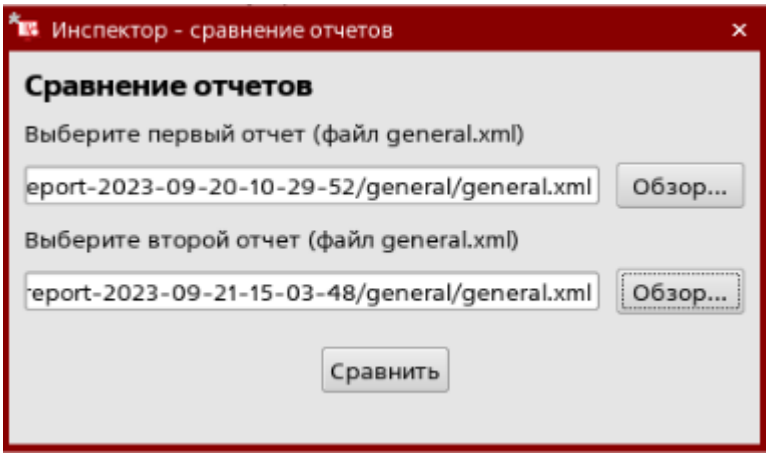


Рис. 307

В результате успешного сравнения отчетов откроется окно с соответствующим сообщением (рис. 308).

Сообщение

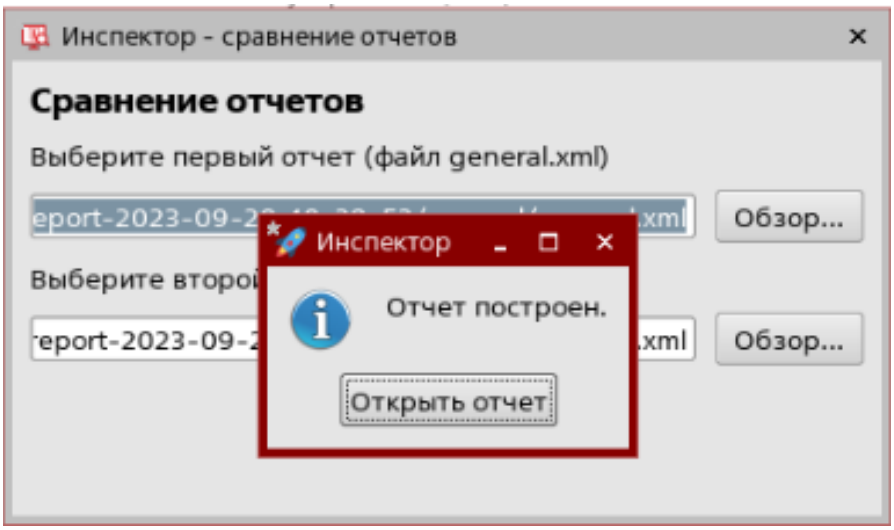


Рис. 308

После нажатия кнопки «Открыть отчет» (рис. 308) откроется отчет с результатами сравнения.

7.5. Завершение работы

Для выхода из компонента «Инспектор» необходимо выбрать в подменю «Проект» параметр «Выход» либо нажать на «крестик» в верхнем правом углу рабочего окна.

8. СООБЩЕНИЯ ОПЕРАТОРУ

Тексты сообщений, выдаваемых пользователю в ходе функционирования Сканер-ВС, представлены в таблице 6.

Таблица 6 – Сообщения пользователю

Сообщение	Описание
«Доступ запрещен»	Данное сообщение появляется в случае, если учетная запись, с помощью которой пользователь пытается пройти авторизацию, не существует либо заблокирована (не активна), а также в случае ввода неверных данных аутентификации
«Пароль не может быть пустым»	Данное сообщение появляется при попытке авторизации в Сканер-ВС с пустым полем «Пароль»
«Логин не может быть пустым»	Данное сообщение появляется при попытке авторизации в Сканер-ВС с пустым полем «Логин»
«Логин не может быть пустым. Пароль не может быть пустым»	Данное сообщение появляется при попытке авторизации в Сканер-ВС с пустыми полями «Логин» и «Пароль» одновременно
«Отчет создан успешно»	Данное сообщение появляется при генерировании нового отчета и сигнализирует об успешном завершении процесса его создания
«Карта сети создана успешно»	Данное сообщение появляется при создании новой карты сети и сигнализирует об успешном завершении процесса ее создания
«Словарь создан успешно»	Данное сообщение появляется при создании нового пользовательского словаря и сигнализирует об успешном завершении процесса его создания
«Удалено успешно»	Данное сообщение появляется в случае успешного создания какого-либо объекта Сканер-ВС
«Обязательное поле»	Сообщение в форме заполнения данных, сигнализирующее о том, что оно обязательно для заполнения
«Ошибка парсинга»	Сообщение в форме заполнения данных, сигнализирующее о том, что данные в нем не соответствуют требуемому формату
«Введенные пароли не совпадают»	Сообщение в форме заполнения данных, сигнализирующее о том, что пароли, введенные в полях «Пароль» и «Повтор пароля» не совпадают

Сообщение	Описание
«Network error»	Данное сообщение появляется в случае разрыва сетевого соединения
«permission denied»	Данное сообщение появляется в том случае, если пользователь Сканер-ВС обращается к функции, недоступной ему настройками ролевой модели разграничения доступа
«Что-то пошло не так»	Данное сообщение появляется в том случае, если по какой-либо причине произошла критическая ошибка в работе Сканер-ВС

ПРИЛОЖЕНИЕ 1. ИНСТРУКЦИЯ ИЗМЕНЕНИЯ ПОРЯДКА ЗАГРУЗКИ В UEFI И РАЗЛИЧНЫХ ТИПАХ BIOS ДЛЯ ЗАПУСКА С LIVE-НОСИТЕЛЯ

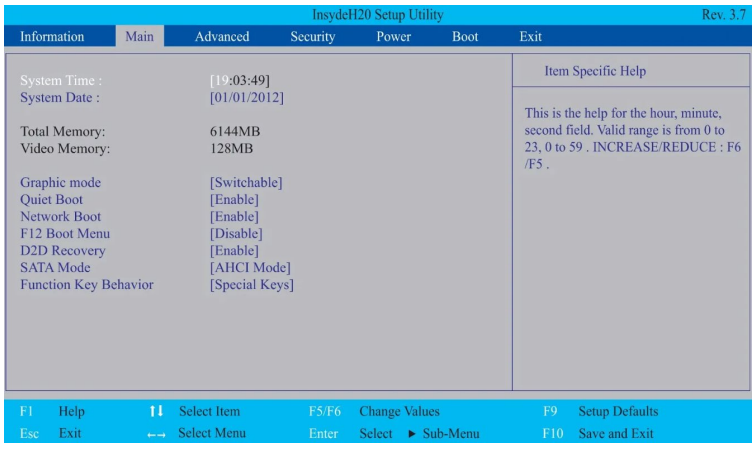
1.1 Вызов базовой системы ввода-вывода при старте изделия

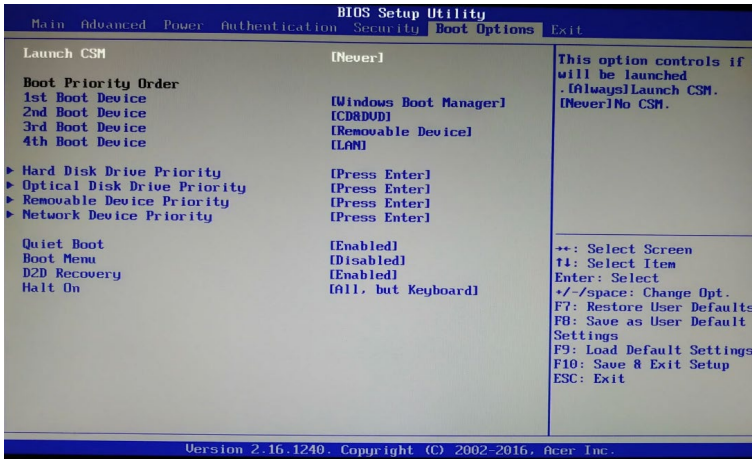
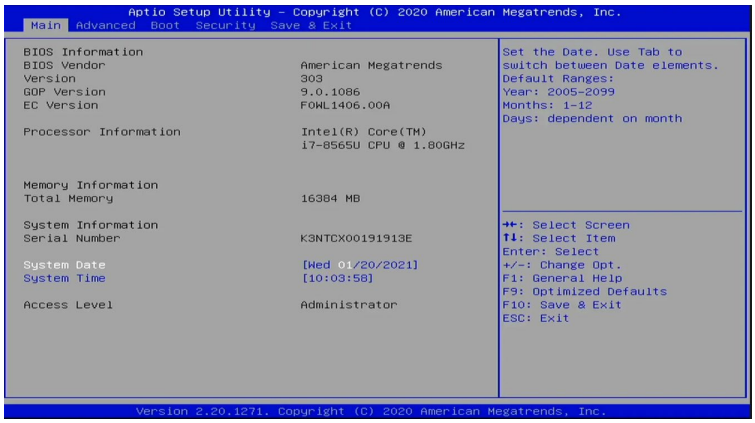
В данной инструкции описан процесс изменения приоритета загрузки для разных типов базовой системы ввода-вывода (далее – BIOS) и интерфейса UEFI.

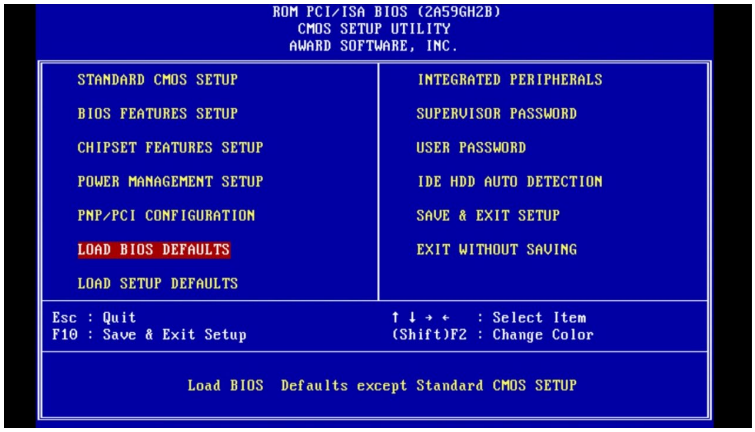
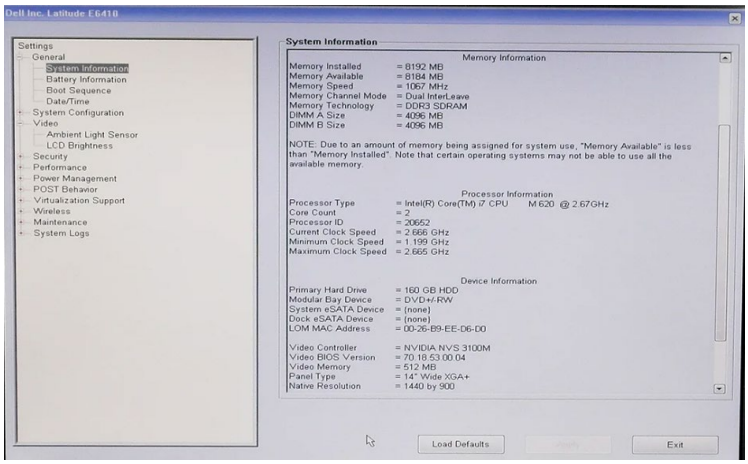
Экран BIOS и UEFI необходимо вызывать при старте системы до загрузки операционной системы изделия, нажав определенную клавишу – в зависимости от типа варианта BIOS / UEFI.

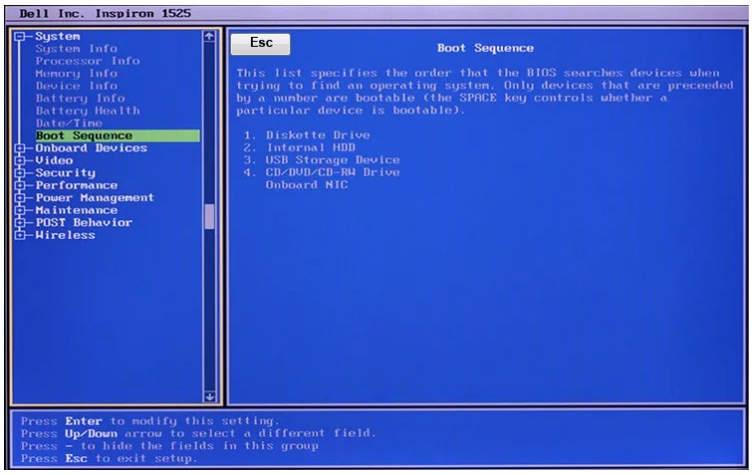
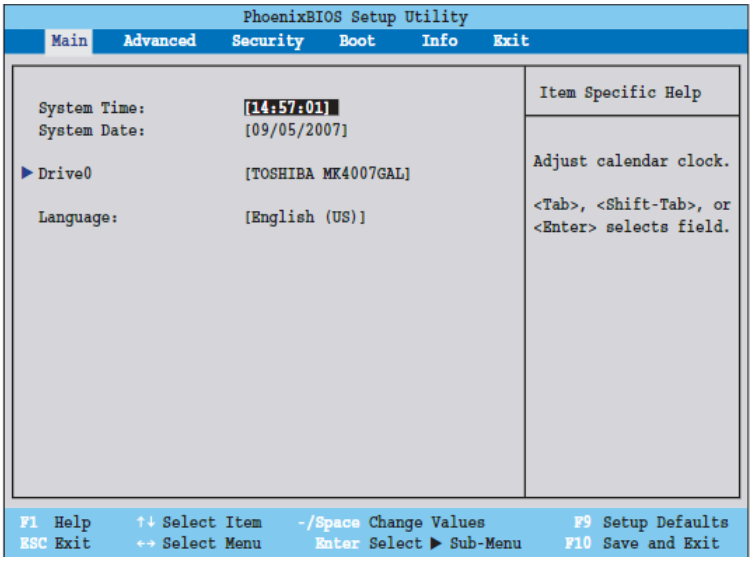
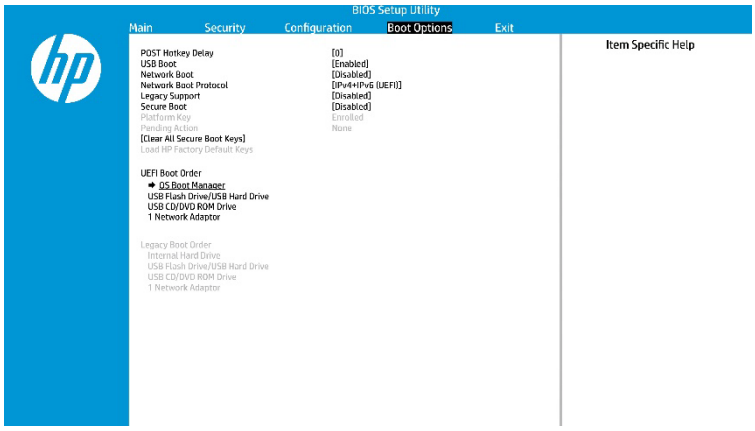
Таблица соответствия вариантов BIOS / UEFI и кнопок вызова на клавиатуре представлена в таблице 1.1 .

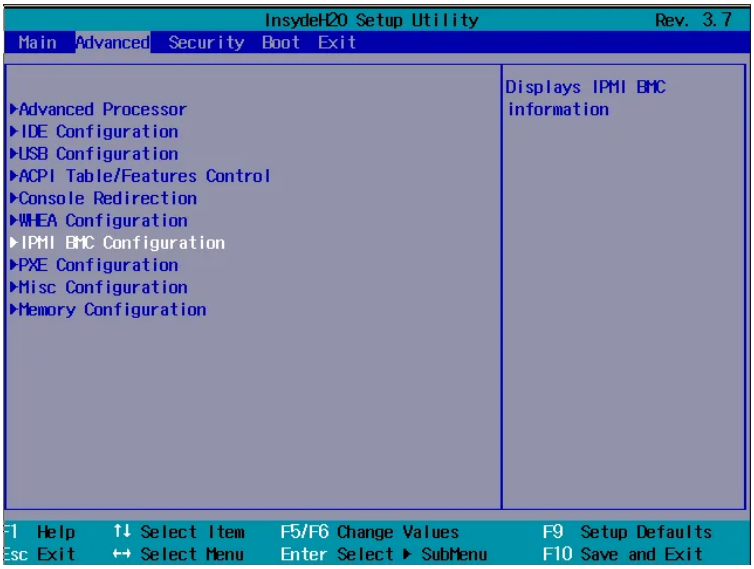
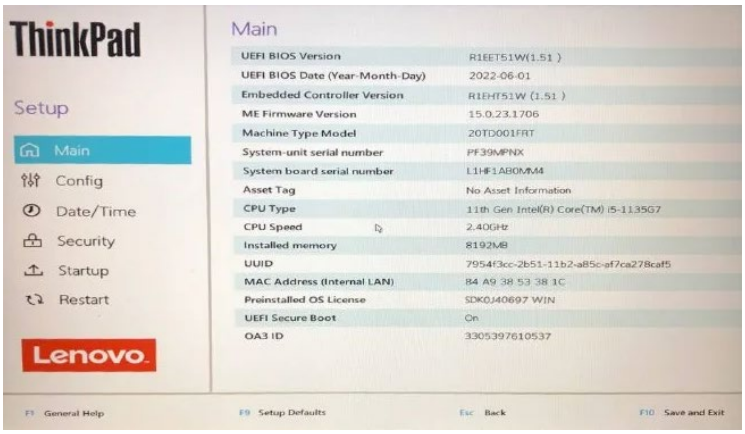
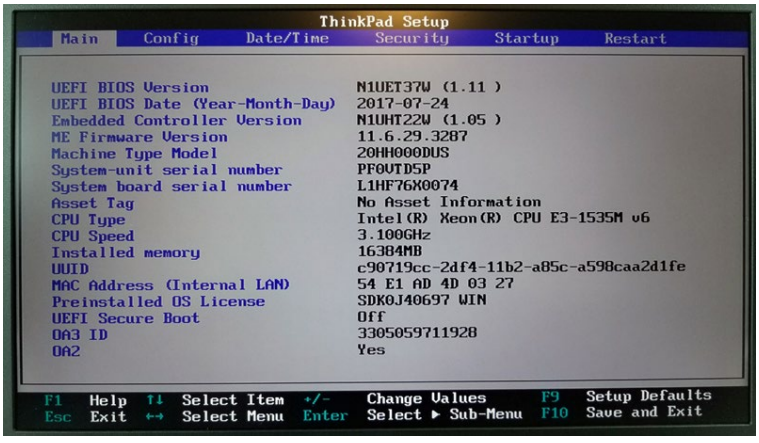
Таблица 1.1 – Соответствия вариантов BIOS / UEFI и кнопок вызова на клавиатуре

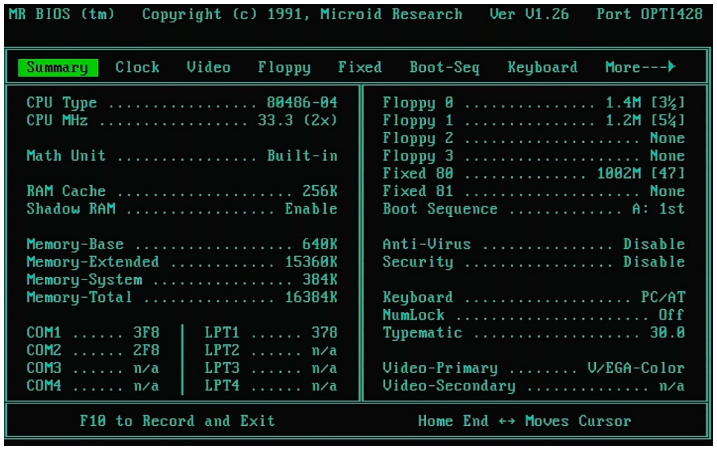
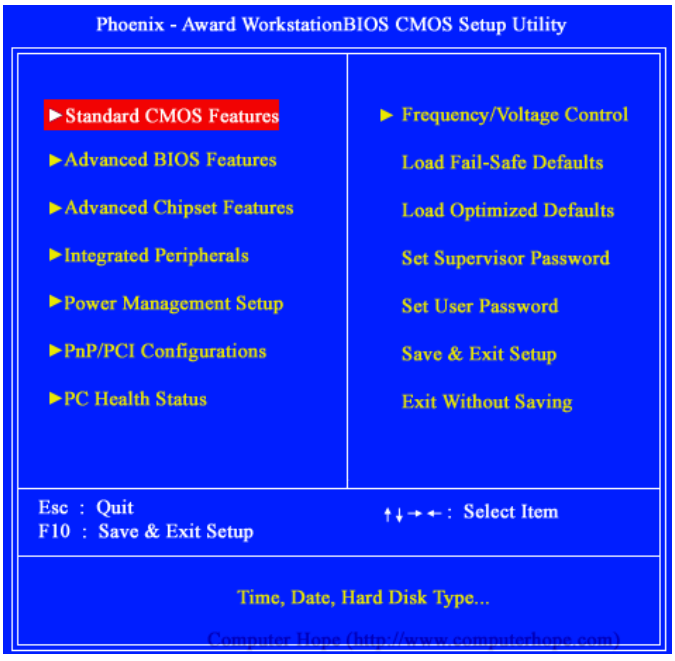
Название типа BIOS / UEFI или оборудования	**Вариант внешнего вида**	**Наиболее популярные кнопки вызова на клавиатуре**
Acer (Aspire, Power, Veriton, Extensa, Ferrari, TravelMate, Altos)		F2, DEL, Esc

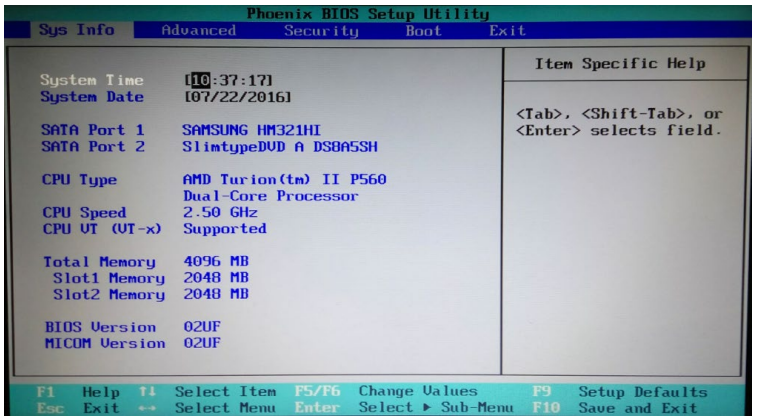
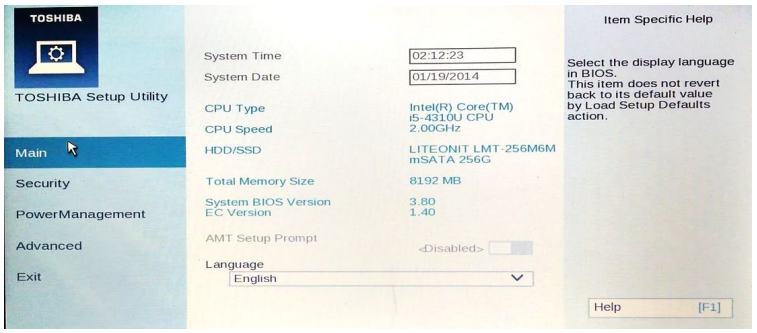
Название типа BIOS / UEFI или оборудования	Вариант внешнего вида	Наиболее популярные кнопки вызова на клавиатуре
Acer (старые версии)		F1, Ctrl+Alt+Esc
AMI (American Megatrends, Inc) BIOS		Del, F2, F1
Asus		Del, F2, F9

Название типа BIOS / UEFI или оборудования	Вариант внешнего вида	Наиболее популярные кнопки вызова на клавиатуре
ASRock		Del, F2
Award BIOS		Del, Ctrl+Alt+Esc
Dell (XPS, Dimension, Inspiron, Latitude. OptiPlex, Precision, Vostro)		F2, Del, у некоторых моделей Reset (нажать кнопку дважды)

Название типа BIOS / UEFI или оборудования	Вариант внешнего вида	Наиболее популярные кнопки вызова на клавиатуре
Dell (старые версии)		Fn+Esc, Fn+F1
Fujitsu		F12
Hewlett-Parkard (HP Pavilion, TouchSmart, Vectra, OmniBook, Tablet)		F9, F10

Название типа BIOS / UEFI или оборудования	Вариант внешнего вида	Наиболее популярные кнопки вызова на клавиатуре
Hewlett-Parkard (HP альтернативные версии)		F2, Esc
Lenovo (ThinkPad, IdeaPad, 3000 Series, ThinkCentre, ThinkStation)		F1, F2
Lenovo (старые версии)		Ctrl+Alt+F3, Ctrl+Alt+Ins, Fn+F1

Название типа BIOS / UEFI или оборудования	Вариант внешнего вида	Наиболее популярные кнопки вызова на клавиатуре
Microid Research MR BIOS		F1
MSI		Del, F2
Phoenix BIOS		Del, для старых моделей: Ctrl+Alt+Esc, Ctrl+Alt+S, Ctrl+Alt+Ins

Название типа BIOS / UEFI или оборудования	Вариант внешнего вида	Наиболее популярные кнопки вызова на клавиатуре
Samsung		Esc
Sony	–	F1, F2, F3
Toshiba (Portégé, Satellite, Tecra with Phoenix BIOS)		F1
Toshiba (Portégé, Satellite, Tecra)		Esc

Примечания:

1. Данные, представленные в таблице, могут отличаться от фактических так как предприятия-производители оборудования могут назначать и/или изменять внешний вид и клавиши вызова на свое усмотрение.

2. В некотором оборудовании для входа в настройки BIOS/UEFI, производители добавили нажатие клавиши Fn, например вместо клавиши F2, теперь нужно нажать сочетание клавиш Fn+F2.

ВНИМАНИЕ!

ВАРИАНТЫ НАСТРОЙКИ ИЗМЕНЕНИЯ ПОРЯДКА ЗАГРУЗКИ В UEFI И РАЗЛИЧНЫХ ТИПАХ BIOS **МОГУТ ОТЛИЧАТЬСЯ ОТ ПРЕДСТАВЛЕННЫХ** ДАЛЕЕ В ЗАВИСИМОСТИ ОТ ТИПА ВАРИАНТА BIOS / UEFI И РАЗРЕШЕННЫХ К ИЗМЕНЕНИЮ ВКЛАДОК НАСТРОЕК ПРЕДПРИЯТИЯ-ПРОИЗВОДИТЕЛЯ ИСПОЛЬЗУЕМОГО ОБОРУДОВАНИЯ.

НЕКОТОРЫЕ ВКЛАДКИ И НАСТРОЙКИ МОГУТ БЫТЬ ЗАБЛОКИРОВАНЫ / СКРЫТЫ ОТ ПОЛЬЗОВАТЕЛЯ. ДЛЯ РЕШЕНИЯ ПОДОБНЫХ СИТУАЦИЙ НЕОБХОДИМО ОБРАТИТЬСЯ К ВАШЕМУ СИСТЕМНОМУ АДМИНИСТРАТОРУ ИЛИ ПРЕДПРИЯТИЮ-ПРОИЗВОДИТЕЛЮ ИСПОЛЬЗУЕМОГО ОБОРУДОВАНИЯ.

1.2 Варианты настроек для изменения порядка загрузки в режиме UEFI и различных типах BIOS

1.2.1 BIOS типа AMI

Для настройки приоритета загрузки BIOS типа AMI необходимо выполнить следующие действия:

– перейти в раздел «Boot» (см. рис. 1.1);

Раздел «Boot» BIOS типа AMI

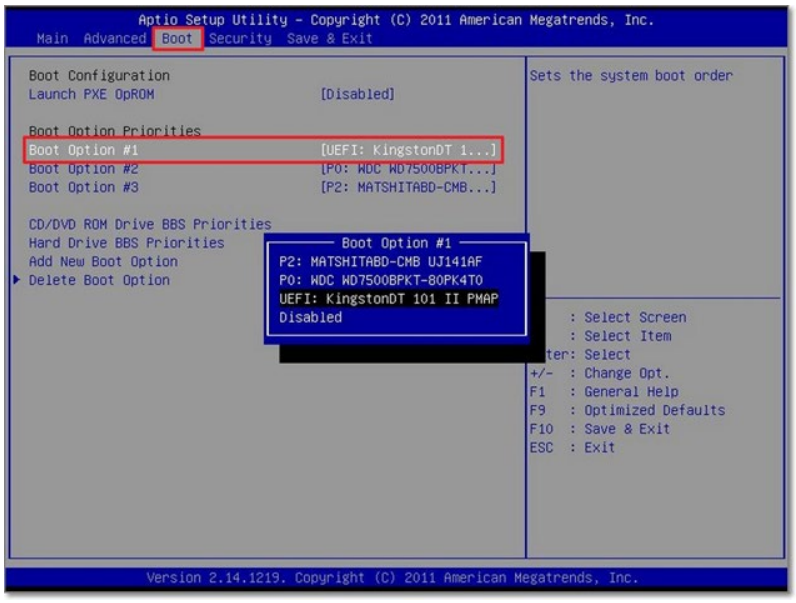


Рис. 1.1

– в данном разделе, в пункте «Boot Option Priorities», в поле «Boot Option #1» указать дисковод или внешний носитель, с которого необходимо загрузить изделие;

– перейти в раздел «Save & Exit» и выбрать пункт «Save Changes & Exit» (см. рис. 1.2);

Раздел «Save & Exit» BIOS типа AMI

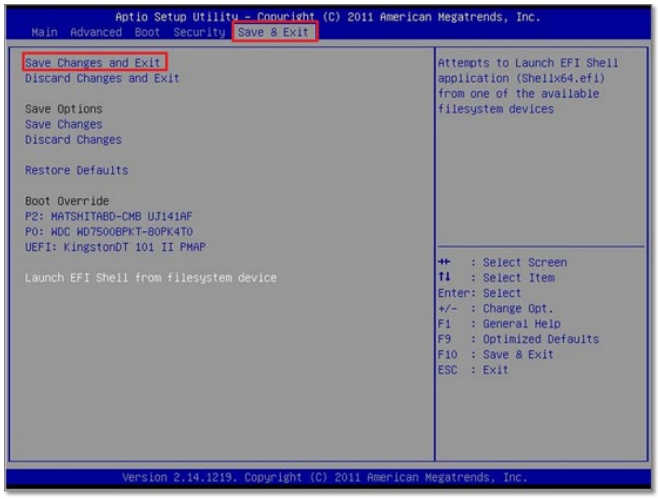


Рис. 1.2

– после перезагрузки изделия войти в BIOS и произвести дополнительные настройки при необходимости (если запуск с носителя не произошел автоматически после перезагрузки оборудования);

– перейти в раздел «Security», выбрать пункт «Secure Boot menu» и нажать клавишу «Enter» (см. рис. 1.3);

Раздел «Security» BIOS типа AMI

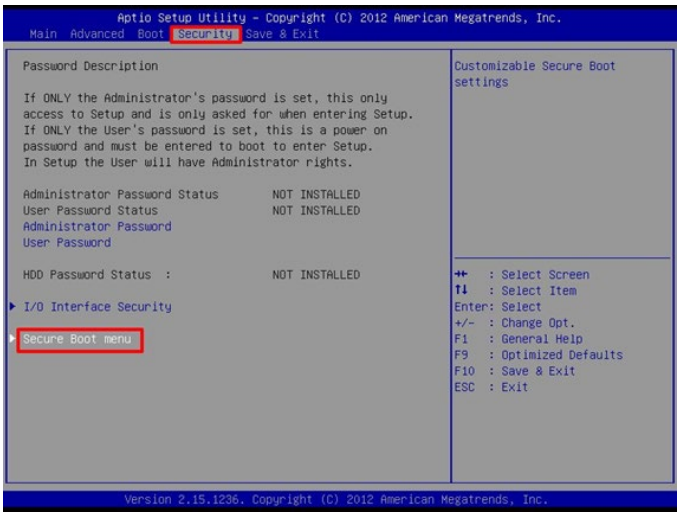


Рис. 1.3

– для отключения функции «Secure Boot Control» в выпадающем списке необходимо выбрать «Disabled» (см. рис. 1.4);

Управление опцией «Secure Boot Control» BIOS типа AMI

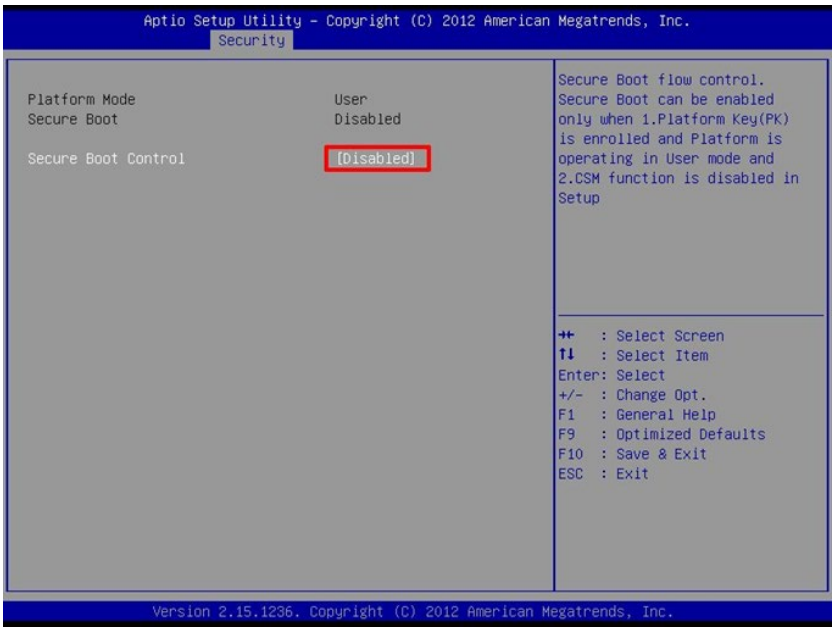


Рис. 1.4

– далее необходимо перейти во вкладку «Boot» и перевести функцию «Launch CSM» в состояние «Enabled» (см. рис. 1.5);

Включение функции «Launch CSM» BIOS типа AMI

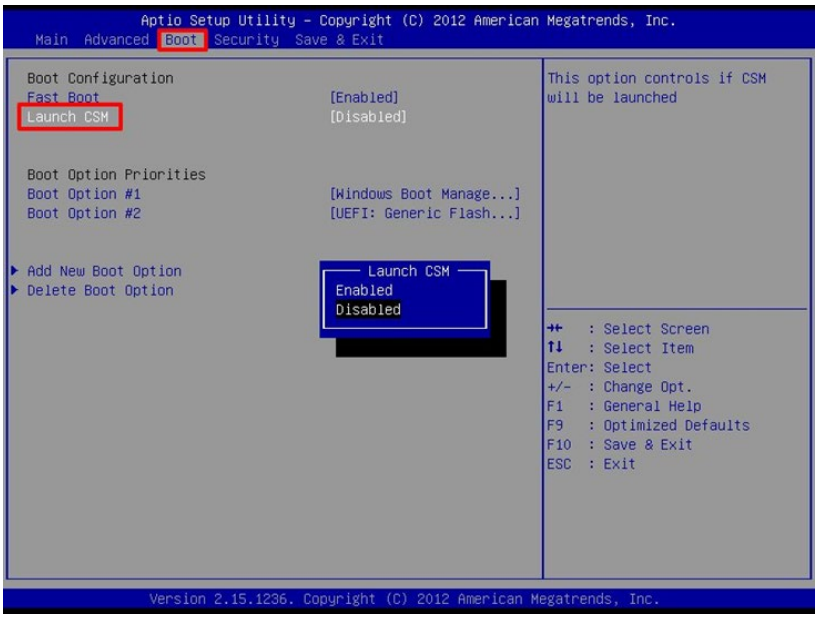


Рис. 1.5

– перейти в раздел «Save & Exit»;

– выбрать пункт «Save Changes & Exit» (см. рис. 1.2) для сохранения изменений.

1.2.2 BIOS типа AWARD, PHOENIX

Для настройки приоритета загрузки в BIOS типа AWARD или PHOENIX необходимо выполнить следующие действия:

– выбрать пункт меню «Advanced BIOS Features» (см. рис. 1.6);

– перейти к редактированию «First Boot Device»;

– указать дисковод или внешний носитель, с которого планируется загрузка изделия (см. рис. 1.7);

Раздел «Advanced BIOS Features»

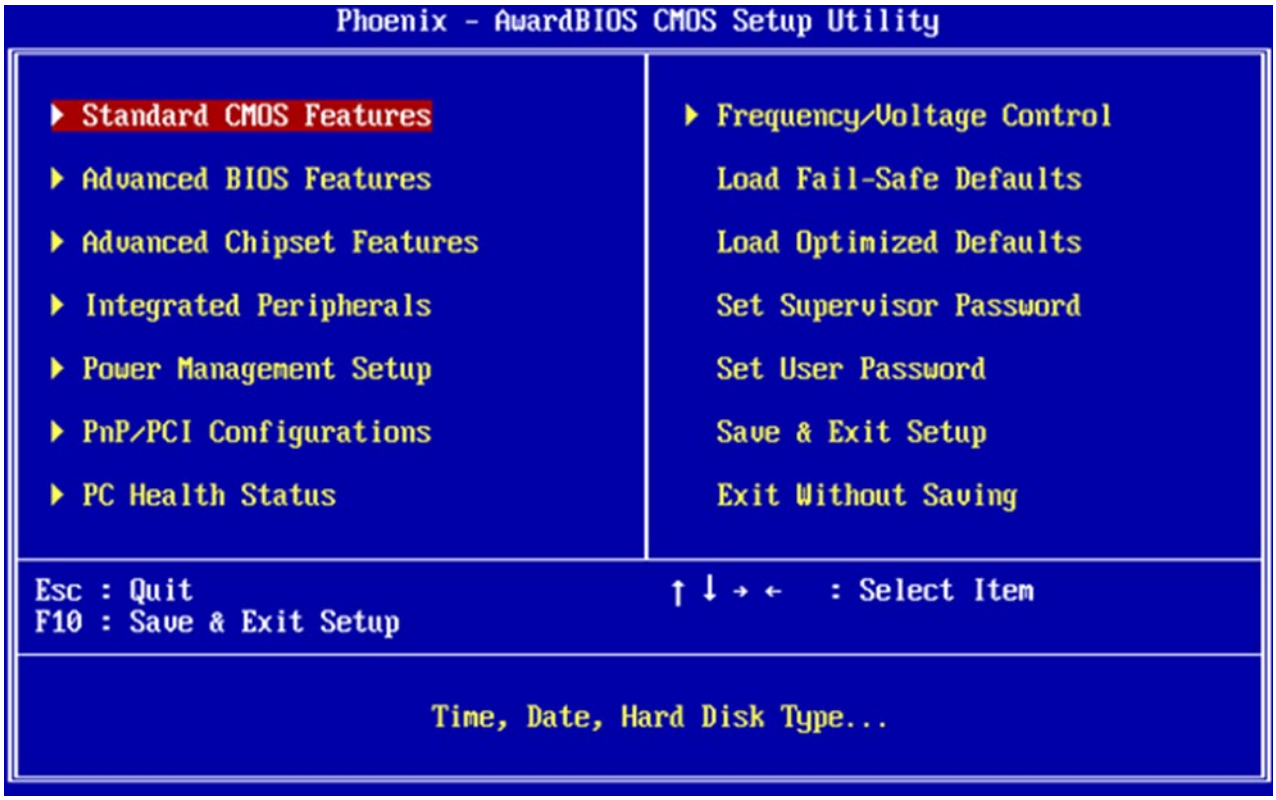


Рис. 1.6

Раздел «First Boot Device»

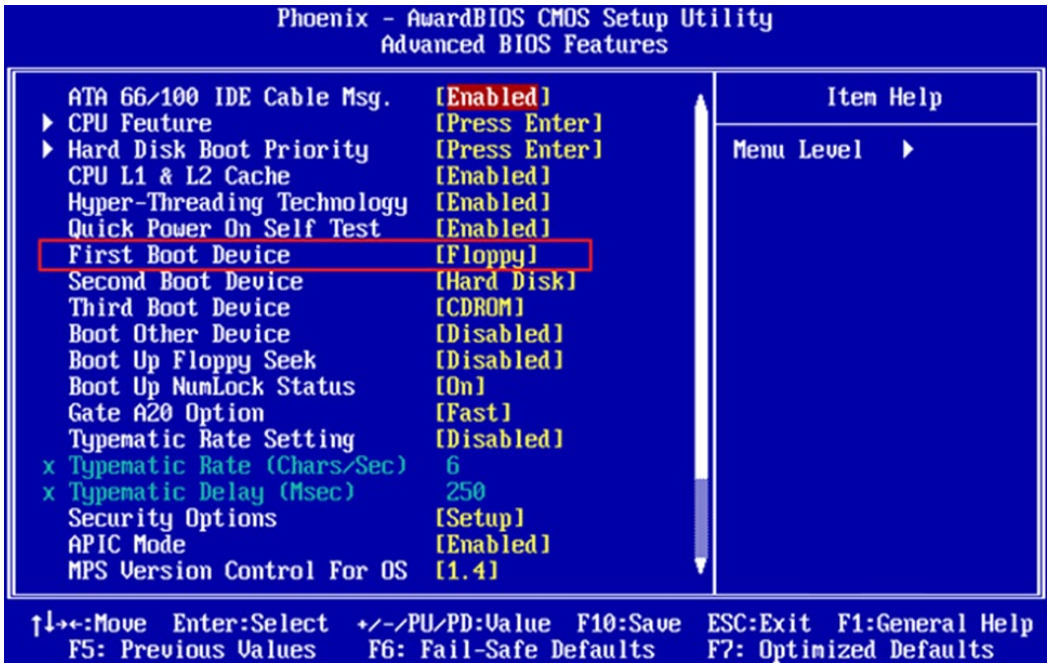


Рис. 1.7

– перейти в раздел меню «Save & Exit Setup» (см. рис. 1.6) для сохранения изменений.

1.2.3 BIOS типа INSYDE H2O

Для настройки BIOS типа Insyde H20, необходимо выполнить следующие действия:

– перейти в раздел «Boot» и включить функцию «External Device Boot» в состояние «Enabled»;

– указать порядок загрузки в пункте «Boot Priority». В случае, если для загрузки изделия используется компакт-диск, то первым в списке должен быть указан «Internal Optic Disc Drive», в случае USB-накопителя – «External Device»;

– далее перейдите на вкладку «System Configuration» и выберите пункт «Boot Options». В этом пункте найдите пункт «Secure Boot» и установите его в состояние «Disabled»;

– перейти в раздел «Exit» и выбрать «Save & Exit Setup» для сохранения изменений.

1.2.4 BIOS с UEFI BOOT

Для успешной загрузки изделия с внешнего носителя важно отключить функцию «Secure Boot». Для этого необходимо выполнить следующие действия:

– перейти во вкладку «Security» и отключить функцию «Secure Boot», выбрав в ниспадающем списке «Disabled» (см. рис. 1.8);

– перейти во вкладку «Boot» и установить у функции «Boot Mode» значение «Legacy Support», а у функции «Boot Priority» – «Legacy First» (см. рис. 1.9);

– в списке «Legacy» перенести в начало списка наименование носителя, с которого будет произведена загрузка изделия;

– перейти в раздел «Exit» и выбрать «Exit Saving Changes» (см. рис. 1.10) для сохранения внесенных изменений.

Управление функцией «Secure Boot»

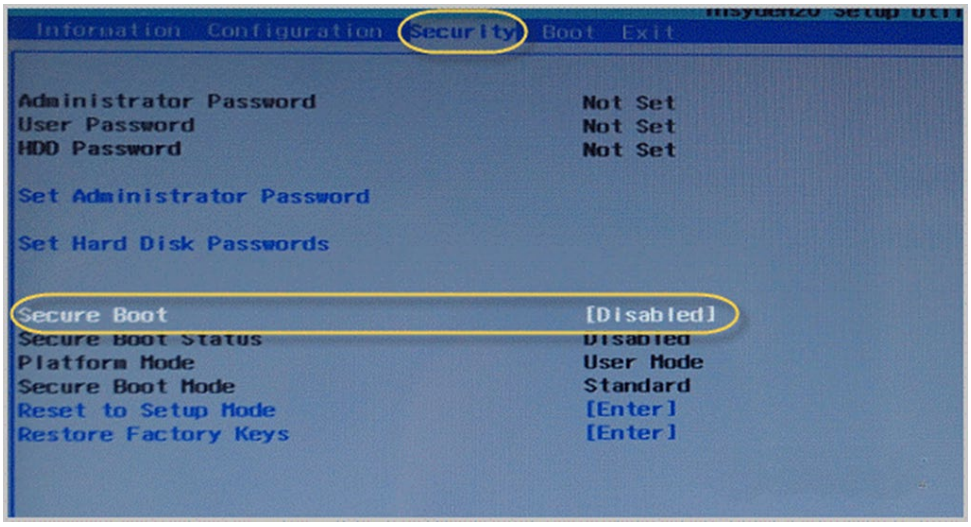


Рис. 1.8

Раздел «Boot»

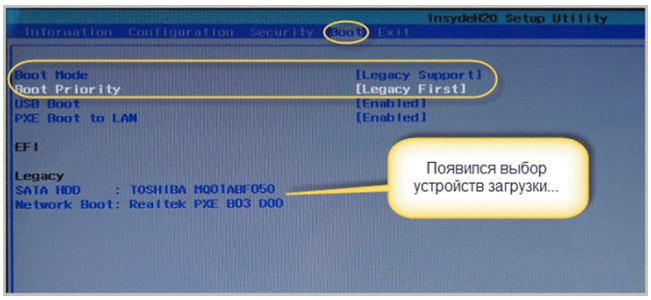


Рис. 1.9

Раздел «Exit»

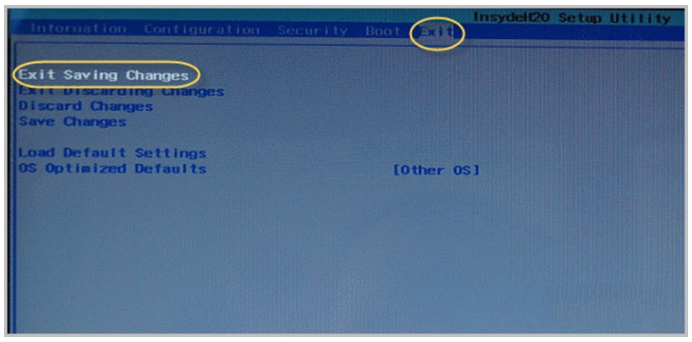


Рис. 1.10

Если USB-накопитель не отображается в списке «Legacy», необходимо перезагрузить изделие.

1.2.5 UEFI

В большинстве интерфейсов UEFI в нижней части главного окна расположена панель «Boot Priority», на которой перечислены устройства загрузки.

Чтобы изменить приоритет загрузки с того или иного носителя, достаточно переместить ярлык устройства в начало панели (см. рис. 1.11) и при выходе из UEFI сохранить настройки.

Интерфейс UEFI

Рис. 1.11

Также приоритет загрузки можно изменить, воспользовавшись «Advanced Mode». Для этого необходимо выполнить следующие действия:

– нажать кнопку «Exit/Advanced Mode» в верхнем правом углу главного окна (см. рис. 1.11);

– перейти в раздел «Boot»;

– в пункте «Boot Option Priorities» указать в «Boot Option #1» вид и наименование загрузочного устройства (см. рис. 1.12);

Раздел «Boot»

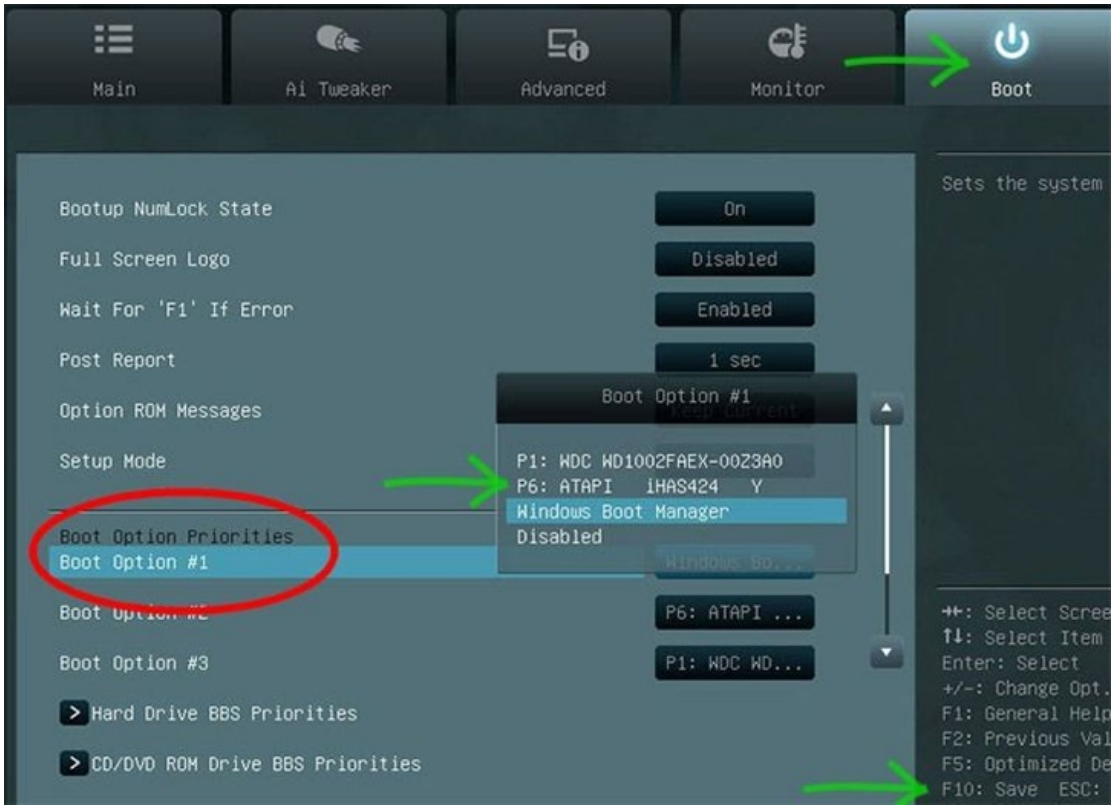


Рис. 1.12

– далее для того, чтобы отключить Secure Boot на оборудовании, в настройках UEFI зайдите на вкладку «Boot» – «Secure Boot» и в пункте «OS Type» установите параметр «Other OS»;

– при выходе из UEFI необходимо сохранить настройки.

ПРИЛОЖЕНИЕ 2. КОМБИНАЦИИ КЛАВИШ ДЛЯ УПРАВЛЕНИЯ КОМПОНЕНТОМ «ИНСПЕКТОР»

Комбинации клавиш для клавиатурного режима работы с компонентом «Инспектор» представлены в таблице 2.1.

Таблица 2.1 – Сообщения Оператору

Клавиша/комбинации клавиш	**Действие**
Общие команды клавиш управления	
ALT	Вход/Выход из меню
CTRL+N	Создание нового проекта
CTRL+O	Просмотр проекта
CTRL+S	Сохранение текущего проекта
CTRL+Q/ESC	Выход из программы
F1	Вызов справки
Область выбора инструментов	
Стрелки вверх/вниз и вправо/влево	Навигация
Пробел/Enter	Смена состояния
Комбинации управления инструментом проверки механизмов очистки	
Tab	Переход между областями инструмента и кнопками «Назад, «Вперед» и «Отмена»
Область проверки механизма очистки оперативной памяти	
Пробел/Enter	Смена состояния
Область проверки механизмов очистки	
Стрелки вверх/вниз	Навигация
Пробел/Enter	Смена состояния
Область поиска по ключевым словам	
Стрелки вверх/вниз	Навигация
Стрелка вправо	Раскрытие папки, если папка уже раскрыта – переход в ее подпапку
Стрелка влево	Скрытие папки, если папка уже скрыта – переход на уровень выше

Клавиша/комбинации клавиш	**Действие**
Комбинации управления инструментом контрольного суммирования	
Tab	Переход между областью «Выбор целей» и «Выбор алгоритмов» и кнопками «Назад», «Вперед», «Отмена»
Область выбора целей	
Стрелки вверх/вниз	Навигация
Стрелка вправо	Раскрытие папки, если папка уже раскрыта – переход в ее подпапку
Стрелка влево	Скрытие папки, если папка уже скрыта – переход на уровень выше
Пробел	Раскрытие/Скрытие папки
Enter	Добавление выбранной папки
Область настройки алгоритмов	
Стрелки вверх/вниз и вправо/влево	Навигация по таблице
Enter на ячейках с выбором	Просмотр вариантов
Delete	Удаление
Комбинации управления инструментом проверки прав доступа	
Tab	Переход между областями «Выбор целей», «Директории», «Пользователи», «Модель прав», «Массовая работа» и кнопками «Назад», «Вперед», «Отмена»
Область выбора целей	
Стрелки вверх/вниз	Навигация
Стрелка вправо	Раскрытие папки, если папка уже раскрыта – переход в ее подпапку
Стрелка влево	Скрытие папки, если папка уже скрыта – переход на уровень выше
Пробел	Раскрытие/Скрытие папки
Enter	Добавление выбранной папки
Область «Директории»	
Delete	Удаление
Стрелки вправо/влево	Навигация
Пробел/Enter на ячейке с уровнем сессии	Смена состояния
Область «Пользователи»	
Delete	Удаление
Стрелки вверх/вниз	Навигация

Клавиша/комбинации клавиш	**Действие**
F5	Обновление списка пользователей
Область «Модель прав»	
Стрелки вверх/вниз и вправо/влево	Навигация по таблице
Пробел на ячейке с именем	Выбор
Пробел/Enter на ячейке с доступом	Смена режима
Область «Массовая работа»	
Стрелки вверх/вниз/ и вправо/влево	Навигация между кнопками

Лист регистрации изменений

Изм	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводитель-ного документа и дата	Подпись	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных					