

УТВЕРЖДЕН НПЭШ.00606-01 34-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС

«СРЕДСТВО АНАЛИЗА ЗАЩИЩЕННОСТИ «СКАНЕР-ВС»

Руководство оператора

НПЭШ.00606-01 34

Листов 286

АННОТАЦИЯ

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

содержание

| 1. Назначение программы | 6 |
|--|----|
| 2. Условия выполнения программы | 9 |
| 2.1. Требования к аппаратному обеспечению | 9 |
| 2.2. Требования к среде функционирования | 10 |
| 3. Выполнение программы | 11 |
| 3.1. Установка и запуск | 11 |
| 3.1.1. Общее описание | 11 |
| 3.1.2. Подготовка к запуску в режиме «Live» | 11 |
| 3.1.3. Запуск программы в режиме LiveCD / LiveUSB | 12 |
| 3.1.4. Установка и запуск в «стандартном» режиме | 14 |
| 3.2. Управление сетевыми подключениями | 17 |
| 3.3. WEB-интерфейс ПК «Сканер-ВС» | 21 |
| 3.3.1. Подключение к WEB-интерфейсу ПК «Сканер-ВС» | 21 |
| 3.3.2. Общее описание web-интерфейса | 21 |
| 3.3.1. Справка | 26 |
| 3.3.1. Обновление изделия | 27 |
| 3.3.2. Управление лицензией | 31 |
| 3.3.3. Информация о продукте | 35 |
| 3.4. Локальный интерфейс | 36 |
| 3.4.1. Запуск локального интерфейса | 36 |
| 3.4.2. Общее описание локального интерфейса | 37 |
| 3.4.3. Справка | 43 |
| 3.4.4. Обновление изделия | 43 |
| 3.4.5. Управление лицензией | 48 |
| 3.5. Администрирование | 49 |
| 3.5.1. Общее описание | 49 |
| 3.5.2. Управление учетными записями пользователей | 50 |
| 3.6. Проекты | 56 |
| 3.6.1. Общее описание | 56 |
| 3.6.2. Создание проекта | 57 |
| 3.6.3. Управление проектами | 60 |
| 3.6.4. Удаление проекта | 71 |

| 3.6.5. Управление ресурсами | 72 |
|---|----------------|
| 3.6.6. Тестирование защищенности | 84 |
| 3.7. Инструменты | 107 |
| 3.7.1. Общее описание | 107 |
| 3.7.2. Инструмент «Аудит OC Astra Linux» | 108 |
| 3.7.3. Инструмент «Локальный аудит паролей» | 123 |
| 3.7.4. Инструмент «Поиск остаточной информации» | 129 |
| 3.7.5. Инструмент «Аудит обновлений ОС MS Windows» | 134 |
| 3.7.6. Инструмент «Системный аудитор» | 138 |
| 3.7.7. Инструмент «Гарантированное уничтожение информации» | 145 |
| 3.7.8. Инструмент «Аудит беспроводных сетей» | 151 |
| 3.7.9. Инструмент «Сетевой анализатор» | 158 |
| 3.7.10. Инструмент «Контрольное суммирование» | 174 |
| 3.8. Информация | 181 |
| 3.9. Уведомления | 182 |
| 3.10. Личная информация | 183 |
| 3.10.1. Вкладка «Профиль» | 184 |
| 3.10.2. Вкладка «Уведомления» | 185 |
| 3.10.3. Вкладка «Персонализация» | 189 |
| 3.11. Компонент «Инспектор» | 199 |
| 3.11.1. Запуск компонента | 200 |
| 3.11.2. Работа с компонентом «Инспектор» в режиме замкнутой программной с | среды OC Astra |
| Linux | 208 |
| 3.11.3. Работа с инструментами | 211 |
| 3.12. Сохранение результатов сканирования на внешние носители | 248 |
| 4. Сообщение оператору | 251 |
| Приложение 1 | 252 |
| 1.1 BIOS типа AMI | 252 |
| 1.2 BIOS типа AWARD, PHOENIX | 255 |
| 1.3 BIOS типа INSYDE H20 | 257 |
| 1.4 BIOS C UEFI BOOT | 257 |
| 1.5 UEFI | 259 |
| Приложение 2 | 261 |
| Приложение 3 | 282 |
| | |

Перечень сокращений

285

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Программный комплекс предназначен для поиска уязвимостей сетей, исследования структуры сетевых сервисов, сетевого и локального аудита паролей, поиска остаточной информации и анализа сетевого трафика.

В состав входит ПК «Сканер-ВС», предназначенный для тестирования функций безопасности при проведении аттестации автоматизированных систем и компонент «Инспектор».

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

ПК «Сканер-ВС» обнаруживает уязвимости кода и конфигурации программного обеспечения (далее — ПО). Для выявления (поиска) уязвимостей ПК «Сканер-ВС» использует встроенную базу данных уязвимостей кода и уязвимостей конфигурации ПО. База данных уязвимостей ПК «Сканер-ВС» содержит унифицированные описания уязвимостей, аналогичные содержащимся в следующих общедоступных источниках: банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru), база данных «Common Vulnerabilities and Exposures (https://cve.mitre.org). ПК «Сканер-ВС» осуществляет тестирование на проникновение путем эксплуатации уязвимостей, выявленных и содержащихся в базе данных уязвимостей.

ПК «Сканер-ВС» осуществляет поиск уязвимостей автоматизировано или по расписанию, задаваемому оператором.

ПК «Сканер-ВС» осуществляет обновление базы данных уязвимостей через сервис обновлений ПК «Сканер-ВС».

ПК «Сканер-ВС» осуществляет поиск остаточной информации на различных носителях информации и гарантированное уничтожение информации путем записи случайной последовательности символов поверх стираемой информации, а также записи случайной последовательности символов в освободившееся пространство накопителей на жестких магнитных дисках, накопителей на основе флэш-памяти и съемных носителей информации.

ПК «Сканер-ВС» осуществляет локальный подбор паролей по словарю для учетных записей пользователей ОС Microsoft Windows: 7, 8.1, 10, а также паролей беспроводных сетей.

ПК «Сканер-ВС» должен осуществлять подбор паролей по словарю для следующих сетевых сервисов: ftp, http, imap, mssql, mysql, oracle, pop3, postgres, rdp, redis, smb, smtp, snmp, ssh, telnet, vnc.

ПК «Сканер-ВС» осуществляет перехват, анализ и фильтрацию сетевых пакетов локальной и внешней сетей информационной системы (далее — ИС) и извлечение из сетевого трафика парольной информации (для протоколов ftp, pop3, http, https, telnet), а также, проверку возможности атак подмены MAC-адресов.

ПК «Сканер-ВС» обеспечивает контрольное суммирование заданных файлов, папок, подпапок, съемных носителей и накопителей на жестких магнитных дисках.

ПК «Сканер-ВС» обеспечивает контроль за установкой обновлений ОС Microsoft Windows: 7, 8.1, 10, Server 2012, Server 2012-R2, Server 2016.

ПК «Сканер-ВС» обеспечивает контроль за настройками комплекса средств защиты ОС специального назначения «Astra Linux Special Edition».

ПК «Сканер-ВС» обеспечивает формирование отчетов по результатам проверок в форматах: HTML, PDF, DOC, CSV.

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-С, СЗИ Secret Net 7, СЗИ НСД Dallas Lock 8.0-К, СЗИ НСД Dallas Lock 8.0-С.

Компонент «Инспектор» из состава ПК «Сканер-ВС» обеспечивает формирование и контроль дискреционных и мандатных полномочий доступа локальных пользователей к выбранным объектам файловой систем ОС специального назначения «Astra Linux Special Edition».

Компонент «Инспектор» из состава ПК «Сканер-ВС» обеспечивает поиск остаточной информации на машинных носителях информации, а также определяет директорию файла с найденной информацией.

Компонент «Инспектор» из состава ПК «Сканер-ВС» обеспечивает тестирование механизмов очистки оперативной памяти ОС семейства Microsoft Windows, ОС специального назначения «Astra Linux Special Edition» и запоминающих устройств рабочей станции.

Компонент «Инспектор» из состава ПК «Сканер-ВС» обеспечивает контрольное суммирование заданных файлов, папок, подпапок, съемных носителей и накопителей на жестких магнитных дисках.

Компонент «Инспектор» из состава ПК «Сканер-ВС» 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.

Компонент «Инспектор» из состава ПК «Сканер-ВС» обеспечивает контроль работоспособности антивирусного ПО на основе использования EICAR-Test-File.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Требования к аппаратному обеспечению

ПК «Сканер-ВС», за исключением компонента «Инспектор», устанавливается на рабочие станции, удовлетворяющие рекомендуемым аппаратным и программным требованиям, представленным в таблице (см. Таблица 1).

| Таблица 1 | - T | ребования к апп | аратному | у обеспечению | ΠК | «Сканер-ВС» |
|-----------|-----|-----------------|----------|---------------|----|-------------|
| | | 1 | | | | |

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

Компонент «Инспектор» программного изделия устанавливается на рабочие станции, удовлетворяющие рекомендуемым аппаратным и программным требованиям, представленным в таблице (см. Таблица 2).

| Параметр | Значение |
|--------------------------|---|
| Операционная система | Microsoft Windows 7 (32 / 64-бит): Starter, Home Basic, Home Premium, Professional, Enterprise, Ultimate; |
| | – Microsoft Windows 8.1 (32 / 64-бит): Core, Professional, Enterprise; |
| | – Microsoft Windows 10 (32 / 64-бит): Home, Professional, Enterprise; |
| | – Astra Linux Special Edition: 1.4, 1.5, 1.6 |
| Процессор | Не ниже Intel Pentium 4 2,2 ГГц или аналоги |
| Объем оперативной памяти | Не менее 2 Гбайт |

Таблица 2 – Требования к аппаратному обеспечению компонента «Инспектор»

Привод / порт USB

Видеоадаптер

Для просмотра отчетов компонента «Инспектор» требуется ПО Microsoft Internet Explorer одной из следующих версий: 8, 9, 10, 11.

Привод DVD-ROM / USB 2.0

SVGA видеоадаптер, совместимый со стандартом VESA 2.0

2.2. Требования к среде функционирования

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

- обеспечение сохранности оборудования и физической целостности системных блоков рабочих станций;
- обеспечение свободной от вирусов программной среды рабочей станции;
- обеспечение контроля изменения прикладной программной среды, исключение установки на рабочую станцию программных средств без гарантированной проверки;
- обеспечение организационно-технических мер защиты каналов передачи данных ПК «Сканер-ВС», расположенных в пределах контролируемой зоны.

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

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Установка и запуск

3.1.1. Общее описание

Запуск и функционирование ПК «Сканер-ВС» возможен в следующих режимах:

- «Live» – без установки на жесткий диск;

- «Стандартный режим» - с установкой на жесткий диск.

При запуске и функционировании ПК «Сканер-ВС» в режиме «Live», все настройки (в том числе созданные учетные записи), выполненные Оператором, сохраняются до перезагрузки ПК «Сканер-ВС». В случае перезагрузки изделия все изменения будут утрачены.

3.1.2. Подготовка к запуску в режиме «Live»

Запуск ПК «Сканер-ВС» в режиме «Live» выполняется без установки на жесткий диск.

Для успешной загрузки ПК «Сканер-ВС» необходимо установить в BIOS / UEFI приоритет загрузки рабочей станции с CD-ROM / USB-накопителя.

При загрузке рабочей станции BIOS / UEFI выводит на экран названия клавиши или сочетания клавиш, нажатие которых в этот момент позволит зайти в меню BIOS / UEFI. В таблице (см. Таблица 3) представлены примеры клавиш и их сочетаний для входа в BIOS / UEFI и меню загрузки для различных материнских плат и производителей ноутбуков.

| Клавиши для входа в BIOS | Клавиши вызова меню загрузки | Тип BIOS |
|--------------------------------|--|---|
| Delete | F11 | AMI |
| Delete | F12 | AWARD |
| Delete | F8 | AMI |
| Delete | Esc | Phoenix / AWARD |
| Delete | F11 | AMI |
| | 2 | Тип BIOS зависит от |
| F2 | Esc | программно- аппаратных |
| | Клавиши для входа в BIOS Delete Delete Delete Delete Delete F2 | Клавиши для входа в BIOSКлавиши вызова меню загрузкиDeleteF11DeleteF12DeleteF8DeleteEscDeleteF11 |

Таблица 3 – Перечень клавиш

| Производитель / устройство | Клавиши для входа в BIOS | Клавиши вызова меню загрузки | Тип BIOS |
|----------------------------|--------------------------------|---------------------------------|----------------------|
| | | | особенностей рабочей |
| | | | Станции |
| Ноутбуки Acer | F2 | F12 | Insyde H20 / Phoenix |
| Ноутбуки Dell | F2 | F12 | Dell |
| Ноутбуки Lenovo | F2 | F12 | AMI |
| Ноутбуки Samsung | F2 | F12 | Phoenix Secure Core |
| Ноутбуки Sony Vaio | F2 | F12 | Insyde H20 |
| Ноутбуки Toshiba | F2 | F12 | Insyde H20 / Phoenix |

12 НПЭШ.00606-01 34

Примечание. Из-за программно-аппаратных особенностей некоторых рабочих станций наименования клавиш могут отличаться от представленных в таблице (см. Таблица 3).

В большинстве версий BIOS параметры загрузки расположены в разделе «Boot». В этом разделе содержится список всех устройств, подключенных к рабочей станции. Первым в списке указано устройство, с которого производится загрузка. При необходимости можно изменить порядок загрузки. Жесткий диск является встроенным компонентом и всегда присутствует в разделе «Boot». Для того, чтобы в списке устройств появился USB-накопитель, необходимо произвести дополнительные настройки.

Для быстрого изменения настроек порядка загрузки рабочей станции можно использовать меню загрузки BIOS / UEFI. Для вызова меню загрузки воспользуйтесь клавишами, представленными в таблице (см. Таблица 3).

В Приложении 1 (см. Приложение 1) представлены примеры необходимых настроек для изменения порядка загрузки в UEFI и различных типах BIOS.

3.1.3. Запуск программы в режиме LiveCD / LiveUSB

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

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

- включить рабочую станцию;

- до загрузки основной ОС подключить носитель с ПК «Сканер-ВС» к рабочей станции.

На первом этапе появляется меню, в котором представлены варианты загрузки, позволяющие запускать программу в различных режимах (рис. 1).



Рисунок 1 – Меню загрузки ПК «Сканер-ВС»

Варианты загрузки:

- стандартная загрузка;

- режим сохранения изменений;

- текстовый режим;

– режим совместимости.

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

В текстовом режиме загружается консольная версия ПК «Сканер-ВС» без графического интерфейса.

Режим сохранения изменений (режим «persistence») позволяет сохранять текущие состояние системы при работе с USB-накопителя, т. е. при перезагрузке состояние системы сохраняется. На USB-накопителе есть специальный раздел «persistence», в который сохраняется текущее состояние системы при выключении. Для того, чтобы работать в данном режиме необходимо загрузиться с USB-накопителя, выбрать пункт в меню «Режим сохранения изменений», дождаться загрузки системы, далее работать как обычно. При выключении состояние системы автоматически сохранится на USB-накопитель в соответствующий раздел.

Примечания:

 В данном режиме скорость работы системы может быть несколько меньше. Это обусловлено тем, что происходит периодический процесс записи текущего состояния на USB-накопитель. 2. Раздел «persistence» не виден под управлением операционных систем семейства MS Windows, только под управлением операционных систем семейства Linux.

Для настройки сети необходимо воспользоваться сетевым менеджером. Подробно настройка сети описана в подразделе 3.2.

3.1.4. Установка и запуск в «стандартном» режиме

Для установки и запуска ПК «Сканер-ВС» в «Стандартном» режиме необходимо выполнить следующие действия:

- запустить ПК в режиме «Live»;
- выбрать пункт «Стандартная загрузка» (рис. 1), чтобы попасть на рабочий стол ПК «Сканер-ВС» (рис. 2);



Рисунок 2 – Рабочий стол ПК «Сканер-ВС»

- дважды кликнуть на ярлык «Установить Сканер-ВС»;
- в интерфейсе установки ПК на жесткий диск (рис. 3) нажать кнопку «Вперед», если необходимо выполнить установку ПК на жесткий диск, в противном случае нажать кнопку «Отмена» и подтвердить отмену установки;



Рисунок 3 – Интерфейс установки ПК на жесткий диск

Откроется интерфейс выбора раздела диска для установки ПК (рис. 4). Если диск не размечен, нажать кнопку «Изменить разметку диска» и разметить его. Чтобы размеченный раздел появился в выпадающем списке, нажать кнопку «Обновить».



Рисунок 4 – Интерфейс выбора раздела диска

 – выбрать раздел диска для установки ПК и нажать кнопку «Вперед», чтобы перейти в меню интерфейса выбора часового пояса (рис. 5).



Рисунок 5 – Интерфейс выбора часового пояса

- в выпадающем меню выбрать часовой пояс и нажать кнопку «Вперед»;

Откроется интерфейс, требующий подтверждения установки ПК, с предупреждением что все данные на жестком диске будут уничтожены (рис. 6).



Рисунок 6 – Интерфейс подтверждения установки ПК

 нажать кнопку «Далее» для подтверждения установки ПК на жесткий диск или кнопку «Назад» для возвращения в предыдущее меню (рис. 7);



Рисунок 7 – Установка ПК на жесткий диск

– нажать кнопку «Готово» (рис. 8) для завершения установки.



Рисунок 8 – Завершение установки

После завершения установки, ПК «Сканер-ВС» будет работать в «Стандартном» режиме.

3.2. Управление сетевыми подключениями

Для управления сетевыми подключениями в ПК «Сканер-ВС» предназначен «Сетевой менеджер».

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

Менеджер запускается из меню операционной системы. Для запуска менеджера существуют два способа.

Способ 1:

 – кликнуть левой кнопкой мыши на значке сетевого подключения (рис. 9), который находится в правом нижнем углу экрана операционной системы.



Рисунок 9-Значок сетевого подключения

Способ 2:

 открыть подменю стартера приложений, находящееся в левом нижнем углу экрана операционной системы (рис. 10);



Рисунок 10 – Меню рабочего стола

- выбрать вкладку «Остальные приложения»;
- выбрать вкладку «Интернет»;
- выбрать «Wicd Network Manager» (рис. 11).

19 НПЭШ.00606-01 34



Рисунок 11 - Сетевой менеджер «Wicd Network Manager»

Если все действия выполнены корректно, откроется рабочее окно менеджера (рис. 12).



Рисунок 12 – Рабочее окно менеджера

Если в сети есть DHCP-сервер, то компьютер, на котором запущен ПК «Сканер-ВС», автоматически получит IP-адрес. Если DHCP-сервера в сети нет, то для взаимодействия с сетью его можно настроить вручную. Для этого необходимо нажать кнопку «Параметры» (рис. 12). Откроется диалоговое окно «Проводная сеть - Параметры» (рис. 13), в котором можно вручную задать параметры сети (рис. 14), поставив отметку напротив пункта «Использовать статические IP».

Примечание. Аналогично производится настройка беспроводных сетей.

| (_) Проводн | ая сеть - Парам | метры – • × |
|-----------------------------|-----------------|----------------------------|
| Использовать статические IP | | |
| IP | | |
| Маска сети | | |
| Шлюз | | |
| Использовать статический DN | S 🗌 Использова | ать глобальные серверы DNS |
| Домен DNS | | |
| Домен поиска имён | | |
| DNS cepsep: 1 | | |
| DNS сервер: 2 | | |
| DNS сервер: 3 | | |
| DHCP Hostname | | scaner-vs |
| 🗆 Использовать шифрование | | |
| IEEE 802.1x with MSCHAPV2 | | 0 |
| Идентификация | | |
| Пароль | | |
| | | |
| | | |
| | | |
| | | |
| Сценарии | | |
| ap eterapin | | |
| | | Отменить |

Рисунок 13 – Параметры сетевого подключения

21 НПЭШ.00606-01 34

| (ј) Прово, | дная сеть - Параме | атры _ □ × |
|------------------------------|--------------------|--------------------------|
| ✓ Использовать статические І | Р | |
| IP | | 192.168.1.100 |
| Маска сети | | 255.255.255.0 |
| Шлюз | | 192.168.1.1 |
| 🗹 Использовать статический [| ONS 🗌 Использоват | ъ глобальные серверы DNS |
| Домен DNS | | |
| Домен поиска имён | | |
| DNS сервер: 1 | | 8.8.8.8 |
| DNS cepbep: 2 | | |
| DNS сервер: 3 | | |
| DHCP Hostname | | scaner-vs |
| 🗌 Использовать шифрование | | |
| IEEE 802.1x with MSCHAPV2 | | 0 |
| Идентификация | | |
| Пароль | | |
| | | |
| | | |
| | | |
| | | |
| Сценарии | | |
| | 20 | Отменить И И ОК |
| | | |

Рисунок 14 – Ручная настройка параметров сети

3.3. WEB-интерфейс ПК «Сканер-ВС»

3.3.1. Подключение к WEB-интерфейсу ПК «Сканер-ВС»

Для удаленного подключения к ПК «Сканер-ВС» Оператор должен настроить «Сетевой менеджер». Операции по настройке сетевого менеджера приведены в подразделе 3.2.

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

Если все настройки выполнены корректно, в окне браузера отобразится окно авторизации ПК «Сканер-ВС», как это представлено на рисунке (рис. 15).

3.3.2. Общее описание web-интерфейса

После запуска ПК «Сканер-ВС» отобразится окно авторизации (рис. 15), где Оператор должен ввести логин и пароль.

| Сканер-ВС анализ защищенности |
|----------------------------------|
| Авторизация |
| Логин |
| Пароль |
| войти |
| |
| |
| |
| |

Рисунок 15 – Окно авторизации

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

При успешной авторизации в WEB-интерфейсе будет отображено рабочее окно ПК «Сканер-ВС» (рис. 16).

| Сканер-ВС | | | ¥ = 0 🖊 + X |
|---|---|--|------------------------|
| проекты Всего проектов: 0 | избранное (+ Добавить проект | (+) Добавить проект | (+) Добавить проект |
| СЛУЖ БЫ Сканер сели Сканер ухавимостей Подбор паролей Эксплуатация ухавимостей Модуль отчетности | РЕСУРСЫ Плагины 48307 Политиям 3 Сповари 10 Списки портов 3 Эксплойты 1807 | Обновление прошло услешної Нахига для завершения обновления | ? Справка |
| ЛИЦЕНЗИЯ Соанер-ВС Лицензия без ограничения № 01 Истехает: 10.01.2038 (6962 дней) Клиент "Мастер-образ" Продлить | РАЗРАБОТЧИК © АО "HITO "Эшелон" https://npo-echelon.ru/ Техническая поддержка: support.sca@npo-echelon.ru | | |

Рисунок 16 – Рабочее окно ПК «Сканер-ВС»

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

– Панель навигации (рис. 17);

– Рабочее окно (рис. 18).

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

- Администрирование;

– Проекты;

- Информация;

- Уведомления;

– Личная информация;

– Полноэкранный режим.

Сканер-ВС
№ снализ зацищености

Рисунок 17 – Панель навигации

Описание пиктограмм блока «Панель навигации» представлено в таблице (см. Таблица 4).

| Таблица 4 – Описание пиктограмм б | блока «Панель навигации» |
|-----------------------------------|--------------------------|
|-----------------------------------|--------------------------|

| Пиктограмма | Описание |
|-------------|---|
| | Пиктограмма «Администрирование» позволяет осуществить переход к интерфейсу, который выполняет управление пользователями, обеспечивает просмотр всех событий, происходящих в ПК «Сканер- BC», а также выполнять настройку логотипа для отчета |
| | Пиктограмма «Проекты» позволяет выполнить быстрый доступ к интерфейсу управления проектами |
| i | Пиктограмма «Информация» осуществляет доступ к интерфейсу, обеспечивающему просмотр информации о продукте |
| | Пиктограмма «Уведомления» при нажатии отображает все события, которые выполняются в ПК «Сканер-ВС» |

| Пиктограмма | Описание | | | | |
|-------------|---|--|--|--|--|
| 2 | Пиктограмма «Личная информация» позволяет управлять профилем учетной записи, под которой вошел Оператор, осуществить выход из учетной записи или смену локали (языка) | | | | |
| 8 | Пиктограмма «Полноэкранный режим» при нажатии позволяет перевести ПК «Сканер-ВС» в полноэкранный режим. Для выхода необходимо нажать клавишу «Esc» | | | | |

Блок «Рабочее окно» (рис. 18) является основной рабочей областью интерфейса ПК «Сканер-

BC», в котором отображается информация о ходе выполнения задач.

| енализ защищенности | | | | ¥ = 0 📮 & X |
|--|--|---------|-----------------------------------|------------------------|
| | ИЗБРАННОЕ | | | |
| проекты Всего проестов: 0 | Добавить проект | | (+) Добавить проект | (+) Добазить проект |
| Службы | РЕСУРСЫ | | | |
| • Сканер сети | Плагины | 48307 | | |
| • Сканер уязвимостей | Политики | 3 | | \bigcirc |
| • Подбор паролей | Словари | 10 | \sim | \odot |
| • Эксплуатация уязвимостей | Списки портов | 3 | Обновление прошло успешно! | СПРАВКА |
| • Модуль отчетности | Эксплойты | 1807 | Нажмите для завершения обновления | |
| | | | | |
| лицензия | РАЗРАБОТЧИК | | | |
| Сканер-ВС Лицензия без ограничения № 01 | © АО "НПО "Эшелон" https://npo-echelon.ru/ Техническая поллержка: support sca@npo.ech | elon ru | | |
| Истекает: 10.01.2038 (6962 дней) | техническая поддержка. support sca@ipo-ecil | 301.10 | | |
| Клиент "Мастер-образ" | | | | |
| Продлить | | | | |

Рисунок 18 – Рабочее окно

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

- управлять данными таблицы;
- экспортировать данные из таблицы.

Для удобства управления таблицами предусмотрены общие элементы управления (рис. 19):

- пиктограмма экспорта данных из таблицы «
- пиктограмма фильтра элементов таблицы «
- пиктограмма отображения элементов таблицы (рис. 21).



Рисунок 19 – Пиктограммы экспорта и фильтра таблицы

3.3.2.1. Пиктограмма экспорта данных из таблицы

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

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

- видимые данные;

– все данные.

После выбора данных откроется окно с параметрами скачиваемых данных (рис. 20).

| экспорт таолицы | |
|-----------------|--|
| | |
| Формат | |
| ● CSV | |
| Поля | |
| 🗷 Логин | |
| 🗷 Роль | |
| 🗷 Заблокирован | |
| | |
| | |

Рисунок 20 - Окно параметров скачиваемых данных

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

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

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

3.3.2.2. Пиктограмма фильтра элементов таблицы

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

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

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

3.3.2.3. Пиктограмма отображения элементов таблицы

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



Рисунок 21 – Пиктограмма отображения элементов таблицы

Вводить количество строк можно с помощью клавиш или стрелочек, которые появляются после наведения курсора на окно. Введя необходимое число, следует нажать на пиктограмму

« », после чего таблица обновится и будет иметь требуемое количество строк.

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

3.3.1. Справка

Для получения справки по управлению ПК «Сканер-ВС», необходимо нажать на раздел «Справка» (рис. 22), после чего откроется новое окно с краткой документацией.



Рисунок 22 – Раздел справка на главном интерфейсе

3.3.1. Обновление изделия

Для обновления ПО программного изделия предназначен «Менеджер обновлений».

«Менеджер обновлений» запускается нажатием на раздел обновления ПК «Сканер-ВС» (рис. 23).



Рисунок 23 – Раздел обновления ПК «Сканер-ВС»

После проверки на сервере «Менеджер обновлений» выдаст данные о наличии обновлений (рис. 24).

28 НПЭШ.00606-01 34



Рисунок 24 – Данные о наличии обновлений

Для скачивания обновлений необходимо нажать на раздел (рис. 24) и дождаться окончания загрузки обновлений (рис. 25).



Рисунок 25 – Загрузка обновлений

После окончания загрузки раздел обновится. Для установки скачанных обновлений необходимо нажать на раздел обновления ПК «Сканер-ВС», изображенный на рисунке (рис. 26).



Рисунок 26 – Раздел обновления ПК «Сканер-ВС»

Далее начнется процесс установки обновлений (рис. 27).



Рисунок 27 – Процесс установки обновлений

После окончания установки обновлений в разделе появится соответствующее сообщение. Для завершения обновления необходимо снова нажать на раздел (рис. 28).



Рисунок 28 – Завершение обновления

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

на этапе скачивания обновлений (рис. 24) нажать на иконку папки в верхнем правом углу.
 Откроется диалоговое окно, как на рисунке (рис. 29);



Рисунок 29 – Выбор носителя

 выпадающем списке выберете необходимый USB-накопитель и нажмите на иконку стрелки (рис. 30);

31 НПЭШ.00606-01 34



Рисунок 30 – Выпадающее меню выбора носителя

Обновления будут успешно скачаны на USB-накопитель в папку:

```
/update/sca5/*
```

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

3.3.2. Управление лицензией

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

Интерфейс управления лицензией представлен на рисунке (рис. 31).

| лицензия | |
|--------------------|----------------|
| Сканер-ВС | |
| Лицензия без огра | ничения № 01 |
| Истекает: 10.01.20 | 38 (6974 дней) |
| Клиент "Мастер-об | ວົກສຸງ. |

Рисунок 31 – Интерфейс управления лицензией

В разделе «Лицензия» содержатся следующие данные:

- информация о наименовании продукта;

- информация о типе лицензии и ее номер;
- информация о сроке действия лицензии;
- информация о владельце лицензии;
- кнопка продления лицензии.

За 30 дней до окончания срока действия лицензии ПК «Сканер-ВС» напоминает пользователю о необходимости продлить срок лицензии. Срок действия лицензии начинает подсвечиваться желтым цветом (рис. 32).

| лицензия |
|--------------------------------------|
| Сканер-ВС |
| Лицензия № 280002399 на 8 IP-адресов |
| Истекает: 04.01.2019 (28 дней) |
| Клиент "hacked" |
| Продлить |

Рисунок 32 – Заканчивается срок действия лицензии

По истечению срока действия лицензии ПК «Сканер-ВС» сообщит пользователю с помощью красного текста (рис. 33). По истечению срока действия лицензии ПК «Сканер-ВС» пользователю становится недоступна функция обновления изделия и функция экспорта отчетов.



Рисунок 33 – Срок действия лицензии истек

Чтобы продлить лицензию ПК «Сканер-ВС», необходимо нажать на кнопку «Продлить». Откроется диалоговое окно «Обновление лицензии» (рис. 34).

| Файл лицензии: | |
|---|---------------------------------|
| Файл лицензии не выбран. | 🕒 Загрузить лицензию |
| Если у вас нет файла лицензии, отпра | вьте заявку на электронную |
| почту sales@npo-echelon.ru. | |
| В заявке укажите: | |
| • параметры запрашиваемой лицензии | і (количество IP-адресов и срок |
| действия); | |
| • параметры текущей лицензии. | |
| Параметры текущей лицензии: | |
| Сканер-ВС | |
| Лицензия без ограничения № 01 | |
| Истекает: 10.01.2038 (6974 дней) | |
| Клиент "Мастер-образ" | |

Рисунок 34 – Диалоговое окно «Обновление лицензии»

Чтобы загрузить новый файл лицензии нажмите на кнопку «Загрузить лицензию» и выберите файл лицензии формата *.lic. Диалоговое окно изменится (рис. 35).





Далее нажмите кнопку «Принять».

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

Если загрузка произошла успешно появится сообщение (рис. 36). Нажмите на крестик, чтобы завершить процесс обновления.

| Обновление лицензии | Х |
|---------------------|---|
| Файл лицензии: | |
| test.lic | |
| Успешно загружен | |

Рисунок 36 – Успешная загрузка файла лицензии

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

3.3.3. Информация о продукте

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

Интерфейс ознакомления с информацией о продукте представлен на рисунке (рис. 37).

| сканер-ВС анализ защищенности | | | 쫕 | - | ≍ | Ċ | 4 | × |
|----------------------------------|--|---|---------------------------------------|-----------|------|---|---|---|
| Главная / Информация | | | | | | | | |
| Информация о продукте | Продукт: Разработчик: Техническая поддержка: Сайт продукта: | Сканер-ВС Лиценз © 2017-2018 AO "H support.sca@cnpo.t scaner-vs.ru | ия без ограничч IПО "Эшелон" ru | ения (v5. | 0.0) | | | |

Рисунок 37 – Информация о продукте

В разделе «Информация о продукте» содержатся следующие данные:

- информация о продукте;
- разработчик продукта;
- электронный адрес технической поддержки;
- сайт продукта.

3.4. Локальный интерфейс

3.4.1. Запуск локального интерфейса

Для установленной версии, после загрузки ПК «Сканер-ВС», появится поле ввода пароля (рис. 38), логин введется автоматически. Необходимо ввести пароль «echelon» и нажать кнопку «enter».



Рисунок 38 – Поле вводе пароля

Если пароль был введен неверно, то появится поле ввода логина (рис. 39). Логин «root» необходимо ввести самостоятельно и нажать кнопку «enter». После этого ввести пароль «echelon» (рис. 38) и нажать кнопку «enter».


Рисунок 39 – Поле вводе логина

Если все действия выполнены правильно, загрузится рабочий стол ПК «Сканер-ВС».

3.4.2. Общее описание локального интерфейса

Локальный интерфейс ПК «Сканер-ВС» запускается иконкой ПК «Сканер-ВС» с рабочего стола операционной системы (рис. 40).



Рисунок 40 – Рабочий стол операционной системы

После запуска ПК «Сканер-ВС» отобразится окно авторизации (рис. 41), где Оператор должен ввести логин и пароль.

| Сканер-ВС анализ защищенности | |
|----------------------------------|--|
| Авторизация Логин | |
| Пароль | |
| | |

Рисунок 41 – Окно авторизации

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

При успешной авторизации в локальном интерфейсе будет отображено рабочее окно ПК «Сканер-ВС» (рис. 42).

| Сканер-ВС | | | ≝ ≅ × 0 ♣ ≛ × |
|--|---|-----------------------------------|------------------------|
| проекты Всего проектов: 0 | избранное ф | (+) Добавить проект | (+) Дрбавить проект |
| СЛУЖБЫ • Сканер сети • Сканер уязвимостей • Подбор паролей • Эксплуатация уязвимостей • Модуль отчетности | РЕСУРСЫ Плалены 47981 Политизи 3 Словари 10 Списки портов 3 Эксплойты 1807 | О Проверить наличие обновлений | ? справка |
| лицензия Сканер-ВС | РАЗРАБОТЧИК © АО "HTO "Эшелон" http://npo-echelon.ru/ | | |

Рисунок 42 – Главный интерфейс ПК «Сканер-ВС»

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

– Панель навигации (рис. 43);

– Рабочее окно (рис. 44).

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

- Администрирование;

– Проекты;

- Инструменты;

- Информация;

- Уведомления;

– Личная информация;

– Полноэкранный режим.

| сканер-ВС снализ защищенности | | | | 쓭 | ۵ | i | 4 | 4 | x |
|----------------------------------|---|----|---|---|---|---|---|---|---|
| | D | 10 | п | | | | | | |

Рисунок 43 – Панель навигации

В таблице (см. Таблица 5) приведено описание пиктограмм.

| Пиктограмма | Описание |
|--------------|---|
| | Пиктограмма «Администрирование» позволяет осуществить переход к интерфейсу, который выполняет управление пользователями, обеспечивает просмотр всех событий, происходящих в ПК «Сканер- ВС», а также выполнять настройку логотипа для отчета |
| 4 | Пиктограмма «Проекты» позволяет выполнить быстрый доступ к интерфейсу управления проектами |
| \mathbf{x} | Пиктограмма «Инструменты» осуществляет доступ к инструментам ПК |
| (i) | Пиктограмма «Информация» осуществляет доступ к интерфейсу, обеспечивающему просмотр информации о продукте и его лицензии |

| Пиктограмма | Описание |
|-------------|---|
| | Пиктограмма «Уведомления» при нажатии отображает все события, которые выполняются в ПК «Сканер-ВС» |
| 2 | Пиктограмма «Личная информация» позволяет управлять профилем учетной записи, под которой вошел Оператор, осуществить выход из учетной записи или смену локали (языка) |
| × | Пиктограмма «Полноэкранный режим» при нажатии позволяет перевести ПК «Сканер-ВС» в полноэкранный режим. Для выхода необходимо нажать клавишу «Esc» |

Блок «Рабочее окно» (рис. 44) является основной рабочей областью интерфейса ПК «Сканер-ВС», в котором отображается информация о ходе выполнения программы.

| | ИЗБРАННОЕ | | | |
|------------------------------------|------------------------|-------|------------------------------|---------------------|
| проекты Всего проектов: 0 | (+) Добавить проект | | | Добавить проект |
| ужбы | РЕСУРСЫ | | | |
| • Сканер сети • Сканер уязвимостей | Плагины | 47981 | \sim | \bigcirc |
| • Подбор паролей | Словари | 10 | \mathbf{S} | \bigcirc |
| • Эксплуатация уязвимостей | Списки портов | 3 | Проверить наличие обновлений | СПРАВКА |
| • Модуль отчетности | Эксплойты | 1807 | | |
| | | | | |

Рисунок 44 – Рабочее окно

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

– управлять данными таблицы;

– экспортировать данные из таблицы.

Для удобства управления таблицами предусмотрены общие элементы управления (рис. 45):

– пиктограмма экспорта данных из таблицы « 📩 »;

– пиктограмма фильтра элементов таблицы « 🚺 »;

– пиктограмма отображения элементов таблицы (рис. 47).

| * | T |
|---|---|
| | |

Рисунок 45 – Пиктограммы экспорта и фильтра таблицы

3.4.2.1. Пиктограмма экспорта данных из таблицы

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

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

- видимые данные;

– все данные.

После выбора данных откроется окно с параметрами скачиваемых данных (рис. 46).

| Формат | |
|----------------|--|
| CSV | |
| | |
| Поля | |
| 🗷 Логин | |
| 🗷 Роль | |
| 🗷 Заблокирован | |
| | |

Рисунок 46 - Окно параметров скачиваемых данных

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

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

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

3.4.2.2. Пиктограмма фильтра элементов таблицы

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

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

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

3.4.2.3. Пиктограмма отображения элементов таблицы

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



Рисунок 47 – Пиктограмма отображения элементов таблицы

Вводить количество строк можно с помощью клавиш или стрелочек, которые появляются после наведения курсора на окно. Введя необходимое число, следует нажать на пиктограмму

« », после чего таблица обновится и будет иметь требуемое количество строк.

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

3.4.3. Справка

Для получения справки по управлению ПК «Сканер-ВС», необходимо нажать на раздел «Справка» (рис. 48), после чего откроется новое окно с краткой документацией.



Рисунок 48 – Раздел справка на главном интерфейсе

3.4.4. Обновление изделия

Обновление ПО программного изделия можно осуществить двумя способами:

- с помощью «менеджера обновлений»;

– с помощью флэш-накопителя с записанными файлами обновления.

«Менеджер обновлений» запускается нажатием на раздел обновления ПК «Сканер-ВС» (рис. 49).

44 НПЭШ.00606-01 34



Рисунок 49 – Раздел обновления ПК «Сканер-ВС»

После нажатия раздел обновится и выдаст данные о наличии обновлений (рис. 50).



Рисунок 50 – Данные о наличии обновлений

Для скачивания обновлений нужно нажать на раздел (рис. 50) и дождаться окончания загрузки обновлений (рис. 51).

45 НПЭШ.00606-01 34



Рисунок 51 – Загрузка обновлений

После окончания загрузки раздел обновится. Для установки скачанных обновлений необходимо нажать на раздел обновления ПК «Сканер-ВС», изображенный на рисунке (рис. 52).



Рисунок 52 – Раздел обновления ПК «Сканер-ВС»

Далее начнется процесс установки обновлений (рис. 53).



Рисунок 53 – Процесс установки обновлений

После окончания установки обновлений в разделе появится соответствующее сообщение. Для завершения обновления необходимо снова нажать на раздел (рис. 54).



Рисунок 54 – Завершение обновления

Если требуется сохранить обновления на USB-накопитель, то необходимо на этапе скачивания обновлений (рис. 50) нажать на иконку папки в верхнем правом углу. Откроется диалоговое окно как на рисунке (рис. 55).

47 НПЭШ.00606-01 34



Рисунок 55 – Выбор носителя

В выпадающем списке выберете необходимый USB-накопитель и нажмите на иконку стрелки (рис. 56).



Рисунок 56 – Выпадающее меню выбора носителя

Обновления будут успешно скачаны на USB-накопитель в папку:

/update/sca5/*

Далее установка происходит аналогично процессу установки обновлений без скачивания обновлений на USB-накопитель.

3.4.5. Управление лицензией

Для управления лицензией ПК «Сканер-ВС» предназначен специальный интерфейс, переход к которому осуществляется нажатием кнопки « Продлить » на рабочем столе ПК «Сканер-ВС». Интерфейс управления лицензией представлен на рисунке (рис. 57).

| бновление лицензии | |
|---|---------------------------|
| Файл лицензии: | |
| Файл лицензии не выбран. | 🗎 Загрузить лицензию |
| Если у вас нет файла лицензии, отправьте : | заявку на электронную |
| почту sales@npo-echelon.ru. | |
| В заявке укажите: | |
| • параметры запрашиваемой лицензии (коли | ичество IP-адресов и срок |
| действия); | |
| параметры текущей лицензии. | |
| Параметры текущей лицензии: | |
| Сканер-ВС | |
| Лицензия без ограничения № 01 | |
| Истекает: 10.01.2038 (6962 дней) | |
| | |

Наши специалисты свяжутся с Вами в ближайшее время.

Рисунок 57 – Интерфейс управления лицензией

В интерфейсе отображается краткая инструкция по заполнению заявки на продление лицензии и механизм загрузки лицензии в ПК «Сканер-ВС».

Для загрузки лицензии в ПК «Сканер-ВС» необходимо нажать кнопку « ^{В Загрузить лицензию}» и выбрать файл с расширением «.lic».

3.5. Администрирование

3.5.1. Общее описание

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

- Пользователь;

- Администратор;

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

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

- управление проектами (п. 3.6.3);

- управление ресурсами (п. 3.6.5);
- управление службами (п. 3.6.6);
- обновление изделия (п. 3.4.4);

– управление лицензией (п. 49).

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

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

Примечание. Если ПК «Сканер-ВС» функционирует в режиме LiveCD/LiveUSB, выполненные Оператором настройки (в том числе созданные учетные записи) сохраняются до перезагрузки ПК «Сканер-ВС», при перезагрузке изделия все изменения будут утрачены.

3.5.2. Управление учетными записями пользователей

3.5.2.1. Общее описание

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

В рамках задач по управление пользователями Оператор может выполнить:

- создание учетной записи (пп. 3.5.2.2);
- управление правами пользователя (пп. 3.5.2.3);
- сброс пароля учетной записи (пп. 3.5.2.4);
- блокировку учетной записи (пп. 3.5.2.5);
- удаление учетной записи (пп. 3.5.2.6).

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

Вид интерфейса «Администрирование» (вкладка «Пользователи») представлен на рис. 58.

| ная Администр | ирование | | | | | | | | | |
|------------------|----------------------|---------------|--------------|--|---|-------|------|-----|---|--|
| ользователи | События Настройки | | | | | | | | | |
| овый пользовател | Ila | | k | | | | | | ¥ | |
| D | Логин | Раль | Заблокирован | | | Дейст | BATH | | | |
| 1 | admin | Администратор | Нет | | | | | | | |
| 2 | komrad | Администратор | Нет | | ÷ | 0 | | ef. | | |
| 7 | 1 | Пользователь | Her | | * | 0 | | ÷ | | |
| 8 | user1234567891011121 | Пользователь | Нет | | | 0 | | - | | |

Рисунок 58 – Интерфейс «Администрирование» (вкладка «Пользователи»)

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

- кнопка «Новый пользователь», предназначена для перехода к интерфейсу «Создание учетной записи пользователя» (пп. 3.5.2.2);
- список учетных записей зарегистрированных пользователей ПК «Сканер-ВС» в табличном формате.

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

- ID - сведения об идентификационном номере пользователя;

- логин сведения об имени учетной записи пользователя;
- роль роль, назначенная Оператору;
- заблокирован сведения о состоянии учетной записи пользователя. «Да» отображается в случае, если учетная запись заблокирована, «Нет» для активных учетных записей;
- действия набор пиктограмм, отображающих управляющие действия, которые можно выполнить с данной учетной записью.
- С существующей учетной записью могут быть выполнены следующие действия:
- смена роли пользователя (пп. 3.5.2.3);
- сброс пароля (пп. 3.5.2.4);
- блокировка / разблокировка (пп. 3.5.2.5);
- удаление (пп. 3.5.2.6).

3.5.2.2. Создание учетной записи пользователя

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

- войти в интерфейс «Администрирование»;

- открыть вкладку «Пользователи»;

- нажать кнопку «Новый пользователь».

Вид интерфейса «Новый пользователь» представлен на рисунке (рис. 59).

| Сканер-ВС | |
|--|--------------|
| Главная / Администрирование / Новый пользователь | |
| | |
| логин * | |
| | |
| Полное имя | |
| Пароль * | |
| | |
| Подтвердить пароль * | |
| Роль | Пользователь |
| Создать Отмена | |



Интерфейс «Новый пользователь» содержит следующие элементы:

- поле ввода «Логин»;
- поле ввода «Полное имя»;
- поле ввода «Пароль»;
- поле ввода «Подтвердить пароль»;
- выпадающий список «Роль»;
- кнопка «Создать»;
- кнопка «Отмена».

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

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

- должен состоять только из одного слова;
- должен состоять только из строчных и прописных (заглавных) букв (А-z), цифр (0-9) и специальных символов (.-);
- максимальная длина 20 символов;
- не должен повторяться с логинами других пользователей.

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

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

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

- «Такой пользователь уже существует»;

- «Обязательное поле».

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

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

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

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

– минимальная длина – 8 символов;

максимальная длина – 255 символов;

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

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

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

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

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

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

- «Введенные пароли не совпадают».

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

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

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

3.5.2.3. Управление правами пользователя

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

В таблицу можно попасть, выполнив следующие действия:

- открыть раздел «Администрирование»;

- зайти во вкладку «Пользователи».

Пиктограмма управления правами пользователей в двух состояниях представлена на рисунке (рис. 60).

Рисунок 60 – Пиктограмма управления правами пользователей в двух состояниях

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

На рисунке (рис. 60) пиктограмма находится в следующих состояниях (сверху вниз):

- пиктограмма управления правами пользователя в данном состоянии предназначена для понижения роли администратора до пользователя;
- пиктограмма управления правами пользователя в данном состоянии предназначена для повышения роли пользователя до администратора.

3.5.2.4. Сброс пароля учетной записи

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

В таблицу можно попасть, выполнив следующие действия:

- открыть Раздел «Администрирование»;

- войти во вкладку «Пользователи».

Для сброса пароля учетной записи пользователя используется пиктограмма, изображенная на рисунке (рис. 61).

Рисунок 61 – Пиктограмма сброса пароля

При нажатии на пиктограмму сбрасывается текущий пароль учетной записи пользователя, находящегося в одной строке с пиктограммой, и появляется окно с новым сгенерированным и назначенным паролем для данной учетной записи (рис. 62).

| Скан | iep-BC | (| _ | | | | | | |
|------|--------|--|---------|--|---|--|------|---|---|
| | | Пользователю 112 назначен новый пароль: Н921 | nFc467D | | | | | | |
| | | | ок | | | | | | |
| | | | | | | | J | 4 | τ |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | * | | aî. | | |
| | | | | | * | | * | | |
| | | | | | * | | si i | | |
| | | | | | * | | - | | |
| | | | | | * | | al. | | |
| | | | | | | | | | |

Рисунок 62 – Окно с новым паролем

3.5.2.5. Блокировка учетной записи

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

В таблицу можно попасть, выполнив следующие действия:

- открыть Раздел «Администрирование»;

- войти во вкладку «Пользователи».

Пиктограмма блокировки учетной записи может находиться в двух состояниях и в зависимости от этого может выполнять разные действия с учетной записью пользователя, находящегося с ней в одной строке (рис. 63).



Рисунок 63 – Пиктограмма блокировки в двух состояниях

На рисунке (рис. 63) пиктограмма находится в следующих состояниях (сверху вниз):

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

3.5.2.6. Удаление учетной записи пользователя

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

В таблицу можно попасть, выполнив следующие действия:

- открыть Раздел «Администрирование»;

- войти во вкладку «Пользователи».

Для удаления учетной записи пользователя используется пиктограмма, изображенная на рисунке (рис. 64). При нажатии на пиктограмму удаляется учетная запись пользователя, находящегося в одной строке с пиктограммой. При удалении учетной записи пользователя, все проекты, созданные данным пользователем, будут удалены без возможности восстановления.

Рисунок 64 – Пиктограмма удаления пользователя

3.6. Проекты

3.6.1. Общее описание

Для каждого нового тестирования создается проект, представляющий собой совокупность всех данных, относящихся к текущему тестированию. Проект включает в себя исходные данные фаз тестирования (поиск целей, поиск уязвимостей, сетевой аудит паролей, поиск эксплойтов) и результаты тестирования в фазе «Отчетность» в виде сгенерированных отчетов. Для проведения

тестирования пользователь может создать новый проект или, в случае продолжения, начатого ранее и сохраненного тестирования, использовать его.

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

В рамках задач по управлению проектами Оператор может выполнить:

- создание проекта (п. 3.6.2);
- настройку проекта (п. 3.6.3);
- удаление проекта (п. 3.6.4).

3.6.2. Создание проекта

Для создания проекта в левой части главной страницы ПК «Сканер-ВС» необходимо нажать левой кнопкой мыши по разделу «Проекты» (рис. 65) или на пиктограмму «Проекты» на панели навигации (рис. 66).



Рисунок 65 – Раздел «Проекты»

В открывшемся интерфейсе необходимо нажать кнопку «Новый проект» или выбрать уже существующий проект из перечисленных в рабочей области элемента «Проекты» (рис. 66).

| Кканер-ВС анализ защищенности | |
|----------------------------------|-------|
| Главная / Проекты | |
| Новый проект | Поиск |
| | |
| test (admin) 🧿 | |
| Хосты | 0 |
| Уязвимости | 0 |
| Подобранные пароли | 0 |
| Подобранные эксплойты | 0 |
| | |
| | |

Рисунок 66 – Рабочая область элемента «Проекты»

При нажатии кнопки «Новый проект» откроется интерфейс «Добавление нового проекта» (рис. 67).

| Сканер-ВС | |
|----------------------------------|--|
| Главная / Проекты / Новый проект | |
| | |
| Добавление нового проекта | |
| RWN | |
| | |
| Описание | |
| | |
| | |
| | |
| | |

Рисунок 67 – Интерфейс «Добавление нового проекта»

Интерфейс «Добавление нового проекта» содержит следующие элементы:

- поле ввода «Имя»;

- поле ввода «Описание».

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

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

- максимальная длина 80 символов;
- не должно повторяться с именами других проектов, если проект создан тем же пользователем.

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

- «Имя обязательное поле»;

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

- «Проект с таким именем уже существует».

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

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

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

После нажатия кнопки «Сохранить» или после выбора ранее сохраненного проекта открывается интерфейс проекта (рис. 68).

| Сканер-ВС анализ защищенности | | | | | | | 썉 | | × | Û | 4 | A - 1 |
|--|---|----------|---------------------|----------|---|--------------------|----|---|---|--------|-------|--------------|
| Главная / Проекты / test | | | | | | | | | | | | |
| 🎯 Поиск целей | | | 🕴 Поиск уязвин | иостей | | | | | | | | |
| Количество хостов | 0 | | Количество уяз | вимостей | | | | | | | | 0 |
| Операционные системы | Нет информации по операционным системам | | Критический уровень | | | | | | | | | 0 |
| | | | Высокий уровень | | | | | | | | | 0 |
| | | | Средный уровень | | | | | | | | | 0 |
| | | | Низкий уровень | | | | | | | | | 0 |
| | Задачи Рет | культаты | | | | | | | | Задачи | Резул | пытаты |
| 🖉 Эксплуатация | | | Отчетность | | | | | | | | | |
| Количество подобранных учетных записей | | 0 | | | C | тчетов не обнаруже | но | | | | | |
| Количество подобранных эксплойтов | | 0 | | | | | | | | | | |
| | Задачи Ре | культаты | | | | | | | | Задачи | Pesy | пьтаты |
| 🚍 Задачи | | | | | | | | | | | | |
| Задача | | = | + | 0 | | н | | / | | 0 | | Î. |
| | | | | | | | | | | | | |

Рисунок 68 – Интерфейс проекта

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

3.6.3. Управление проектами

3.6.3.1. Общее описание

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

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

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

3.6.3.2. Управление задачами

3.6.3.2.1 Общее описание

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

В рамках управления задачами проектов Оператор может выполнить:

- поиск целей (пп. 3.6.6.2);
- поиск уязвимостей (пп. 3.6.6.3);
- эксплуатацию (пп. 3.6.6.4);
- отчетность (пп. 3.6.6.5);
- задачи (пп. 3.6.6.6).

Для управления задачами ПК «Сканер-ВС» предназначен специальный интерфейс, доступ к которому осуществляется нажатием в левой части веб-интерфейса по разделу «Проекты» или нажатием кнопки «Проекты» в верхнем правом углу веб-интерфейса (рис. 65). Далее необходимо выбрать проект из рабочей области элемента «Проекты», нажатием на необходимый проект (рис. 66), после чего будет открыт интерфейс проекта.

Вид интерфейса проекта представлен на рисунке (рис. 69).

| () Сканер-ВС | | | | | | | | × o | 🔑 🔺 э |
|---|---|----------------|--------------|---------|-----|---|-----|-----|--------------|
| Anness Conserve Cold Conserve Cold Conserve Conserve Cold Conserve Cold Conserve Conserve Cold Conserve Co | | | | erer et | | | | | |
| | | | | | | | | | |
| Sport to send | | | Case of Case | | | | | | |
| Digitational sectors | | | | | | | | | 1 |
| | 1 | Jugen Property | | | | 2 | | | are Reported |
| Chargenee . | | | B overects | | | | | | |
| Spinor as reprinted private and a | | | | | | | | | |
| Appropriate transporter and the | | 4 | | | | | | | |
| | 3 | Same Report | | (anal | | 4 | | | un hyuni |
| a sure | | | | | | | | | |
| Jagen | | | | | | | i.e | 0 | |
| Para grad | | | | | 1 | 4 | | 1 | |
| Party presidents | | | 5 | | | | | | |
| Denkin haging topping? | | 1.00 | | | | | 1 | | 1 |
| hourses | | | | | | | | | |
| distant. | | | | | 1.0 | | | | |

Рисунок 69 – Интерфейс проекта

Интерфейс проекта содержит следующие элементы:

- 1. Поиск целей (пп. 3.6.6.2).
- 2. Поиск уязвимостей (пп. 3.6.6.3).
- 3. Эксплуатация (пп. 3.6.6.4).
- 4. Отчетность (пп. 3.6.6.5).
- 5. Задачи (пп. 3.6.6.6).

3.6.3.2.2 Вкладка «Задачи»

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

- поиск целей (пп. 3.6.6.2);
- поиск уязвимостей (пп. 3.6.6.3);
- эксплуатацию (пп. 3.6.6.4);
- отчетность (пп. 3.6.6.5).

При выполнении тестирования защищенности ПК «Сканер-ВС» используется специальный интерфейс, доступ к которому осуществляется нажатием кнопки «Задачи» (в секторе с номером 1-4 на рисунке (рис. 69), после чего откроется вкладка «Задачи» (рис. 70).

| Новое ск | анирование | | | | | |
|----------|------------|-----------------|-----------------|-----------|-----------|----------|
| # | Имя | Время последнег | Время последнег | Подробнее | Состояние | Действия |
| | | | Задач не | найдено | | |
| | | | | | | |

Рисунок 70 – Вкладка «Задачи»

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

- номер задачи;
- имя задачи;
- время последнего запуска;
- время последнего завершения;
- подробные данные о задаче;
- состояние задачи;
- действия с задачей.

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

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

Чтобы перейти в подробный режим необходимо нажать кнопку списка в верхнем правом углу таблицы (рис. 71).

| | канер- ализ защищен | вс | | | | 썉 | | ж | Û | | 4 | |
|-------------|------------------------|-------------|--------------|---------------------|-----------|---|-----------|---|--------|--------------|------|------|
| лавная / Пр | оекты / 112 / | Поиск целей | | | | | | | | | | |
| Хосты | Порты | Задачи | Топология | | | | | | | | | |
| Новое ска | нирование | | | | | | | | | ٣ | | |
| # | Имя | Время по | оследнего за | Время последнего за | Подробнее | 0 | Состояние | | | Дейст | гвия | |
| 1 | 112 | | | | | C | Создана | | 2 | 111 • | Ø | Û |
| | | | | | | | 25 | ۲ | 1 из 1 | « < | 1 | ». » |

Рисунок 71 – Включение режима подробного отображения

Пример отображения рабочего пространства в подробном режиме показан на рисунке (рис. 72). Для развертывания задачи необходимо нажать на темно-серую стрелку соответствующей задачи, раскроется список подзадач, представленный на рисунке (рис. 73). Для Оператора доступны следующие действия при работе с подзадачами: «Запустить», «Отменить», «Приостановить». Задачи, которые были созданы без параметра «Разбивать на подзадачи» развернуть нельзя, поэтому стрелка будет светло-серого цвета (рис. 72).

| С | канер- ализ защищен | вс | | | | 썉 | | × | i | | 4 | × |
|--------------|------------------------|-------------|-----------|--|---------|---|----|---|--------|-----|-----|---|
| Главная / Пр | юекты / 112 / | Поиск целей | | | | | | | | | | |
| Хосты | Порты | Задачи | Топология | | | | | | | | | |
| Новое скан | нирование | | | | | | | | | | ■ | = |
| ~ | | 112 | | | Создана | 2 | | Ø | Û | | | |
| | | | | | | | 25 | ۲ | 1 из 1 | « < | 1 > | * |

Рисунок 72 – Подробный режим отображения

| оозание / Поиск целей дачи Топология | | | | | | | |
|---|----------------------------|--|----------|---|--|--|--|
| зачи Топополия | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Сканирование 192.168.5.100-120 | 676 | 0 | | 0 | | | |
| | Захерцена | | | | | | |
| | Завершена | | | | | | |
| | Завершена | | | | | | |
| | Заверцена | | | | | | |
| | Запершена | | | | | | |
| | Завершена | | | | | | |
| | Закронч | | | | | | |
| | Заперияна | | | | | | |
| | Замериена | | | | | | |
| | Завериена | | | | | | |
| | Закериена | _ | | | | | |
| | Завершена | _ | | | | | |
| | Jacquera | _ | | | | | |
| | | 1000 | 100 | | | | |
| | | 0 | | | | | |
| | Cotgava | - × | | | | | |
| | Сездана | • | | | | | |
| | Создана | • | | | | | |
| | Сездана | • | | | | | |
| | Саздана | | | | | | |
| | Сацина | • | | | | | |
| | | | | | | | |
| | Сканирование 192.168.5.123 | Саздана Саздана Саздана Саздана | Catagona | | Caspana Caspana Ca | Caspina Caspina Caspi | |

Рисунок 73 – Подзадачи

При задании диапазона IP-адресов в качестве целей, ПК «Сканер-ВС» предложит использовать дополнительную настройку «Разбивать на подзадачи» (рис. 73).

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

После создания задачи на сканирование, во вкладке «Задачи» в таблице появится номер задачи, ее имя, текущий статус (цветной индикатор с комментарием) и перечень доступных действий. Перечень возможных состояний задач и доступных действий представлен в таблице (см. Таблица 6).

Таблица 6 – Перечень состояний задач и доступных действий

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

| 65 | |
|---------------|----|
| НПЭШ.00606-01 | 34 |

| Состояние задачи | Цвет | Доступные действия |
|------------------|------|--------------------|
| | | – повторить; |
| | | – удалить |

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

После нажатия откроется интерфейс описания задачи (рис. 74).

| анализ зац | цищенности | | | 썉 | - | * | i | - | ۵ |
|--|---|--|-----------------------------------|---------|--------|----------|------------|---------|---|
| Задача 2 Имя: Сканирова Тип: Поиск целе Статус: Заверши Автор: Админис | ние 192.168.5.76 й ена стратор Сканер-ВС | Дата соз | дания: 25.10.2018 12:17:38 | | | | | | |
| Результаты | Параметры | Расписание | | | | | | | |
| 25.10. | 2018 | | | | - | | 11022-1102 | | |
| 12:17: | :40 | Автор Админия 12:17:40 25.10. Хосты: 1 | стратор Сканер-ВС,Сост 2018 | ояние " | Заверш | ена", Вр | емя за | зершени | |
| | | Перейти | | | | | | | |

Рисунок 74 – Интерфейс описания задачи

Интерфейс содержит следующие вкладки:

– результаты;

- параметры;
- расписание.

Для получения подробной информации по задаче необходимо нажать левой кнопкой мыши на конкретную задачу во вкладке «Задачи», откроется интерфейс с информацией о задаче, как на рисунке (рис. 75).

| (ј) Сканер-ВС | | 쓭 | - | × | 0 | ٠ | ۵ | x |
|--|--|-------------|----------|------------|-----------|-----|---|---|
| Плавная / Проекты / Новое тестирование / Понск целей | 2 | | | | | | | |
| Задача 2 Имя: Сканорование 192,168,5,100-120 Тик: Гокоссцепей Статус: Завершена Автор: Адининстратор Сканер-ВС | Дата создания: 10.09.2018 13:16.59 | | | | | | | |
| Параметры Результаты Расписания | 1 | | | | | | | |
| 13:17:10 | Автор Администратор Сканер-ВС,Состояние "Заверия Хосты: 13 Перейти | она", Вромя | манранон | wa 13 17 1 | 0 10 09 2 | 018 | | |
| | | | | | 25 | • • | | 3 |

Рисунок 75 – Интерфейс с информацией о задаче

Во вкладке «Результаты» содержатся результаты сканирования каждого запуска задачи (рис. 75). Во вкладке «Параметры» содержится подробная информация о параметрах запущенной задачи (рис. 76). Во вкладке «Расписание» содержатся правила по расписанию запуска задачи (рис. 77).

| | | | ж | 0 | ٠ | ۵ | x |
|------------------------------------|------------------------------------|--------------------------------------|------------------------------------|------------------------------------|---------|---|---|
| | | | | | | | |
| | | | | | | | |
| Дата создания: 10.09.2016 13.16.59 | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | Дата создания: 10.09.2018 13.16.59 | ▲ Дата создания: 10.09.2018 13.16.59 | Дата создания: 10.09 2018 13.16.59 | Asta создания: 10.09 2016 13.16.59 | 🚰 🚔 🗙 🔮 | 🔮 🚔 🗙 🕢 🜲 Дата создания: 10.09.2018 13.16.59 | 🔮 🚖 🗙 💽 🌲 🛓 Дата создания: 10.09.2018 13.16.59 |

Рисунок 76 – Параметры задачи

| (і) Сканер-ВС | | | | 9 | - | × | 0 | | - | × |
|---|------------------|---------------------------|-----------------------|-------|-------------|--------------|------|------|------|---|
| Trankal / Tpoents / Honoe techyponawe / | Roick spinel / 2 | | | | | | | | | - |
| Задача 2 | | | | | | | | | | |
| Имя: Сканирование 192.168.5.100-120 Тие: Сюнса целей Статуе: Завершена Автор: Адахимистратор Сканер-ВС | | Дата создания: 10.09 2011 | 0 13 16 59 | | | | | | | |
| Параметры Результаты | Расписание | | | | | | | | | |
| Ten sanyoxa | | | | | | | | | | |
| Ten | Дня недети | Epewer satycea | Начало исполнения пра | 047.0 | Colorrianse | ROTOTIVENES | rpa_ | Дейс | 7568 | |
| Реховый | | 20.09.2018, 11.40.26 | 20.09.2018, 11.40.26 | R. | 20.09 | 2018, 11.403 | 26 | 1 | 0 | |
| Повторяющийся | 00 | 22.30 | 11.09.2018, 11.39.40 | 0 | | | | 1 | 0 | |
| | | | | | | | | | | |

Рисунок 77 – Расписание задачи

Для перехода к результатам сканирования конкретного запуска необходимо во вкладке «Результаты» нажать на соответствующую строчку с информацией по нему. В рабочем окне появятся результаты запуска задачи, а также подробная информация по возникшим ошибкам (если имеются) во вкладке «Ошибки» (рис. 78).

| 0.9 | канер-ВС | | | | * | - | × | 0 | - | × |
|-------------|----------------------------|--------------------------|-------|------------|----------|--------|---|---------|---------|---|
| парная / Пр | ховяты / Новое теспиров | anne / Novcx geneil / 1/ | 1 | | | | | | | |
| Результаті | ы 1 | | | | | | | | | |
| Автор: Адни | exceptop Ckavep-BC | | | | | | | | | |
| Openn sabeş | parevers: 10.09.2018, 13.0 | 06.42 | | | | | | | | |
| Хосты | Серенсы | | | | | | | | | |
| | Alpec | Retoion | flogr | Coctoniese | Cepes | c · | 0 | 0,02,47 | Bepowe. | |
| 1 | 192 168 5 123 | tcp | 1110 | thered | ntso sta | dus. | | | | |
| .2 | 192.168.5.123 | tep . | 135 | titlered | misp | e . | | | | |
| 3 | 192,168,5,123 | top | 139 | thered | nethios | 550 | | | | |
| 4 | 192.168.5.123 | tcp | 19780 | Mered. | unikno | en i | | | | |
| 0 | 192,168.5.123 | top | 2009 | titlered | icsia | | | | | |
| 6 | 192.168.5.123 | top | 445 | Mered | microsof | 1-01 | | | | |
| 7 | 192,168,5,123 | кp | 49152 | open | unknow | 10 | | | | |
| .0 | 192 168.5.123 | top | 49153 | open | unknow | 10 | | | | |
| . 9 | 192,168,5,123 | top | 49154 | open | unkney | - | | | | |
| 10 | 192 168.5 123 | top | 49155 | open | unknow | um) | | | | |
| 11 | 192.168.5.123 | top | 49156 | open | unknow | with l | | | | |
| | 100 100 1 100 1 | 444 | | | | | | | | |

Рисунок 78 – Результаты запуска задачи

Подробная информация об управлении расписанием выполнения задач представлена в подпункте 3.6.3.2.4.

3.6.3.2.3 Настройка целей для сканирования

При создании задачи на новое сканирование (при поиске целей и поиске уязвимостей) настраиваются цели для сканирования. Цели поиска уязвимостей можно задавать несколькими способами: вводя вручную адреса в поле «Цели», импортируя цели из активов или загружая из файла.

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

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

3.6.3.2.4 Управление расписанием выполнения задач

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

Во вкладке «Задачи» (см. пп. 3.6.3.2.2) в столбце «Действия» необходимо нажать кнопку «Запланировать», откроется диалоговое окно добавления правила (рис. 79). Далее нужно выбрать тип запуска: разовый или повторяющийся. Если был выбран разовый запуск, то далее необходимо настроить дату и время запуска и нажать кнопку «Добавить правило». Правило появится в сводной таблице правил по задаче (рис. 80). Если выбран повторяющийся запуск, то далее необходимо выбрать дни недели повторений, время запуска, дату начала исполнения правила, дату окончания исполнения правила и нажать кнопку «Добавить правило». Правило появится в сводной таблице правил по задаче (рис. 80). Жобое правило можно удалить, для этого необходимо нажать кнопку «Удалить» в столбце «Действия».

| linical | ine 2 | | | | |
|---------|------------|---------------|---------------|-------------|----------|
| Гип зап | уска | | | • | |
| | | Время запу | Начало исл | Оконизние | Пейстена |
| Тип | дни недели | aponin contym | | Onon-tanine | дельтопл |
| Тип | дни недели | Нет правил д | ля расписания | Oron-tanite | Делетони |

Рисунок 79 – Добавление правила

| Тип зап | іуска | | Разовый | • | |
|-----------------------------|------------------------|------------------------------|---|--------------------------|----------|
| Выбрат | гь дату | 1 | 2 сент. 2018 1:00:0 | 0 | 0 |
| Добав | зить правило | | | | |
| | Duu uono | Время запуска | Начало испол | Оконча | Действия |
| Тип | дни неде | | | | |
| Тип Повторяющ | дни неде вт, чт, сб | 11:00 | 17.09.2018, 12:27 | 17.10.2018 | • |
| Тип Повторяющ Разовый | дни неде вт, чт, сб | 11:00 12:09:2018, 1:00:00 | 17.09.2018, 12:27 12.09.2018, 1:00:0 | 17.10.2018 12.09.2018 | 0 |

Рисунок 80 – Результат добавления правил

Запланировать задачу аналогичным способом можно, также, во вкладке «Расписание» конкретной задачи (рис. 77). Порядок добавления правила аналогичен описанному выше первому способу.

Независимо от результатов сканирования любую задачу можно перезапустить или дублировать. Для этого необходимо нажать кнопку «Дублировать» или «Повторить» (рис. 81), расположенные справа от индикатора статуса сканирования.

| вная | / Проекты / 123 / По | риск целей | | | | | | | | |
|------|----------------------|---------------------|---------------------|-----------|-----------|---|----------|-------|----|--|
| ост | ы Порты | Задачи Топс | ология | | | | | | | |
| юво | е сканирование | | | | | | | ۲ | | |
| # | Имя | Время последнег | Время последнег | Подробнее | Состояние | | Ļ | ейств | пя | |
| ~ | Сканирование 192.10 | 25.10.2018 12:32:01 | 25.10.2018 12:32:11 | | Завершена | 2 | m | C | Û | |
| 2 | | | | | | _ | | | | |
| 2 | Сканирование 192.16 | 25.10.2018 11:55:50 | 25.10.2018 11:56:01 | | Завершена | 2 | Ê | C | Û | |

Рисунок 81 – Процесс сканирования

Для получения подробной информации об ошибке в процессе выполнения задачи, нажмите левой кнопкой мыши по индикатору статуса сканирования (в этом случае он красного цвета), после чего откроется новое окно с информацией о задаче, деталях запуска и ошибках во время запуска задачи.

Изменение статуса выполнения задачи будет отражено в правом верхнем углу вебинтерфейса (кнопка Уведомления) (рис. 82).



Рисунок 82 – Уведомления

3.6.3.2.5 Элемент «Задачи»

Элемент «Задачи» предназначен для просмотра статуса созданных задач (рис. 83).

| ≡ Задрчи | | | | | | | | | | | | |
|-----------------------|---|---|---|---|---|---|---|---|--|--|--|--|
| Задача | = | + | 0 | | п | ~ | 0 | | | | | |
| Поиск целей | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | | | | |
| Поиск уязвимостей | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| Онлайн подбор паролей | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| Эксплуатация | 0 | 0 | 0 | 0 | 0 | 0 | O | 0 | | | | |
| Отчет | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| | | | | | | | | | | | | |

Рисунок 83 – Элемент «Задачи»

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

- тип задачи;
- сумма всех имеющихся задач;
- созданные задачи;
- задачи, находящиеся в обработке;
- активные задачи;
- приостановленные задачи;
- завершенные задачи;
- отмененные задачи;
- ошибки при выполнении задач.

3.6.4. Удаление проекта

Для удаления проекта в левой части главной страницы ПК «Сканер-ВС» необходимо нажать левой кнопкой мыши по разделу «Проекты» (рис. 65) или нажать на пиктограмму «Проекты» на панели управления.

В открывшемся интерфейсе нужно нажать на значок «крестик» в правом верхнем углу того проекта, который необходимо удалить. После нажатия появится окно с просьбой подтвердить удаление проекта (рис. 84).

| :::: Сканер-ВС | | | |
|-----------------------|---------------------------------|---|---------|
| | Удаление п | проекта | |
| | Вы уверены, чт восстановить. | по хотите удалить этот проект? Данные невозможн | ю будет |
| | Отмена | | Принять |
| | _ | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Рисунок 84 – Окно с просьбой подтвердить удаление проекта

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

3.6.5. Управление ресурсами

3.6.5.1. Общее описание

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

В рамках задач по управлению ресурсами Оператор может выполнить:

– управление плагинами (пп. 3.6.5.2);

- управление политиками (пп. 3.6.5.3);

- управление словарями (пп. 3.6.5.4);

- управление списками портов (пп. 3.6.5.5);

– управление эксплойтами (пп. 3.6.5.6).

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

Вид интерфейса «Ресурсы» представлен на рисунке (рис. 85).

| сканер-ВС анализ защищенности | | | | 딸 ㅎ | × e | | 4 | × |
|---|--------|---|--|--|-----|---|---|---|
| Главная / Ресурсы | | | | | | | | |
| Плагины База плагинов сканера уязвимостей с подробной информацией по каждому. | م ا | Политики Базовые политики сканера уязвимостей. Со: пользовательских политик сканирования. | здание | Словари База словарей для аудита учетных записей. | | | | |
| Списки портов Диапазоны портов, используемые сканером уязвимостей. | | | Эксплойты База эксплойтов с подробной информацией | і по каждому. | | ಹ | | |

Рисунок 85 – Вид интерфейса «Ресурсы»

Интерфейс «Ресурсы» содержит следующие элементы:

- плагины (пп. 3.6.5.2);

- политики (пп. 3.6.5.3);
- словари (пп. 3.6.5.4);
- списки портов (пп. 3.6.5.5);
- эксплойты (пп. 3.6.5.6).
3.6.5.2. Управление плагинами

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

- открыть раздел «Ресурсы»;

- войти в интерфейс «Плагины».

Вид интерфейса «Плагины» представлен на рисунке (рис. 86).

| 1 | сканер-ВС анализ защищенности | | | | 쓭 | × | 6 | . 🦉 | 4 | × |
|--------|----------------------------------|---|-----------|---|---|-----|---------|---------|---|---|
| Главна | я / Ресурсы / Плагины | | | | | | | | | |
| Плаг | ины | | | | | | | | | |
| # | OID | Имя | Семейство | Описание | CVE | Уро | вень ог | асности | | |
| 1 | 1.3.6.1.4.1.25623.1.0.804830 | Mozilla Firefox ESR Multiple Vulnerabilities-01 Septer | General | This host is installed with Mozilla Firefox ESR and is $_{\rm I}$ | CVE-2014-1562 CVE-2014-1567 | | Критине | ский | | |
| 2 | 1.3.6.1.4.1.25623.1.0.803855 | Mozilla Firefox ESR Multiple Vulnerabilities - August t | General | The host is installed with Mozilla Firefox ESR and is p | CVE-2013-1701 CVE-2013-1706 CVE-2013-1707 CVE-2013-1709 CVE-2013-1710 CVE-2013-1712 CVE-2013-1713 CVE-2013-1714 CVE-2013-1717 | | Критиче | :Kanki | | |
| з | 1.3.6.1.4.1.25623.1.0.802993 | Mozilla Firefox 'WebSockets' Denial of Service Vulnei | General | The host is installed with Mozilla firefox and is prone | CVE-2012-4191 | | Критиче | ский | | |
| 4 | 1.3.6.1.4.1.25623.1.0.806102 | Множественные уязвимости Mozilla Firefox ESR (M | General | Этот хост установлен с Mozilla Firefox ESR и подве | CVE-2015-4497 CVE-2015-4498 | | Критиче | ский | | |
| 5 | 1.3.6.1.4.1.25623.1.0.806101 | Множественные уязвимости Mozilla Firefox ESR (W | General | Этот хост установлен с Mozilla Firefox ESR и подве | CVE-2015-4497 CVE-2015-4498 | | Критиче | ский | | |
| 6 | 1.3.6.1.4.1.25623.1.0.806022 | Множественные уязвимости Mozilla Firefox ESR - # | General | Этот хост установлен с Mozilla Firefox ESR и подве | CVE-2015-4473 CVE-2015-4475 CVE-2015-4478 CVE-2015-4479 | | Критиче | сазий | | |

Рисунок 86 – Интерфейс «Плагины»

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

- номер строки плагина в таблице;
- OID плагина (уникальный идентификатор);
- имя плагина;
- семейство плагина;
- описание плагина;
- номер плагина в базе данных общеизвестных уязвимостей информационной безопасности (CVE);

– уровень опасности плагина.

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

Вид интерфейса описания плагина представлен на рисунке (рис. 87).

| Сканер-ВС | 쑵 | • | ж | 6 | - | 4 | × |
|--|---|---|---|---|---|---|---|
| Главная / Ресурсы / Платины / 1-3-6-1-4-1-25623-1-0-804830 | | | | | | | |
| | | | | | | | |
| 1.3.6.1.4.1.25623.1.0.804830 | | | | | | | |
| Nexe: Mozilla Firefox ESR Multiple Vulnerabilities-01 September14 (Mac OS X) | | | | | | | |
| Уровень опасности: Критический | | | | | | | |
| Семейство: General | | | | | | | |
| Onvcawve: This host is installed with Mozilla Firefox ESR and is prone to multiple vulnerabilities. | | | | | | | |
| Влияние: Successful exploitation will allow attackers to disclose potentially sensitive information and compromise a user's system. | | | | | | | |
| Onpegenewie: Checks if a vulnerable version is present on the target host. | | | | | | | |
| Содержание: Multiple flaws exist due to, - A use-after-free error when setting text directionality An unspecified error. | | | | | | | |
| Pewerwe: Upgrade to Mozilla Firefox ESR version 24.8 or 31.1 or later. | | | | | | | |
| CVE: CVE-2014-1562 CVE-2014-1567 | | | | | | | |
| CVSS 2.0: 10 | | | | | | | |
| Berrop CVSS 2.0; AV:N/AC.L/AU:N/C.C/I:C/A:C | | | | | | | |
| Ccs/nor: • http://www.mozilla.org/security/announce/2014/mtsa2014-67.html • http://www.mozilla.org/security/announce/2014/mtsa2014-72.html • http://www.mozilla.com/en-US/irelov/all.html | | | | | | | |

Рисунок 87 – Интерфейс описания плагина

В интерфейсе описания плагина содержится следующая информация:

- имя плагина;
- уровень опасности плагина;
- семейство плагина;
- описание плагина;
- решение для устранения уязвимости;
- CVE;
- BDU (если идентификатор присутствует);
- CVSS (оценка уязвимости);
- ссылки на подробное описание плагина.

3.6.5.3. Управление политиками

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

- войти в раздел «Ресурсы»;
- выбрать интерфейс «Политики».

Вид интерфейса «Политики» представлен на рисунке (рис. 88).

| Сканер-ВС анализ защищенности | | | 📽 🛎 🗙 🛛 📮 🛔 X |
|--------------------------------------|-------------------------------------|---------------------------|---|
| Главная / Ресурсы / Политики | | | |
| Политики | | | |
| L ↓ | r c | F C | |
| Импорт | Быстрая | Веб-приложения | Полное сканирование |
| Загрузка политики из файла | Быстрый поиск критичных уязвимостей | Сканирование веб-сервисов | Сканирование всех известных уязвимостей |
| | | | |
| + | | | |
| Новая | | | |
| Создание собственной политики с нуля | | | |
| | | | |
| | | | |

Рисунок 88 – Интерфейс «Политики»

В данном интерфейсе содержатся следующие разделы:

- Импорт (пп. 3.6.5.3.1);
- Политика быстрого сканирования (пп. 3.6.5.3.2);
- Политика сканирования веб приложений (пп. 3.6.5.3.3);
- Политика полного сканирования (пп. 3.6.5.3.4);
- Новая политика (пп. 3.6.5.3.5).

3.6.5.3.1 Импорт

Импорт предназначен для загрузки собственной политики сканирования из файла в ПК «Сканер-ВС». Импорт осуществляется нажатием на раздел «Импорт» (рис. 89), после чего необходимо выбрать файл соответствующего формата в проводнике и нажать кнопку «Открыть».

↓ Импорт

Загрузка политики из файла

Рисунок 89 – Вид раздела «Импорт» в интерфейсе «Плагины»

3.6.5.3.2 Политика быстрого сканирования

Политика быстрого сканирования предназначена для быстрого поиска критичных уязвимостей. Вход для просмотра политики быстрого сканирования осуществляется нажатием на раздел политики «Быстрая» (рис. 90).



ſΓ

Быстрая

Быстрый поиск критичных уязвимостей

Рисунок 90 – Вид раздела политики «Быстрая» в интерфейсе «Плагины»

В правом верхнем углу политики «Быстрая» в разделе «Плагины» (рис. 90) есть две пиктограммы. Данные пиктограммы отвечают за экспорт политики и ее дублирование.

Вид интерфейса политики быстрого поиска представлен на рисунке (рис. 91).

| сканер-ВС анализ защищенност | C M | | 월 🚔 🗶 0 | 🚨 🔺 🕺 |
|--|--|----------------|-----------------------|---------|
| Главная / Ресурсы / Политики | (1) | | | |
| Быстрая | | | | |
| Имя: Был Описание: Был Пользовательская: Нет Количество плагинов: 106 | страя стрый поиск критичных уязвимостей т 516 | | | Экспорт |
| | Семейство | Всего плагинов | Использовано плагинов | 1 |
| | Buffer overflow | 562 | 562 | |
| | Databases | 550 | 550 | |
| | Gain a shell remotely | 106 | 106 | |
| | General | 4347 | 4347 | |
| | Nmap NSE | 154 | 154 | |
| | Nmap NSE net | 177 | 177 | |
| | Port scanners | 15 | 2 | |
| | Privilege escalation | 64 | 64 | |
| | Product detection | 2098 | 2098 | |
| Назад | | | | |

Рисунок 91 – Интерфейс политики быстрого поиска

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

– имя политики;

- описание политики;

- является ли политика пользовательской;
- количество используемых в политике плагинов.
- В таблице интерфейса содержится следующая информация об используемых плагинах:
- семейства плагинов, используемых в данной политике;
- общее число плагинов в семействе;
- общее число плагинов, используемых в семействе.

3.6.5.3.3 Политика сканирования веб-приложений

Политика сканирования «Веб-приложения» предназначена для сканирования веб-сервисов. Вход для просмотра политики сканирования веб-приложений осуществляется нажатием на раздел политики «Веб-приложения» (рис. 92).



rî (Ĉ

Веб-приложения

Сканирование веб-сервисов

Рисунок 92 – Раздел политики «Веб-приложения» в интерфейсе «Политики»

В правом верхнем углу политики «Быстрая» в разделе «Плагины» (рис. 90) есть две пиктограммы. Данные пиктограммы отвечают за экспорт политики и ее дублирование

Вид интерфейса политики «Веб-приложения» представлен на рисунке (рис. 93).

| Сканер-ВС онализ защищенности | | 월 호 × 0 📕 호 × | | | | | | |
|--|--------------------------|---------------|--|--|--|--|--|--|
| Главная / Ресурсы / Политики / З | | | | | | | | |
| Веб-приложения | | | | | | | | |
| Имя: Веб-приложения Описание: Сканирование веб-сервисов Пользовательская: Нет Количество плагинов: 6119 | | Экспорт | | | | | | |
| Семейство | Семейство Всего платинов | | | | | | | |
| Port scanners | 15 | 2 | | | | | | |
| Settings | 12 | 12 | | | | | | |
| Web Servers | 402 | 402 | | | | | | |
| Web application abuses | 5703 | 5703 | | | | | | |
| Назад | | | | | | | | |

Рисунок 93 – Интерфейс политики «Веб-приложения»

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

– имя политики;

- описание политики;

– является ли политика пользовательской;

- количество используемых в политике плагинов.

В таблице интерфейса содержится следующая информация об используемых плагинах:

- семейства плагинов, используемых в данной политике;

- общее число плагинов в семействе;

- общее число плагинов, используемых в семействе.

3.6.5.3.4 Политика полного сканирования

Политика полного сканирования предназначена для сканирования всех известных уязвимостей. Вход для просмотра политики полного сканирования осуществляется нажатием на раздел политики «Полное сканирование» (рис. 94).



Полное сканирование

Сканирование всех известных уязвимостей

Рисунок 94 – Раздел политики «Полное сканирование» в интерфейсе «Политики»

Вид интерфейса «Полное сканирование» представлен на рисунке (рис. 95).

| Сканер-ВС | | 8 8 × 0 📕 4 × |
|--|----------------|-----------------------|
| Главная / Ресурсы / Политики / 4 | | |
| Полное сканирование | | |
| Имя: Полное сканирование Описание: Сканирование всех известных уязвимостей Пользовательская: Нет Количество плагинов: 47968 | | Экспорт |
| Семейство | Всего плагинов | Использовано плагинов |
| AIX Local Security Checks | 1 | 1 |
| Amazon Linux Local Security Checks | 748 | 748 |
| Brute force attacks | 9 | 9 |
| Buffer overflow | 562 | 562 |
| CISCO | 648 | 648 |
| CentOS Local Security Checks | 2476 | 2476 |
| Certified security software | 6 | 6 |
| Citrix Xenserver Local Security Checks | 30 | 30 |
| Compliance | 7 | 7 |
| Назад | | |

Рисунок 95 – Интерфейс «Полное сканирование»

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

- имя политики;
- описание политики;
- является ли политика пользовательской;
- количество используемых в политике плагинов.
- В таблице интерфейса содержится следующая информация об используемых плагинах:
- семейства плагинов, используемых в данной политике;
- общее число плагинов в семействе;
- общее число плагинов, используемых в семействе.

3.6.5.3.5 Новая политика

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

Вход для создания новой политики сканирования осуществляется нажатием на раздел создания политики «Новая» (рис. 96).



Создание собственной политики с нуля

Рисунок 96 – Раздел создания политики «Новая» в интерфейсе «Политики»

Вид интерфейса создания политики «Новая» представлен на рисунке (рис. 97).

| Сканер-ВС | | | | | | 썉 | × | 0 | - | 4 | × |
|--|---------------------------|-----|---|---|--|---|---|---|---|---|---|
| Главная / Ресурсы / Политики / 2 / Новая п | олитика | | | | | | | | | | |
| Базовые | Имя | | | | | | | | | | |
| Плагины | - | | | | | | | | | | |
| | Описание | | | | | | | | | | |
| | | | | | | | | | | | |
| | Выбор иканки для политики | × 🕑 | • | 3 | | | | | | | |
| Сохранить Отмена | | | | | | | | | | | |



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

- Базовые;

– Плагины.

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

– Имя политики;

- Описание политики;

– Выбор иконки для политики.

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

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

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

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

Вкладка «Плагины» представлена на рисунке (рис. 98).

| авная / Ресурсы / Политики / 2 | // Новая политика | |
|--------------------------------|--|---|
| Базовые | Санийство плогинов | Bassue |
| Плагины | | |
| | Nacra I | Buns |
| | Button AIX Local Security Checks | Buxon Mozilla Firefox ESR Multiple Vulnerabilities-01 September14 (Mac OS X) |
| | Выкл Amazon Linux Local Security Checks | Buxa Mozilla Firefox ESR Multiple Vulnerabilities - August 13 (Mac OS X) |
| | Brute force attacks | Build Firefox 'WebSockets' Denial of Service Vulnerability (Mac OS X) |
| | Buffer overflow | вымя Множественные уязвимости Mozilla Firefox ESR (Mac OS X) |
| | Biblikh CISCO | выхя Множественные уязвимости Mozilla Firefox ESR (Windows) |
| | Buikn CentOS Local Security Checks | вымя Множественные уязвимости Mozilla Firefox ESR - Aug15 (Windows) |
| | Bisikn Certified security software | Buxe Moxa NPort Devices Multiple Vulnerabilities |
| | Bision Citrix Xenserver Local Security Checks | Baxon Mozilla Firefox 'Password' Information Disclosure Vulnerability (Windows) |
| | Boxa Compliance | выкл Mozilla Firefox 'WebSockets' Denial of Service Vulnerability (Windows) |

Рисунок 98 – Интерфейс создания политики «Новая» (вкладка «Плагины»)

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

- Port scanners;

- Settings.

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

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

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

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

3.6.5.4. Управление словарями

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

- войти в раздел «Ресурсы»;

- выбрать интерфейс «Словари».

Вид интерфейса «Словари» представлен на рисунке (рис. 99).

| анализ защищенности | | * = × 0 🗜 ± x |
|-----------------------------|-----------------------------------|--|
| Главная / Ресурсы / Словари | | |
| Словари | | |
| # | Имя | Описание |
| 1 | Пользователи по-умолчанию (en+ru) | Самые популярные пользователи по-умолчанию для сетевых сервисов. |
| 2 | Топ 10 пользователей (en) | 10 самых популярных имен пользователей. |
| 3 | Топ 25 женских имен (en) | 25 самых популярных женских имен на латинице. |
| 4 | Топ 25 мужских имен (en) | 25 самых популярных мужских имен на латинице. |
| 5 | Цифры | 121 популярная цифирная комбинация. |
| 6 | Женские имена (en) | Более 140 самых популярных русских женских имен на латинице. |
| 7 | Клавиатурные сочетания (en) | Более 60 самых популярных клавиатурных сочетаний на латинице. |
| 8 | Мужские имена (en) | Более 120 самых популярных русских мужских имен на латинице. |
| 9 | Ton 150 (en) | 150 самых популярных паролей на латинице. |
| 10 | Ton 25 (en) | 25 самых популярных паролей на латинице. |
| | | 25 |

Рисунок 99 – Интерфейс «Словари»

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

- порядковый номер в таблице;

– имя;

– описание.

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

Вид интерфейса с подробным описанием словаря представлен на рисунке (рис. 100).

| Сканер-ВС | | 쑵 | | - | 4 | |
|-----------------------------------|-------|---|--|---|---|---|
| Главная / Ресурсы / Словари / 1 | | | | | | |
| Пользователи по-умолчанию (en+ru) | | | | | | T |
| ID | Имя | | | | | |
| 1 | root | | | | | |
| 2 | admin | | | | | |
| 3 | test | | | | | |



В интерфейсе подробного описания словаря присутствует таблица с двумя столбцами:

- номер пароля в словаре;

– имя (сам логин / пароль).

3.6.5.5. Управление списками портов

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

- войти в раздел «Ресурсы»;

- выбрать интерфейс «Списки портов».

Вид интерфейса «Списки портов» представлен на рисунке (рис. 101).

| Скан | нер-ВС ащищенности | | | 쓭 | - | * | 6 | | 4 | × |
|-------------------|-----------------------|---|---|---|----|-----|--------|-----|-----|---|
| Главная / Ресурсы | / Списки портов | | | | | | | | | |
| Списки портов | Имя | Описание | ТСР | | | UDP | | | | |
| 1 | Общеизвестные | Диапазон общеизвестных или системных ТСР портов для сканирова | 1-1023 | | | | | | | |
| 2 | Стандартные | Набор стандартных, зарегистрированных ТСР портов для сканиров: 1-80,82-113,11 | 15-224,242-248,256-257,259-269,280-284,286-287,308- | | | | | | | |
| 3 | Bce TCP | Полный диапазон ТСР портов (1-65535). Подходит для углубленного | 1-65535 | | | | | | | |
| | | | | | 25 | ۲ | 1 из 1 | « < | 1 > | » |

Рисунок 101 – Интерфейс «Списки портов»

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

- номер в таблице;
- имя;
- описание;
- ТСР-порты;
- UDР-порты.

3.6.5.6. Управление эксплойтами

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

- войти в раздел «Ресурсы»;

- выбрать интерфейс «Эксплойты».

Вид интерфейса «Эксплойты» представлен на рисунке (рис. 102).

| | | | | | | _ |
|---------|--|---|-------|----------|--------|----|
| | Сканер-ВС анализ защищенности | 8 a × 0 | i) | • | ۵. | |
| Главная | Ресурсы / Эксплойты | | | | | |
| Экспло | йты Имя | Описание | Легко | сть эксп | луатац | ии |
| 1 | Штрих-код Firefox Exec из привилегированной оболочки Javascript | штрих-код Firefox Exec из привилегированной оболочки Javascript Этот модуль позволяет выполнять собственные полезные нагрузи из привилегированной оболочки Firefox Javascript. Он помещает уназанную полезную нагрузиу в памяль, добавляет необходимые флаги защиты и вызывает ее, что может быть полезно для обновления оболочки јаvascript Firefox на сеанс Meterpreter, не касавсь диска. | | | | |
| 2 | Демон службы службы диспетчера календаря AIX (rpc.cmsd) Переполнение буфера переполнения кода 21 | Этот модуль использует уязвимость переполнения буфера в коде 21 операции, обрабатываемом грс.сmsd в AIX. Делая запрос с длинной строкой, переданной первому аргументу RPC Ytable_create, происходит переполнение буфера на основе стека. Это приводить и произовлютения оказа ПРИМЕЧАНИЕ Неуданены польтия моут привести к тому, что ineld / portmapper войдет в состояние, когда дальнейшие польтки невозможны. | | Высок | ая | |

Рисунок 102 – Интерфейс «Эксплойты»

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

- номер в таблице;

– имя;

– описание;

- легкость эксплуатации.

3.6.6. Тестирование защищенности

3.6.6.1. Общее описание

Для каждого тестирования защищенности создается проект, представляющий собой совокупность всех данных, относящихся к текущему тестированию. Проект включает в себя исходные данные фаз тестирования (поиск целей, поиск уязвимостей, сетевой аудит паролей, поиск эксплойтов) и результаты тестирования в фазе «Отчетность» в виде сгенерированных отчетов. Для проведения тестирования защищенности пользователь может создать новый проект или, в случае продолжения, начатого ранее и сохраненного тестирования, использовать его.

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

В рамках задач по тестированию защищенности Оператор может выполнить:

- поиск целей (пп. 3.6.6.2);

- поиск уязвимостей (пп. 3.6.6.3);

– эксплуатацию (пп. 3.6.6.4);

- отчетность (пп. 3.6.6.5).

3.6.6.2. Поиск целей

3.6.6.2.1 Общее описание

В начале тестирования обязательным этапом является поиск целей – обзор локальной сети, к которой подключен ПК «Сканер-ВС», с целью выявления объектов тестирования для следующих фаз проверки. Поиск целей производится путем сканирования IP-адресов и портов (TCP- и UDPпортов) компьютеров, присоединенных к локальной сети. Без поиска целей невозможно использовать все возможности ПК «Сканер-ВС», в частности, невозможно производить поиск эксплойтов (см. пп. 3.6.6.4 «Эксплуатация»). Найденные в результате поиска целей действующие подключения с IP-адресами и задействованными TCP- и UDP-портами далее будем называть «Активами». Данные о них располагаются в секторе «Поиск целей» вовкладках «Хосты» и «Порты» в виде таблиц. Дополнительно поиск целей может быть использован для определения сервисов (служб), запущенных на включенном в сеть компьютере, для идентификации ОС и приложений, а также для трассировки маршрутов следования данных в сетях для построения топологии сети.

3.6.6.2.2 Поиск целей

Настройки, необходимые для запуска сканирования сети, находятся во вкладке «Базовые», где в поле ввода «Цели» Оператор задает цели сканирования: конкретный IP-адрес, множество IPадресов, сеть или подсеть. Данное поле является обязательным к заполнению (рис. 103).

| Сканер- | ВС юсти | | 쑙 | * | i | 5 | 4 | × |
|----------------------------|--------------------------------|---|-------|---|---|---|---|---|
| Главная / Проекты / 1 / По | иск целей / Новое сканирование | | | | | | | |
| Базовые | Цели 📀 📩 | Пример: 192.168.1.1, 192.168.1.0/24, 192.168.0. | .1-16 | | | | | |
| Расширенные | | | | | | | | |
| Задача | | Цели - обязательное поле. | | | | | | |
| | | 🗮 Импорт целей из активов 🛛 🕒 Импорт из ф | райла | | | | | |
| Создать Отмена | | | | | | | | |

Рисунок 103 – Пример базовых настроек

Дополнительные настройки сканирования сети расположены во вкладке «Расширенные» и используются пользователем при необходимости (рис. 104).

| анализ защищенн | вс | | 쓭 | ∗ | Û | 4 | × |
|----------------------------|------------------------------------|-------------|---|---|---|---|---|
| Главная / Проекты / 1 / По | иск целей / Новое сканирование | | | | | | |
| Базовые | Сканировать конкретные ТСР-порты 😡 | | | | | | |
| Расширенные | Определять версию сервисов 🚱 | P | | | | | |
| Залаца | Трассировка пути 🚱 | | | | | | |
| бидичи | Сканировать конкретные UDP-порты 🕜 | | | | | | |
| | Скорость сканирования 😡 | Оптимальная | | | - | | |
| | Таймаут сканирования, сек 😡 | | | | | | |
| | Игнорировать результаты Ping 😡 | 0 | | | | | |



Рисунок 104 – Дополнительные настройки сканирования

Расширенный настройки представлены в виде следующих опций:

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

Скорость сканирования. Опция включается для выбора скорости сканирования:

- 1) минимальная, низкая попытка обхода систем обнаружения вторжения;
- 2) нормальная незначительное использование пропускной способности сети и ресурсов;
- 3) оптимальная обычный режим(рекомендуется);
- 4) высокая, максимальная возможно снижение точности результатов сканирования сети.
- Таймаут сканирования, сек. Опция используется, для пропуска целевых хостов, время сканирования которых превышает установленный таймаут;
- Игнорировать результаты Ping. Опция включается, если необходимо обнаружение хостов с помощью TCP SYN вместо Ping.

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

Во вкладке «Задача» Оператор задает имя и описание текущего сканирования в соответствующих пустых полях (рис. 105). Если поля оставить пустыми, они будут заполнены автоматически, исходя из установленных настроек сканирования. При включении тумблера «Автозапуск» задача автоматически запуститься сразу после ее создания.

| сканер | Э-ВС енности | | - | i | 4 | 4 | 5 |
|---------------------|--|------------------|---|----|---|---|---|
| ная / Проекты / Нов | вое тестирование / Поиск целей / Новое ска | нирование | | | | | |
| азовые | Имя @ | Введите имя | | | | | |
| асширенные | | | | | | | |
| адача | Описание 😡 | Введите описание | | | | | |
| | | | | li | | | |
| | Автозапуск 🚱 | | | | | | |
| оздать Отмена | | | | | | | |

Рисунок 105 – Имя и описание сканирования

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

3.6.6.2.3 Запуск задачи

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

Успешное завершение сканирования представлено на рисунке (рис. 106).

| | Сканер-ВС | | | | * = | × 6 | - 🦊 i | s x |
|---------|-----------------------------|--------------------------|--------------------------|-----------|-----------|----------------------------|----------|------|
| Главная | / Проекты / 1 / Поиск целей | | | | | | | |
| Хость | и Порты Тополо | гия Задачи | | | | | | |
| Новое | сканирование | | | | | | T | |
| # | Имя | Время последнего запуска | Время последнего заверше | Подробнее | Состояние | | Действия | |
| 1 | Сканирование 172.16.10.11 | 19.12.2018 9:36:54 | 19.12.2018 9:37:10 | | Завершена | 2 | 🛍 C 🗈 | |
| | | | | | 25 | 1 из 1 | « < 1 | > >> |

Рисунок 106 – Процесс сканирования

После завершения сканирования можно просмотреть подробную информацию о выполненной задаче (см. пп. 3.6.3.2.2).

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

После завершения сканирования во вкладке «Хосты» в таблице показаны IP-адрес, имя хоста, МАС-адрес, операционная система (далее – ОС) и тип устройства, который им соответствует (рис. 107).

| | Сканер- | •ВС | | | | | 썉 | ÷ | * | 6 | 5 | 4 | × |
|-----------|-----------------|------------|---------|-----------|-----------|--------------|---------|----|-------|-----------|--------------------------|---------|---|
| Главная / | Проекты / 1 / П | оиск целей | | | | | | | | | | | |
| Хосты | Порты | Топология | Задачи | | | | | | | | | | |
| | | | | | | | | | | * | T | | |
| # | Адрес | Обновл | пено | Имя хоста | МАС-адрес | Операционна | я систе | ма | | Тип у | стройства | a | |
| 1 | 172.16.10.11 | 19.12.2018 | 9:37:09 | | | Linux 2.6.16 | - 2.6.2 | 1 | устро | ойство об | іщег <mark>о н</mark> аз | значени | я |
| | | | | | | | | 25 | • | 1 из 1 | κ κ | 1 > | * |

Рисунок 107 – Вкладка «Хосты»

После завершения сканирования во вкладке «Порты» появятся данные об открытых портах, запущенных сервисах, продуктах и номерах версий, которые будут сгруппированы в таблицу (рис. 108).

89 НПЭШ.00606-01 34

| | Сканер- | вс | | | | | 쌸 | | × | 6 | 5 | 4 | × |
|-----------|------------------|------------|------|-----------|--------------------|--------------|-----|------|---|---|--------|---|---|
| Главная / | Проекты / 1 / По | риск целей | | | | | | | | | | | |
| Хосты | Порты | Топология | 3a, | дачи | | | | | | | | | |
| | | | | | | | | | | ± | T | | |
| # | Адрес | Протокол | Порт | Состояние | Обновлено | Сервис | Про | дукт | | | Версия | | |
| 1 | 172.16.10.11 | tcp | 22 | открыт | 19.12.2018 9:37:09 | ssh | | | | | | | |
| 2 | 172.16.10.11 | tcp | 25 | открыт | 19.12.2018 9:37:09 | smtp | | | | | - | | |
| 3 | 172.16.10.11 | tcp | 53 | открыт | 19.12.2018 9:37:09 | domain | | | | | | | |
| 4 | 172.16.10.11 | tcp | 111 | открыт | 19.12.2018 9:37:09 | rpcbind | | | | | | | |
| 5 | 172.16.10.11 | tcp | 139 | открыт | 19.12.2018 9:37:09 | netbios-ssn | | | | | - | | |
| 6 | 172.16.10.11 | tcp | 445 | открыт | 19.12.2018 9:37:09 | microsoft-ds | | | | | 2 | | |
| 7 | 172.16.10.11 | tcp | 1099 | открыт | 19.12.2018 9:37:09 | rmiregistry | | | | | | | |
| 8 | 172.16.10.11 | tcp | 2049 | открыт | 19.12.2018 9:37:09 | nfs | | | | | | | |
| 9 | 172.16.10.11 | tcp | 2121 | открыт | 19.12.2018 9:37:09 | ccproxy-ftp | | | | | 2 | | |
| 10 | 172.16.10.11 | tcp | 3306 | открыт | 19.12.2018 9:37:09 | mysql | | | | | - | | |
| 11 | 172.16.10.11 | tcp | 5432 | открыт | 19.12.2018 9:37:09 | postgresql | | | | | - | | |

Рисунок 108 – Вкладка «Порты»

После завершения сканирования во вкладке «Топология» (рис. 109). Во вкладке приведена топология сети в виде рисунка. Слева приведены примеры значков и их значение.

| C C | канер- | вс | |
|-------------|----------------|------------|--------|
| Главная / П | роекты / 1 / П | оиск целей | |
| Хосты | Порты | Топология | Задачи |
| | | | |
| | | | |
| Компью | тер | | |
| | • | | |
| Принт | ep | | |
| Неизвес | стно | | |
| 3 | | | |
| Маршрути | ізатор | | |
| 2 | | | |
| Веб-кам | ера | | |
| Terech | 04 | | |
| Tenet | UN I | | |
| Подсе | ть | | |
| 0 | 1 | | |

Рисунок 109 – Вкладка «Топология»

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

- « = » выбор источника отображения топологии;
- « 😵 » выбор опции отображения топологии (анимированные значки или статические);
- « « сохранение топологии в графический файл.

3.6.6.2.4 Завершение работы

После завершения работы «Поиск целей» состояние задачи изменится на «Завершена» (рис 110).

| # | Имя | Время последнего запуска | Время последнего заверше | Подробнее | Состояние | | Д | ейств | ИЯ |
|---|---------------------------|--------------------------|--------------------------|-----------|-----------|---|---|-------|----|
| 1 | Сканирование 172.16.10.11 | 19.12.2018 9:36:54 | 19.12.2018 9:37:10 | | Завершена | 2 | m | C | Û |

Рисунок 110 – Завершение поиска целей

Для завершенной задачи доступны следующие действия:

– « ² » – клонировать. Создается копия клонируемой задачи;

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

- « ^С » перезапустить. Задача перезапускается;
- « ^т » удалить. Происходит удаление задачи из списка.

3.6.6.3. Поиск уязвимостей

3.6.6.3.1 Общее описание

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

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

- 0,1-3,9 - низкий уровень;

- 4,0-6,9 - средний уровень;

- 7,0-8,9 - высокий уровень;

– 9,0-10,0 - критический уровень.

3.6.6.3.2 Поиск уязвимостей

Настройки, необходимые для запуска поиска уязвимостей, находятся во вкладке «Базовые» (рис. 111), где Оператор задает цели поиска уязвимостей (IP-адреса проверяемых компьютеров, сетей или подсетей) и выбирает политику сканирования (набор правил сканирования): базовую

(быструю, сканирование веб-сервисов, либо полное сканирование) или пользовательскую, настраиваемую Оператором. Создание пользовательской политики описано в подпункте 3.6.5.3.

| сканер-В | C TH | 2 | 8 | × | 0 | 5 | 4 | × |
|-------------------------------|------------------------------------|--|----|---|---|----------|---|---|
| Главная / Проекты / 1 / Поисн | к уязвимостей / Новое сканирование | | | | | | | |
| Базовые | Политика сканирования 😡 | Быстрая | | • | | | | |
| Выявление хостов | Цели 😧 📩 | Пример: 192.168.1.1, 192.168.1.0/24, 192.168.0.1-1 | 6 | | | | | |
| Сканирование портов | | | | | | | | |
| Расширенные | | ≡ Импорт целей из активов 🛛 🕒 Импорт из фай. | ла | | | | | |
| Задача | | | | | | | | |
| Создать Отмена | | | | | | | | |

Рисунок 111 – Основные настройки сканирования

Далее необходимо выбрать политику сканирования. По умолчанию установлена «Быстрая». Если необходимо сменить политику сканирования, нужно нажать кнопку «Быстрая» (по умолчанию) и выбрать одну из базовых политик или создать свою (рис. 112). Описание создания политики приведено в пп. 3.6.5.3.5.

| Сканер-ВС анализ защищенности | | 쌸 | | ≭ | i | - | 4 | × |
|---|--------------------------------------|--|--|------------------------|---|---|---|---|
| Главная / Проекты / 123 / Поиск уязвимосте | й / Новое сканирование | | | | | | | |
| Базовые Выявление хостов Сканирование портов Расширенные Задача | Политика сканирования © Цели © | Быстрая Быстрая Веб-прило Полное ска 192.168.0.1 Цели обязате | жения анирова -16 ельное по целей из | ние оле. активов | | | | |
| | | 💾 Импорт и | 13 файла | | | | | |
| Создать Отмена | | | | | | | | |
| | | | | | | | | |

Рисунок 112 – Выбор политики сканирования

Во вкладке «Задача» (рис. 113) Оператор задает имя и описание в соответствующие пустые поля. Если поля оставить пустыми, они будут заполнены автоматически, исходя из указанных настроек сканирования.

| Сканер-В | Сти | | 쑵 | ∗ | i | 5 | 4 | × |
|------------------------------|------------------------------------|------------------|---|---|---|---|---|---|
| Главная / Проекты / 1 / Поис | к уязвимостей / Новое сканирование | | | | | | | |
| Базовые | Имя 😡 | Введите имя | | | | | | |
| Выявление хостов | | | | | | | | |
| Сканирование портов | Описание 😡 | Введите описание | | | | | | |
| Расширенные | | | | | | | | |
| Задача | Автозапуск 🚱 | | | | | | | |
| Создать Отмена | | | | | | | | |

Рисунок 113 – Имя и описание сканирования

Дополнительные опции сканирования расположены во вкладках «Выявление хостов», «Сканирование портов», «Расширенные» (рис. 113) и используются Оператором при необходимости.

Опции, расположенные во вкладке «Выявление хостов»:

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

Опции, расположенные во вкладке «Сканирование портов»:

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

Опции, расположенные во вкладке «Расширенные»:

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

- Количество проверок. Максимальное количество проверок, которые будут выполняться одновременно с данным хостом.
- Для начала процесса сканирования необходимо нажать кнопку «Создать» (рис. 113).

3.6.6.3.3 Завершение работы

После завершения сканирования в таблицу во вкладке «Задачи» будет добавлена строка, содержащая следующие поля (рис. 114):

- номер задачи;
- имя;
- время последнего запуска;
- время последнего завершения;
- подробнее;
- состояние;
- действия.

Для завершенной задачи доступны следующие действия:

- « ^С » клонировать. Создается копия клонируемой задачи;
- « ^ш » запланировать. Задается дата и время запуска задачи;

- « ^С » – перезапустить. Задача перезапускается;

– « ^¹ » – удалить. Происходит удаление задачи из списка.

| | Сканер-ВС анализ защищенности | | | | 뿉 | - | * | 0 | 2 | ۵ | × |
|--------|-----------------------------------|--------------------------|--------------------------|-----------|------|-------|-----|------|-------|-----|---|
| Главна | ая / Проекты / 1 / Поиск уязвимос | тей | | | | | | | | | |
| Уязі | вимости Задачи | | | | | | | | | | |
| Нов | ое сканирование | | | | | | | | T | | |
| # | Имя | Время последнего запуска | Время последнего заверше | Подробнее | Сост | ояние | | | Дейст | зия | |
| 4 | Поиск уязвимостей для 192.168 | 19.12.2018 10:51:40 | 19.12.2018 10:54:14 | | Заве | ршена | | 20 | C | Û | |
| 3 | Поиск уязвимостей для 172.16. | 19.12.2018 10:48:27 | 19.12.2018 11:00:19 | | Отм | енена | | 20 | C | Û | |
| | | | | | | 25 | ۰ 1 | из 1 | « ‹ | 1 > | > |

Рисунок 114 – Результат сканирования

После завершения сканирования во вкладке «Уязвимости» появятся данные об обнаруженных уязвимостях, которые будут сгруппированы в таблицу (рис. 115).

| Уязви | мости | Задачи | | | | | |
|-------|------------|--------|--|---------------------|-----|-----------|-------------------|
| | | | | | | | ± T |
| # | Адрес | Порт | Описание | Обновлено | CVE | BDU | Уровень опасности |
| 1 | 192.168.1. | 1 - | Удаленный хост использует временные метки TCP, с их помощью злоумышленник может вычислить время безотказной работы. | 19.12.2018 10:54:13 | | | Низкий |
| | | | | | 25 | 💿 (1 из 1 | « < 1 > » |

Рисунок 115 – Результаты поиска

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

3.6.6.4. Эксплуатация

3.6.6.4.1 Общее описание

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

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

3.6.6.4.2 Поиск эксплойтов

Для проведения тестирования возможности несанкционированного удаленного использования ресурсов компьютера необходимо выбрать вкладку «Поиск эксплойтов» (рис. 116).

| | сканер | Р-ВС | | | 쌸 | - | × | 6 | _ | ۵ | × |
|-----------|---------------|-----------------------|-----------|--------------------|---|---------|---|-----|-----------|---------|----|
| Главная / | Проекты / 1 / | Эксплуатация | | | | | | | | | |
| Поиск | эксплойтов | Сетевой аудит паролей | Задачи | | | | | | | | |
| Новое | сканирование | | | | | | | | | | |
| # | Адрес | Путь | Обновлено | Название эксплойта | O | писание | | Лег | кость экс | плуатац | ии |
| | | | Эксплой | ітов не обнаружено | | | | | | | |
| | | | | | | | | | | | |

Рисунок 116 – Вкладка «Поиск эксплойтов»

После нажатия кнопки «Новое сканирование» откроется интерфейс нового поиска эксплойтов (рис. 117) с тремя вкладками настроек:

- базовые;
- расширенные;
- задача.

| Сканер- | 쑙 | ÷ | * | 6 | - | 4 | × | | |
|---------------------------|----------------------------------|---------------------------------|---|-----------|----------|---|---|--|--|
| Главная / Проекты / 1 / З | жсплуатация / Новое сканирование | | | | | | | | |
| Базовые | Тил 😡 | Автоматический поиск эксплойтов | | | | • | | | |
| Расширенные | Цели 😡 🔹 | Выделить все | E | выбрано > | остов: 0 | | | | |
| Задача | | 45 | | | | | | | |
| | | 172.16.10.11 | | | | | | | |
| | | 192.168.1.1 | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| Создать Отмена | | | | | | | | | |

Рисунок 117 – Интерфейс нового поиска эксплойтов

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

При выборе автоматического поиска эксплойтов, во вкладке «Расширенные» нужно указать критерии поиска эксплойтов: «Тип сервиса», «Продукт», «Версия». Тумблер «Строгий поиск» добавляет условие, что по выбранным критериям будет проведен поиск эксплойтов, для которых все выбранные параметры поиска будут иметь заданные значения, если тумблер выключен, будет произведен поиск эксплойтов, для которых совпадает хотя бы один параметр поиска.

При выборе ручного поиска эксплойтов, во вкладке «Расширенные» в многострочное поле «Ключевые слова» необходимо ввести параметры поиска – фрагменты текста, которые должны обязательно присутствовать в названии, описании и других данных эксплойта из базы эксплойтов. Одна строка многострочного поля должна содержать только одно значение. Поиск будет производиться аналогично строгому поиску.

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

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

Результаты завершения работы приведены в пп. 3.6.6.4.4.

3.6.6.4.3 Сетевой аудит паролей

Для проведения сетевого аудита паролей необходимо перейти во вкладку «Сетевой аудит паролей» и нажать кнопку «Новое сканирование» (рис. 118).

| | Сканер | -ВС | | | | | | * | ∗ | 0 | 13 | 4 | × |
|---------|-----------------|--------------|--------------|--------|------------------|----------------------|-------|----|-------|-----|--------|---|---|
| Главная | / Проекты / 1 / | Эксплуатация | | | | | | | | | | | |
| Поис | к эксплойтов | Сетевой а | удит паролей | Задачи | | | | | | | | | |
| Новое | сканирование | | | | | | | | | | | | |
| # | Адрес | Порт | Обновл | ено | Сервис | Логин | Парол | ٦ь | | Сто | йкость | | |
| | | | | | | สดษับเอ อธิบอตาสะดบอ | | | | | | | |
| | | | | | подооранных паро | лей не обнаружено | | | | | | | |

Рисунок 118 – Интерфейс запуска подбора паролей

После нажатия кнопки «Новый подбор паролей» откроется интерфейс нового подбора пароля (рис. 119) с пятью вкладками настроек:

- базовые;
- пользователи;
- пароли;

– расширенные;

– задача.

| Сканер-ВС | | | | * | • | 6 | , | د ۵ | c . |
|---|----------------|---|----|---|---|---|----------|-----|-----|
| Павная / Проекты / 123 / Экоплуатация / Новый пор | dop naponeń | | | | | | | | |
| Базовые | Сервис 😡 🔹 | ftp | ٣ | | | | | | |
| Пользователи | Указать порт 😡 | ()P | | | | | | | |
| Пароли | Цели 🔍 🔸 | Danwer 1921981.02 1921981.024 | | | | | | | |
| Расширенные | | Цели обязательное поле | 11 | | | | | | |
| Задача | | ≡ Импорт целей из активов Мипорт из файла | | | | | | | |
| Создать Отмена | | | | | | | | | |

Рисунок 119 – Интерфейс нового подбора пароля

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

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

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

- Пользователи по умолчанию (en+ru);

- Топ 10 пользователей (en);

- Топ 25 женских имен (en);

- Топ 25 мужских имен (en).

Во вкладке «Пароли» в поле «Пароли» необходимо указать комбинации букв и цифр, которые будут использоваться в качестве аутентификационной информации. Каждая комбинация должна находиться на отдельной строке. Настройки программы поддерживают загрузку паролей из файла в формате ТХТ, где одна строка документа должна содержать только один пароль.

Дополнительно, можно включить следующие опции:

– Проверить пустой пароль;

– Проверить пароль, совпадающий с логином;

– Проверить пароль, совпадающий с логином в обратном порядке.

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

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

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

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

Результаты завершения работы приведены в пп. 3.6.6.4.4.

3.6.6.4.4 Завершение работы

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

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

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

- очень слабый - любой ПК, несколько минут;

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

- нормальный - специализированный ПК, один год;

- надежный - большая скоординированная атака, более года;

– очень надежный – практически невозможно подобрать.

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

Информация о выполненной задаче появится во вкладке «Задачи» (рис. 120).

| | Сканер-ВС анализ защищенности | 8 8 | * • | • | 14 | 4 | × | | | |
|---------|----------------------------------|--------------------------|--------------------------|-----------|-----------|-----------|-----------|---------|-----|---|
| Главная | а / Проекты / 1 / Эксплуатация | | | | | | | | | |
| Поис | ск эксплойтов Сетевой а | удит паролей Задачи | 0 | | | | | | | |
| | | | | | | | | T | | |
| # | Имя | Время последнего запуска | Время последнего заверше | Подробнее | Состояние | | р | lействи | я | |
| 7 | Онлайн подбор паролей для 1: | 19.12.2018 12:28:49 | 19.12.2018 12:43:40 | A | Ошибка | 2 | m | C | Û | |
| 6 | 1 | 19.12.2018 12:27:25 | 19.12.2018 12:27:27 | | Завершена | 2 | 61 | C | Û | |
| 5 | 1 | 19.12.2018 12:21:53 | 19.12.2018 12:21:55 | | Завершена | 2 | m | C | ŧ. | |
| | | | | | 25 | 💿 (1 из 1 | × | < | 1 > | * |

Рисунок 120 – Данные о завершенной задаче

Для завершенной задачи доступны следующие действия:

– « ^С » – клонировать. Создается копия клонируемой задачи;

- « ^ш » запланировать. Задается дата и время запуска задачи;
- « ^С » перезапустить. Задача перезапускается;
- « ^¹ » удалить. Происходит удаление задачи из списка.

3.6.6.5. Отчетность

3.6.6.5.1 Общее описание

Документирование является неотъемлемой частью анализа защищенности информационной системы. Для объединения результатов всех этапов тестирования в ПК «Сканер-ВС» используется сектор «Отчет» (номер 4 на рисунке (рис. 69), с помощью которого можно построить отчет с результатами тестирований.

3.6.6.5.2 Настройки отчета

После того как был выбран сектор «Отчет», в нем отображается страница с двумя вкладками (рис. 121).

– отчеты;

– задачи.

| Сканер-ВС | | | | | |
|--------------------------------------|--------------------------|-----------------------------|-----------|-----------|----------------------|
| Главная / Проекты / 123 / Отчетность | | | | | |
| Отчеты Задачи | | | | | |
| Новый отчет | | | | | |
| # Имя | Время последнего запуска | Время последнего завершения | Подробнее | Состояние | Действия |
| | | Задач не найдено | | | |
| | | | | | |
| | | | | 25 | • 0x0 < < > > |

Рисунок 121 - Сектор «Отчет»

Во вкладке «Отчеты» отображаются готовые отчеты.

Во вкладке «Задачи» выполняется создание нового отчета.

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

Интерфейс создания нового отчета представлен на рисунке (рис. 122).

| Сканер | сканер-ВС | | | | | | ∗ | i | 14 | 4 | × |
|-------------------------|--------------------------|--|-----------------------|--|--|--|------------|---|----|---|---|
| Главная / Проекты / 1 / | Отчетность / Новый отчет | | | | | | | | | | |
| Базовые | Тип отчета | | Краткий | | | | | · | | | |
| Цели | Дата | | 19 дек. 2018 13:51:13 | | | | m 0 | | | | |
| Расширенные | | | | | | | | | | | |
| Задача | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| Создать Отмена | | | | | | | | | | | |

Рисунок 122 – Интерфейс создания нового отчета

В интерфейсе создания нового отчета присутствует четыре вкладки настроек:

- базовые;
- цели;
- расширенные;
- задача.

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

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

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

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

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

Отчет может быть:

– кратким;

– полным;

- динамическим.

Краткий отчет состоит из минимума основных сведений:

1) резюме для руководства;

2) границы проекта;

3) порты и сервисы;

4) уязвимости:

- уязвимость 1;

- уязвимость 2;

- уязвимость 3;

• • • • •

- уязвимость n;

5) скомпрометированные учетные данные;

6) эксплойты.

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

Отчет можно экспортировать в формат HTML, PDF, DOC.

Полный отчет содержит следующие разделы:

1) резюме для руководства;

2) границы проекта;

3) тестируемый хост 1:

– порты и сервисы;

- уязвимости;

- скомпрометированные учетные данные;

- эксплойты;

4) тестируемый хост 2:

- порты и сервисы;

- уязвимости;

- скомпрометированные учетные данные;

- эксплойты;

• • • • •

5) тестируемый хост п:

- порты и сервисы;

- уязвимости;

- скомпрометированные учетные данные;

– эксплойты.

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

Отчет можно экспортировать в формат HTML, PDF, DOC.

Динамический отчет содержит следующие разделы:

- резюме для руководства;

- границы проекта;

- порты и сервисы;

- уязвимости;

- скомпрометированные учетные данные;

- эксплойты.

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

Отчет можно экспортировать в формат HTML, PDF, DOC.

3.6.6.5.3 Завершение работы

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

3.6.6.6. Задачи

В Разделе «Задачи» представлен перечень всех задач проекта (рис. 123):

- поиск целей;
- поиск уязвимостей;
- эксплуатация;
- отчетность.

| а/ П | роекты / 1 / Залачи | | | | | | | | |
|------|-------------------------------|--------------------------|-------------------------|-----------|-----------|----------|----------|--------|---|
| | poonder it output | | | | | | | | |
| адач | ни Расписание | | | | | | | | |
| | | | | | | | | T | |
| # | Имя | Время последнего запуска | Время последнего заверш | Подробнее | Состояние | | Д | ействи | я |
| 9 | Краткий отчет по проекту 1 на | 19.12.2018 14:03:51 | 19.12.2018 14:03:53 | | Завершена | a | Û | | |
| 8 | полный | 19.12.2018 14:01:15 | 19.12.2018 14:01:17 | | Завершена | 2 | Û | | |
| 7 | Онлайн подбор паролей для | 19.12.2018 12:28:49 | 19.12.2018 12:43:40 | A | Ошибка | 2 | | C | Û |
| 6 | 1 | 19.12.2018 12:27:25 | 19.12.2018 12:27:27 | | Завершена | 2 | | С | Û |
| 5 | 1 | 19.12.2018 12:21:53 | 19.12.2018 12:21:55 | | Завершена | 2 | | C | Û |
| 4 | Поиск уязвимостей для 192.16 | 19.12.2018 10:51:40 | 19.12.2018 10:54:14 | | Завершена | 2 | | C | Û |
| 3 | Поиск уязвимостей для 172.16 | 19.12.2018 10:48:27 | 19.12.2018 11:00:19 | | Отменена | a | | C | Û |
| 1 | Сканирование 172.16.10.11 | 19.12.2018 9:36:54 | 19.12.2018 9:37:10 | | Завершена | 2 | m | C | Û |

Рисунок 123 – Раздел «Задачи»

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

- задачи;
- расписание.

3.6.6.6.1 Вкладка «Задачи»

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

| a | Сканер-ВС нализ защищенности | | | | <u> </u> | * | 1 | 18 | * | |
|-------|---------------------------------|--------------------------|-------------------------|-----------|-----------|----------|----------|---------|----|--|
| a / T | Троекты / 1 / Задачи | | | | | | | | | |
| ада | чи Расписание | | | | | | | | | |
| | | | | | | | | T | | |
| # | Имя | Время последнего запуска | Время последнего заверш | Подробнее | Состояние | | Ļ | Цействи | 19 | |
| 9 | Краткий отчет по проекту 1 на | 19.12.2018 14:03:51 | 19.12.2018 14:03:53 | | Завершена | 4 | D | | | |
| 8 | полный | 19.12.2018 14:01:15 | 19.12.2018 14:01:17 | | Завершена | 4 | D | | | |
| 7 | Онлайн подбор паролей для | 19.12.2018 12:28:49 | 19.12.2018 12:43:40 | A | Ошибка | 4 | | C | Û | |
| 6 | 1 | 19.12.2018 12:27:25 | 19.12.2018 12:27:27 | | Завершена | e e | | C | Û | |
| 5 | 1 | 19.12.2018 12:21:53 | 19.12.2018 12:21:55 | | Завершена | e e | | C | Û | |
| 4 | Поиск уязвимостей для 192.16 | 19.12.2018 10:51:40 | 19.12.2018 10:54:14 | | Завершена | e e | | C | Û | |
| 3 | Поиск уязвимостей для 172.16 | 19.12.2018 10:48:27 | 19.12.2018 11:00:19 | | Отменена | 4 | | C | â | |
| 1 | Сканирование 172.16.10.11 | 19.12.2018 9:36:54 | 19.12.2018 9:37:10 | | Завершена | e e | 6 | C | Û | |

Рисунок 124 – Вкладка «Задачи»

В таблице (см. Таблица 7) содержится описание столбцов вкладки «Задачи».

Таблица 7 – Описание полей вкладки «Задачи»

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

Для задачи доступны следующие действия:

– « ^С » – клонировать. Создается копия клонируемой задачи;

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

– « ^С » – перезапустить. Задача перезапускается;

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

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

Для создания или редактирования задач необходимо перейти в соответствующие разделы.

3.6.6.6.2 Вкладка «Расписание»

Во вкладке «Расписание» (рис. 125) представлены только запланированные задачи.

| Сканер-ВС анализ защищенности | | | | 쓭 | - | | | | 4 | |
|----------------------------------|----------------------|------------|----------------------|---|----|--------------|------------|-----|-----|--|
| Главная / Проекты / 1 / Задачи | | | | | | | | | | |
| Задачи Расписание | | | | | | | | | T | |
| Задача | Время | Дни недели | Начало | | | Кон | ец | | | |
| 1 | 07.12.2018, 10:57:55 | | 07.12.2018, 10:57:55 | | 07 | .12.2018 | 8, 10:57:5 | 5 | | |
| | | | | 2 | 5 | • <u>1</u> и | a1 « | < 1 | > » | |

Рисунок 125 – Вкладка «Расписание»

В таблице (см. Таблица 7) содержится описание столбцов вкладки «Расписание».

Таблица 8 – Описание полей вкладки «Расписание»

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

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

3.6.6.6.3 Завершение работы

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

– « ^С » – клонировать. Создается копия клонируемой задачи;

– « ⁽¹¹⁾ » – запланировать. Задается дата и время запуска задачи;

– « ^С » – перезапустить. Задача перезапускается;

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

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

3.7. Инструменты

3.7.1. Общее описание

Раздел «Инструменты» (рис. 126) объединяет в себе основные инструменты для работы ПК «Сканер-ВС». В раздел «Инструменты» можно попасть, нажав на пиктограмму «



Рисунок 126 – Раздел «Инструменты»

- В Разделе «Инструменты» представлены следующие виды инструментов:
- аудит OC Astra Linux (п. 3.7.2);
- локальный аудит паролей (п. 3.7.3);
- поиск остаточной информации (п. 3.7.4);
- аудит обновлений ОС MS Windows (п. 3.7.5);
- системный аудитор (п. 3.7.6);
- гарантированное уничтожение информации (п. 3.7.7);
- аудит беспроводных сетей (п. 3.7.8);
- сетевой анализатор (п. 3.7.9);
- контрольное суммирование (п. 3.7.10).

Примечание. Раздел «Инструменты» и пиктограмма «Инструменты» доступны только в Локальной версии ПК «Сканер-ВС».

3.7.2. Инструмент «Аудит ОС Astra Linux»

Инструмент «Аудит OC Astra Linux» предназначен для аудита настроек комплекса средств защиты OC специального назначения «Astra Linux Serial Edition» по требованиям безопасности.

3.7.2.1. Запуск инструмента

Инструмент запускается из веб-интерфейса «Аудит ОС Astra Linux» или из подменю стартера приложений. Для запуска инструмента необходимо выполнить следующие действия:

- запустить подменю стартера приложений;

- выбрать вкладку «Поиск уязвимостей»;
- выбрать инструмент «Аудит ОС Astra Linux» (рис. 127).



Рисунок 127 – Инструмент «Аудит ОС Astra Linux»

После запуска откроется окно терминала (рис. 128).


Рисунок 128 – Окно терминала

3.7.2.2. Работа с инструментом

Для запуска процесса аудита, необходимо запустить скрипт на проверяемой рабочей станции. Для этого в терминале необходимо прописать команду, в которой указаны пользователь и IP-адрес тестируемой рабочей станции и нажать клавишу «Enter». Дополнительно можно указать папку для сохранения отчета. На рисунке (рис. 129) показан пример команды запуска скрипта на рабочей станции с IP-адресом 192.168.5.76 под учетной записью пользователя echelon и указанной папкой / для сохранения отчета.



Рисунок 129 – Пример команды

В терминале будет отображено сообщение о подтверждении проведения аудита на рабочей станции, указанной в команде (рис. 130). Необходимо ввести в терминале «yes» и нажать клавишу «Enter».



Рисунок 130 - Сообщение о подтверждении

Для начала аудита необходимо указать пароль пользователя, указанного в команде (рис. 131). Если аудит ОС Astra Linux проводится на рабочей станции впервые, пароль будет запрошен дважды. Нужно ввести в терминале пароль и нажать клавишу «Enter».

| - roo | t@scaner-vs: /usr/lib/sca-web-backend _ | • × |
|--|---|-------|
| Файл Правка Вкладки | Справка | |
| Утилита для удаленного а inux SE по требованиям Для запуска аудита запу ирования Вторым аргументом можно Например: sca-astra-audit user@19 root@scaner-vs:/usr/lib The authenticity of hos ECDSA key fingerprint i Are you sure you want to Warning: Permanently ad echelon@192.168.5.76's | аудита настроек комплекса средств защиты (КСЗ) ОС Astri Desonacности. CTUTE СКРИПТ, УКАЗАВ ПОЛЬЗОВАТЕЛЯ И IP-адрес объекта то yKaзать папку для coxpaнения отчета, по умолчанию ~/ 2.168.1.1 /home/user/reports (sca-web-backend# sca-astra-audit echelon@192.168.5.76 (sca-web-backend# sca-astra-audit echelon@192.168.5.76 t '192.168.5.76 (192.168.5.76)' can't be established. s SHA256:LQxeXYbtTPRzs6mbXpdBqJg951cf4jwvY8by8AcAixk. o continue connecting (yes/no)? yes ded '192.168.5.76' (ECDSA) to the list of known hosts. Dassword: | а L П |

Рисунок 131 – Сообщение о запросе пароля

В окне терминала будет показан процесс аудита (рис. 132).

| 📮 root@scaner-vs: /usr/lib/sca-web-backend _ 🛚 × |
|---|
| Файл Правка Вкладки Справка |
| echelon@192.168.5.76's password: /usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa .pub" /usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed /usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed if you are prompt |
| ed now it is to install the new keys echelon@192.168.5.76's password: |
| Number of key(s) added: 1 |
| Now try logging into the machine, with: "ssh 'echelon@192.168.5.76'" and check to make sure that only the key(s) you wanted were added. |
| astra_test.sh 100% 33KB 6.7MB/s 00:00 Log file name: /usr/lib/parsec/tests/tests.log Start testing |
| [audit_file.sh]: start test Test PASS [audit_file.sh]: stop test |
| [audit_proc.sh]: start test |

Рисунок 132 – Процесс аудита

О завершении процесса аудита в терминале будет выведено сообщение (рис. 133).

| 114 | |
|-----------------|---|
| НПЭШ.00606-01 3 | 4 |

| 🚽 root@scaner-vs: /usr/lib/sca-web-backend _ 🛚 × |
|---|
| Файл Правка Вкладки Справка |
| Добавляется пользователь «test123» в группу «cdrom» Добавляется пользователь «test123» в группу «floppy» Добавляется пользователь «test123» в группу «audio» Добавляется пользователь «test123» в группу «video» Добавляется пользователь «test123» в группу «plugdev» Добавляется пользователь «test123» в группу «users» Новый пароль : НЕУДАЧНЫЙ ПАРОЛЬ: основан на слове из словаря |
| Добавляется пользователь «test123» в группу «sudo» Добавление пользователя test123 в группу sudo Готово. ln: не удалось создать символьную ссылку «./test.txt»: Отказано в доступе sudo: нет tty и не указана программа askpass |
| tests/postgresql.log tests/chkconfig.log tests/all_errors.log tests/parsec_test.log tests/netstat.log tests/security_updates_1.5.log |
| tests/other_tests.tog test.tar 100% 70KB 25.8MB/s 00:00 done root@scaner-vs:/usr/lib/sca-web-backend# |

Рисунок 133 – Завершение аудита

В папке, указанной для сохранения отчета, после завершения аудита будет расположен архив с файлами отчетов. Для разархивации нужно ввести в терминале команду, представленную на рисунке (рис. 134), и нажать «Enter».

| 7 | | oot@sca | ner-vs | : / | | | - | • × |
|---|-------------------------------------|----------|--------|------|---------|----------|-------|-----|
| Файл Правка Ви | кладки Справка | | | | | | | |
| <pre>tests/all_errors.l tests/parsec_test tests/netstat.log tests/security_upg tests/security_upg</pre> | log .log dates_1.5.log | | | | | | | |
| test.tar | . Log | | 1 | 00% | 70KB 25 | 5.8MB/s | 00:00 | |
| done | | | | | | | | |
| root@scaner-vs:/us root@scaner-vs:~# root@scaner-vs:/# | <pre>sr/lib/sca-web-b cd / ls</pre> | ackend# | cd | | | | | |
| 0 | etc | lib | mnt | run | tmp | vmlinu | z.old | |
| 192.168.5.76.tar | home | lib64 | opt | sbin | usr | Theatron | | |
| bin | initrd.img | libx32 | proc | STV | var | | | |
| dev | initrd.img.old | media | root | sys | vmlinuz | z | | |
| root@scaner-vs:/# | tar -xvf 192.16 | 8.5.76.t | ar | | | | | |
| tests/ | | | | | | | | |
| tests/postgresql. | log | | | | | | | |
| tests/chkconfig.ld | og | | | | | | | |
| tests/all_errors. | log | | | | | | | |
| tests/parsec_test. | .log | | | | | | | |
| tests/netstat.log | | | | | | | | |
| tests/security_upo | dates_1.5.log | | | | | | | |
| tests/other_tests | .log | | | | | | | |
| root@scaner-vs:/# | | | | | | | | |

Рисунок 134 – Команда разархивации

В папке, указанной для сохранения отчета, после завершения процесса разархивации будут расположены файлы отчета (рис. 135).

116 НПЭШ.00606-01 34



Рисунок 135 – Файлы отчетов

В файле «all_errors.log» содержится информация об обнаруженных ошибках (рис. 136).

| Открыть 🔻 🖪 | all_errors.log /tests | [| Сохранить | ≡ | - | • | × |
|--|--|-----------------|------------|-----------|----|---|-----|
| Отчеты по parsec и PostgreSQL см | иотрите в соответствующи» | логах | | | | | |
| Security Updates for 1.5 BDU:Z-Z Неверные права доступа для файла | 2016-01583 & BDU:Z-2016-0 a /usr/bin/lnstat (rwx r- |)1584 x r-x) | FAIL | | | | |
| Security Updates for 1.5 BDU:Z-2 Разрешена автоматическая загрузн | 2016-01589 ка модуля ядра libertas_c | s | FAIL | | | | |
| Security Updates for 1.5 BDU:Z-2 Разрешена автоматическая загрузн | 2016-01590 ка модуля ядра kalmia | FAIL | | | | | |
| Security Updates for 1.5 BDU:Z-2 Разрешена автоматическая загрузн | 2016-01591 ка модуля ядра smsc75xx | FAIL | | | | | |
| Режим ЗПС выключен | FAIL | | | | | | |
| Запрет установки исполняемого би | ита выключен | FAIL | | | | | |
| Сервис gpm включен | FAIL | | | | | | |
| РАМ модуль отключен | FAIL | | | | | | |
| Порог неудачных введений пароля | превышает 8 раз | FAIL | | | | | |
| Неверные настройки защищенного о | сервера СУБД | FAIL | | | | | |
| Неверные права доступа для файла | a /lib32/libpcprofile.so | (rw- r r |) | FAIL | | | |
| Неверные права доступа для файла FAIL | a /lib/x86_64-linux-gnu/l | ibpcprofile. | so (rw- r | r) | | | |
| Очистка SWAP не активна | FAIL | | | | | | |
| | | | | | | | |
| | Текст 👻 Ши | ирина табуляци | и: 8 🔻 Стр | о 1, Стлб | 51 | • | BCT |

Рисунок 136 – Отчет об обнаруженных ошибках

В файле «chkconfig.log» содержится список системных служб и их состояния (рис. 137).

| 118 | |
|---------------|----|
| НПЭШ.00606-01 | 34 |

| Открыть 🔻 🖪 | | | ch | kconfig. | log | | Сохра | анить | ≡ | - | | × |
|---------------------------------|--------|-------|-------|----------|--------|---------|---------|-------|--------|----|---|-----|
| acpi-support | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| acpid | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| alsa-utils | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| anacron | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| apache2 | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | | | | | |
| avahi-daemon | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| bind9 | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | | | | | |
| bluetooth | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| bootlogs | 0:off | 1:on | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| bootmisc.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| checkfs.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| checkroot-bootclean.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| checkroot.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| console-setup | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| cron | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| cups | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| dbus | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| exim4 | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | | | | | |
| fly-dm | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| gpm | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| hostname.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| hwclock.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| isc-dhcp-server | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | | | | | |
| kbd | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| keyboard-setup | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| killprocs | 0:off | 1:on | 2:off | 3:off | 4:off | 5:off | 6:off | | | | | |
| kmod | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| lwresd | 0:off | 1:off | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| motd | 0:off | 1:on | 2:on | 3:on | 4:on | 5:on | 6:off | | | | | |
| mountall-bootclean.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| mountall.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| mountdevsubfs.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| mountkernfs.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| mountnfs-bootclean.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| mountnfs.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| mtab.sh | 0:off | 1:off | 2:off | 3:off | 4:off | 5:off | 6:off | S:on | | | | |
| networking | Ainff | 1.off | 2.off | Rinff | 4∙off | 5.off | 6.nff | Sinn | | | | |
| Загрузка файла «/tests/chkconfi | g.log» | | | Текст 🔻 | Ширина | табуляц | ии: 8 🔻 | Стр | 1, Стл | б1 | • | BCT |

Рисунок 137 – Список системных служб

В файле «netstat.log» содержится список портов функционирующих на них процессах (рис. 138).

| Отн | крыть 🔻 | æ | | netstat.log /tests | Сохранить | | - | ۰ | × |
|-------|-----------|----------|------------------------|-----------------------|---------------|----------|------|---|-----|
| Activ | e Interne | t con | nections (w/o servers) | | | | | | |
| Proto | Recv-Q S | end-Q | Local Address | Foreign Address | State | | | | |
| tcp | Θ | Θ | localhost:57852 | localhost:1266 | TIME WAIT | | | | |
| tcp | 0 | 0 | localhost:36634 | localhost:1267 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:53106 | localhost:1268 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:36640 | localhost:1267 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:36632 | localhost:1267 | TIME WAIT | | | | |
| tcp | Θ | 0 | localhost:36644 | localhost:1267 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:36628 | localhost:1267 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:36630 | localhost:1267 | TIME WAIT | | | | |
| tcp | Θ | 0 | localhost:36636 | localhost:1267 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:53990 | localhost:1269 | TIME WAIT | | | | |
| tcp | Θ | 0 | localhost:53092 | localhost:1268 | TIME WAIT | | | | |
| tcp | Θ | 0 | localhost:53994 | localhost:1269 | TIME WAIT | | | | |
| tcp | Θ | 0 | localhost:53098 | localhost:1268 | TIME WAIT | | | | |
| tcp | Θ | Θ | astra.echelon.lan:ssh | 192.168.5.98:41476 | ESTABLISHED | | | | |
| tcp | 0 | 0 | localhost:36626 | localhost:1267 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:54010 | localhost:1269 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:59220 | localhost:1264 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:55232 | localhost:1265 | TIME WAIT | | | | |
| tcp | 0 | 0 | localhost:54006 | localhost:1269 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:53104 | localhost:1268 | TIME WAIT | | | | |
| tcp | Θ | 0 | localhost:53094 | localhost:1268 | TIME WAIT | | | | |
| tcp | 0 | 0 | localhost:59234 | localhost:1264 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:53112 | localhost:1268 | TIME WAIT | | | | |
| tcp | Θ | 0 | localhost:53108 | localhost:1268 | TIME WAIT | | | | |
| tcp | 0 | 0 | localhost:54002 | localhost:1269 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:53100 | localhost:1268 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:55246 | localhost:1265 | TIME WAIT | | | | |
| tcp | 0 | 0 | localhost:53090 | localhost:1268 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:36646 | localhost:1267 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:53110 | localhost:1268 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:53102 | localhost:1268 | TIME WAIT | | | | |
| tcp | 0 | 0 | localhost:36642 | localhost:1267 | TIME WAIT | | | | |
| tcp | Θ | Θ | localhost:53992 | localhost:1269 | TIME WAIT | | | | |
| tcp | 0 | 0 | localhost:57838 | localhost:1266 | TIME_WAIT | | | | |
| tcn | • • • • • | 0 | localhost 54008 | localhost 1269 | TTME WATT | | | | |
| Загру | зка файла | «/tests/ | netstat.log» | Текст 👻 Ширина табуля | яции: 8 🔻 Стр | 0 1, Стл | ıб 1 | • | BCT |

Рисунок 138 – Список портов и процессов

В файле «other_tests.log» содержится информация о результатах прочих тестов аудита безопасности ОС Astra Linux (рис. 139).

Рисунок 139 – Список портов и служб

В файле «parsec_test.log» содержится информация о результатах тестирования подсистемы безопасности PARSEC (рис. 140).

| Открыть 💌 🖪 | parsec_test.log /tests | 1 | Сохранить | ∍ ≡ | - | • | × |
|---|---|--|-----------|------------|----|---|-----|
| [audit_file.sh]: start test Запуск системы протоколированияУСПЕШНО # Проверка системы протоколирования Установка параметров флагов аудита для катал Установка флагов аудита для файла /tmp/file- Создание события аудита chmod /tmp/file-1163 Создание события аудита chmod /tmp/file-1163 Создание события аудита setfaud /tmp/file-116 Создание события аудита setfaud /tmp/file-1163 Создание события аудита setfaud /tmp/file-1163 Создание события аудита setfaud /tmp/file-1163 Создание события аудита parsec_chmac /tmp/file- 1163 Создание события аудита parsec_chmac /tmp/file- 1163 Создание события аудита unlink /tmp/file-1163 Создание события аудита unlink /tmp/file-1163 Создание флагов аудита с каталога /tmpУСП Поиск событий ореп в журнале УСПЕШНО | нога /tmp/tmp 11639успе 9успешно 99успешно 639успешн 1639успешн 1639успешно 39успешно 339успешно 16шно | 0/file-11639. ШНО Ю Ю СПЕШНО | УСПЕШНО | | | | |
| поиск сооытии exec в журнале УСПЕШНО Поиск событий unlink в журнале | | | | | | | |
| УСПЕШНО Поиск событий chmod в журнале | | | | | | | |
| УСПЕШНО Поиск событий chown в журнале УСПЕШНО | | | | | | | |
| Поиск событий setfacl в журнале УСПЕШНО | | | | | | | |
| Поиск событий audit в журнале УСПЕШНО | | | | | | | |
| Поиск событий mac в журнале УСПЕШНО | | | | | | | |
| Поиск событий create в журнале УСПЕШНО | | | | | | | |
| Запуск системы протоколированияУСПЕШНО Test PASS | | | | | | | |
| Загрузка файла «/tests/parsec_test.log» | Текст 🔻 Ши | ирина табуляци | и: 8 🔻 | Стр 1, Стл | 61 | • | BCT |

Рисунок 140 – Результат аудита

В файле «PostgreSQL.log» содержатся результаты тестирования комплекса средств защиты системы управления базами данных PostgreSQL (рис. 141).

122 НПЭШ.00606-01 34

| Файл Правка Поиск Параметры Справка Подготовка к выполнению тестов СУБД PostgreSQL Создание тестовых пользователей Создание пользователя и_0_00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) минимальная категория: Нет(0) Создание пользователя и2_0_00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) максимальный уровень: Нет(0) |
|--|
| Подготовка к выполнению тестов СУБД PostgreSQL Создание тестовых пользователей Создание пользователя u_0_00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) максимальная категория: Нет(0) максимальная категория: Нет(0) Создание пользователя u2_0_00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) максимальная категория: Нет(0) максимальная категория: Нет(0) |
| Создание тестовых пользователей Создание тестовых пользователей Создание пользователя u_0_00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) минимальная категория: Нет(0) Создание пользователя u2_0_00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) максимальный уровень: Нет(0) максимальный уровень: Нет(0) максимальный уровень: Нет(0) максимальныя категория: Нет(0) максимальныя категория: Нет(0) |
| Создание пользователя и_0_00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) минимальная категория: Нет(0) Создание пользователя и2_0_00 с мандатной меткой {0,0} Минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) максимальный уровень: Нет(0)_0 минимальная категория: Нет(0)_0 |
| минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) минимальная категория: Нет(0) Создание пользователя и2_0_00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) максимальный уровень: Чровень_0(0) минимальная категория: Нет(0) |
| максимальный уровень: Уровень_0(0) минимальная категория: Нет(0) максимальная категория: Нет(0) Создание пользователя и2_0_00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) максимальный хотегория: Нет(0) минимальная категория: Нет(0) |
| минимальная категория: Her(0) максимальная категория: Her(0) Создание пользователя u2_0_00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) минимальная категория: Her(0) максимальная категория: Her(0) |
| максимальная категория: Нет(0) Создание пользователя u2_0_00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) минимальная категория: Нет(0) максимальная категория: Нет(0) |
| Создание пользователя и <u>2 0</u> 00 с мандатной меткой {0,0} минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) минимальная категория: Нет(0) максимальная категория: Нет(0) |
| минимальный уровень: Уровень_0(0) максимальный уровень: Уровень_0(0) минимальная категория: Нет(0) максимальная категория: Нет(0) |
| максимальный уровень: Уровень 0(0) минимальная категория: Нет(0) максимальная категория: Нет(0) |
| минимальная категория: Нет(0) |
| MAKCHMARLUAG KATOFORNG' HOT(A) |
| |
| Создание пользователя u_0_01 с мандатной меткой {0,1} |
| минимальный уровень: Уровень_0(0) |
| максимальный уровень: Уровень 0(0) |
| минимальная категория: категория 1(1) |
| MakCuManbhas Kateropus: kateropus_1(1) |
| |
| |
| максимальный уровень. Уровень 1(1) |
| Muhamanbhas kaleiophs. Kaleiophs_1(1) |
| Marcumanbran Kalelopun, Kalelopun_ (1) |
| |
| Marchandshuhu yuberb. Yuberb.(0) |
| Marcumaninamu Spotents. Spotents. (0) |
| Makrimanhan kateronus: Kateronus (2) |
| Позпание пользователя и 1 10 с манатной меткой {1 2} |
| минимальный уровень : Уровень 1(1) |
| максимальный уровень: Уровень 1(1) |
| минимальная категория: Категория 2(2) |
| максимальная категория: Категория 2(2) |
| Создание пользователя и 1 11 с мандатной меткой {1.3} |
| минимальный уровень: Уровень 1(1) |
| максимальный уровень: Уровень 1(1) |
| минимальная категория: Категория 1,Категория 2(3) |
| максимальная категория: Категория_1,Категория_2(3) |
| Создание пользователя u2_1_11 с мандатной меткой {1,3} |
| минимальный уровень: Уровень_1(1) |
| максимальный уровень: Уровень_1(1) |
| минимальная категория: Категория 1,Категория 2(3) |

Рисунок 141 – Результаты тестирования

В файле «security_updates_1.5.log» содержится информация о результатах аудита по методическим указаниям по нейтрализации угроз эксплуатации уязвимостей ОС специального назначения «Astra Linux Special Edition» (версия 1.5) в информационных системах (рис. 142).

| Открыть 🔻 🖪 | security_updates_1.5.log /tests | Сохранить | ≡ - | ۰ | × |
|--|--------------------------------------|--------------|-----------|---|-----|
| Уязвимость BDU:2016-01146 | | | | | |
| Пакет imagemagick не установлен | ОК | | | | |
| Уязвимость BDU:2016-01573 Пакет libgraphicsmagick3 не установлен | ок | | | | |
| Уязвимость BDU:Z-2016-01583 & BDU:Z-201 Неверные права доступа для файла /usr/b | 16-01584 pin/lnstat (rwx r-x r-x) | FAIL | | | |
| Уязвимость BDU:Z-2016-01585 Пакет gpsd-clients не установлен | ОК | | | | |
| Уязвимость BDU:Z-2016-01586 Пакет speech-tools не установлен | ОК | | | | |
| Уязвимость BDU:Z-2016-01587 Пакет texlive-binaries не установлен | ОК | | | | |
| Уязвимость BDU:Z-2016-01588 Пакет firebird2.5-classic-common не уст | гановлен ОК | | | | |
| Уязвимость BDU:Z-2016-01589 Разрешена автоматическая загрузка модул | пя ядра libertas_cs | FAIL | | | |
| Уязвимость BDU:Z-2016-01590 Разрешена автоматическая загрузка модул | пя ядра kalmia FA | IL | | | |
| Уязвимость - RDII · 7-2016-01591 | | | 1 (776 1 | _ | DOT |
| Загрузка фаила «/tests/security_updates_1.5.log». | текст 👻 ширина табуля | ции: 8 🗸 Стр | 1, СТЛО 1 | * | RCI |

Рисунок 142 – Результаты аудита

3.7.2.3. Завершение работы с инструментом

Для завершения работы необходимо нажать «Крестик» в верхнем правом углу терминала.

3.7.3. Инструмент «Локальный аудит паролей»

Инструмент «локальный аудит паролей» предназначен для поиска и выявления на локальной рабочей станции неустойчивых к взлому паролей.

3.7.3.1. Запуск инструмента

Инструмент запускается из веб-интерфейса «Локальный аудит паролей» или из подменю стартера приложений. Для запуска инструмента необходимо выполнить следующие действия:

- запустить подменю стартера приложений;
- выбрать вкладку «Атаки на пароли»;

- выбрать инструмент «Локальный аудит паролей» (рис. 143).



Рисунок 143 – Инструмент «Локальный аудит паролей»

После запуска появится рабочее окно средства локального аудита паролей (рис. 144).



3.7.3.2. Работа с инструментом

Для аудита необходимо импортировать файл с хешами паролей. Для импорта файла с хешами паролей в ОС семейства MS Windows необходимо выполнить следующие действия:

- войти в подменю «Файл»;

- войти в подменю «Импорт из SAM»;

- выбрать параметр «указать папку Windows» либо указать непосредственно SAM файл (рис. 145).

Для ОС семейства Linux необходимо выполнить следующие действия:

- войти в подменю «Файл»;

- выбрать параметр «Импорт из shadow»;

- указать каталог / etc / (рис. 145).

Для импорта файлов, находящихся вне директорий по умолчанию, необходимо выполнить следующие действия:

- войти в подменю «Файл»;

- выбрать параметр «Импорт из файла» (рис. 145).

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

| F | | | Локаль | ный ауди | т паролей | | | | |
|--|--------|----|------------|----------|-----------|------------------|----------|------------|--------|
| Файл Аудит Импорт из файла Импорт из SAM | > | | 1 Примитив | Словари | Перебор | Радужные таблицы | | <u>a</u> (| 9 |
| 🚯 Импорт из shadow | | os | Home | Хэш | Формат | Пароль | Класс тр | ебований | і к АС |
| Отчет | | | | | | | | | |
| 🔀 Параметры | Ctrl+O | | | | | | | | |
| Θ Выход | Ctrl+Q | - | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Рисунок 145 – Меню «Файл»

Импортировать файлы с хешами паролей можно при помощи пиктограмм, расположенных на панели инструментов (рис. 146).



Рисунок 146 – Пиктограммы панели инструментов

Описание пиктограмм, изображенных на рисунке (рис. 146) (сверху вниз).

- импорт из файла;
- импорт из SAM с указанием папки Windows;
- импорт из SAM с непосредственным указанием файла;
- импорт из shadow.

Перед запуском процедуры аудита необходимо в подменю «Аудит» указать методы, с помощью которых будет осуществляться анализ (рис. 147). Эти методы можно выбрать и на панели инструментов.

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

Поле Gecos (рис. 144) содержит вспомогательную информацию: номер телефона, адрес, полное имя пользователя и т.п.

| * | | | Локаль | ный аудит | паролей | | _ | - • × |
|------|---|---|------------|-----------|------------|-----------------|------------|--------------|
| Файл | Аудит | | | | | | | |
| | ✓ 1 Примитив □ Словари | * | 1 Примитив | Словари | Перебор Ра | адужные таблицы | | b 🕑 |
| RID | □ Словари □ Перебор □ Радужные таблицы | | Home | Хэш | Формат | Пароль | Класс треб | ований к АС |
| | | | | | | | | |

Рисунок 147 – Меню «Аудит»

Для настройки словарей и наборов символов, которые будут использованы при последовательном переборе паролей, необходимо выполнить следующие действия:

- войти в подменю «Файл»;

- выбрать параметр «Параметры» (рис. 145).

Окно «Параметры» можно вызвать, нажав кнопку с изображением инструментов на панели инструментов.

| * | | | Локалы | ный аудит | паролей | | | - • × |
|------|-------|---|------------|--|---|--|---------------|----------|
| Файл | Аудит | | | | | | | |
| | 🐔 🗊 🚷 | 🗻 욿 🖬 | 1 Примитив | Словари | Перебор Ра | адужные таблицы | 🛃 🖄 | ٢ |
| RID | Логин | Gecos Ho | ome | Хэш | Формат | Пароль | Класс требова | ний к АС |
| | | Наборы симво Цифры У Буквы Цифробун Ци Все | рлов Слої | Парамет варь //ш одификаци Подклю | тры sr/share/dict/0 я слов чить радужни Оті | _ = = 01Dict ые таблицы <u>м</u> ена <u>О</u> К | | |
| | | | | | | | | |

Рисунок 148 – Окно «Параметры»

Для запуска процедуры аудита необходимо выбрать параметр «Старт / Стоп» в меню «Аудит» (рис. 147) или нажать кнопку « . Процесс анализа может быть остановлен в любой момент с помощью повторного выбора параметра «Старт / Стоп» в подменю «Аудит»

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

Для сохранения отчета нужно выбрать параметр «Отчет» в подменю «Файл» или нажать кнопку « . В открывшемся окне необходимо выбрать путь для сохранения файла отчета (рис. 149).

| % | Локальный аудит паролей | - 0 X |
|------------------------|---|-------|
| Файл Аудит | | |
| 🎩 🐔 🗿 🚷 🔀 | 🝰 🛯 Примитив Словари Перебор Радужные таблицы 🛛 🛃 🏄 | |
| RID Логин Gec | Сохранить отчет _ п × | |
| 0 root root Перейти к: | 💼/media 🔝 📀 🛷 😤 🛅 🔳 | |
| 🧾 Компьют | ep | |
| <u>И</u> мя файла: | | |
| Типы файлов: | Техt (*.txt) Ст <u>м</u> ена | |
| | | |
| Готово | | |

Рисунок 149 – Сохранение отчета

3.7.3.3. Завершение работы с инструментом

Для выхода из инструмента необходимо воспользоваться параметром «Выход» в подменю «Файл» или нажать кнопку «.

3.7.4. Инструмент «Поиск остаточной информации»

Инструмент «Поиск остаточной информации» предназначен для поиска по ключевым словам на запоминающем устройстве удаленных данных.

3.7.4.1. Запуск инструмента

Инструмент запускается из веб-интерфейса «Поиск остаточной информации» или из подменю стартера приложений. Для запуска инструмента необходимо выполнить следующие действия:

– запустить подменю стартера приложений;

- выбрать вкладку «Форензика»;

- выбрать инструмент «Поиск остаточной информации» (рис. 150).



Рисунок 150 – Инструмент «Поиск остаточной информации»

После запуска инструмента поиска остаточной информации откроется рабочее окно инструмента (рис. 151).

| Поиск остаточн | юй инфо | рма | ци | И | - | _ | - | - | _ | | - |
|----------------------------------|---------|-----|-----|----|----|----|----|----|----|----|----|
| /стройство | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Физический диск: sr0 | 0x00E0 | f8 | 7b | 66 | 13 | 16 | fc | 7b | 66 | 52 | 66 |
| Размер: 3.32 ГБ (6967360 блоков) | 0x00F0 | 10 | 89 | e6 | 66 | f7 | 36 | e8 | 7b | c0 | e4 |
| 🗌 Анализировать ФС | 0x0100 | f6 | 36 | ee | 7b | 88 | сб | 08 | e1 | 41 | b٤ |
| № блока | 0x0110 | cd | 13 | 8d | 64 | 10 | 66 | 61 | c3 | e8 | 16 |
| 0 🗘 Отобразить | 0x0120 | 74 | 69 | 6e | 67 | 20 | 73 | 79 | 73 | 74 | 65 |
| Тараметры поиска | 0x0130 | 20 | 65 | 72 | 72 | 6f | 72 | 2e | 0d | 0a | 56 |
| Кодировки | 0x0140 | 04 | b3 | 07 | cd | 10 | Зc | 0a | 75 | f1 | с |
| Типы локументов | 0x0150 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| | 0x0160 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| ип поиска | 0x0170 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| поиск фразы | 0x0180 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 🗋 по словарям 🗘 | 0x0190 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Редактировать словари | 0x01A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Лобавить новый словарь | 0x01B0 | Зc | 08 | 00 | 00 | 00 | 00 | 00 | 00 | 0e | as |
| Содировка отображаемых данных | 0x01C0 | 01 | 00 | 17 | d4 | e0 | fd | 40 | 00 | 00 | 00 |
| ASCII | 0x01D0 | c1 | fe | 01 | 2b | e0 | fe | c0 | 4a | 6a | 00 |
| | 0x01E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Начать поиск | 0x01F0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| | | | 124 | | | _ | - | | | | |

Рисунок 151 – Рабочее окно инструмента

3.7.4.2. Работа с инструментом

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

Для запуска процесса поиска остаточной информации необходимо нажать «Начать» поиск. Процесс поиска может быть приостановлен нажатием кнопки «Приостановить».

Результаты поиска остаточной информации выводятся в виде списка, содержащего номер блока и величину смещения (рис. 152). Для просмотра найденной информации необходимо дважды нажать левой кнопкой мыши на интересующем секторе. При этом в рабочем окне будет показана информация о выбранном секторе и выделено найденное слово (рис. 153).

| | Строка | № блока 🗸 | Смещение | Кодировка | Тип файла | уть к файл |
|----|----------|-----------|----------|-----------|-----------|------------|
| 1 | security | 4551 | 0x0004 | utf8 | RAW | |
| 2 | security | 4552 | 0x0045 | utf8 | RAW | |
| 3 | security | 4552 | 0x0060 | utf8 | RAW | |
| 4 | security | 13388 | 0x01B4 | utf8 | RAW | |
| 5 | security | 13389 | 0x01F5 | utf8 | RAW | |
| 6 | security | 13390 | 0x0010 | utf8 | RAW | |
| 7 | security | 18456 | 0x0042 | utf8 | RAW | |
| 8 | security | 18461 | 0x0028 | utf8 | RAW | |
| 9 | security | 18726 | 0x01CE | utf8 | RAW | |
| 10 | security | 18727 | 0x001B | utf8 | RAW | |
| 11 | security | 18727 | 0x0048 | utf8 | RAW | |
| 12 | security | 18727 | 0x0075 | utf8 | RAW | |
| | | | | | | |

Рисунок 152 – Общие результаты поиска

| 132 | |
|---------------|----|
| НПЭШ.00606-01 | 34 |

| | 1 | | | _ | | | | | | | |
|----------------------------------|--------|----|----|----|----|----|----|----|----|----|----|
| /стройство | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Физический диск: sr0 | 0x0060 | 73 | 65 | 63 | 75 | 72 | 69 | 74 | 79 | 20 | 73 |
| Размер: 3.32 ГБ (6967360 блоков) | 0x0070 | 73 | 20 | 75 | 6e | 74 | 69 | бc | 20 | 72 | 65 |
| Анализировать ФС | 0x0080 | 65 | 61 | 6c | 74 | 68 | 00 | 44 | 69 | 73 | 70 |
| 🛚 блока | 0x0090 | 41 | 52 | 54 | 20 | 68 | 65 | 61 | 6c | 74 | 68 |
| 4552 🗘 Отобразить | 0x00A0 | 73 | 2e | 00 | 61 | 61 | 6d | 00 | 53 | 65 | 74 |
| | 0x00B0 | 61 | 74 | 69 | 63 | 20 | 41 | 63 | 6f | 75 | 73 |
| араметры поиска | 0x00C0 | 6e | 61 | 67 | 65 | 6d | 65 | 6e | 74 | 0a | 28 |
| Кодировки | 0x00D0 | 20 | 31 | 32 | 38 | 3d | 71 | 75 | 69 | 65 | 74 |
| Типы документов 🛄 🗘 | 0x00E0 | 20 | 32 | 35 | 34 | Зd | 66 | 61 | 73 | 74 | 29 |
| ип поиска | 0x00F0 | 64 | 62 | 79 | 2d | 74 | 69 | 6d | 65 | 6f | 75 |
| 🗆 поиск фразы | 0x0100 | 73 | 74 | 61 | 6e | 64 | 62 | 79 | 20 | 74 | 69 |
| 🗆 по словарям 🗍 😂 | 0x0110 | 28 | 30 | 3d | 6f | 66 | 66 | 2c | 20 | 31 | 30 |
| | 0x0120 | 31 | 30 | 73 | 2c | 20 | 2e | 2e | 2e | 2c | 20 |
| Редактировать словари | 0x0130 | 6d | 2c | 20 | 32 | 34 | 31 | 3d | 33 | 30 | 60 |
| Добавить новый словарь | 0x0140 | 2e | 00 | 53 | 65 | 74 | 20 | 64 | 72 | 69 | 76 |
| одировка отображаемых данных | 0x0150 | 74 | 61 | 6e | 64 | 62 | 79 | 20 | 6d | 6f | 64 |
| ASCII | 0x0160 | 65 | 70 | 00 | 53 | 65 | 74 | 20 | 64 | 72 | 69 |
| | 0x0170 | 73 | 6c | 65 | 65 | 70 | 20 | 6d | 6f | 64 | 65 |
| Начать поиск | | | | | | | | | •. | | |

Рисунок 153 – Найденное слово в блоке № 4552

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

Оператор может сохранить полученный отчет, нажав кнопку «Сохранить отчет» (рис. 152). В появившемся окне необходимо указать формат и директорию сохранения отчета (рис. 154).

| Ø | Сохранение отчета | _ = × |
|---------------------------|--|-------------------------|
| <u>И</u> мя: | diskfind-2018-06-14T10:29:07dev_sr0-100% <mark>.xml</mark> | |
| Сохранить в <u>п</u> апке | < 🔂 root | Создать п <u>а</u> пку |
| <u>М</u> еста | Имя ~ | Размер Изменён |
| 🔍 Поиск | 🐻 Desktop | Суббота |
| 🕙 Недавние доку | 🛅 Видео | 10:15 |
| 📄 sca-web-backend | 🛅 Документы | 10:15 |
| 📷 root | 🔁 Загрузки | 10:15 |
| 🛅 Рабочий стол | 🛅 Изображения | 10:15 |
| 📃 Файловая сист | 词 Музыка | 10:15 = |
| 📃 tmp | 🛜 Общедоступные | 10:15 |
| 📃 Корень файлов | 🛅 Шаблоны | 10:15 |
| | | × |
| + - | | Xml files 😂 |
| | • О <u>т</u> мени | ть 🔛 Со <u>х</u> ранить |

Рисунок 154 – Сохранение отчета

Для удаления найденной информации необходимо нажать «Удалить найденное с диска» (рис. 152). Перед удалением появится сообщение с предупреждением (рис. 155).

| | Строка | № блока 🗸 | Смещение | Кодировка | Тип файла | уть к файл |
|----------|----------|-----------------------------|-----------------|-----------------|-----------|------------|
| 1 | security | 4551 | 0x0004 | utf8 | RAW | |
| 2 | security | 4552 | 0x0045 | utf8 | RAW | |
| 3 | security | 4552 | 0x0060 | utf8 | RAW | |
| 4 | security | 13388 | 0x01B4 | utf8 | RAW | |
| 5 | security | 12200 | Сообщение | u+f0 | | |
| 6 7 | secur | Вы действительн объекты? | ю хотите уничто | эжить выбранные | e | |
| 8 | secur | | | Нет | Да | |
| 9 | secur | | 1 | | | |
| | security | 18727 | 0x001B | utf8 | RAW | |
| 10 | | | 1 | | | |
| 10 11 | security | 18727 | 0x0048 | utf8 | RAW | |

Рисунок 155 – Сообщение

3.7.4.3. Завершение работы с инструментом

Для выхода из инструмента необходимо нажать «Крестик» в верхнем правом углу рабочего окна. Затем в появившемся окне нужно нажать кнопку «Да».

3.7.5. Инструмент «Аудит обновлений ОС MS Windows»

3.7.5.1. Запуск инструмента

Инструмент запускается из веб-интерфейса «Аудит обновлений ОС MS Windows» или из подменю стартера приложений. Для запуска инструмента необходимо выполнить следующие действия:

- запустить подменю стартера приложений;
- выбрать вкладку «Поиск уязвимостей»;
- выбрать инструмент «Аудит обновлений ОС MS Windows» (рис. 156).

| 🔍 01 - Сбор информации | > | | |
|---------------------------------|---|-------------------------------|-----|
| 💊 02 - Поиск уязвимостей | > | 😼 • OpenVAS | > |
| 🖏 03 - Анализ веб-приложений | > | 🔆 • Нагрузочное тестирование | > |
| 😼 04 - Аудит баз данных | > | 😼 • Утилиты Cisco | > |
| 🛹 05 - Атаки на пароли | > | 🚢 • Утилиты для VoIP | > |
| 🗑 06 - Аудит беспроводных сетей | > | 😼 • Утилиты для фаззинга | > |
| 🕱 07 - Реверс-инжиниринг | > | 🐨 golismero | |
| 🚿 08 - Эксплуатация уязвимостей | > | 💿 lynis | |
| 益 09 - Сниффинг и спуфинг | > | 👽 nikto | |
| 🏂 10 - Пост-эксплуатация | > | 👁 nmap | |
| 🖐 11 - Форензика | > | 🖗 sparta | |
| 🗉 12 - Генерация отчётов | > | 🐵 unix-privesc-check | |
| 🏂 13 - Социальная инженерия | > | 🖉 Аудит обновлений OC Windows | |
| 🚹 14 - Управление сервисами | > | 🌶 Аудит OC Astra Linux | - 1 |
| 🧼 15 - Справка | > | | |
| 😬 Остальные приложения | > | | |
| 📟 Параметры | > | | |
| Выполнить | | | |
| 🛃 Завершить сеанс | | | |
| >_ 🗃 🕀 | | | |

Рисунок 156 – Инструмент «Аудит обновлений ОС MS Windows»

После запуска средства аудита обновлений ОС MS Windows откроется рабочее окно (рис. 157).

| 8 💽 🕕 | Аудит обновлений ос windows | |
|--|--|---|
| ель сканирования | | Перечень обновлений |
| Логин (администратор) admin | Ір-адрес 192.168.0.х | Операционная система |
| Пароль | Порт 139 | Xp - service pack 0 Xp - service pack 1 Xp - service pack 2 |
| 🗹 Скрыть пароль | 성 Старт | Xp - Service pack 2 Xp - service pack 3 Vista - service pack 0 |
| Сурнал | | Vista - service pack 1 |
| 14/06/18 11.47: Запуск прошел 14/06/18 11.47: Внимание: пр открытом виде | 1 успешно и сканировании пароль будет передан в | Vista - service pack 2 7, 2008 - service pack 0 7, 2008 - service pack 1 8, 8 10, 10 Windows Server 2012 |
| | | Windows Server 2012-R2 Windows Server 2016 |

Рисунок 157 – Рабочее окно

3.7.5.2. Работа с инструментом

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

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

Проверить состояние порта можно, например, в командной строке с помощью утилиты netstat: команда «netstat –a» (рис. 158).

| C:A. | | Командная строка | | - 🗆 | × |
|----------------------------|---|---|--|---------|---|
| Microsoft <c> Kopne</c> | t Windows [Version 6. эрация Майкрософт (М: | .3.9600] icrosoft Corporation), | 2013. Все права за | щищены. | ^ |
| C:\Users' | ∖Jane>netstat -a | | | | |
| Активные | подключения | | | | |
| | Локальный адрес 0.0.0.0:135 0.0.0.0:445 0.0.0.0:5357 0.0.0.0:49152 0.0.0.0:49153 0.0.0.0:49153 0.0.0.0:49155 0.0.0.0:49156 0.0.0.0:49156 0.0.0.0:49161 0.0.0.0:55126 127.0.0.1:49217 127.0.0.1:49217 127.0.0.1:49217 127.0.0.1:49217 127.0.0.1:49217 127.0.0.1:49216 127.0.0.0.0.0.0.0.0.0.0.0.0.0.0. | Внешний адрес production:0 | Coctornue LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING ESTABLISHED ESTABLISHED ESTABLISHED | | |
| ŤČP TCP | 192.168.5.89:55647 192.168.5.89:55737 | 192.168.0.6:3128 192.168.0.6:3128 | ESTABLISHED ESTABLISHED | | |

Рисунок 158 – Проверка состояния порта

Затем необходимо запустить сканирование с помощью кнопки «Старт» или из панели инструментов с помощью зеленой кнопки.

Процесс сканирования отображается в окне «Журнал» (рис. 159), список доступных обновлений – в окне «Перечень обновлений».

После завершения сканирования в окне «Журнал» появится список неустановленных обновлений (рис. 159).

| . 🚯 💿 (). – | | Аудит ооно | влении ОС Window | - |
|--|---|------------------------|------------------|--|
| ель сканирования | | | | Перечень обновлений |
| Логин (администратор) | Vlad | Ір-адрес | 192.168.5.57 | Операционная система |
| Пароль | **** | Порт | 139 | Xp - service pack 0 Xp - service pack 1 |
| 🗹 Скрыть пароль | | | 🚺 Старт | > Xp - service pack 2 > Xp - service pack 3 |
| урнал | | | | Vista - service pack 0 Vista - service pack 1 |
| 20/06/18 07.51: Результа | аты сканирова | ания: | | Vista - service pack 2 7, 2008 - service pack 0 |
| Версия ОС: microsoft wir Версия Service Pack: ser | ndows 7 Домац vice pack 1 | иняя расширенн | ая | |
| Дата и время сканирова | ания: 2018-06- | 20 07:51:07 | | 890830 |
| Список неустановленны Всего известно обновле | іх обновлений ний: 973, уста | : ановлено: 1, не у | становлено: 972. | 925681 |
| http://support.microsoft.c http://support.microsoft.c http://support.microsoft.c | :om/kb/238671 :om/kb/977132 :om/kb/980302 | 7 | | 941158 |

Рисунок 159 – Результат сканирования

Сохранить результаты можно с помощью кнопки, расположенной справа от кнопки старта на панели инструментов. При нажатии на эту кнопку появится окно (рис. 160), в котором необходимо указать папку для сохранения отчета.

| Ø | Аудит с | обновлений OC Windows | | - • × |
|------------------------------------|--------------------|-------------------------------|------------------------------|-----------------|
| 🙆 🙆 🕠 🎧 . | | | | |
| | | Cox | ранить в | × |
| Цель сканирования | Перейти к: | 🛜 /root | \$ | 📑 📰 🔳 |
| Логин (администратор) Vlad | 📃 Компьютер | Имя | ✓ Размер Тип | Дата измен |
| Пароль **** | ka root | 🛅 Видео | Папка | 20.06.18 7: |
| | _ | 📄 Документы | Папка | 20.06.18 7: |
| 🗹 Скрыть пароль | | 🛅 Загрузки | Папка | 20.06.18 7: |
| | | 📒 Изображения | Папка | 20.06.18 7: |
| Журнал | | Музыка | Папка | 20.06.18 7: |
| 20/06/10 07 E1. Deputy ToTL 6/20 | | Общедоступные | Папка | 20.06.18 7: |
| 20/06/18 07.51: Результаты скан | | иаблоны | Папка | 20.06.18 7: |
| Версия OC: microsoft windows 7 J | | Desktop | Папка | 19.06.18 17 |
| Версия Service Pack: service pack | | | | |
| Дата и время сканирования: 201 | | | | |
| | | | | |
| Список неустановленных обнов. | | | | |
| bttp://support.microsoft.com/kb/2 | | | | |
| http://support.microsoft.com/kb/91 | | $\boldsymbol{\boldsymbol{<}}$ | III | > |
| http://support.microsoft.com/kb/9 | <u>И</u> мя файла: | Отчет аудита обновлений | windows. 2018-06-20T07:53:57 | <u>О</u> ткрыть |
| | Типы файлов: | Все файлы (*) | 0 | От <u>м</u> ена |

Рисунок 160 – Сохранение отчета

3.7.5.3. Завершение работы с инструментом

Для выхода из инструмента необходимо нажать «Крестик» в верхнем правом углу рабочего окна.

3.7.6. Инструмент «Системный аудитор»

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

3.7.6.1. Запуск инструмента

Инструмент запускается из веб-интерфейса «Системный аудитор» или из подменю стартера приложений. Для запуска инструмента необходимо выполнить следующие действия:

- запустить подменю стартера приложений;
- выбрать вкладку «Форензика»;
- запустить инструмент «Системный аудитор» (рис. 161).



Рисунок 161 – Инструмент «Системный аудитор»

Если все действия выполнены корректно, откроется рабочее окно (рис. 162).

139 НПЭШ.00606-01 34

| 0 | | | Системный аудитор | | - • × |
|--------------|-----------------------|----------------|-------------------------|-----------------------|------------|
| Отчет Аудит | База отчетов Спра | вка | | | |
| 🕢 Запуск | аудита 🔀 Настрой | ки аудита 💾 | Сохранить html-отчёт ка | ак 🥳 Открыть в браузе | ре 😈 Выход |
| Отчет сканир | ования | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Журнал | | | | | |
| 18/05/29 12: | 08: Удачный запуск си | стемного аудит | a. | | |
| | | | | | |
| | | | | | |
| | | | | | |

Рисунок 162 – Рабочее окно

3.7.6.2. Работа с инструментом

Для получения отчета об аппаратных комплектующих достаточно запустить сканирование, нажав кнопку « Запуск аудита» или выбрать параметр «Запуск аудита...» в подменю «Аудит».

Для получения в отчете дополнительной информации о системе необходимо нажать кнопку «Настройки аудита» и в появившемся окне (рис. 163) отметить нужные пункты и нажать «Принять».

140 НПЭШ.00606-01 34

| 💿 Настройки | 🔊 Настройки аудита 💷 × | | | | | |
|-----------------------------|-------------------------|--|--|--|--|--|
| Включить в отчет | | | | | | |
| х Аппаратное обес | печение | | | | | |
| Usb накопите. | ли | | | | | |
| Usb устройств | a | | | | | |
| Операционные с | истемы | | | | | |
| программное | программное обеспечение | | | | | |
| пользователи, пароли и WiFi | | | | | | |
| 🗌 статистика по | сещения сайтов | | | | | |
| Отметить все Снять все | | | | | | |
| Принять | Отмена | | | | | |
| Принять | Отмена | | | | | |

Рисунок 163 – Настройки аудита

Вызвать окно «Настройки аудита» можно альтернативным способом, выбрав параметр «Настройки аудита...» в подменю «Аудит».

После выбора нужных настроек для анализа информации о системе необходимо нажать кнопку «Запуск аудита».

Результаты анализа представлены в тематических разделах: «Операционные системы», «Система», «Память», «Периферия» и «Коммуникации» (рис. 164). Каждый раздел содержит подробную информацией о конкретных системах и устройствах.

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

В разделе «Система» (рис. 164) представлены характеристики основных системных устройств, таких как центральный процессор, материнская плата, мост (вкладки «Центральный процессор», «Материнская плата», «Мост» соответственно).

141 НПЭШ.00606-01 34

| 🕞 Системный аудитор – | θ× |
|--|----|
| Отчет Аудит База отчетов Справка | |
| 🔕 Запуск аудита 🔀 Настройки аудита 💾 Сохранить html-отчёт как 🞯 Открыть в браузере ⊍ Выход | |
| Отчет сканирования | |
| Банерона безопасность Конкленсная безопасность Сканирования: Сканирования: | |
| Операционные системы Система Память Нахопители Периферия Коммуникации | |
| Система Центральный процессор, материнская плата, мост. | |
| Центральный процессор Материнская плата Мост | |
| Центральный процессор | • |
| Журнал | |
| 18/05/29 12:09: Начало сканирования системы: 18/05/29 12:09: Поиск ОС windows 18/05/29 12:09: Поиск ОС GNU/Linux 18/05/29 12:09: Создание технический информации 18/05/29 12:09: Создание технический информации | |
| sologes recordered and solepacho. | |

Рисунок 164 – Отчет сканирования системного аудита

Раздел «Память» содержит информацию о виде и объеме оперативной памяти.

Раздел «Накопители» (рис. 165) содержит информацию об основных устройствах хранения данных и их свойствах. Во вкладках CD / DVD, Жесткие диски, Тома приводятся основные данные соответствующих носителей информации.

| Аудит База отчетов Справка апуск аудита 💥 Настройки аудита 💾 Сохранить html-отчёт как 🞯 Открыть в браузере Выход :канирования | |
|--|----------|
| апуск аудита 🛛 💥 Настройки аудита 💾 Сохранить html-отчёт как 🞯 Открыть в браузере 🕑 Выход :канирования | |
| сканирования | |
| | |
| | E |
| хопители | |
| нные о накопителях информации. | |
| ОООО Жёсткие диски Тома | |
| | |
| | |
| | |
| | |
| адин нумканур. о Описание: DVD reader | - |
| • AR RAIL | |
| n | |
| 29 12:08: Удачный запуск системного аудита. 29 12:09: Начало сканирования системы: | <u>.</u> |
| 29 12:09: Поиск ОС windows 29 12:09: Поиск ОС GNU/Linux | |
| 29 12:09: Создание технической информации | |

Рисунок 165 – Раздел «Накопители»

Раздел «Периферия» (рис. 166) содержит основную информацию о мультимедийных устройствах и видеокарте (вкладки «Мультимедиа» и Видео соответственно).

142 НПЭШ.00606-01 34

| | Системный аудитор | |
|--|---|--|
| т Аудит База | отчетов Справка | |
| Запуск аудита | 🔆 Настройки аудита 💾 Сохранить html-отчет как 🞯 Открыть в браузере Выход | |
| ет сканирования | | |
| Информация | о мультимедиа, видеокарте, мониторе | |
| тарортацая | , mynaniameeuu, aaeeonaprile, menaniope. | |
| Видео Мульти | медиа | |
| | | |
| Видео | | |
| C | | |
| 1 | | |
| LES | | |
| Идентификатор: | 0 | |
| Описание: | VCA compatible controller | |
| Продукт: | Mobile 4 Series Chipset Integrated Graphics Controller | |
| Производитель: | Intel Corporation | |
| Физ.идентификат | op: 2 | |
| bus into: | pc@0000:00:02.0 | |
| Версия: | 07 | |
| | | |
| идентификатор. | 1 Dimine controller | |
| Описание: | Display controller | |
| рнал | | |
| /10/22 16:23: Ope | ra | |
| /10/22 16:23: Inter | net Explorer | |
| /10/22 10:23: Chro /10/22 16:23: Cost | лле технической информации | |
| /10/22 16:24: CK2 | | |

Рисунок 166 – Раздел «Периферия»

В разделе «Коммуникации» (рис. 167) приводятся данные о сетевых системных устройствах (беспроводных, Ethernet и т.д.).

| _ | Системный аудитор | - 0 |
|---------------|--|-----|
| ет Аудит Б | База отчетов Справка | |
| Эапуск ауд | дита 🔣 Настройки аудита 💾 Сохранить html-отчёт как 🞯 Открыть в браузере Выход | |
| ет сканирова | ания | |
| Коммуника | ации | |
| Информац | иа o ethernet wifi и m п | |
| информац | an o einemet, win a m.n. | |
| | | |
| 5 | | |
| | | |
| идентификатор | 0. 0 Etharnat interface | |
| Продукт | 82540EM Ginabit Ethernet Controller | |
| Производитель | s: Intel Corporation | |
| Физ.идентифик | tatop: 3 | |
| bus info: | pc@0000:00:03.0 | |
| Версия: | 02 | |
| | | |
| | | |
| рнал | | |
| /05/29 12:08: | Удачный запуск системного аудита. | |
| /05/29 12:09: | Начало сканирования системы: | |
| /05/29 12:09: | | |
| /05/29 12:09: | | |

Рисунок 167 – Раздел «Коммуникации»

3.7.6.3. Работа с отчетами системного аудита

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

Для сохранения отчета в формате HTML необходимо нажать кнопку « Сохранить html-отчет как... » или воспользоваться параметром «Сохранить html-отчет...» в подменю «Отчет» и выбрать директорию сохранения отчета.

Чтобы сохранить отчет в формате XML, необходимо выбрать параметр «Сохранить xmlотчет...» в подменю «Отчет».

Для сохранения отчета в формате PDF, необходимо выбрать параметр «Печатать html-отчета в pdf...» в подменю «Отчет».

В инструменте «Системный аудитор» реализована функция хранения и сравнения отчетов за различные периоды времени. Для этого необходимо задать месторасположение базы отчетов, выбрав параметр «Открыть базу» в подменю «База отчетов». В появившемся окне «База отчетов» (рис. 168) необходимо нажать «Задать базу» и указать месторасположение базы в заранее созданном каталоге. Отчеты сохраняются в базе в формате XML.

| | База отчетов | _ = × |
|----------|--------------|--|
| сотчетов | | |
| Цель | Дата и время | Задать базу |
| | | Загрузить отчеты |
| | | Открыть отчет |
| | | Удалить отчет |
| | цель | База отчетов с отчетов Цель Дата и время |

Рисунок 168 – База отчетов

После задания базы для добавления текущего отчета необходимо выбрать параметр «Добавить отчет» в подменю «База отчетов» (рис. 168).

Для просмотра отчетов в указанной базе необходимо в окне «База отчетов» нажать «Загрузить отчеты» (рис. 169).

| | | База отчетов | , |
|------------|------|----------------|------------------|
| Список отч | етов | | |
| | Цель | Дата и время | Задать базу |
| 1 VM1 | | 18:06:07 14:01 | |
| 2 VM2 | | 18:06:07 13:59 | загрузить отчеты |
| | | | Открыть отчет |
| | | | Удалить отчет |
| | | | Удалить отч |

Рисунок 169 – Список загруженных отчетов

Для просмотра выделенного отчета необходимо в окне «База отчетов» нажать «Открыть отчет». Отчет отображается в рабочем окне инструмента.

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

Для сравнения отчетов в базе необходимо выбрать параметр «Сравнить отчеты» в подменю «База отчетов». Появится окно «Сравнение отчетов» (рис. 170).

| | Цель | Дата и время | | Цель | Дата и время |
|---|------|----------------|---|------|----------------|
| 1 | VM1 | 18:06:07 14:01 | 1 | VM1 | 18:06:07 14:01 |
| 2 | VM2 | 18:06:07 13:59 | 2 | VM2 | 18:06:07 13:59 |
| • | | | • | | |

Рисунок 170 – Сравнение отчетов

В данном окне необходимо нажать «Загрузить отчеты», выбрать отчеты и нажать «Сравнить».
В рабочем окне инструмента будет отображена информация о сравнении отчетов. Результаты сравнения располагаются в тематических разделах, среди которых «Операционные системы», «Программное обеспечение», «Пользователи» (рис. 171).

| © Системный аудитор | _ @ × |
|--|--------|
| Отчет Аудит База отчетов Справка | |
| 🔕 Запуск аудита 🔣 Настройки аудита 💾 Сохранить html-отчет как 🚱 Открыть в браузере 🕑 Выход | |
| Отчет сравнения | |
| Сравнение отчетов. | |
| Цель: | |
| Первое сканирование: 18/06/07 13:59 | |
| Второе сканирование: 18/06/07 14:01 | |
| Операционные системы | |
| Установленные ОС: изменений нет | |
| _ Журнал | |
| 18/06/07 14:01: Поиск ОС GNU/Linux 18/06/07 14:01: Создание технической информации 18/06/07 14:01: Сканирование уданно завершено. 18/06/07 14:01: Отчет добавлен в базу | ▲ ▲ |
| тородо такоз, сравнение удачно завершено. | |

Рисунок 171-Результаты сравнения

3.7.6.4. Завершение работы с инструментом

Для выхода из инструмента необходимо воспользоваться кнопкой «Выход» на панели инструментов в главном окне.

3.7.7. Инструмент «Гарантированное уничтожение информации»

Инструмент «Гарантированное уничтожение информации» предназначен для удаления информации путем затирания файла случайным набором символов для предотвращения восстановления данных.

3.7.7.1. Запуск инструмента

Инструмент запускается из веб-интерфейса «Гарантированное уничтожение информации» или из подменю стартера приложений. Для запуска инструмента необходимо выполнить следующие действия:

- запустить подменю стартера приложений;
- выбрать вкладку «Форензика»;
- выбрать инструмент «Гарантированное уничтожение информации» (рис. 172).

| 🔍 01 - Сбор информации | > | | |
|---------------------------------|---|--|---|
| 😼 02 - Поиск уязвимостей | > | 🖐 • PDF форензика | > |
| 🐻 03 - Анализ веб-приложений | > | 🖐 • Восстановление данных | > |
| 😼 04 - Аудит баз данных | > | 🖐 • Работа с образами | > |
| 🦯 05 - Атаки на пароли | > | 🖐 • Утилиты Sleuth Kit | > |
| 👕 06 - Аудит беспроводных сетей | > | 🖐 • Цифровая форензика | > |
| 🕱 07 - Реверс-инжиниринг | > | 🛓 autopsy | |
| 🚿 08 - Эксплуатация уязвимостей | > | 📲 binwalk | |
| 益 09 - Сниффинг и спуфинг | > | // bulkextractor | |
| 🎘 10 - Пост-эксплуатация | > | chkrootkit | |
| 🖐 11 - Форензика | | 📳 foremost | |
| 🗐 12 - Генерация отчётов | > | 🗇 galleta | |
| 🏂 13 - Социальная инженерия | > | 🗤 hashdeep | |
| 📊 14 - Управление сервисами | > | volafox | |
| 🧼 15 - Справка | > | 🕲 volatility | |
| 👑 Остальные приложения | > | 🔁 xplico | |
| 📾 Параметры | > | 🗼 yara | |
| Выполнить | | 🍐 Гарантированное уничтожение информации | |
| | | 🔉 ПИК Эшелон | |
| 🛃 Завершить сеанс | | 💭 Поиск остаточной информации | |
| >_ 🖿 | | 🐨 Системный аудитор | |

Рисунок 172 – Инструмент «Гарантированное уничтожение информации»

После запуска инструмента появится рабочее окно (рис. 173).

| 🍗 🛛 Гарантированное уничтожение информации 💷 🖙 |
|---|
| ⊕ ⓒ ⊙-ュ:: + - × 🙆 🚽 📃 🗭 📇 🕦 |
| 💽 Файлы/Каталоги для удаления 😪 < > |
| Имя |
| <pre>> // 0 > bin > dev > dev > dev > etc home > lib > lib > lib64 media mnt > opt > proc </pre> |
| |
| Добавьте файлы в список на уничтожение и нажмите 'Старт' |

Рисунок 173 – Рабочее окно

В верхней части рабочего окна находится панель инструментов. Кнопки, расположенные на панели инструментов, представлены в таблице (см. Таблица 9).

Таблица 9 – Описание кнопок инструмента

| Пиктограмма | Название | Описание |
|-------------|----------------------|--|
| | Домой | Программа возвращает пользователя в домашнюю директорию (домашнюю папку) |
| Ċ | Обновить | При нажатии кнопки обновляется список файлов |
| | Отображение | Возможные варианты отображения: показать все, показать все, кроме скрытого и показать только папки |
| 1 | Количество затираний | Количество затираний файла случайным набором символов что предотвращает возможность восстановления файла |
| + | Добавить в список | Добавление выбранного файла в список на уничтожение |
| | Удалить из списка | Удаление выбранного файла из списка на уничтожение |
| × | Очистить список | Очистка списка на уничтожение |
| | Старт / Стоп | Запуск / остановка процесса уничтожения информации |
| | Выход | Выход из инструмента |
| | Журнал | При нажатии кнопки в блокноте открывается журнал, содержащий имена удаленных файлов и результаты выполнения операции удаления |
| S | Загрузка отчета | При нажатии кнопки появится окно, в котором необходимо выбрать папку с отчетом средства поиска остаточной информации (рис. 174) |
| | Отчет | При нажатии кнопки предлагается выбор форматов отчетов для сохранения |

| Пиктограмма | Название | Описание |
|-------------|----------|---|
| 1 | Помощь | При нажатии кнопки отображается окно с информацией о инструменте и о горячих клавишах |

| | Выберите отче | ет diskfind _ в × |
|--------------------|--|--|
| Перейти к: | inoot/Desktop | : 🗇 🚸 🖆 📰 🔳 |
| 💻 Компьют | . Имя | ✓ Размер Тип Дата измен |
| i root | base MyProject diskfind-2018v_sr0-1 sca-installer.desktop sca-web.desktop trash.desktop | Папка 29.05.18 12 Папка 29.05.18 14 00%.xml 4 K6 xmlайл 05.06.18 9: 209 байт desайл 24.05.18 20 180 байт desайл 25.05.18 10 274 байт desайл 25.05.18 10 |
| <u>И</u> мя файла: | diskfind-2018-06-05T09:18:56c | ш > lev_sr0-100%.xml Открыть |
| Типы файлов: | Все файлы (*) | ≎ От <u>м</u> ена |

Рисунок 174 – Загрузка отчета

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

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

3.7.7.2. Работа с инструментом

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

Список выбранных файлов на уничтожение отображается в правой части рабочего окна инструмента. (рис. 175).

| 🍾 Гарантированное уничтожение информации | - • × |
|--|------------------|
| 🔁 📀 • ፲ 🖨 🕂 🗕 🗡 🚱 🕌 🗐 💭 🖆 | <mark>-</mark> • |
| 🜓 Файлы/Каталоги для удаления 👒 < > /etc/skel/Desktop/Base | |
| Имя | |
| 🛅 mnt | |
| 👂 🫅 opt | |
| proc | |
| 🗢 🛅 root | |
| 🖵 🛅 Desktop | |
| 🗢 💼 Base | |
| #18:06:07_13:59.xml | |
| #18:06:07_14:01.xml | |
| sca-installer.desktop | |
| sca-web.desktop | |
| trasn.desktop | |
| 🔤 Видео | |
| П Зэрруги | |
| Загрузки 🗸 | |
| | |
| Добавьте файлы в список на уничтожение и нажмите 'Старт' | |

Рисунок 175 – Выбранные для уничтожения файлы

Затем необходимо указать количество затираний в поле «Количество затираний».

Примечание. Максимальное количество затираний – 35.

Для запуска процедуры гарантированного уничтожения информации необходимо воспользоваться зеленой кнопкой «Старт / Стоп» на панели инструментов. Процесс уничтожения может быть остановлен в любой момент с помощью повторного нажатия кнопки «Старт / Стоп».

Перед началом процесса уничтожения появляется сообщение, требующее подтвердить удаление файлов (рис. 176).

| 🌜 Гарантированное уничтожение информации – 🗉 🗙 |
|--|
| 👦 🕹 බ~⊥≙ 🕂 🗕 🗡 🙆 🚽 📃 🔎 ≟ 🕕 |
| 🕼 Файлы/Каталоги для удаления 👒 < > /etc/skel/Desktop/Base |
| Имя mnt D Cont |
| 🔉 📄 🍾 Сообщение – 🗉 × |
| Вы действительно хотите уничтожить выбранные объекты? |
| <u>Н</u> ет <u>Д</u> а |
| |
| sca-web.desktop |
| |
| Покументы |
| Загрузки |
| |
| Добавьте файлы в список на уничтожение и нажмите 'Старт' |

Рисунок 176 – Сообщение

Примечание. При попытке уничтожения системных файлов, появится предупреждение, показанное на рисунке (рис. 177).

| 2 | Гарантированное уничтожение информации | × |
|---|---|------------|
| 🔁 🖒 💿 | -1 🕂 🕂 — 🗡 🔕 🚽 🗐 👰 🖆 | 1 ~ |
| Файлы/Катал Имя Ы | логи для удаления 💽 /etc/skel/Desktop/Base | |
| ▷ ☐ lib64 ☐ media | ъ Внимание _ □ × | |
| E mnt ▷ E opt ▷ F proc | Следующие каталоги: /sys являются системными и будут пропущены. | |
| ▶ ☐ root ▶ ☐ run ▶ ☐ sbin | <u>O</u> K | |
| ▷ in srv ▷ in sys | | |
| ▷ Imp ▷ Imp ▷ Imp □ usr ▷ Imp var | | |
| | бавьте файлы в список на уничтожение и нажмите 'Старт' | |
| д., | | |

Рисунок 177 – Предупреждение

3.7.7.3. Завершение работы с инструментом

Для выхода из инструмента необходимо воспользоваться параметром «Выход» в подменю «Файл» или нажать кнопку « » на панели инструментов и в появившемся окне нажать кнопку «Да».

3.7.8. Инструмент «Аудит беспроводных сетей»

Инструмент «Аудит беспроводных сетей» предназначен для обнаружения, сканирования и проведения пассивных и активных атак на подбор паролей в беспроводных сетях с WEP, WPA, WPA-2 шифрованием.

3.7.8.1. Запуск инструмента

Инструмент запускается из веб-интерфейса «Аудит беспроводных сетей» или из подменю стартера приложений. Для запуска инструмента необходимо выполнить следующие действия:

- запустить подменю стартера приложений;

- выбрать вкладку «Аудит беспроводных сетей»;

- выбрать инструмент «Аудит беспроводных сетей» (рис. 178).



Рисунок 178 – Инструмент «Аудит беспроводных сетей»

После запуска появится рабочее окно инструмента «Аудит беспроводных сетей» (рис. 179).

| \$ Аудит беспроводных сетей | | - • | × |
|--------------------------------|-----------|----------------------------|---|
| 🔤 wlan0 | • | 😂 Обновить | |
| Режим мониторинга включен н | ıa wlan0ı | mon | |
| (₍)) | | Сканирование точек доступа | |
| WIFI WEP | | Статус обнаружения | |
| WIFI WPA | 0 | Статус обнаружения | |
| База ключей | ĸ | (лючи отсутствуют | |
| Гараметры WI-FI | атаки | | |

Рисунок 179 – Рабочее окно

Примечание. Список поддерживаемых адаптеров приведен в приложении (см. Приложение 2).

3.7.8.2. Прослушивание сети, использующей WEP шифрование

Для обнаружения точек доступа необходимо указать интерфейс в поле «Выбрать интерфейс» и нажать кнопку «Сканирование точек доступа». После сканирования в рабочем окне будет отражена информация о количестве найденных точек доступа (рис. 180).



Рисунок 180 – Обнаруженные точки доступа

Для перехода к настройке атаки на точку доступа с WEP шифрованием необходимо нажать кнопку «WEP». В открывшемся окне нужно уточнить точку доступа и вид атаки.

Чтобы указать дополнительные настройки атаки в рабочем окне инструмента необходимо нажать кнопку «Параметры WI-FI атаки» и в открывшемся окне указать необходимые параметры (рис. 181).

| | Настройки Wi-Fi атаки – 🗉 🛪 |
|-----|--|
| | астройки МАС-адреса по-умолчанию |
| Уст | гановить МАС-адрес по умолчанию для проведения Wi-Fi атак |
| | Установить МАС-адрес |
| □ H | астройки файла захвата |
| Уст | гановить каталог для сохранения файлов захвата для оффлайн использования |
| | Обзор |

Рисунок 181 – Параметры атаки

Для начала или остановки атаки нужно нажать кнопку «Атака / Стоп», расположенную справа от точек доступа (рис. 182).

| | | Па | нель атаки | | | - 1 |
|---|--|---|------------------------------|--|-----------------------------------|---|
| Выберите целевую т | очку доступа | $1 \\ 1 \\ 1$ | 1 ~_1 | ^ . | | |
| (()) | | | | | | |
| testwep | | | | | | 🗙 Стоп |
| | | | | | | Автоматизация |
| | | | | | 1 | |
| ESSID: testwon BSS | ID: 78.64.89.5D | 9A-44 Channe | | Th: 60 Illectron | NEP T | Толлерживает WPS |
| ESSID: testwep BS | SID: 78:6A:89:5D: | 9A:44 Channe | ы: 9 Мощнос | ть: ² -60 Шифрон | ание: WEP Г | Тоддерживает WPS |
| ESSID: testwep BS Настройки атаки | 51 D: 78:6А:89:5 D: ⊙ Обычна | 9А:44 Channe 1 ая атака 0 | ы: 9 Мощнос | ть: -60 Шифроі О Атак | ание: WEP Г a WPS | Іоддерживает WPS |
| ESSID: testwep BS Настройки атаки Контрмера безопасноо | SID: 78:6А:89:5D: Обычна ти активирована | 9А:44 Channe ая атака () | !: 9 Мощнос 1 0 | ть: 60 Шифрог | ание: WEP Г a WPS | Іоддерживает WPS |
| ESSID: testwep BS Настройки атаки Контрмера безопасною Сбор пакетов | SID: 78:6А:89:5D: О Обычна ти активирована | 9А:44 Channe 1 ая атака 0 | н: 9 Мощнос | ть? -60 Шифрон) Атак | ание: WEP Г а WPS Статус и | loддерживает WPS нъекции wlan1mon |
| ESSID: testwep BS: Настройки атаки Контрмера безопаснос Сбор пакетов Пассивный режим акт | SID: 78:6А:89:5D: | 9А:44 Channe 1 ая атака 0 0 0 | н: 9 Мощнос | ть: -60 Шифрог | ание: WEP Г а WPS Статус и | loддерживает WP нъекции wlan1mor ~ |
| ESSID: testwep BS Настройки атаки Контрмера безопаснос Сбор пакетов Пассивный режим акт Взлом шифрования | SID: 78:6А:89:5D: О Обычна Ти активирована ивирован | 9А:44 Channe 1 ая атака 0 0 | 2 !: 9 Мощнос | ть: -60 Шифрон) Атак IVS Статус | ание: WEP Г а WPS Статус ин | loддерживает WP9 нъекции wlan1mor ~ |

Рисунок 182 – Настройки атаки

После завершения атаки в нижней части окна настроек атаки будет отображен результат взлома (рис. 183).

| | | Па | нель ата | ки | | | | - |
|---|---|--|------------------|----------------------|-----------------------|---------------------------|---------------------------------------|------------------------------|
| Выберите целевую то | чку доступа | | | | | | | |
| (c) (c) testwep | | $\begin{array}{ccc} 1 & 1 \\ 0 & 0 \\ 1 & 1 \end{array}$ | 1 0 0 | 0 | 0 | 1 0 0 |) ¹ 0 | 🗴 Стоп |
| | | | | | | | 🗹 Авт | оматизаци |
| | | | | | | | | |
| Свойства точки досту ESSID: testwep BSSI | ıa D: 78:6A:89:5D:9 | 9A:44 Channe | el: 9 Мощ | ность: -60 | Шифрова | | р Поддерх | кивает WPS |
| Свойства точки досту ESSID: testwep BSS Настройки атаки | זמ D: 78:6A:89:5D:5 | 9A:44 Channe | əl: 9 Мощ | ность: -60 | Шифрова | ние: WEF | Р Поддерх | кивает WPS |
| Свойства точки досту ESSID: testwep BSSI Настройки атаки | аа D: 78:6А:89:5D:9 Обычна | 9А:44 Channe 1 ая атака О | əl: 9 Мощ | ность: -60 | Шифрован 〇 Атака V | ние: WEF | • Поддер» | кивает WPS |
| Свойства точки досту ESSID: testwep BSS Настройки атаки Контрмера безопасност Сбор пакетов | та D: 78:6А:89:5D: О Обычна и активирована | 1 9A:44 Channe 1 ая атака О | аl: 9 Мощ | ность: -60 | Шифрова О Атака V | ние: WEF VPS Статус | Р Поддер» | кивает WPS 4 wlan1mor |
| Свойства точки досту ESSID: testwep BSS Настройки атаки Контрмера безопасност Сбор пакетов Пассивный режим акти | та D: 78:6А:89:5D: О Обычна и активирована зирован | 1 9А:44 Channe 1 ая атака 0 0 0 | аl: 9 Мощ | ность: -60 0 0 | Шифрова О Атака V | чие: WEF VPS Статус | ^э Поддерх О инъекции | кивает WP 4 wlan1mor ~ |
| Свойства точки досту ESSID: testwep BSS Настройки атаки Контрмера безопасност Сбор пакетов Пассивный режим акти Взлом шифрования | аа D: 78:6А:89:5D: О Обычна и активирована зирован | 1 9A:44 Channe 1 ая атака 0 0 | al: 9 Mou | ность: -60 | Шифрова О Атака V | иие: WEF VPS Статус | Р Поддерх инъекции | кивает WP 1 wlan1mor 2 |
| Свойства точки досту ESSID: testwep BSS Настройки атаки Контрмера безопасност Сбор пакетов Пассивный режим акти Взлом шифрования Завершено | аа D: 78;6А:89;5D: О Обычна и активирована Вирован | 1 9A:44 Channe 1 ая атака 0 | | ность: -60 | Шифрован О Атака V | иие: WEF VPS Cтатус | Р Поддер> | кивает WP 4 wlan1mor ~ |

Рисунок 183 – Результат взлома

Для просмотра взломанных паролей в рабочем окне (рис. 179) необходимо нажать кнопку «База ключей». В открывшемся окне будет отражена информация о найденных паролях в процессе аудита. Чтобы добавить новый ключ вручную, нужно воспользоваться кнопкой «Добавить новый ключ» (рис. 184).

| | | | База ключе | й | | | - • × |
|-----------|--|--------------|----------------|------------|---|---------|-------|
| По ата | Подобранные ключи беспроводных сетей автоматически сохраняются после успешнатаки. Вы также можете добавить ключи вручную | | | | | | |
| | 🛶очка доступ | 🔤 МАС-адрес | Шифрование | 🔕 Ключ | ٢ | Канал | |
| 1 | testwpa | 78:6A:89:5D: | WPA | Qmsp10049 | 3 | | |
| 2 | testwep | 78:6A:89:5D: | WEP | 1111111111 | 9 | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| C | охранить измен | ения | Цобавить новый | ключ | 7 | /далить | |

Рисунок 184 – База ключей

3.7.8.3. Прослушивание сети, использующей WPA шифрование

Для обнаружения точек доступа необходимо указать интерфейс в поле «Выбрать интерфейс» и нажать кнопку «Сканирование точек доступа». После сканирования в рабочем окне инструмента будет отражена информация о количестве найденных точек доступа (рис. 180).

Для перехода к настройке атаки на точку доступа с WPA шифрованием необходимо нажать кнопку «WPA». В открывшемся окне нужно указать точку доступа и вид атаки. Для осуществления атаки также необходимо загрузить файл с возможными комбинациями паролей. Для этого нужно нажать кнопку «Обзор» и выбрать необходимый файл. Чтобы указать дополнительные настройки атаки в рабочем окне инструмента необходимо нажать кнопку «Параметры WI-FI атаки». В открывшемся окне укажите необходимые параметры (рис. 181).

Для начала или остановки атаки нужно нажать кнопку «Атака / Стоп», расположенную справа от точек доступа (рис. 185).

| | | Пане | ель атаки | | | |
|---|--|-----------------------------------|---|------------------------------|--|---|
| Выберите целевую точку до | ступа | ^и ч 1 ч | * ^ _ | | | |
| RT SAR SIBREG | Slesarka SMSNG | S8+ Starsys2 | StepUp2 | | | |
| SUNTROPIC support T | CHP testwpa | (လ) EXUNA VP | ($\rotal)$ XSTREAM_Guest | | | 🛯 🖗 Атака |
| (()) (()) | | | | | | Автоматизация |
| | | | | | 0 V v | |
| Свойства точки доступа | | 1 4 | | | | |
| Свойства точки доступа ESSID: testwpa BSSID: Настройки атаки | 78:6A:89:5D:9A:44 | 1 Channel: 3 | о Мощность: 48 | Шифрование: W | /PA Поддержи | вает WPS |
| Свойства точки доступа ESSID: testwpa BSSID: Настройки атаки | 78:64:89:5D:9A:44 • Обычная а | 1 Channel: 3 | 0 Мощность: 48 | Шифрование: W 〇 Атака WPS | /PA Поддержи | вает WPS |
| Свойства точки доступа ESSID: testwpa BSSID: Настройки атаки Пробую точку доступа | 78:6А.89:5D:9А:44 О Обычная а | 1 Channel: 3 1 тақа | Мощность: -48 | Шифрование: W) Атака WPS | /РА Поддержи | Baet WPS |
| Свойства точки доступа ESSID: testwpa BSSID: Настройки атаки Пробую точку доступа Статус деаутентификации | 78:64:89:5D:9A:44 | 1 Сhannel: 3 1 така | О Мощность: 48 | Шифрование: W | /PA Поддержи rockme.txt | вает WPS Обзор |
| Свойства точки доступа ESSID: testwpa BSSID: Настройки атаки Пробую точку доступа Статус деаутентификации Handshake статус | 78:64:89:5D:9A:44 | 1 Channel: 3 | О 1 Мощность: 48 1 1 0 0 0 1 1 0 0 1 0 0 | Шифрование: W) Атака WPS | /РА Поддержи rockme.txt 78:6A:89:5D:9 | вает WPS Обзор А:44 |
| Свойства точки доступа ESSID: testwpa BSSID: Настройки атаки Пробую точку доступа Статус деаутентификации Handshake статус Атака шифрования полным пе | 78:6А-89:5D:9А-44 Обычная а ребором Автомати | 1 Channel: 3 така | Мощность: 48 | Шифрование: W Атака WPS | /РА Поддержи rockme.txt 78:6A:89:5D:9 :нтов, пожалуйс | вает WPS Обзор A:44 ~ та, подождите . |

Рисунок 185 – Настройки атаки

После завершения атаки в нижней части окна настроек атаки будет отображен результат взлома (рис. 186).

| | Пан | нель атаки | | |
|--|-----------------------|----------------------|---|---|
| Выберите целевую точку доступа | | | | |
| (ϕ)(ϕ)(ϕ)SUNTROPICsupportTCHPtestw | pa TEXUNA VP | (O) XSTREAM_Guest | $\begin{smallmatrix}1&0&1&0&0\\0&0&0&0&0\\0&1&0&0&1\end{smallmatrix}$ | |
| (() ZP ZTE_A0F35C | | | | Автоматизация |
| Свойства точки доступа ESSID: testwpa BSSID: 78:6A:89: | D:9A:44 Channel: 3 | Мощность: 48 | Шифрование: WPA По | оддерживает WPS |
| Настройки атаки О О | бычная атака | | 🔘 Атака WPS | |
| Тробую точку доступа | | | | |
| leaутентификация 78:6A:89:5D:9A:44 | | | roci | с me.txt Обзор |
| | | | | |
| Handshake перехвачен | | | 0 /8:64 | A:89:5D:9A:44 ~ |
| Handshake перехвачен Атака полным перебором WPA шифровани | ия Автоматическое опр | | 78:64 ние МАС-адресов клиентов, п | а:89:5D:9A:44 × ожалуйста, подождите |
| Handshake перехвачен Атака полным перебором WPA шифровани Готово | ия Автоматическое опр | еделение и добавле | 78:64 ние МАС-адресов клиентов, п | а:89:5D:9A:44 ~ ожалуйста, подождите |

Рисунок 186 – Результат взлома

Для просмотра взломанных паролей в рабочем окне инструмента (рис. 179) нужно нажать кнопку «База ключей». В открывшемся окне будет отражена информация о найденных паролях в процессе аудита (рис. 184).

3.7.8.4. Выход из аудита беспроводных сетей

Для выхода из инструмента необходимо нажать «Крестик» в верхнем правом углу окна.

3.7.9. Инструмент «Сетевой анализатор»

Инструмент «Сетевой анализатор» предназначен для перехвата, анализа и фильтрации сетевого трафика.

3.7.9.1. Запуск инструмента

Инструмент запускается из веб-интерфейса «Сетевой анализатор» или из подменю стартера приложений. Для запуска инструмента необходимо выполнить следующие действия:

- запустить подменю стартера приложений;

- выбрать вкладку «Сниффинг и спуфинг»;

- выбрать инструмент «Сетевой анализатор» (рис. 187).



Рисунок 187 – Инструмент «Сетевой анализатор»

После запуска инструмента появляется рабочее окно (рис. 188).

159 НПЭШ.00606-01 34



Рисунок 188 – Рабочее окно

3.7.9.2. Начало работы с инструментом

Для начала работы необходимо выбрать в подменю «Мониторинг» вид сети для анализа (рис. 189).

Сетевой анализатор □ × Файл Мониторинг Настройки Image: Oblive Hag Cetb... Ctrl+U Image: Kommyrupyemag Cetb... Ctrl+B Image: Bagatb фильтр pcap... Ctrl+P Image: Dol 111 Dol 111 Image: Dol 111 Dol 111 Image: Dol 111 Dol 111

160 НПЭШ.00606-01 34

Рисунок 189 – Выбор сети для анализа

Для запуска процесса анализа сетевого трафика необходимо выбрать параметр «Запустить анализатор» в подменю «Начало» (рис. 190).



Рисунок 190 – Начало мониторинга

Для начала анализа необходимо определить IP-адреса хостов сети. Для этого необходимо выполнить следующие действия:

- выбрать подменю «Хосты»;

- выбрать параметр «Сканирование хостов» (рис. 191).

Параметр «Список хостов» отображает информация о просканированных хостах сети (рис. 192).

| 1,7 | | | | Сетев | зой анализ | атор | | - | • × |
|-----------|---------|-----------------------|---------|-----------------------|------------|-----------|-------|---------|-----|
| Начало | Цели | Хосты | Вид | MITM | Фильтры | Журналиро | вание | Плагины | |
| | | 🐻 Спис | сок хо | стов | | Ctrl+H | | | |
| | | Вкли | очить | IPv6 ск | анировани | e | | | |
| | | Q Скан | ирова | ание хо | остов | Ctrl+S | | | |
| | | 🖻 Загр | узить | из фа | йла | | | | |
| | | 🔓 Coxp | анит | ь <mark>в ф</mark> ай | л | | | | |
| | | | | | | | | | |
| | | | | | 11 | | | | |
| | | | | | _ | | | | |
| | | | | | 201 | | | | |
| | | | | | 001 | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| 57 ПОРТ | OB OCMO | трено | 12000 | UTO DOŬ | | | | | ^ |
| 1766 tcp | OS find | ecos ripol erprint | извод | ителеи | | | | | |
| 2182 cep | висов и | звестно | | | | | | | |
| Lua: не у | казаны | сценари | ии, зап | туск не | возможен! | | | | |
| запуск м | онитор | NHI 9 OOF | ычнои | сеги | | | | | ≡ |
| | | | | | | | | | ~ |

Рисунок 191 – Меню «Хосты»

| 162 | |
|---------------|----|
| НПЭШ.00606-01 | 34 |

| L¥ | Сетевой анали | затор | - • × |
|---|-------------------|--------------------|-------------|
| Начало Цели Хосты Вид | ц MITM Фильтрь | ы Журналирование | Плагины |
| Список хостов 🗶 | | | |
| ІР-адрес | МАС адрес | Описание | |
| 192.168.5.1 | 90:8D:78:4A:03: | 60 | |
| 192.168.5.23 | C8:D3:FF:AD:E2: | 93 NPIADE293.local | |
| 192.168.5.25 | 9C:93:4E:09:6E: | CF | |
| 192.168.5.38 | DE:10:96:E2:8C: | 95 | |
| 192.168.5.39 | D4:3D:7E:02:45: | C3 | |
| 192.168.5.41 | 40:F0:2F:97:DF:I | DE | |
| 192.168.5.43 | 54:AB:3A:10:B0: | 84 | |
| fe80::200:aaff:fedb:8cbb | 00:00:AA:DB:8C: | BB | |
| fe80::4dcf:3e74:ee5e:eab6 | DE:10:6A:C9:D9: | 69 | |
| fe80::682a:c152:7118:315c | 54:AB:3A:10:B0: | 84 | ~ |
| Удалить хост | Добавить к Це | ель 1 Добави | ть к Цель 2 |
| | | | 10 |
| 20388 MAC адресов произво, 1766 tcp OS fingerprint | дителеи | | |
| 2182 сервисов известно | | | |
| Lua: не указаны сценарии, за | апуск не возможен | 1! | |
| Запуск мониторинга обычно | й сети | | |
| Мониторинг обычной сети у: | же запущен | | 3 |
| | | | |

Рисунок 192 – Список хостов

В меню «Цели» необходимо указать адреса хостов, которые будут проанализированы. Для выбора нового хоста необходимо выполнить следующие действия:

- нажать «Выбор цели (целей)» (рис. 193);

- указать IP-адрес или из списка хостов выбрать IP-адрес;

– нажать «Добавить к цели 1» или «Добавить к цели 2» (рис. 192).

Для просмотра и редактирования списка текущих целей необходимо выбрать параметр «Текущие цели» в подменю «Цели» (рис. 194).



Рисунок 193 - Меню «Цели»

| L.F | | | | Сетев | юй а | нализа | атор | | - | • × |
|-------------------------------------|------------------------------|-------------------------------|-------|--------|------|--------|------------|-------|----------|-----|
| Начало | Цели | Хосты | Вид | MITM | Фил | ьтры | Журналиров | вание | Плагины | |
| Цели 🛛 | Списо | ок хосто | B % | | | | | | | |
| Цель 1 | | | | | | Цель | 2 | | | |
| 192.168 | .5.135 | | | | | | | | | |
| Уда | алить | | Доб | бавить | | | Удалить | | Добавить | |
| 20388 MA 1766 tcp (2182 cept | C адре OS fing зисов и | сов про erprint звестно | извод | ителей | BO3M | ожені | | | | |
| вапуск мо | онитор | инга обы | ычной | сети | DU3M | U/KCH: | | | | _ |
| Кост 192. | 168.5.1 | 135 доба | авлен | к цели | 1 | | | | | |

Рисунок 194 – Список текущих целей

Для определения протокола, по которому будет производиться анализ выбранных целей, необходимо выбрать параметр «Протокол...» в подменю «Цели» и в открывшемся окне (рис. 195) выбрать протокол. Для использования всех протоколов необходимо выбрать «all».

| L <u>7</u> | Протоко | л: – – | × |
|------------|----------------------------|---------------|---|
| Выберите г | протокол- О <u>t</u> ср | ⊖ <u>u</u> dp | |
| Отмен | нить | <u> Ф</u> К | |

Рисунок 195 – Выбор используемых протоколов

Для просмотра информации о параметрах установленных соединений необходимо выбрать параметр «Соединения» в подменю «Вид» (рис. 196 и рис. 197).

| L.F | _ | | c | етевой | і анализат | ор | - • × |
|------------------------|---------------------|---------------------|------------------|-----------------|-------------|-------------------|--------------|
| Начало | Цели | Хосты | | мітм | Фильтры | Журналирование | Плагины |
| | | | ≡ Co | единен | ния | | Shift+Ctrl+C |
| | | | 을 Ub | офили | | | Ctrl+0 |
| | | | ୍ଦି 🖸 | гатисти | ка | | |
| | | | 🗆 Pa | зрешен | ние IP-адре | ОВ | |
| | | | Be Cr | тособ ві | изуализаци | и | Shift+Ctrl+V |
| | | | Q Pe | егулярн | ое выраже | ние визуализации: | Ctrl+R |
| | | | Q yo | танови | ть ключ Wi | -Fi | Ctrl+F |
| | | | | 2 | 01 | | |
| 57 порт | ов осмо | трено | | J | | | 2 |
| 20388 M/ 1766 tcp | чC-адре OS finge | есов про erprint | извод | ителей | | | |
| 2182 cep | висов и | звестно | | | | | |
| Lua: не ун Запуск м | казаны онитор | сценари инга обы | іи, заг ачной | іуск не сети | возможен! | | |
| | | | | | | | |
| | | | | | | | |

Рисунок 196 – Меню «Вид»



Рисунок 197 – Подменю «Соединения»

Параметр «Профили» в подменю «Вид» отображает список IP-адресов анализируемой сети, который может быть преобразован в список хостов (рис. 198).

| 1.7 | Сетевой ан | нализатор | - • × |
|---|-----------------------------|-------------------------------|-------------|
| Начало Цели Хосты Вид | МІТМ Фильтры Журналирование | Плагины | |
| Цели 🛛 Список хостов 🛪 🕻 | Соединения 🛪 Профили 🛪 | | |
| ІР-адрес | Имя хоста | | |
| 172.16.10.14 | | | = |
| 172.16.11.1 | | | |
| 192.168.5.1 | | | |
| 192.168.5.4 | | | |
| 192.168.5.18 | | | |
| 192.168.5.21 | | | |
| 192.168.5.22 | | | |
| 192.168.5.26 | | | |
| 192.168.5.30 | | | |
| 192.168.5.43 | | | |
| Очистить локальные | Очистить удалённые | Преобразовать в список хостов | Дамп в файл |
| 20388 МАС адресов произволи | ителей | | [^ |
| 1766 tcp OS fingerprint | | | |
| 2182 сервисов известно | | | |
| Lua: не указаны сценарии, зап Запуск мониторинга обычной | уск не возможен! сети | | |
| | | | = |
| Хост 192.168.5.135 добавлен | к цели 1 | | |
| | | | |

Рисунок 198 – Подменю «Профили»

Параметр «Статистика» в подменю «Вид» отображает подробную информацию о получении и передачи пакетов (рис. 199).

| 17 | Сетевой анализатор | - × |
|---|-----------------------------------|-----|
| Начало Цели Хосты Вид МІТМ Фильтры Журна | лирование Плагины | |
| Цели 🛚 Список хостов 🕷 Соединения 🕷 Профили | ж Статистика ж | |
| Полученные пакеты: | 26249 | |
| Отброшенные пакеты: | 0 0,00 % | |
| Переданные пакеты: | 0 bytes: 0 | |
| Текущая длина очереди: | 0/6 | |
| Частота замеров: | 50 | |
| Получено пакетов в нижней половине: | pck: 26249 bytes: 5969915 | |
| Получено пакетов в верхней половине: | pck: 530 bytes: 76776 | |
| Интересные пакеты: | 2,02 % | |
| Пакетов в секунду в нижней половине: | worst: 8952 adv: 13934 p/s | |
| Пакетов в секунду в верхней половине: | worst: 110132 adv: 156494 p/s | |
| Пропускная способность в нижней половине: | worst: 796371 adv: 3171983 b/s | |
| Пропускная способность в верхней половине: | worst: 16286343 adv: 22497651 b/s | |
| 20388 МАС адресов производителей | | ^ |
| 1766 tcp OS fingerprint | | |
| 2182 сервисов известно Lua: не указаны сценарии, запуск не возможен! | | |
| Запуск мониторинга обычной сети | | |
| Хост 192.168.5.135 добавлен к цели 1 | | = |

Рисунок 199 – Подменю «Статистика»

Параметр «Способ визуализации...» в подменю «Вид» позволяет настроить различные варианты отображения и форматирования пакетов и символов, а также установить кодировку, которую инструмент сможет преобразовать в UTF8 (рис. 200).

| u# | Способ визуализации – | | | | | | | | |
|-------------------------------|---|-----|----|--|--|--|--|--|--|
| О Выводить | пакеты в hex формате. | | | | | | | | |
| ascii Выв | одить только печатные символы, остальные будут отображаться точкой ' | | | | | | | | |
| 🔾 text Выв | одить только печатные символы, остальные пропускать. | | | | | | | | |
| О Переводи | ть текст из EBCDIC в ASCII. | | | | | | | | |
| 🔿 Убирать и | із текста все html тэги. Тэгом считается любая последовательность между | < и | >. | | | | | | |
| 🔿 Преобраз | овывать текст перед выводом из выбранной ниже кодировки в UTF-8. | | | | | | | | |
| Кодировка: | UTF-8 | | \$ | | | | | | |
| | Отменить 420 | ĸ | | | | | | | |

Рисунок 200 – Способы визуализации

Параметр «Регулярное выражение визуализации» в подменю «Вид» задает выражение для визуализации (рис. 201).



Рисунок 201 – Регулярное выражение визуализации

Параметр «Установить ключ Wi-Fi...» в подменю «Вид» указывает ключ, применяемый в анализируемой беспроводной сети (рис. 202).



Рисунок 202 – Ввод ключа Wi-Fi

Для сортировки информации, полученной в ходе анализа, необходимо выбрать параметр «Загрузить фильтр...» в подменю «Фильтры» (рис. 203).



Рисунок 203 - Меню «Фильтры»

Оператор может вести журнал, в котором фиксируются запрашиваемые параметры. Для этого необходимо в меню «Журналирование» (рис. 204) выбрать информацию для сохранения («Запись всех пакетов и информации», «Запись только информации», «Запись сообщений пользователя»). В открывшемся окне необходимо указать имя и директорию сохранения файла журнала.

| 17 | Сетевой анализатор | - • × |
|---|--|-------|
| Начало Цели Хосты Вид МІТМ Фильтры | Журналирование Плагины | |
| Цели ж Список хостов ж Соединения ж Пр Полученные пакеты: | Запись всех пакетов и информации Shift+Ctrl+I Запись только информации Ctrl+I Остановить запись информации | |
| Оторошенные пакеты: Переданные пакеты: Текущая длина очереди: | Запись сообщений пользователя Ctrl+M Остановить запись сообщений Сжатый файл | |
| Получено пакетов в нижней половине: Получено пакетов в верхней половине: | pck: 28249 bytes: 6225101 pck: 541 bytes: 78668 | |
| Интересные пакеты: Пакетов в секунду в нижней половине: | 1,92 % worst: 8952 adv: 13835 p/s | |
| Пакетов в секунду в верхней половине: | worst: 110132 adv: 156494 p/s | |
| Пропускная способность в нижнеи половине: Пропускная способность в верхней половине: | worst: /963/1 adv: 3050962 b/s worst: 16286343 adv: 22497651 b/s | |
| 20388 МАС адресов производителей 1766 tcp OS fingerprint 2182 сервисов известно Lua: не указаны сценарии, запуск не возможен! Запуск мониторинга обычной сети | | |
| Хост 192.168.5.135 добавлен к цели 1 | | = |

Рисунок 204 – Меню «Журналирование»

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

Для использования необходимого плагина следует загрузить его с помощью параметра «Менеджер плагинов» в подменю (рис. 205).

| L# | с | етевой а | нализатор | | _ = × |
|---|-----------------------------|----------|---------------------------------------|------------------|----------|
| Начало Цели Хосты Вид МІТМ | 1 Фильтры Журнали | ирование | Плагины | | |
| Цели 🗶 Список хостов 🛚 Соеди | нения 🛚 Профили 🕷 | Статист | Менеджер плагинов Загрузить плагин | Ctrl+P Ctrl+O | |
| Цель 1 | | | Цель 2 | | |
| 192.168.5.135 | | | | | |
| Удалить | Добавить | | Удалить | | Добавить |
| 20388 МАС адресов производителе 1766 tcp OS fingerprint 2182 сервисов известно Lua: не указаны сценарии, запуск н Запуск мониторинга обычной сети Хост 192.168.5.135 добавлен к цели | й е возможен! и 1 | | | | 2 |

Рисунок 205 – Меню «Плагины»

В появившемся окне следует выбрать необходимые плагины из представленного списка с помощью двойного нажатия левой кнопки мыши на их именах (рис. 206).

| 📭 Сетевой анализатор – 🗉 × | | | | | | | | |
|----------------------------|--|---|--|--|--|--|--|--|
| Начало Цели Хосты Ви | Начало Цели Хосты Вид MITM Фильтры Журналирование Плагины | | | | | | | |
| Цели 🛪 Список хостов 🛪 | Цели 🛪 Список хостов 🛪 Соединения 🛪 Профили 🛪 Статистика 🛪 Плагины 🗙 | | | | | | | |
| Имя Версия | Информация | | | | | | | |
| arp_cop 1.1 | Сообщает о подозрительных ARP активностях | | | | | | | |
| autoadd 1.2 | Автоматически добавляет новые жертвы в целевом диапазоне | Ξ | | | | | | |
| chk_poison 1.1 | Проверяет было ли заражение успешным | | | | | | | |
| dns_spoof 1.2 | Отправляет поддельные ответы mDNS | | | | | | | |
| dos_attack 1.0 | Запускает DOS атаку против указанного IP-адреса | | | | | | | |
| dummy 3.0 | Шаблон | | | | | | | |
| find_conn 1.0 | Ищет соединения в локальной сети с коммутатором | | | | | | | |
| find_ettercap 2.0 | атается обнаружить активность другого сетевого анализатора | | | | | | | |
| find_ip 1.0 | цет неиспользуемые IP-адреса в подсети | | | | | | | |
| finger 1.6 | Получает Fingerprint удалённого хоста | | | | | | | |
| finger_submit 1.0 | Отправляет неизвестный fingerprint разработчикам | • | | | | | | |
| 20388 МАС адресов произв | одителей | ^ | | | | | | |
| 1766 tcp OS fingerprint | | | | | | | | |
| 2182 сервисов известно | | | | | | | | |
| Запуск мониторинга обычн | запуск не возможен: ОЙ СЕТИ | | | | | | | |
| | | Ξ | | | | | | |
| Хост 192.168.5.135 добавле | ен к цели 1 | | | | | | | |
| i | | Ľ | | | | | | |

Рисунок 206 – Выбор плагина

3.7.9.3. Работа с инструментом в обычной сети

Для запуска процесса анализа локальной сети необходимо выбрать параметр «Обычная сеть...» в подменю «Мониторинг» (рис. 189).

Далее в появившемся окне необходимо указать сетевой интерфейс и нажать «ОК» (рис. 207).

| 0,5 | | Сетевой анализатор | - 0 | ж |
|------|------------------|--|------|---|
| Файл | Мониторинг | Настройки | | |
| | ∎ <u>₹</u> ?> | Обычная сеть – о × Сетевой интерфейс: eth0 Отменить С | | |
| | | | | |
| | | | | Ξ |

Рисунок 207- Выбор сетевого интерфейса

Для запуска процесса анализа сетевого трафика необходимо выбрать параметр «Запустить анализатор» в подменю «Начало» (рис. 190).

3.7.9.4. Атаки типа МІТМ

Для начала анализа необходимо определить IP-адреса хостов сети. Для этого необходимо выбрать параметр «Сканирование хостов» в подменю «Хосты» (рис. 191). Параметр «Список хостов» в подменю «Хосты» отображает информацию о просканированных хостах сети (рис. 192).

В меню «Цели» необходимо указать адреса хостов, которые будут проанализированы (рис. 193).

Для осуществления атаки ARP-poisoning необходимо выбрать параметр «ARP poisoning...» в подменю «MITM» (рис. 208).

| 1. 7 | | | | | | Сетево | й ан | нализатор - | - × - |
|---|--|---|------------------|--|---|----------------------------|------|-------------|-------|
| Начало | Цели | Хосты | Вид | MITM | Фильтры | Журналирова | ние | Плагины | |
| | | | | ARP ICMI Port DHC NDP Oct | poisoning P redirect : stealing :P spoofing ' poisoning ановить МГ | ТМ атаку 11 3001 | | | |
| 57 порт 20388 М/ 1766 tcp 2182 cep | ов осмо AC адре OS fing висов и | отрено сов про Jerprint 13вестно | извод) | ителей | | | | | |
| Lua: не у Запуск м | казаны онитор | сценари инга обы | ии, заг ычной | туск не сети | возможен! | | | | Ξ |

Рисунок 208 - Меню «МІТМ»

В открывшемся окне (рис. 209) необходимо указать дополнительные параметры.

| 1,7 | MITM-атака: ARP Poisoning 🛛 – 🛚 🗴 |
|-----|---|
| ? | Дополнительные параметры Мониторинг удаленных соединений Выполнять "Poisoning" только в одном направлении |
| | О <u>т</u> менить С |

Рисунок 209 – Дополнительные параметры

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

Чтобы остановить атаку необходимо выбрать параметр «Остановить МІТМ атаку» в подменю «МІТМ» (рис. 208).

Для осуществления атаки ICMP redirect необходимо выбрать параметр «ICMP redirect...» в подменю «МІТМ» (рис. 208). В появившемся окне необходимо указать сведения о шлюзе сети (рис. 210).

171 НПЭШ.00606-01 34

| 1. 7 | MITM-атака: ICMP Redirect 💷 🗷 🛪 |
|-----------------|---|
| ? | Информация о шлюзе МАС-адрес IP-адрес |
| | О <u>т</u> менить <i>С</i> |

Рисунок 210-Информация о шлюзе

В результате атаки ICMP пакеты будут перенаправлены от цели на хост ПК «Сканер-ВС». Чтобы остановить атаку необходимо выбрать параметр «Остановить МІТМ атаку» в подменю «МІТМ» (рис. 208).

Для осуществления атаки Port stealing необходимо выбрать параметр «Port stealing...» в подменю «МІТМ» (рис. 208). В появившемся окне можно указать дополнительные параметры атаки (рис. 211).



Рисунок 211 – Параметры атаки

Результатом атаки будет являться перенаправление трафика от цели к какому-либо порту на хост ПК «Сканер-ВС». Чтобы остановить атаку необходимо выбрать параметр «Остановить МІТМ атаку» в подменю «МІТМ» (рис. 208).

Для осуществления атаки DHCP spoofing необходимо выбрать параметр «DHCP spoofing ...» в подменю «MITM» (рис. 208). В появившемся окне необходимо указать информацию о сервере (рис. 212).

| L. | MITM атака: DHCP Spoofing _ | × |
|----|--------------------------------|-------|
| | Информация о сервере | 7 |
| | Пул IP-адресов (необязательно) | |
| | Маска подсети | |
| | IP-адрес DNS-сервера | |
| | О <u>т</u> менить | |

Рисунок 212 – Информация о сервере DHCP

В результате атаки хост ПК «Сканер-ВС» будет использоваться как DHCP-сервер сети по умолчанию. Чтобы остановить атаку необходимо выбрать параметр «Остановить MITM атаку» в подменю «MITM» (рис. 208).

Для осуществления атаки NDP poisoning необходимо выполнить следующие действия:

- выбрать параметр «Включить IPv6 сканирование» в подменю «Хосты» (рис. 191);
- выбрать параметр «NDP poisoning» в подменю «МІТМ» (рис. 208).

В появившемся окне можно указать дополнительные параметры атаки (рис. 213).



Рисунок 213 – Дополнительные параметры

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

Чтобы остановить атаку необходимо выбрать параметр «Остановить МІТМ атаку» в подменю «МІТМ» (рис. 208).

3.7.9.5. Работа с инструментом в коммутируемой сети

Для работы инструмента в коммутируемой сети необходимо выбрать параметр «Коммутируемая сеть...» в подменю «Мониторинг» (рис. 189).

Для корректной работы анализатора в коммутируемой сети необходимо указывать первый и второй сетевые интерфейсы (рис. 214).

| 0,5 | | | Сетев | зой анализат | гор | - | × |
|------|----------|------------|-----------------------------|---|------------------------------|---|---------|
| Файл | Монитори | инг | Настройки | | | | |
| | 1,7 | | Комм | 901 утируемая с | :еть – п × | | |
| | ? | Пер Вто | овый сетевой рой сетевой | интерфейс: интерфейс: О <u>т</u> мени | eth0 \$ Local Loopback \$ | | |
| | | | | | | | < III > |

Рисунок 214 – Мониторинг коммутируемой сети

В рабочем окне (рис. 188) необходимо задать цели, протокол и другие параметры анализа.

3.7.9.6. Завершение работы с инструментом

Для выхода из инструмента необходимо воспользоваться подменю «Выход» меню «Начало» (рис. 190) или подменю «Выход» меню «Файл».

3.7.10. Инструмент «Контрольное суммирование»

Инструмент «Контрольное суммирование» предназначен для контроля целостности информации.

3.7.10.1. Запуск инструмента

Инструмент запускается из веб-интерфейса «Контрольное суммирование» или из подменю стартера приложений. Для запуска инструмента необходимо выполнить следующие действия:

– запустить подменю стартера приложений;

- выбрать вкладку «Форензика»;

- выбрать инструмент «ПИК Эшелон».

После запуска инструмента «Контрольное суммирование» появится рабочее окно (рис. 215).

| | | | пик | Эшелон _ 🛛 × |
|--------|-----------------------|------------------------|----------|-------------------------------------|
| Проект | Добавить | Настройк | и Помоц | ць |
| ⊛ Ko | нтрольное су | ммирован (|) Инспек | ционный контрол: 🕨 Запустить проект |
| Цели | Алгоритмы | Фильтры | Отчёты | Выполнение |
| Цел | и для суммир | ования | | Доступные цели |
| Пе | реместите фа в эту | йлы и/или к область | аталоги | |

Рисунок 215 – Рабочее окно

3.7.10.2. Работа с инструментом

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

3.7.10.3. Контрольное суммирование

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

Вкладка «Цели» позволяет выбирать файлы для суммирования и содержит поля «Цели для суммирования» и «Доступные цели» (рис. 215).

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

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

Во вкладке «Алгоритмы» приведены краткие описания алгоритмов, используемых для проведения контроля (рис. 216). Выбрать алгоритмы суммирования можно вручную или воспользоваться кнопками «Выбрать стойкие» и «Выбрать все». Для очистки списка выбранных алгоритмов можно воспользоваться кнопкой «Очистить всё».

176 НПЭШ.00606-01 34



Рисунок 216 – Алгоритмы контрольного суммирования

В инструменте реализована функция фильтрации по расширениям файлов. Во вкладке «Фильтры» указаны типовые расширения файлов (рис. 217).

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

При нажатии на правую кнопку мыши в поле «Доступные фильтры» появится меню (рис. 217), позволяющее удалить или изменить расширение из списка подменю («Удалить» и «Изменить» соответственно). При выборе подменю «Загрузить стандартные расширения» будет восстановлен список по умолчанию.

| | 1 | ПИК Эшелон – 🕫 × |
|---------------|-------------------|---|
| Іроект Добави | ть Настройки П | омощь |
| ⊚ Контрольное | е суммирован 🔿 Ин | спекционный контроль 🕨 Запустить проект |
| Цели Алгоритм | иы Фильтры Отчё | ёты Выполнение |
| Выбранные фи | ільтры | Доступные фильтры |
| Все файлы | | Все файлы Архивы (tar,gz,tgz,gzip,bz2,bzip2,tbz: Все файлы без расширения |
| | | Объектные и отлалочные файлы (о Добавить Загрузить из целей |
| | | Загрузить стандартные расширения |
| | | Изменить |
| | | Удалить |
| | | РЕ-файлы (exe,dll,ocx,sys,scr,drv,cpl, |
| | | Perl (pl,pm,cgi) |
| | | PHP (php,php3,php4,php5,inc) |
| | | Buby (rb) |
| | | SQL (sql) |
| 🗹 Учитывать | регистр для расши | рений (|
| 1 | | |
| | | |

Рисунок 217 – Доступные фильтры

Чтобы вручную указать расширения, принимаемые на контроль, необходимо выбрать подменю «Добавить». С помощью подменю «Загрузить из целей» можно добавить фильтр из расширений файлов, выбранных для контрольного суммирования (рис. 217).

Во вкладке «Отчёты» можно указать директорию для сохранения отчетов (по умолчанию -Рабочий стол), ввести название папки для сохранения отчетов (по умолчанию - MyProject), выбрать вид отчетов и указать другие настройки (рис. 218).

|) Ko | нтрольное су | имирован С |) Инспен | сционный | конт | роль 🕨 | Запуст | ить проект |
|----------------------------|--------------|------------|-----------|----------|------------|-----------------------------|-----------------------|------------------------------|
| ели | Алгоритмы | Фильтры | Отчёты | Выполне | ение | | | |
| Дир | ектория отчё | тов | | | | | | |
| /roo | t/Desktop | | | | | | ~ | Обзор |
| Дир | ектория прое | кта | | | | | | |
| MyF | roject | | | | | | | ~ |
| Отчё | ты КС: | | | | нт | ML-отчёт | | |
| ✓ H | ITML sv | | | | Оторас | чёт в формат крывающее | е HTML о ся дерев | содержит о локаций |
| ∎т | хт | | | | про | ректа с контр формацию о | ольным дублика | и суммами, тах имён и |
| ⊽т | RE-отчёт | | | | рас | трольных су ширений пр | ими, табл оекта. | ицу |
| | | | | | Для вкл | я просмотра ючённым lav | требует /aScript. | ся браузер с |
| Настройки отчётов: | | | | | Под | цдерживаем | ые брауз | еры: IE6+, |
| Создать обложку для дисков | | | | | Goo 3.0 | gle Chrome +, Opera 10. | 9.0+, Mo 50+, Safa | zilla Firefox ari 5.0.5+, |
| | | | енения фа | йлов | Elk | browser 10.0 | .2+. | |

Рисунок 218 – Вкладка «Отчеты»

Для запуска процесса контрольного суммирования необходимо нажать «Запустить проект». После запуска процесса во вкладке «Выполнение» будет отображаться процесс выполнения задачи. После завершения контрольного суммирования необходимо нажать кнопку «Открыть директорию с отчётами» (рис. 219).

| Цели | Алгоритмы | Фильтры | Отчёты | Выполнение | |
|---------|--------------|---------|--------|------------|--|
| Прот | гокол работы | | | | |
| 16 - 1- | e reports | | | | |

Рисунок 219 – Вкладка «Выполнение»

Отчет в формате HTML может содержать следующие вкладки: «Статистика проекта» (рис. 220), «Контрольные суммы» (рис. 221), «Дополнительные отчеты» (рис. 222).

| Статистика проекта | Контроль | ные суммы Дополнители | ные отчёты | | | | |
|---|---|---|--|--|---------|--|--|
| Локации | | "/root/Изображения" | | | | | |
| Фаилов оораоотано | | 0 | | | | | |
| директорий обработано | | 1 | | | | | |
| Размер Время анализа | | 0 байт Начался: 29-05-2018 14:06:35 Закончился: 29-05-2018 14:06:35 | | | | | |
| Повторяющиеся имена | | 0 | | | | | |
| Повторяющиеся КС | | 0 | | | | | |
| Количество расширений | | 0 | | | | | |
| Использованные фильтры | | Все файлы | | | | | |
| | | Контрольные | суммы проекта | | | | |
| ГОСТ 34.11-94 (S-блок | CryptoPro | 59ae4b6c3f2c6c82776 | a681dac5bb1e171bf | bee6cb9443c3e03692fd3e | ecld70a | | |
| | Ko | нтрольные суммы лока | ции "/root/Изобрал | жения" | | | |
| ГОСТ 34.11-94 (S-блок | CryptoPro | 981e5f3ca30c8414878 | 30f84fb433e13ac110 | 01569b9c13584ac483234 | d656c0 | | |
| | Контакт | елон программное обеспечения и технической поддержки продуг | © АО "НПО "Эшелон" <u>http</u> па: <u>support.pik@cnpo.ru</u> | ://cnpo.ru/ | | | |
| | 6 | Рисунок 220 | – Статистика | проекта | | | |
| | ыным | Рисунок 220 суммам (КС) прое | – Статистика кта "MyProject" | проекта от 29.05.2018 | | | |
| Чёт по контрол ПИК Эшелон 1.0.06 Владелец лицензии: "Ма | БНЫМ (стер-образ" N | Рисунок 220 суммам (КС) прое | – Статистика кта "MyProject" ^{09,2017 по 10.01.2038.} | проекта от 29.05.2018 | | | |
| Чёт по контрол Пик Эшелон 1.0.06 Владелец лицензии: "Ма тистика проекта Контроле | Ъ Стер-образ" N ные суммы | Рисунок 220 Суммам (КС) прое е 01. Срок действия лицензии с 13 Дополнительные отчёты | - Статистика кта "MyProject" 09.2017 по 10.01.2038. | проекта от 29.05.2018 | | | |
| Чёт по контрол Пик Эшелон 1.0.06 Владелец лицензии: "Ма тистика проекта Контроле | Б стер-образ" N ные суммы Размер | Рисунок 220 суммам (КС) прое е 01. Срок действия лицензии с 13 Дополнительные отчёты время создания время | - Статистика кта "MyProject" 09.2017 по 10.01.2038. | проекта от 29.05.2018 гост 34.11-94 (S-блок Cryp | toPro) | | |

Рисунок 221 – Контрольные суммы

В селессий бориалисть ПИК Эшелон программное обеспечение © АО "НПО "Эшелон" <u>http://спро.nu/</u>Контакты технической поддержки продукта: <u>support.pik@cnpo.nu</u>


Рисунок 222 – Дополнительные отчеты

3.7.10.4. Завершение работы с инструментом

Для выхода из инструмента необходимо воспользоваться параметром «Выход» в подменю «Проект» или нажать «Крестик» в верхнем правом углу окна.

3.8. Информация

В разделе «Информация» (рис. 223) приведены такие сведения, как:

- Продукт;
- Разработчик;
- Техническая поддержка;
- Сайт продукта.

| Сканер-ВС онализ защищиности | | 쓥 | * | 6 | 2 | 4 | × |
|--|---|---|---|---|---|---|---|
| Главная / Информация | | | | | | | |
| Информация о продукте | | | | | | | |
| Продукт Разраборника Техническая продукта: Сайт продукта: | Сканер-ВС Лицензия без ограничения (v5.0.0) © 2017-2018 АФ "НПО "Эшелон" scaner vs.ru | | | | | | |

Рисунок 223 – Раздел «Информация»

В раздел «Информация» можно перейти, нажав на пиктограмму «

3.9. Уведомления

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

Количество уведомлений отображается на пиктограмме «Уведомления» в числовом виде (рис. 224).



Рисунок 224 – Пример наличия непрочитанных уведомлений

При нажатии на пиктограмму «Уведомления», на панели навигации, открывается всплывающее окно со списком непрочитанных уведомлений (рис. 225).



Рисунок 225 – Всплывающее окно

Для работы с уведомлениями Оператору доступны следующие действия:

– переход к источнику уведомления;

- очистка всех уведомлений.

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

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

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

Настройка получения уведомлений происходит в профиле пользователя, в разделе «Личная информация» (п. 3.10.2).

3.10. Личная информация

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

В инструмент «Личная информация» можно перейти по пиктограмме « ²» на панели навигации.

Инструмент «Личная информация» выполнен в форме всплывающего окна (рис. 226).



Рисунок 226 - Всплывающее окно «Личная информация»

Инструмент «Личная информация» позволяет Оператору выполнить следующие действия:

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

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

- войти в профиль;

– выйти из ПК «Сканер-ВС».

Информация о профиле доступна вверху всплывающего окна (рис. 226) и отображается в виде: «Ваш логин: xxx». Где, xxx – это название профиля.

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

Выход из ПК «Сканер-ВС» осуществляется по нажатию кнопки «». После выхода Оператор попадает в окно авторизации (рис. 41).

При нажатии кнопки « Профиль », Оператор переходит в рабочее окно личного кабинета (рис. 227).

| сканер-ВС анализ защищенности | | 쓭 | ÷ | × | Û | 2 | ۵ | × |
|----------------------------------|---|---|---|---|---|---|---|---|
| Главная / Личный кабинет | | | | | | | | |
| Профиль | Bau norus: admin | | | | | | | |
| Укеломления | Ваше имя: Администратор Сканер-ВС | | | | | | | |
| уведомления | Ваша почта: Не указано 🖉 | | | | | | | |
| Персонализация | Статус: Не заблокирован Пароль: **** 🕼 | | | | | | | |
| | | | | | | | | |

Рисунок 227 – Личный кабинет

В личном кабинете присутствуют следующие вкладки:

- Профиль;
- Уведомления;
- Персонализация.

3.10.1. Вкладка «Профиль»

Во вкладке «Профиль» (рис. 227) отображается информация о профиле Оператора:

– логин;

– имя;

```
- ваша почта (электронная почта);
```

– пароль.

«Логин» и «Имя» задается в разделе «Администрирование» при создании нового пользователя (см. пп. 3.5.2.2).

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

После ввода нового адреса электронной почты нажать кнопку «Сохранить» (рис. 228).

| Ваша почта: | | |
|-------------|--------|--|
| Сохранить | Отмена | |

Рисунок 228 – Окно ввода электронной почты

При изменении пароля открывается форма смены пароля (рис. 229).

| Старый пароль * | Ι |
|----------------------|---|
| Новый пароль * | |
| Подтвердить пароль * | |
| Применить Отмена | |

Рисунок 229 – Форма смены пароля

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

Правила создания нового пароля описаны в подпункте 3.5.2.2.

После завершения ввода нового пароля нажать кнопку «Применить». Если все действия выполнены правильно, то откроется всплывающее окно с подтверждением смены пароля (рис. 230).

Информация

Пароль успешно изменен!

Рисунок 230 – Подтверждение смены пароля

3.10.2. Вкладка «Уведомления»

Вкладка «Уведомления» (рис. 231) разделена на вкладки «События» и «Правила».

| Сканер-ВС | | | | | 容 | | ∗ | Ó | 18 | 4 |
|-----------------------|-----------------|-----------------------|----------------|--------------|----|---------|---|---|----|---|
| вная / Личный кабинет | | | | | | | | | | |
| Профиль | | | | | | | | | | |
| Уведомления | События | Правила | | | | | | | | |
| Персонализация | Добавить правил | o | | | | | | | | |
| | ID | Правило | Способ | Конфигурация | Де | ействия | | | | |
| | 1 | Внутренние уведомлени | Веб-приложение | | | | | | | |

Рисунок 231 – Рабочее окно вкладки «Уведомления»

3.10.2.1. Вкладка «Правила»

Вкладка «Правила» (рис. 232) предназначена для добавления правил для событий.

| сканер-ВС анализ защищенности | | | | 1 | 4 | - | ✻ | i | 18 | 8 | 5 |
|----------------------------------|------------------|---------------------|----------------|-----------------------|---|---------|---|---|----|---|---|
| лавная / Личный кабинет | | | | | | | | | | | |
| Профиль | Coburya | 2014/02 | | | | | | | | | |
| Уведомления | Соовтия ттр | авила | | | | | | | | | |
| Персонализация | Добавить правило | | | | | | | | | | |
| | ID | Правило | Способ | Конфигурация | Ļ | цействи | я | | | | |
| | 1 | Внутренние уведомле | Веб-приложение | - | | | | | | | |
| | 2 | Правило | http | {"hostname":"localhos | | Û | | | | | |

Рисунок 232 - Вкладка «Способы»

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

- ID Порядковый номер правила;
- правило название правила;
- способ способ уведомления;
- конфигурация краткая конфигурация правила;
- действия разрешенные действия с правилом.

Правило можно упорядочивать, нажав на заголовок столбца таблицы.

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

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

Для создания нового правила необходимо нажать кнопку «Добавить правило». Откроется форма добавления нового сервера (рис. 233).

| Профиль | События Правида | |
|----------------|-----------------------------------|--------------------------------|
| Уведомления | Привили | |
| Персонализация | Добавить новое правило для отправ | ки уведомлений |
| | Имя 😡 * | Отправка событий в SIEM КОМРАД |
| | Способ | HTTP |
| | Адрес сервера 🕢 🔺 | 192.168.0.1 или localhost |
| | Порт 🕝 | 8080 |
| | Путь 🚱 | /events |
| | Создать Отмена | |

Рисунок 233 – Форма добавления нового сервера

Форма содержит следующие поля:

- Имя название правила отправки уведомлений;
- Способ способ доставки уведомления;
- Адрес сервера IP-адрес (без протокола) сервера, на который будут отправляться уведомления;
- Порт порт, на который будут отправляться уведомления;
- Путь адрес директории на сервере, в которой будут сохраняться уведомления (автоматически не создается).

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

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

Значок « 😰 » информирует о наличии подсказки по данному полю.

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

3.10.2.2. Вкладка «События»

Вкладка «События» представлена в виде таблицы (рис. 231). В левой ее части содержится перечень событий, по которым ПК «Сканер-ВС» отправляет уведомления. В правой части таблицы содержатся правила уведомления.

По умолчанию, в ПК «Сканер-ВС», создано правило «Внутренние уведомления», которое выводит уведомления о событиях на пиктограмму «

В таблице содержатся следующие события:

- вход в систему;
- выход из системы;
- создание пользователя;
- изменение информации о пользователе;
- изменение привилегий пользователя;
- блокировка пользователя;
- разблокировка пользователя;
- обновление пароля пользователя;
- удаление пользователя;
- создание проекта;
- удаление проекта;
- редактирование проекта;
- создание задачи;
- редактирование задачи;
- удаление задачи;
- запуск задачи;
- запуск задачи по планировщику;
- приостановление задачи;
- возобновление задачи;

- отмена задачи;

– планирование задачи;

- задача завершена;

- задача отменена;

- задача завершена с ошибкой.

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

Добавление правил для событий происходит во вкладке «Правила» (см. пп. 232).

3.10.3. Вкладка «Персонализация»

Вкладка «Персонализация» (рис. 234) содержит настройки по персонализации следующих элементов ПК «Сканер-ВС»:

- форма поиска целей;
- форма поиска уязвимостей;
- форма подбора паролей;
- форма автоматического поиска эксплойтов;
- форма ручного поиска эксплойтов;
- форма создания проекта;
- гибкая настройка языков.

| Сканер-ВС | | |
|--------------------------|--------------------------------|--------------------|
| Главная / Личный кабинет | | |
| Профиль | | |
| Уведомления | Форма поиска целей | Пользовательская 🕼 |
| Персонализация | Форма поиска уязвимостей | По умолчанию 🗷 |
| | φορικό ποιδούο ποροποιά | |
| | Формалодоора паролея | Поумолчанию с |
| | Форма создания проекта | По умолчанию 🕜 |
| | Форма поиска эксплойтов | По умолчанию 🕼 |
| | Язык Гибкая настройка языка | |
| | | |

Рисунок 234 – Вкладка «Персонализация»

Настройки персонализации можно изменить, нажав на значок « 🖾 ».

После изменения и сохранения настроек надпись «По умолчанию» изменится на «Пользовательская» (рис. 234).

3.10.3.1. Форма поиска целей

На рисунке (рис. 235) представлена форма поиска целей.

| UMR @ | VIMR |
|---|---|
| | |
| Описание 🛛 | Описание |
| | |
| Цели 😡 | Пример: 127.0.0.1, 192.168.0.1/24, 192.168.0.2-24 |
| | |
| Сканировать конкретные ТСР-порты 😡 | Пример: 1-1023, 21-25, 80 |
| | |
| Определять версию • | 0 |
| Трасировка 😡 | 0 |
| Сканировать конкретные UDP-порты 😡 | Пример: 53, 10-111 |
| | |
| Скорость сканирования 🛛 | Оптимальная |
| Таймаут сканирования, сек 🖗 | |
| | |
| Игнорировать 🛛 | ()a |
| результаты Ping | |
| Committee and the second se | |

Рисунок 235 – Форма поиска целей

В таблице (см. Таблица 10) представлено описание полей формы поиска целей.

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

| 192 | |
|------------------|---|
| НПЭШ.00606-01 34 | ŀ |

| Параметр | Описание |
|------------------------------|---|
| Игнорировать результаты Ping | Настройка для обнаружения хостов с помощью TCP SYN вместо Ping |

Значок « ²⁰ » информирует о наличии подсказки по данному полю.

Для сохранения результатов необходимо нажать кнопку «Создать».

3.10.3.2. Форма поиска уязвимостей

На рисунке (рис. 236) представлена форма

| анализ защищенности | |
|---|---------------------------|
| Главная / Личный кабинет / Форма поиска уязвимостей | |
| Имя 🚱 | Имя |
| Описание 🚱 | Описание |
| Политика сканирования 🥝 | Быстрая |
| Цели 😡 | Цели |
| Методы ping | ARP TCP ICMP |
| Тип сети 📀 | Mixed (use RFC 1918) |
| Рассматривать несканируемые как 🕢 закрытые | |
| Сканировать конкретные ТСР-порты 😧 | Пример: 1-1023, 21-25, 80 |
| | |
| Списки портов 🔞 | Общеизвестные |
| Безопасные 🕜 проверки | |
| Πορτ | |
| Таймаут сети, сек 🕑 | |
| Таймаут между запросами 🕑 | |
| Создать | |

Рисунок 236 – Форма поиска уязвимостей

В таблице (см. Таблица 11) представлено описание полей формы поиска уязвимостей.

| Параметр | Описание |
|---|---|
| Имя | Имя задачи |
| Описание | Описание задачи |
| Политика сканирования | Политика сканирования определяет перечень сетевых проверок безопасности, которые будут запущены в ходе сканирования уязвимостей. Выберите одну из предустановленных или создайте собственную в подпункте 3.6.5.3 |
| Цели | IP-адрес |
| Mетоды ping | Параметр выбора метода ping: – ARP; – TCP; – ICMP |
| Тип сети | Параметр, указывающий тип сети |
| Рассматривать несканируемые, как закрытые | Настройка отключения сканирования неизвестных портов |
| Сканировать конкретные ТСР-порты | Параметр для сканирования нестандартных TCP- портов или диапазонов TCP-портов |
| Сканировать конкретные UDP-порты | Параметр для сканирования нестандартных UDP- портов или диапазонов UDP-портов |
| Списки портов | Параметр выбора предустановленного диапазона портов для сканирования. Общеизвестные - сканирование будет проводиться по списку портов от 1 до 1024. Стандартные (рекомендуется) - сканирование будет проводиться по списку часто используемых портов (4481). Все - будут просканированы все порты, при выборе данной опции время сканирования может существенно увеличиться |
| Безопасные проверки | Параметр для отключения проверок, которые могут вызвать нарушение доступности проверяемых сетевых сервисов и хостов |
| Порт | Перечень портов |
| Таймаут сети, сек | Параметр для пропуска целевых хостов, время сканирования которых превышает установленный таймаут |
| Таймаут между запросами | Параметр для установки значения тайм-аута для сетевых сокетов во время сканирования |

Таблица 11 – Описание полей формы поиска уязвимостей

Значок « 💿 » информирует о наличии подсказки по данному полю.

Для сохранения результатов необходимо нажать кнопку «Создать».

3.10.3.3. Форма подбора паролей

На рисунке (рис. 237) представлена форма подбора паролей.

| Сканер-ВС анализ защищенности | |
|--|---|
| Главная / Личный кабинет / Форма подбора паролей | |
| Имя 🕑 | Имя |
| Описание 🚱 | Описание |
| | |
| Порт 🥹 | |
| Цели 🕜 | Пример: 127.0.0.1, 192.168.0.1/24, 192.168.0.2-24 |
| Пользователи | Пример: admin, root |
| Найденные ранее пользователи 🕢 Пароли 🕜 | Оример: 123456, qwerty |
| Найденные ранее 🕜 пароли | |
| Проверить пустой 🛛 🕢 Пароль | |
| Проверить пароль, совпадающий 🕜 с логином | |
| Проверить пароль, совпадающий с логином в 🛛 🚱 обратном порядке | |
| Закончить подбор при первом 🕢 🕢 | |
| Таймаут сканирования, сек 🖗 | |



В таблице (см. Таблица 12) представлено описание полей формы подбора паролей.

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

| тſ | 10 | 0 | v | 1 | ~ | |
|------------|------|----------|-------|---------|---------|-------------|
| Гаолина | 12 - | Описание | полеи | формы | полоора | паролеи. |
| 1 worningw | | • | | TOPHILL | megeep. | in point in |

Значок « 💿 » информирует о наличии подсказки по данному полю.

Для сохранения результатов необходимо нажать кнопку «Создать».

3.10.3.4. Форма поиска эксплойтов

На рисунке (рис. 238) представлена форма поиска эксплойтов

| сканер-ВС анализ защищенности | | 쓥 | - | ж | Û | <mark>_18</mark> | 4 | × |
|--|-------------------------------------|---|---|---|---|------------------|---|---|
| Главная / Личный кабинет / Форма поиска эксплойтов | | | | | | | | |
| Тип 😡 сервиса | | | | | | | | |
| Продукт © | > | | | | | | | |
| Версия © | O | | | | | | | |
| Строгий 😡 поиск | 0 | | | | | | | |
| Ключевые слова 🚱 | Пример: java rmi server, phpmyadmin | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |



В таблице (см. Таблица 13) представлено описание полей формы поиска эксплойтов.

| Таблица 13 – Описание полей | формы поиска | эксплойтов |
|-----------------------------|--------------|------------|
|-----------------------------|--------------|------------|

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

Значок « 😰 » информирует о наличии подсказки по данному полю.

Для сохранения результатов необходимо нажать кнопку «Создать».

3.10.3.5. Гибкая настройка языков

На рисунке (рис. 239) представлена форма гибкой настройка языков.

| Язык 🗸 Гибкая настройка языка | |
|----------------------------------|---------|
| Язык интерфейса | Русский |
| Язык эксплойтов | Русский |
| Язык плагинов | Русский |

Рисунок 239 – Гибкая настройка языков

В таблице (см. Таблица 14) представлено описание полей формы гибкой настройка языков.

Таблица 14 – Описание полей формы гибкой настройка языков

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

3.11. Компонент «Инспектор»

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-К, СЗИ НСД Dallas Lock 8.0-С;

- 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.

Примечание. Для просмотра отчетов компонента «Инспектор» требуется ПО Microsoft Internet Explorer одной из следующих версий: 8, 9, 10, 11 и Mozilla Firefox for Ubuntu версии 44.0.2.

3.11.1. Запуск компонента

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

После запуска откроется окно активации лицензии (рис. 240).



Рисунок 240 – Окно активации лицензии

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. 241).



Рисунок 241 – Окно с информацией об успешной активации лицензии

Далее необходимо повторно запустить компонент «Инспектор».

После запуска откроется стартовое окно компонента «Инспектор» (рис. 242).



Рисунок 242 - Стартовое окно

После запуска Оператору необходимо создать новый проект или выбрать проект из ранее созданных (рис. 242).

Для того, чтобы продолжить работу с ранее созданным проектом необходимо нажать кнопку «Продолжить работу» и в открывшемся окне выбрать сохраненный проект (рис. 243).

| 强 Открыть проект | | | | × |
|-------------------------------|--|------------------|---------------------|---------|
| 🔶 -> - 🛧 -> Это | от компьютер » Рабочий стол » InspectorP | roject v Ö | Поиск: InspectorPro | ject 🔎 |
| Упорядочить 🔻 Нова | ая папка | | | - 🔳 🕐 |
| | Имени | Дата изменения | Тип | Размера |
| Рабоний сто | Test | 28.03.2018 16:51 | Папка с файлами | |
| | Test.inpj | 29.03.2018 17:27 | Файл "INPJ" | 1 КБ |
| 🐳 загрузки 🗶 🚆 Документы 🖈 | | | | |
| 📰 Изображени 🖈 🗸 | | | | |
| <u>И</u> мя с | файла: Test.inpj | ~ | Файл проекта (*.in | pj) |
| | | | <u>О</u> ткрыть | Отмена |

Рисунок 243 - Сохраненный проект

Для создания нового проекта необходимо нажать кнопку «Новый проект». В открывшемся окне (рис. 244) 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.

| 🖳 Инспектор | × |
|-----------------------------------|-----------|
| Создание нового проекта | |
| Имя проекта: | |
| Test | |
| Расположение: | |
| C:\Users\Desktop\InspectorProject | Обзор |
| Организация: | |
| Test | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| <u>З</u> аверши | ть Отмена |

Рисунок 244 – Ввод параметров нового проекта

После нажатия кнопки «Завершить» по указанному адресу будет автоматически создана папка с конфигурациями проекта, содержащая файл проекта с расширением «.inpj» (рис. 245), и откроется рабочее окно компонента «Инспектор» (рис. 246).

| 📙 🛃 📕 🖛 Insp | ectorProject | | | | | | | - | | × |
|---|--------------|--------|--|-------------------|------------------|----------------------------------|----------------------|---|-------------------------|------|
| Файл Главная | Поделитьс | я | Вид | | | | | | | ^ 🕐 |
| Закрепить на панели к быстрого доступа | Копировать | Встав | 🔏 Вырезать 🚾 Скопировать путь ить 🖻 Вставить ярлык | 🙀 Переместить в 👻 | 🗙 Удалить 👻 | <mark>∎</mark> Новая папка | Свойства • Журнал | Выделить во Снять выдел Обратить вы | :е 1ение ыделение | |
| | Буфер об | бмена | | Упоря | дочить | Создать | Открыть | Выделит | ть | |
| $\leftarrow \rightarrow \cdot \cdot \uparrow$ | > Inspector | Projec | t | | | | | ~ Ū | Поиск: In | . ,o |
| | | ^ | Имени | | Дата изменения | Тип | Размера | | | |
| 🖈 Быстрый достуг | п | | — • | | | | | | | |
| — Рабочий стол | * | | est 🕞 | | 09.04.2018 16:05 | Папка с файла | NN | | | |
| 🖊 Загрузки | A | | Test.inpj | | 06.04.2018 15:16 | Файл "INPJ" | 1 КБ | | | |
| 🔮 Документы | * | | | | | | | | | |
| Изображения Элементов: 2 | * | * | | | | | | | | :== |

Рисунок 245 – Папка проекта

| 🖳 Test - Инспектор | – 🗆 X |
|--|---|
| Проект Тестирование Отчет Помощь | |
| Инспектор - Test (Test) | |
| окббјк hvwpK73h hCEKPET8P WE82rTm WggBt | □□ □□ [□] Системный аудит |
| Проверка механизмов очистки оперативной памяти и запоминающих устройств, поиск остаточной информации по ключевым словам. | Инвентаризация программных и аппаратных средств. |
| 💟 🛛 Контрольное суммирование | 🗾 🖓 Проверка прав доступа |
| Контрольное суммирование заданных файлов (папок, подпапок, съемных носителей). | Тестирование прав доступа к выбранным объектам (каталогам и файлам) в различных сессиях. |
| Владелец лицензии: Echelon, № 2. Срок действия лицензии с 27.11.2016 до 01.06.2018 | Вперед > |

Рисунок 246 – Рабочее окно

В рабочем окне (рис. 246) 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. 247);



Рисунок 247 – Подменю «Проект»

 – «Тестирование» содержит утилиты: «Проверка прав доступа», «Проверка механизма очистки памяти», «Тестирование антивируса» (рис. 248);



Рисунок 248 – Подменю «Тестирование»

 - «Отчет» открывает отчеты, которые были созданы ранее, и содержит утилиту сравнения отчетов (рис. 249);



Рисунок 249 - Подменю «Отчет»

 – «Помощь» (рис. 250) открывает окно с информацией о версии, лицензии и ее продлении (кнопка «Продлить лицензию») (рис. 251).



Рисунок 250 – Подменю «Помощь»



Рисунок 251 – Окно с информацией о лицензии

Примечание. Комбинации клавиш для клавиатурного режима работы с компонентом представлены в приложении (см. Приложение 3).

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

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

3.11.2.1. 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. 220):

DIGSIG ENFORCE=1

DIGSIG LOAD KEYS=1



Рисунок 252 – Установленные параметры для запуска ЗПС

Далее необходимо закрыть файл digsig_initramfs.conf и сохранить изменения, после чего, нужно ввести команду update-initramfs -u -k all и выполнить перезагрузку (рис. 253).

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# <mark>_</mark>

Рисунок 253 – Ввод команды для запуска ЗПС

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

3.11.2.2. 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. 254).



Рисунок 254 – Путь к панели управления

Далее необходимо открыть вкладку «Безопасность» и открыть программу «Политика безопасности» (рис. 255).

| Панель | управле | ения | | | | |
|---|------------------------------------|--------------------|------------------------|--------------------------------------|--|---------|
| Рабочий стол Оборудование Прочее Сеть Сеть Безопасность Программы | Проверка целостности системы | Системный киоск | Санкции PolicyKit-1 | Управлен Политика безопасности | ние политикой безопасности Журнал безопасности | |
| Фильтр Справка | | | | | | Закрыть |

Рисунок 255 – Вкладка «Безопасность»

После запуска программы «Политика безопасности» нужно перейти во вкладку «Замкнутая программная среда» и выбрать пункт «Включить» в окне контроля исполняемых файлов (рис. 256).

| 🦁 Управление политикой безопасно | ости - Настроки замкнутой программной среды 🚊 🗖 🗙 |
|---|--|
| Файл Правка Настройки Помоц | te Bce ~ |
| ∽ 🖵 inspector-test | Настроки замкнутой программной среды |
| >- 🛒 Аудит >- 🏩 Группы | Настройки 🖉 Ключи 🦻 Подпись |
| >- 😼 Замкнутая программная с | Панель упр |
| >- 🕡 Мандатные атрибуты — 🖲 Мандатный контроль цело — 🛅 Монитор безопасности >- 🚺 Настройки безопасности | Контроль исполняемых файлов Выключить Отладка Включить |
| >- 🚑 Политики учетной записи >- 🏩 Пользователи >- 🚋 Привилегии >- [Устройства и правила | Шаблон <mark>Включает проверку</mark> рторых будет производи подписи /etc/digsiисполняемых файлов |

Рисунок 256 – Включение ЗПС

Далее необходимо в меню выбрать пункт «Правка» и нажать «Применить» (рис. 257).

| 🦁 Управление политикой безопасн | ости - Настроки замкнутой программной среды 💶 🛛 🗙 |
|--|---|
| Файл Правка Настройки Помол | щь |
| - Удалить Del | Настроки замкнутой программной среды |
| >- 1 Создата Санти >- 2 С Примонить Ctrl+S | 🚰 Настройки 🖉 Ключи 📝 Подпись |
| 🗸 🖉 Отменить Esc | Панель упр |
| Ключи Подпись Мандатные атрибуты Мандатный контроль ц Монитор безопасности Настройки безопасности | Контроль исполняемых файлов Выключить (Отладка Включить (Шаблоны имён файлов для которых будет производи (etc/diesig/yattr_control |
| | |

Рисунок 257 – Применение настроек

После нажатия кнопки «Применить» появится сообщение с предупреждением о запуске ЗПС (рис. 258). Нужно нажать «Да» и дождаться перезагрузки, после чего ОС Astra Linux 1.6 будет работать в режиме ЗПС.



Рисунок 258 – Сообщение с предупреждением о запуске ЗПС

3.11.3. Работа с инструментами

В рамках одного проекта для проведения тестирования можно выбрать один, несколько или все инструменты компонента «Инспектор». Работа инструментов и утилит 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.

3.11.3.1. 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. 246). Откроется рабочее окно инструмента «Проверка механизмов очистки» (рис. 259).

| 🗜 Теst - Инспектор | - | | × |
|---|---------|-------|-----|
| роект Тестирование Отчет Помощь | | | |
| Проверка механизма очистки оперативной памяти | | | |
| Проверить механизм очистки оперативной памяти | | | |
| Проверка механизмов очистки | | | |
| Выбор устройств: | | | |
| С. NTFS 439.73 Гбайт | | | |
| Тоиск по ключевым словам Выбор устройств: > ☐ WDC WD5000ААКХ-08U6АА0 (465.76 Гбайт) | | | |
| | | | |
| | | | |
| | | | |
| Выбор ключевых слов и настройка поноха | | | |
| Зладелец лицензии: Echelon, № 2. Срок действия лицензии с 27.11.2016 до 01.06.2018 | < Назад | Bnepe | д > |

Рисунок 259 – Инструмент «Проверка механизмов очистки»

Инструмент «Проверка механизмов очистки» (рис. 259) предназначен для проверки эффективности работы средств гарантированного уничтожения информации, осуществляющих оперативное удаление данных в автоматизированных системах, и решает следующие задачи:

- проверка механизма очистки оперативной памяти;
- проверка механизмов очистки устройств;
- поиск по ключевым словам.

3.11.3.1.1 Проверка механизма очистки оперативной памяти

Для запуска нужно поставить галочку в квадратном поле рядом с «Проверить механизм очистки оперативной памяти» (рис. 260) и нажать кнопку «Вперед». Откроется новое окно с информацией о настройках проекта (рис. 261). 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.

| 强 Test - Инспектор | - | | × |
|--|---------|--------|-----|
| Проект Тестирование Отчет Помощь | | | |
| Проверка механизма очистки оперативной памяти | | | |
| Проверить механизи очистки оперативной памяти | | | |
| Проверка механизмов очистки | | | |
| Выбор устройств: | | | |
| С. NTF5 439.73 Гбайт | | | |
| Поиск по ключевым словам Воборустройств: | | | |
| > 🗌 WDC WD5000ААКХ-08U6АА0 (465.76 Гбайт) | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Выбор ключевых слов и настройка поиска | | | |
| Владелец лицензии: Edhelon, № 2. Срок действия лицензии с 27.11.2016 до 01.06.2018 | < Назад | Bnepe, | д > |

Рисунок 260 – Проверка механизма очистки оперативной памяти

| Test - Инспектор | | - c |] |
|--|--------|------|-------|
| рект Тестирование Отчет Помощь | | | |
| отовы начать | | | |
| h.t | | | |
| нформация о проекте | | | |
| азвание: iest рганизация: Test | | | |
| уть до проекта: C:/Users/Desktop/InspectorProject1 | | | |
| астройки проверки механизмов очистки | | | |
| | | | |
| росрка пехапизна очистки оперативной напити. | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | < Hase | an B | перел |

Рисунок 261 – Информация о проекте

В открывшемся окне (рис. 262) будет представлена информация о ходе выполнения проверки.

214 НПЭШ.00606-01 34

| | | | | | |
|--|---|--|------|------|--|
| | | | 100% | | |
| .03.2018 12:26:37 Запуск п .03.2018 12:26:43 Заверше .03.2018 12:26:44 Формирс .03.2018 12:26:44 Формирс .03.2018 12:26:45 Формирс | роверки механизма очис ние проверки механизма звание итогового отчета. звание итогового отчета з | тки оперативной памяти. очистки оперативной пам завершено. | яти. | | |
| стирование завершено у ожмите "Открыть отчет" д | спешно. µля просмотра отчетов. | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Рисунок 262 – Ход выполнения проверки

После успешного завершения тестирования необходимо выбрать в подменю «Тестирование» пункт «Проверка механизма очистки памяти» (рис. 263).

| Test | 14 | | | | | | | | | |
|-----------------|---|--|-----------------|------------|-----|--|---------------|--------------|------------|----|
| nest - | Тестирование | Отнет Помошь | | | | | | | | |
| | Проверка | прав доступа | Ctrl+T | | | | | | | |
| од | 🥟 Проверка | механизма очистки памяти | Ctrl+M | | | | | | | |
| | Тестирова | ние антивируса | Ctrl+Y | | | | | | | |
| | | | | | 00% | | | | | |
| г вы | полнения: | | | | | | | | | |
| 9.03.3 9.03. | дия насими Фордина 2018 12:26:45 Фор органие завери инте "Открыть от | эмирование итоговото отчета. эмирование итоговото отчета з емо успешно. чет" для просмотра отчетов. | авершено. | | | | | | | |
| | | | | | | | Открыть отчет | Открыть ката | лог с отче | та |
| аделец | ц лицензии: Echelo | л, № 2. Срок действия лицензии | с 27.11.2016 до | 01.06.2018 | | | | Готово | Отм | er |

Рисунок 263 – Подменю «Тестирование»

В появившемся окне необходимо нажать кнопку «Начать проверку» (рис. 264).

215 НПЭШ.00606-01 34

| | 100% | | | |
|---|---|-------|--|--|
| выполнения: | | | | |
| 04.2018 14:18:59 Запуск проверки механ | низма очистки оперативной памяти. | | | |
| .04.2018 14:19:05 Завершение проверки .04.2018 14:19:05 Формирование изоголи | механизма очистки оперативной памяти. | | | |
| .04.2018 14:19:06 Формирование итогово | ого отчета завершено. | | | |
| | , | | | |
| стирование завершено успешно. | | | | |
| жмите "Открыть отчет" для просмотра | | × | | |
| | Проверка механизма очистки оперативной памяти | ^ | | |
| | Проверка механизма очистки оперативной п | | | |
| | | амяти | | |
| | | иткмы | | |
| | · · · · · | иткмр | | |
| | 0% | амяти | | |
| | 0% Начать проерку | ИТКМБ | | |
| | 0% Начать проверку | | | |
| | 0% Начать проверку | | | |
| | 0% Начать проверку | | | |
| | 0% Начать проверку | | | |
| | 0% Манать проверку | | | |
| | 0% Начать проверку | | | |
| | 0% Начать проверку | | | |

Рисунок 264 – Проверка механизма очистки оперативной памяти

По завершению проверки появится соответствующее сообщение (рис. 265). Далее нужно нажать кнопку «ОК».

| Ход выполнения | | |
|--|--|--|
| | 100% | |
| ог выполнения: | | |
| 05.04.2018 14:19:05 Формирование итогово 05.04.2018 14:19:06 Формирование итогово Тестирование завершено успешно. Нажмите "Открыть отчет" для просмотра | го отчета. отчета завершено. Опчетоя. Проверка меданича дочисток поелативной дамяти Инспектор Тестирование прошло услешно ОК Такжа тот 50000,Ку | |

Рисунок 265 - Сообщение об окончании тестирования

Для просмотра отчета о проверке механизма очистки оперативной памяти нужно нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 3.11.3.5).

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

3.11.3.1.2 Проверка механизмов очистки устройств

Для запуска нужно отметить галочкой устройство в поле «Выбор устройств» рабочего окна инструмента и нажать кнопку «Вперед» (рис. 266).

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.

| p rear micherop | |
|---|--|
| оект Тестирование Отчет Помощь | |
| Іроверка механизма очистки оперативной памяти | |
| Проверить механизм очистки оперативной памяти | |
| Іроверка механизмов очистки ыбор устройств: | |
| С: Дата (b) F: G: NTFS FAT32 439.73 Гбайт <u>126.01 Мбайт</u> | |
| ОИСК ПО КЛЮЧЕВЫМ СЛОВАМ бор устройств: //////////////////////////////////// | |
| | |
| | |

Рисунок 266 – Проверка механизмов очистки устройств

Откроется новое окно с информацией о проекте и настройках проверки (рис. 267). 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».
| est - Инспектор | - | - 0 | 2 | > |
|---|---------|-----|-------|---|
| жт Тестирование Отчет Помощь | | | | |
| этовы начать | | | | |
| | | | | |
| аформация о проекте | | | | |
| ізвание: Test эганизация: Test | | | | |
| ть до проекта: C:/Users/Desktop/InspectorProject | | | | |
| | | | | |
| астройки проверки механизмов очистки | | | | |
| ібранные диски: | | | | |
| •D: | | | | |
| | | | | - |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| 2001 00101000 Echelen NO.2. Conv. anternet proping c.27.11.2016 on 01.06.2019 | < Hazar | | Renea | |

Рисунок 267 – Информация о проекте

В открывшемся окне (рис. 268) будет представлена информация о ходе выполнения проверки.

| Test - Инспектор | | - | | × |
|---|------------------|---------------|------------|-----|
| оект Тестирование Отчет Помощь | | | | |
| Код выполнения | | | | |
| | | | | |
| 100% | | | | |
| м волилитични. 05.04.2018 17.09:37 Запуск проверки механизма очистки жесткого диска D:. 05.04.2018 17:09:53 Завершение проверки механизма очистки жесткого диска. 05.04.2018 17:09:53 Формирование итогового отчета. | | | | |
| 05.04.2018 17:09:54 Формирование итогового отчета завершено. | | | | |
| Тестирование завершено успешно. Нажмите "Открыть отчет" для просмотра отчетов. | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Открыть отчет От | гкрыть катало | г с отчета | ами |
| делец лицензии: Echelon, № 2. Срок действия лицензии с 27.11.2016 до 01.06.2018 | | Готово | Отмен | на |

Рисунок 268 – Ход выполнения проверки

После завершения проверки для просмотра отчета необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 3.11.3.5).

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

3.11.3.1.3 Поиск по ключевым словам

Для запуска нужно отметить галочкой устройство в прямоугольном поле и нажать кнопку «Выбор ключевых слов и настройка поиска» (рис. 269).

| Test - Инспектор | | - | - 0 | 1 |
|----------------------------------|---|---------|-----|-------|
| оект Тестировани | не Отчет Помощь | | | |
| Проверка мех Проверить механи | канизма очистки оперативной памяти зм очистки оперативной памяти | | | |
| Проверка мех Зыбор устройств: | канизмов очистки | | | |
| С: NTFS 439.73 Гбайт | ☑ DATA (D-) □ F: □ G: FAT32 126.01 Мбайт | | | |
| | | | | |
| онск по клю | чевым словам | | | |
| > WDC WD500 | ЭААКХ-08U6AA0 (465.76 Гбайт) | | | |
| Generic Flash | Disk USB Device (7.50 Гбайт) ition table 1.00 Мбайт | | | |
| DATA, D: | , FAT32, 128.00 Мбайт | | | |
| □ F;, EXT4, - | 4.08 Гбайт 2.0 Гбайт | | | |
| G., EX12, | 3.2910801 | | | |
| | | | | |
| | | | | |
| | | | | |
| Выбор ключевых сло | в и настройка поиска | | | |
| | | | | |
| anoneu naueuzaa: Ech | No. 2 Cook вействия пинензии с 27.11.2016 во 01.06.2018 | < Haza | n B | nenen |
| аделец лицензии; со | Cion, Nº 2. CPUR Действия лицепзии с 27.11.2010 до 01.00.2010 | < Hd3d, | - 0 | перед |

Рисунок 269 – Поиск по ключевым словам

В открывшемся окне «Выбор ключевых слов и настройка поиска» необходимо указать ключевые слова для поиска остаточной информации (рис. 270).

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 ТХТ 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.

Примечание. 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».

| Test - Инспектор | | | | | | | | - |) |
|--|--|--|-----------------|-----------------------------|---------|----------|---|---|---|
| оект Тестирование Отчет Г | Іомощь | | | | | | | | |
| Проверка механизма о | чистки опера | тивной пам | ияти | | | | | | |
| Проверить механизм очистки опер | ативной памяти | | | | | | | | |
| Проверка механизмов | очистки | | | | | | | | |
| Зыбор устройств: | 强 Выбор ключев | ых слов и настроі | йка поиска | | | | × | | |
| 5 I. | Слова для поиска | | | | | | | | |
| □ C: ☑ DA' | | | | | | 0.6 | | | |
| NTFS F. 439.73 Гбайт 126.0 | Фраза | | | | | дооавить | | | |
| | | | Импортироват | ъ из словаря | | | | | |
| | password | | | | | | | | |
| | security | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| Поиск по ключевым си | | | | | | | | | |
| Поиск по ключевым си ыбор устройств: | Настройка поиска | | | | | | | | |
| Поиск по ключевым с ыбор устройств: > WDC WD5000AAKX-08U6A ↓ Generic Flash Disk USB Devi | Настройка поиска Колиполки | IITE-8. CP1251 | | | | • | | | |
| Douck по ключевым слыбор устройств: > WDC WD5000AAKX-08U6A Second Seco | Настройка поиска Кодировки | UTF-8, CP1251 | | | | - | | | |
| Image: Display the second s | Настройка поиска Кодировки Типы документов | UTF-8, CP1251 RAW | | | | • | | | |
| Object Romon < | Настройка поиска Кодировки Типы документов | UTF-8, CP1251 RAW истр | | | | • | | | |
| Oduck по ключевым сл befop устрайств: > WDC WD5000AAKX-08U6A Generic Flash Disk USB Devi UD SPartition table, 1.00 Ø DATA, Dc, FAT32, 128.00 F, EXT4, 4.08 Főaŭr G, EXT2, 3.29 Főaŭr | Настройка поиска Кодировки Типы документов Учитывать рег Определять пр | UTF-8, CP1251 RAW истр 7ги до файлов, сод | гержащих найден | ные ключевые слов | a | • | | | |
| ODMCK ПО КЛЮЧЕВЫМ СГ befop ycrpoicts: > WDC WD5000AAKX-08U6A Y Generic Flash Disk USB Devi Do DS Partition table, 1.00 Ø DATA, Di, FAT32, 128.00 F, EXT4, 4.08 főaŭr G, EXT2, 3.29 főaŭr | Настройка поиска Кодировки Типы документов Учитывать рег Определять п Потраничить о | UTF-8, CP1251 RAW истр ти до файлов, сод ибласть поиска | гержащих найден | ные ключевые слов | a | | | | |
| Image: Constraint of the second s | Настройка поиска Кодировки Типы документов Учитывать рег Определять пу Отранячить о Начало: | UTF-8, CP1251 RAW истр ити до файлов, сод бласть поиоса | гержащих найден | ные ключевые слов | a | • | | | |
| Touck по ключевым слыбор устройста: > > > OBC WD5000AAKX-08U6A * Generic Flash Disk USB Devi DOS Partition table, 1.0. > DOS Partition table, 1.0. > DATA, Dr., FAT32, 128.00 □ Fr, EXT4, 4.08 f6añr □ Gr, EXT2, 3.29 F6añr | Настройка поиска Кодировки Типы докунентов Учитывать рег Определять пу Ограничить о Начало: | UTF-8, CP1251 RAW истр илстр софайлов, сод бласть поиска | ержащих найден | ные ключевые слов | a | • | | | |
| Поиск по ключевыи с выбор устройств: → Шкороналакх-овиба → Пос мирс уклована и и и и и и и и и и и и и и и и и и | Настройка поиска Кодировки Типы докунентов Определать пре Определать пр Потранкить о Начало: | UTF-8, CP1251 RAW истр ти до файлов, сод бласть поиоса | гержащих найден | ные ключевые слов Конец: | a OK | Отмена | | | |

Рисунок 270 – Выбор ключевых слов и настройка поиска

Откроется новое окно с информацией о проекте и настройках проверки (рис. 271). В случае обнаружения ошибки в настройках проверки необходимо нажать кнопку «Назад» и скорректировать настройки. Для начала проверки нужно нажать кнопку «Вперед».

220 НПЭШ.00606-01 34

| | | _ | |
|---|---------|-------|-----|
| Ца, Test - Инспектор | - | | × |
| Проект Тестирование Отчет Помощь | | | |
| Готовы начать | | | |
| Информация о проекте | | | |
| Hassamue: Test Opramusaus: Test Nyrta zo nposta: C:/Jsers/Desktop/InspectorProject1 | | | |
| Поиск по ключевым словам | | | |
| Выбранные диски: | | | |
| •D | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Владелец лицензии: Echelon, № 2. Срок действия лицензии с 27.11.2016 до 01.06.2018 | < Назад | Впере | д > |

Рисунок 271 – Параметры тестирования

В открывшемся окне (рис. 272) будет представлена информация о ходе выполнения проверки.

| · · · · · · · · · · · · · · · · · · · | | |
|--|--------------------------------|---------|
| од выполнения | | |
| | | |
| 100% | | |
| г выполнения: | | |
| .04.2018 17:26:16 Запуск поиска по ключевым словам. | | |
| .04.2018 17:26:35 Завершение поиска по ключевым словам. | | |
| .04.2018 17:26:35 Формирование итогового отчета. | | |
| .04.2018 17:26:35 Формирование итогового отчета завершено. | | |
| | | |
| жмите "Открыть отчет" для просмотра отчетов. | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | OTKONITH OTHET OTKONITH KATADO | сотчета |

Рисунок 272 – Ход выполнения проверки

После завершения проверки для просмотра отчета нужно нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 3.11.3.5).

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

3.11.3.2. 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. 273).



Рисунок 273 – Рабочее окно инструмента «Контрольное суммирование»

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. 274).

| 1мя файла | | Путь | Алгоритм |
|-----------|--|----------------------------|----------------------------------|
| 🖕 C: | 1 🖬 C:/U | sers/Desktop/Tect/Tect.bmp | ГОСТ 34.11-94 (S-блок CryptoPro) |
| | 2 🗎 C:/U | sers/Desktop/Tect/Tect.txt | CRC-16 |
| | 3 G:/U | sers/Desktop/Tect | ГОСТ 34.11-2012 (512 бит) |
| | | | |
| | | | |
| | | | |
| | | | |
| | Выбрать вс | с Снять выделение | |
| | Выбрать вся — С выбране Алгоритя | е Снять выделение | ryptoPro) yстановит |

Рисунок 274 – Выбор объектов и алгоритмов для контрольного суммирования

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. 274), 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. 275). В случае обнаружения ошибки в настройках контрольного суммирования необходимо нажать кнопку «Назад» и скорректировать настройки. Для начала суммирования нужно нажать кнопку «Вперед».

223 НПЭШ.00606-01 34

| Test - Инспектор | - | |
|---|----------------------------------|-------|
| кт Тестирование Отчет Помощь | | |
| этовы начать | | |
| нформация о проекте | | |
| звание: Test ганизация: Test ть до проекта: C:/Users/Desktop/InspectorProject | | |
| астройки контрольного суммирования | | |
| Путь | Алгоритм | |
| :/Users/Desktop/Tect/Tect.bmp | ГОСТ 34.11-94 (S-блок CryptoPro) | |
| /Users/Desktop/Tect/Tect.txt | CRC-16 | |
| /Users/Desktop/Tect | ГОСТ 34.11-2012 (512 бит) | |
| | | |
| | | |
| | | |
| елец лицензии: Echelon, № 2. Срок действия лицензии с 27.11.2016 до | 1.06.2018 < Hasan | Впере |

Рисунок 275 – Информация о проекте

В открывшемся окне (рис. 276) будет представлена информация о ходе выполнения проверки.

| од выпол | нения | | | | | | | | | | | | | |
|-----------------|----------------------------|----------|-------------|-------------------------|---------------------|---------------|---------------|--------------|---------------|--------------|----------------|-------------|------------|-------|
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | 100% | | | | | | | |
| выполнения: | | | | | | | | | | | | | | |
| 3.04.2018 16:46 | 5:27 Запуск | контрол | ьного сумм | ирования, л | юкация: С:/ | Users/Deskt | р/Тест/Тест | bmp, алгори | гм: ГОСТ 34. | 11-94 (S-бло | ик CryptoPro). | | | |
| 04.2018 16:40 | 6:28 Заверц 6:28 Запуск | иение ко | нтрольного | суммирова ирования и | ния. юкация: С./ | l Icerc/Deckt | n/Tect/Tect | tyt anronumu | CRC-16 | | | | | |
| .04.2018 16:46 | 5:28 Завери | цение ко | нтрольного | суммирова | ния. | OSCIS, DESKO | ap, reci/reci | or on obium | rene for | | | | | |
| 3.04.2018 16:46 | 5:28 Запуск | контрол | ьного сумм | ирования, л | юкация: С:/ | Users/Deskt | р/Тест, алго | ритм: ГОСТ 3 | 4.11-2012 (51 | 2 бит). | | | | |
| .04.2018 16:46 | 5:28 Завери | цение ко | нтрольного | суммирова | ния. | | | | | | | | | |
| 8.04.2018 16:46 | 6:28 Форми с 20 Ф | рование | итогового с | тчета. | | | | | | | | | | |
| .04.2018 10:40 | о:29 Форми | рование | итогового с | тчета завер | шено. | | | | | | | | | |
| естирование | завершено | успешн | D. | | | | | | | | | | | |
| ажмите "Отк | рыть отчет | ″для про | смотра отч | тов. | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | _ | |
| | | | | | | | | | | OT | крыть отчет | открыть кат | anor, c o. | тчета |

Рисунок 276 – Ход выполнения контрольного суммирования

После завершения проверки для просмотра отчета нужно нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 3.11.3.5).

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

3.11.3.3. Системный аудит

Для запуска инструмента «Системный аудит» необходимо установить соответствующую галочку, нажав на пиктограмму или название инструмента, и нажать кнопку «Вперед» (рис. 246). В открывшемся окне будет показана информация о проекте (рис. 277). Для начала проверки устройств и программного обеспечения нужно нажать кнопку «Вперед».

| а техпрование Orver Tomoup TOEN HAVATD Формация о провекте жи: Ref 2000 2000 2000 2000 2000 2000 2000 200 | est - Ин | пектор | | | | | | - | |
|---|----------|--|--------------------|-----------------|-------|------|------|---|-------|
| Obbit HavaTb Формация о проекте Bit Markan Strep Bit Markan Strep Bit Markan Strep | кт Те | тирование Отчет | Помощь | | | | | | |
| формация о проекте зачазания Тей за за проекта: С:/Матя/Deaktop/InspectorProject1 роверить установленное программное обеспечение и устройства. | TOB | начать | | | | | | | |
| формация о проекте важи: те те за проекта: C:/Users/Desktop/InspectorProject] воерить установленное программное обеспечение и устройства. | | | | | | | | | |
| ite state: if the if t | форм | ация о проекте | | | | | | | |
| тан кали тра и протекта: С:/Users/Desktop/InspectorProject1 | звание | Test | | | | | | | |
| оверить установленное программное обеспечение и устройства. | ганиза | я: Test av. Tast C: Usars (Dackton) | TorpactorProject 1 | | | | | | |
| оверить установленное программное обеспечение и устройства. | ть до п | Jekra: C:/Users/Desktop/ | inspectorProject1 | | | | | | - |
| | nonon | | nornaumoo ofocn | | crno. | | | | |
| | ровер | тв установленное | программное обеспо | ечение и устрои | CIBA. | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | _ |
| | | | | | | | | | |
| | | | | | | | | | ſ |

Рисунок 277 – Информация о проекте

В открывшемся окне будет представлена информация о ходе выполнения проверки (рис. 278).

| 100% | |
|---|--|
| ог выполнения: | |
| 90.32.013 13:37:01 Запуск системного аудита. 99.03.2018 13:37:04 Завершение работы системного аудита. 99.03.2018 13:37:04 Формирование итогового отчета. 99.03.2018 13:37:05 Формирование итогового отчета завершено. Гестирование завеошено успешно. | |
| ижмите "Открыть отчет" для просмотра отчетов. | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Рисунок 278 – Ход выполнения аудита

После завершения проверки для просмотра отчета нужно нажать кнопку «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 3.11.3.5).

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

3.11.3.3.1 Тестирование антивируса

Для тестирования антивируса необходимо запустить утилиту «Тестирование антивируса» из подменю «Тестирование» (рис. 248).

Примечание. Функция тестирования антивируса не доступа в среде функционирования под управлением ОС специального назначения «Astra Linux Special Edition».

После запуска утилиты высветится сообщение о создании тестового файла (рис. 279). Необходимо нажать «ОК», чтобы открыть директорию с созданным тестовым файлом (рис. 279).

| 🕎. Тестирование антивируса | × |
|--|----|
| EICAR тестовый файл 'C:/Users/Olga/Desktop/InspectorProject/EICAR.com' сформирован. После проверки с помощью антивируса удалите этот файл. Нажмите "ОК", чтобы открыть директорию с созданным файлом. | |
| | DK |

Рисунок 279 – Тестирование антивируса

После завершения проверки необходимо удалить тестовый файл, используя антивирусное ПО.

3.11.3.4. Проверка прав доступа

Для запуска инструмента «Проверка прав доступа» необходимо установить соответствующую галочку нажатием на пиктограмму или название инструмента, и нажать «Вперед» (рис. 246). Откроется рабочее окно инструмента «Проверка прав доступа» компонента «Инспектор» (рис. 280).

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.



Рисунок 280 – Рабочее окно

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» (рис. 281). Максимально можно создать двадцать уровней (сессий).

Примечание. Изменить уровни доступа необходимо до выбора проверяемых объектов.

| Номер сессии | Название сессии | | | |
|------------------------|-----------------|--|--|--|
|) | Несекретная | | | |
| 1 | Секретная | | | |
| 2 Совершенно секретная | | | | |
| | | | | |

Рисунок 281 – Окно «Настройка уровней доступа»

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. 282).

| MR | Имя | Уровень доступа | Пользователи | |
|-----------------------------|-------------------------|------------------|----------------------------|------|
| 🟪 C: | 1 C:/Users/Desktop/Tect | 0: Несекретная 1 | Администратор | |
| | | 2 | Гость | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Добавить общую папку | | | | |
| дель доступа | | | | |
| мя | | Ч 3 | В Выбрать все Снять выде | лени |
| ' 🗌 📙 С:/Users/Desktop/Тест | | + + | С выбранными | |
| 🔲 🖬 Тест.bmp | | + + | 🕂 Чтение Разрешить Запре | тить |
| Tecr.bt | | + + | + Запись Разрешить Запре | тить |
| | | | Выполнение Разрешить Запре | тить |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Рисунок 282 - Список каталогов в перечне проверяемых объектов

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. 283).

Чтобы добавить пользователя из домена, необходимо нажать правой кнопкой мыши в области списка пользователей, вызвав контекстное меню, и выбрать пункт «Добавить» (рис. 283). В открывшемся окне (рис. 284) 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. 284).

| | Ина | | VDORENE ADCTURE | | | Пользователи | | |
|-----------------------------|-----------------|----------|-----------------|---|---------------|------------------|-------------|----|
| " C: | 1 C:/Users/Desk | top/Tect | 0: Несекретная | 1 | Администратор | пользователи | | |
| | | | | 2 | - 0CTD | | | |
| | | | | 2 | 0018 | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | Добавить | | | |
| | | | | | Уладить | | | |
| | | | | | лалить | ŭ | 00 | |
| Добавить общую папку | | | | | ыз загрузить | пользователеи из | | |
| одель доступа | | | | | | | | |
| fms | | | ч | 3 | в Выбр | ать все Сн | ять выделен | ие |
| 🛩 🔲 📙 C:/Users/Desktop/Tecт | | | + | + | С выбра | нными | | |
| 🔲 📓 Тест.bmp | | | + | + | Чтение | Разрешить | Запретить | ь |
| Tecr.txt | | | + | + | 🕂 Запись | Разрешить | Запретить | ь |
| | | | | | Выполн | ение Разрешить | Запретить | ь |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Рисунок 283 – Обновление списка пользователей

| 强 Добавление пользователя | > | × |
|--------------------------------------|-----------------|---|
| Имя пользователя: | | |
| | | |
| Домен (оставьте пустым для локальных | пользователей): | |
| | | - |
| | ОК Отмена | |

Рисунок 284 – Добавление пользователя

3.11.3.4.1 Построение модели прав доступа

Построение модели прав доступа происходит путем редактирования в перечне проверяемых объектов прав доступа пользователей к файлам и каталогам автоматизированной системы. 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.

3.11.3.4.2 Тестирование прав доступа

Для тестирования прав доступа после построения модели прав доступа необходимо нажать кнопку «Вперед» (рис. 283).

Откроется новое окно с информацией о настройках проекта (рис. 285). 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».

230 НПЭШ.00606-01 34

| 🔀 Test - Инспектор | _ | | × |
|--|---------|-------|------|
| Троект Тестирование Отчет Помощь | | | |
| Готовы начать | | | |
| | | | _ |
| Информация о проекте | | | |
| Название: Test Организация: Test | | | |
| Путь до проекта: C:/Users/Desktop/InspectorProject1 | | | _ |
| Провелить систему управления лоступом | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Владелец лицензии: Echelon, № 2. Срок действия лицензии с 27.11.2016 до 01.06.2018 | < Назал | Впере | -n > |

Рисунок 285 – Информация о проекте

В открывшемся окне будет представлена информация о ходе выполнения проверки (рис. 286).

| Теst - Инспектор | | - | | × |
|--|-----------------|--------------|--------|--------|
| хект Тестирование Отчет Помощь | | | | |
| Сод выполнения | | | | |
| | | | | |
| 100% | | | | |
| ог выполнения: | | | | |
| 29.03.2018 17:27:18 Формирование итогового отчета. 29.03.2018 17:27:19 Формирование итогового отчета завершено. | | | | |
| Гестирование завершено успешно. Научните "Плупыть отнет" але просмотра отнетов | | | | |
| annin origina original function original | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | OTVOLITE OTVICT | | | - |
| | Unpbille Unque | ing wat drie | Conven | un für |
| делец лицензии: Echelon, № 2. Срок действия лицензии с 27.11.2016 до 01.06.2018 | r | отово | Отме | на |

Рисунок 286 – Ход выполнения проверки

После завершения тестирования необходимо запустить утилиту «Проверка прав доступа» для проверки прав доступа пользователей в различных сессиях к выбранным каталогам и файлам.

Для запуска утилиты необходимо выбрать в меню «Тестирование» утилиту «Проверка прав доступа» (рис. 287).

| 🖪 Test | - Инспектор | | | | _ | | × |
|-------------------------|---------------------|--|-----------------|---------------------|-----------|------------|-----|
| Проект | Тестирование | Отчет Помощь | | | | | |
| Von | Проверка г | прав доступа | Ctrl+T | 1 | | | |
| ход | 🥟 Проверка м | механизма очистки памяти | Ctrl+M | | | | |
| | Тестирован | ние антивируса | Ctrl+Y | | | | |
| | | | | 100% | | | |
| Лог вы | полнения: | | | | | | |
| 29.03. Тести Нажи | 2018 17:27:19 Форн | мирование итогового отчета з жо успешно. кет ² для просмотра отчетов. | авершено. | | | | |
| | | | | Открыть отчет Откры | ь каталог | г с отчета | ыми |
| Владеле | ц лицензии: Echelon | л, № 2. Срок действия лицензии | с 27.11.2016 до | 01.06.2018 | тово | Отмен | la |

Рисунок 287 – Подменю «Тестирование»

В открывшемся окне необходимо указать текущий уровень сессии (рис. 288).

| | 100% | | | |
|--|---|--------------------|------------|----------|
| ог выполнения: 29.03.2018 17:27:18 Формирование итогового | отчета. | | | |
| 29.03.2018 17:27:19 Формирование итогового | отчета завершено. | | | |
| естирование завершено успешно. | | | | |
| | Выберите уровень сессии: Несекретная • Очистить предыдущие результаты: | | | |
| | | Открыть отчет Откр | ыть катало | г с отче |

Рисунок 288 – Выбор уровня сессии и пользователя для проведения проверки

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. 289).

232 НПЭШ.00606-01 34

| | | | _ |
|---|---|------|---|
| | 100% | | |
| и выполнетии. 19.03.2018 17:27:18 Формирование итогового отчет 19.03.2018 17:27:19 Формирование итогового отчет | га. га завершено. | | |
| Гестирование завершено успешно. Нажмите "Открыть отчет" для просмотра отчетов | Инспектор - проверка прав доступа Х | | |
| | Инспектор - проверка прав доступа Выберите уровень сессии: Несекретная • | | |
| | ☐ о вылистрицацијана разулотата ✓ Проверить для пользователя "Гость" Паколь | | |
| | Проверить для пользователя "Администратор" | | |
| | Проверить доступ | | |
| | | | |
| | | | |

Рисунок 289 – Выбор пользователей для проверки прав доступа в несекретной сессии

Тестирования прав доступа в режимах «Секретно» и «Совершенно Секретно» проводится только для авторизированного пользователя.

После проведения тестирования появится соответствующее сообщение (рис. 290).

| 🖅 Инсп | ектор - проверка прав доступа | × |
|--------|-------------------------------|------|
| i | Тестирование прав прошло успе | шно. |
| | OK | |

Рисунок 290 – Сообщение

После завершения проверки для просмотра отчета необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (подробнее см. пп. 3.11.3.5).

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

3.11.3.4.3 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. 246). Откроется рабочее окно инструмента «Проверка прав доступа» компонента «Инспектор» (рис. 280).

Примечание. Функция тестирования прав доступа к общей папке не доступа, 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. 291).

| 🔀 Test - Инспектор | | | | | | - | | > |
|---|--------------------------------------|--|---|---------------|--|---------|-------------------------------------|---|
| проект Тестирование Отчет Помощь Проверка прав доступа | | | | | | | | |
| Имя > ≝ C: | Имя Переместите файлы и (или) кат | Уровень доступа илоги в эту область | 1 | User User2 | Пользовате | ли | | |
| Добевить общую папку Модель доступа Ичя | | ч | 3 | в | Выбрать все | Снять | » Выделение | e |
| | | | | | Чтение Разреши Запись Разреши Выполнение Разреши | пъ . | Запретить Запретить Запретить | |
| | | | | | Настройка уровн | ей дост | ryna | |

Рисунок 291 – Рабочее окно

В открывшемся окне (рис. 292) нужно указать путь и нажать кнопку «ОК».



Рисунок 292 – Добавление общей папки

Если появится окно авторизации, то необходимо ввести логин и пароль пользователя (рис. 293).

| Безопасность Windows | | | | | | |
|--|--------|--|--|--|--|--|
| Ввод сетевых учетных данных | | | | | | |
| Введите свои учетные данные для подключения к 192.168.5.219 | | | | | | |
| user1 | | | | | | |
| •••• | | | | | | |
| Запомнить учетные даннь | ble | | | | | |
| ОК | Отмена | | | | | |

Рисунок 293 – Ввод сетевых учетных данных

Для запуска тестирования нужно нажать кнопку «Вперед». (рис. 294).

| Test - Инспектор | | | | | | | | | - | . 🗆 |
|---|------|------------------------|----------------|----|---|-----|------------|------------|--------|-------------|
| ект Тестирование Отчет Помощь | | | | | | | | | | |
| роверка прав доступа | | | | | | | | | | |
| Мя | 1 | Имя | Уровень достуг | па | Γ | | п | ользовате | ли | |
| 🟪 G | 1 | L \\192.168.5.134\Test | 0: Несекретная | • | 1 | Use | r | | | |
| | | | | | 2 | Use | r2 | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| Добавить общую папку | | | | | | | | | | |
| юдель доступа | | | | | | | | | | |
| бия | | | ч | | 3 | E | Выбрать | BCE | Снят | ь выделение |
| ✓ ∐ ↓ \\192.168.5.134\Test | | | + | | t | 1 | С выбранны | 454 | | |
| | | | | | t | 1 | Чтение | Разреши | ть | Запретить |
| | | | | | t | 1 | Запись | Разреши | пь | Запретить |
| L Est.bmp | | | | | t | 1 | Выполнение | Разреши | пь | Запретить |
| | | | | | + | 1 | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | Настр | ойка уровн | ей дос | тупа |
| | | | | | | | | | | |
| аелен лицензии: Echelon, Nº 2, Слок действия лицензии с 2 | 27.1 | .2016 до 01.06.2018 | | | | | | < | Назал | Впер |

Рисунок 294 – Проверка прав доступа

В открывшемся окне будет представлена информация о проекте. Для начала тестирования необходимо нажать кнопку «Вперед» (рис. 295).

235 НПЭШ.00606-01 34

| т Тестирование Отчет Помощь | | |
|---|------|---|
| товы начать | | |
| формация о проекте | | _ |
| | | |
| anvia. rest anviauvis: Test | | |
| ъ до проекта: C:/Users/Desktop/InspectorProject | | |
| | | |
| оверить систему управления доступом. | | |
| | | _ |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | _ |
| | | |
| | | - |

Рисунок 295 – Информация о проекте

После завершения тестирования необходимо запустить утилиту «Проверка прав доступа» для проверки прав доступа пользователей в различных сессиях к выбранным каталогам и файлам.

Для запуска утилиты необходимо выбрать в подменю «Тестирование» параметр «Проверка прав доступа» (рис. 296).

| 🖪 Test | Инспектор | | | - | | × |
|-------------------------|---|----------------|---------------------|-----------|------------|-----|
| Проект | Тестирование Отчет Помощь | | | | | |
| Хол | Проверка прав доступа | Ctrl+T | | | | |
| | 🥟 Проверка механизма очистки памяти | Ctrl+M | | | | |
| | Тестирование антивируса | Ctrl+Y | | | | |
| | | | 100% | | | |
| Лог вы | полнения: | | | | | |
| 04.04. Тести Нажа | сию г нэжи. Формирование итогового отчета з рование завершено успешно. ите "Опкрыть отчет" для просмотра отчетов. | авершено. | | | | |
| | | | Открыть отчет Откры | гь катало | г с отчета | ами |
| Владеле | ц лицензии: Echelon, № 2. Срок действия лицензии | с 27.11.2016 д | o 01.06.2018 | T080 | Отмен | на |

Рисунок 296 – Запуск утилиты

В открывшемся окне нужно указать уровень сессии, пользователей, для которых необходимо провести проверку и нажать кнопку «Проверить доступ» (рис. 297).

236 НПЭШ.00606-01 34

| | 100% | | |
|--|---|------|--|
| ог выполнения: 24.04.2018.11:39:01.Формирование итогового | 111073 | | |
| 24.04.2018 11:39:02 Формирование итогового | 🔹 Инспектор - проверка прав доступа 🛛 🗙 | | |
| Тестирование завершено успешно. Нажмите "Открыть отчет" для просмотра отч | Инспектор - проверка прав доступа Выберите уровењ сесон: Несекретная • Очистить предыдущие результаты Проверить для пользователя "User2" | | |
| | Пароль Проверить для пользователя "User" Пароль | | |
| | Проверить доступ | | |
| | | | |

Рисунок 297 – Настройка тестирования прав доступа

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 «OK».

После успешной проверки прав доступа появится соответствующее сообщение (рис. 290).

После завершения проверки для просмотра отчета необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (рис. 296) (подробнее см. пп. 3.11.3.5).

3.11.3.4.4 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. 246). Откроется рабочее окно инструмента «Проверка прав доступа» компонента «Инспектор» (рис. 280).

Примечание. Функция тестирования прав доступа с установленным СЗИ Dallas Lock не доступа 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. 298).

| ₽ B | 1 - Инспекто | p | = 🗆 X |
|---|------------------------------|-------------------------|--|
| Проект Тестирование Отчет Помощь Проверка прав доступа | | | |
| Имя | А Имя | Уровень доступа | Пользователи |
| ↓ C: ↓ SRecycle.Bin ↓ 1 inspector_win ↓ Inspector_win.zip ↓ ↓ ↓ | 1 C/1/1.bt | 0: Hecexpetrias 1 user1 | |
| Модель доступа | | | |
| //ws | | + + + | Выбрать вой Онять выделение С выбраньям Запретить Запись Разрешить Запись Разрешить Выполнение Разрешить Запретить Запретить Настройка уровней доступа |
| Владелец лицензии: Echelon, № 2. Срок действия лицензи | а с 27.11.2016 до 01.06.2018 | | < Назад Вперед > |

Рисунок 298 – Запуск проверки прав доступа

В окне с информацией о тестировании нужно нажать кнопку «Вперед» (рис. 299).

| 强 1 - Инспектор | _ 0 X |
|---|-----------------|
| Проект Тестирование Отчет Помощь | |
| Готовы начать | |
| Информация о проекте | |
| Haseavue: 1 Opravinauus: 1 Nyrs. Lo nopeara: C.;Users/jechelon/Desktop/InspectorProject | |
| Проверить систему управления доступом. | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| Владелец лицензии: Echelon, № 2. Срок действия лицензии с 27.11.2016 до 01.06.2018 | <Назад Вперед > |

Рисунок 299 – Информация о проекте

После завершения тестирования необходимо запустить утилиту «Проверка прав доступа» для проверки прав доступа пользователей в различных сессиях к выбранным каталогам и файлам.

Для запуска утилиты необходимо выбрать в подменю «Тестирование» параметр «Проверка прав доступа» (рис. 300).

| <u>B</u> | | | | | | 1 - Инспектор | | x |
|-------------------|------------------------|---|--------------------------------------|--|--------------------------------|--------------------------------|--------------|-----|
| Прое | ст | Тестиров | ние Отче | т Помощь | | | | |
| Xo | л | Про | ерка прав д | юступа | Ctrl+T | | | |
| | - | 🥔 Про | ерка очист | ки памяти | Ctrl+M | | | |
| | | Тест | рование ан | тивируса | Ctrl+Y | | | |
| | | | | | | 100% | | |
| Лог | вып | олнения: | | | | | | |
| 04. 04. Teo | .04.2 .04.2 :тир | 018 09:11:4 018 09:11:4 ювание за | 1 Формиро 1 Формиро ершено усі | вание итогово вание итогово пешно. | ого отчета. ого отчета завн | ршено. | | |
| Ha | жмі | ите "Открь | ть отчет" д/ | 1я просмотра | отчетов. | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | Открыть отчет Открыть ката | лог с отчета | эми |
| Владе | лец | лицензии: | Echelon, № 2 | . Срок действ | ия лицензии с 2 | 7.11.2016 до 01.06.2018 Готово | Отмен | -ta |

Рисунок 300 – Запуск утилиты

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. 301).

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).

239 НПЭШ.00606-01 34

| | 1 - Инспектор | |
|---|---|---|
| оект Тестирование Отчет Помощь Ход выполнения | | |
| | 100% | |
| ог выполнения: | | |
| 04.04.2018 09:11:41 Формирование итогового 04.04.2018 09:11:41 Формирование итогового Тестирование завершено успешно. | отчета. отчета завершено. Инспектор – проверка прав достипа X | |
| | Инспектор - проверка прав доступа | |
| | | Открыть отчет Открыть каталог с отчетам |

Рисунок 301 – Настройка тестирования прав доступа

После успешной проверки прав доступа появится соответствующее сообщение (рис. 290).

После завершения проверки для просмотра отчета необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (рис. 300).

3.11.3.4.5 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. 246). Откроется рабочее окно инструмента «Проверка прав доступа» компонента «Инспектор» (рис. 280).

Примечание. Функция тестирования прав доступа с установленным СЗИ Secret Net не доступа 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. 302).

240 НПЭШ.00606-01 34

| | Имя | Уровень доступа | | | Пользова | тели |
|--|-------------|--|---|------------------------------|---|--|
| · 🕰 C: | C:/data | 0: Несекретная | 1 | user0 | | |
| | | | 2 | user1 | | |
| | | | 3 | user2 | | |
| добавить общую папку | | | | | | |
| одель доступа | | | | | | |
| Иня | | ч з | | в ^ | Выбрать все | Снять выделени |
| /like / C:/data | | ч : | _ | 8 ^ + | Выбрать все С выбранными | Снять выделении |
| /hea //ea // []]] C:/data // []]]] S | | 4 5 + 4 + 4 | | ₽ ^ + + | Выбрать все С выбранными Чтение Разра | Снять выделения вшить Запретить |
| //ea | | 4 5 + 4 + 4 + 4 | - | 8 ^ + + + | Выбрать все С выбранными Чтение Разре Запись Разре | Снять выделения ешить Запретить ешить Запретить |
| Alee Alee Cr/data Cr/data S S S S S S S S S S S S S | | 4 5 + 4 + 4 | | B ▲ + + = | Выбрать все С выбранными Чтение Разре Запись Разре Выполнение Разре | Снять выделения ашить Запретить ашить Запретить ашить Запретить |
| Alea Alea C/data C/data S S S S S S S S S S S S S | | 4 5 + 4 + 4 + 4 + 4 + 4 | - | 8 ▲ + + + = + | Выбрать все С выбранными Чтение Разре Запись Разре Выполнение Разре | Снять выделения ашить Запретить ашить Запретить ашить Запретить |
| Area Area Area Area Area Area Area Area | | 4 5 + 4 + 4 - 4 + 4 - 7 + 4 - 7 | - | B + + = = + = . | Выбрать все С выбранныни Чтение Разри Запись Разри Выполнение Разри | Снять выделения ашить Запретить ашить Запретить ашить Запретить |
| Area Ar | | 4 4 + 4 + 4 + 4 | | B + + = = + | Выбрать все С выбранныни Чтение Разри Запись Разри Выполнение Разри | Снять выделения ашить Запретить ашить Запретить ашить Запретить |

Рисунок 302 – Запуск проверки прав доступа

В окне с информацией о тестировании необходимо нажать кнопку «Вперед» (рис. 303).

| - Инспектор | |
|--|--|
| рект Тестирование Отчет Помощь | |
| ОТОРЫ НАЧАТЬ | |
| | |
| информация о проекте | |
| Название: 1 | |
| opravnisauvis: 1 brat. au gnoesta: C-il kers/echelon/Deskton/InspectorProject | |
| уть допроскта: слова усставлярская порес | |
| Поверить систему управления доступом. | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Рисунок 303 – Информация о проекте

После завершения тестирования необходимо запустить утилиту «Проверка прав доступа» для проверки прав доступа пользователей в различных сессиях к выбранным каталогам и файлам.

Для запуска утилиты 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. 304).

Примечание. В данном случае выбор сессии для проверки не требуется.

| 🖫 1- Инспектор Проект Тестирование Отчет Помощь Ход выполнения | | |
|--|--|--|
| | 100% | |
| Лог выполнения: | | |
| 0.3.4.2.02.1/48:48 чормирование итотового от 0.3.04.2.012 1/48:49 чормирование итотового от Тестирование завершено успешно. Нажмите "Открыть отчет" для просмотра отчет отчет" для просмотра отчет | Инспектор - проверка прав доступа: Searet Net Верон: 8.2 Подостетена анадатного управления доступон: включена Подоістена нандатного управления доступон: включена Контроль потоков: включен Текуций уровен: всекие: 0. Неконфиденциально Очистить предыдущие результаты Очистить предыдущие результаты Очистить предыдущие результаты Очистить предыдущие результаты Проверить для пользователя "user0" Пароль ••••• Проверить для пользователя "user1" Пароль ••••• Проверить для пользователя "user2" Пароль ••••• | |
| | | Открыть отчет Открыть каталог с отчетами |
| Владелец лицензии: Версия для тестирования (несерти | фицированная), № Срок действия лицензии с 02.04.2018 до 02.10.2018 | Готово Отмена |

Рисунок 304 – Настройка тестирования прав доступа

После успешной проверки прав доступа появится соответствующее сообщение (рис. 290). После завершения проверки для просмотра отчета необходимо нажать «Открыть отчет» или «Открыть каталог с отчетами» (рис. 304).

3.11.3.5. Генерация отчетов

Итоговый отчет строится автоматически. Сгенерированный отчет разделен на вкладки с результатами работы каждого задействованного инструмента (рис. 305).

| Отчет работы Инспектора от 06.04.2018 12:18:30 | | | | | | | | | | |
|---|--|---|-----------------|-----------------------|-------------------|--|--|--|--|--|
| Название проекта: Test Организация: Test | B Название проекта: Test | | | | | | | | | |
| Проверка механизмов очистки | Поиск по ключевым словам | Контрольное суммирование | Системный аудит | Проверка прав доступа | Журнал выполнения | | | | | |
| Проверка механизмов очистки Информация о результатах поиска остаточной информации. Тоиск последовательности до и после удаления файлов производится по всему разделу диска. | | | | | | | | | | |
| Вазовая последователь | HOCTS: HOLTATORSA2A8AAE6390EC HC7T1BCA1E8789EB16CDB8 749DA7693BCCF3FC3E4FD38 749DA7693BCCF3FC3E4FD38 749DA7693BCCF3FC3E4FD38 749DA7693BCCF3FC79531304F530 328C2B8304F93649725795 826C2108034401064719DA7597 FF83EC70AC30534F53304 80A0E83A5F5715894E53D43 471394617392063278F220952 1643004028060786279622 5926250470306398E54 HC7394E72FC3FC3052865 467394E72FC3FC757659E5765 668471 до удаления | 1A729CA322589E238 61A064110701CC731 4691Ac681937E4896E 87A1280A420C77701F 465591c6500741047 635591c6500741047 63550738124762896619 580A38ERA87E1R83E 6270B74501326471CC 3962A592EA8A5620B 47E5922E487671E07 798626892EFA8A5E0B 17E5922E487671E07 798626892EFA8A5E0B 17E5922487671E07 24590284676139666 425014056318C671 | Поиск после уда | пения | | | | | | |
| Адрес : смещение | Количеств | о Адрес : с | мещение | Количество | Статус | | | | | |
| 2084352:0 | 1 | 2084 | 352:0 | 1 | Tect monster | | | | | |

Рисунок 305 – Общий вид отчета

3.11.3.5.1 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. 305).

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. 305).

Во вкладке «Оперативная память» содержится итоговый статус проверки механизмов очистки оперативной памяти (рис. 306).

| Отчет работы Ин | Отчет работы Инспектора от 06.04.2018 12:18:30 | | | | | | | | |
|--|---|--|---|------------------------------|-------------------|--|--|--|--|
| Название проекта: Test Организация: Test | | | | | | | | | |
| Проверка механизмов очистки | Поиск по ключевым словам | Контрольное суммирование | Системный аудит | Проверка прав доступа | Журнал выполнения | | | | |
| Проверка механия Информация о результатах по Поиск последовательности до | вмов очистки иска остаточной информации и после удаления файлов пр | 1. оизводится по всему разделу | л диска. | | | | | | |
| Диск D: Оперативная памя | ть | | | | | | | | |
| Тест пройден успешно. | | | | | | | | | |
| Вланиканан Вланиканананананананананананананананананан | аделец лицензии: Echelon № спектор Версия: 2.3 Програм нтакты технической поддерж | Срок действия лицензии с мное обеспечение © АО "НПС ки продукта: <u>support.sca@cn</u> | 27.11.2016 до 01.06 О "Эшелон" <u>http://w</u> <u>po.ru</u> | 5.2018 www.npo-echelon.ru | | | | | |

Рисунок 306 – Отчет проверки механизма 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. 307).

| Отчет работы Ин | спектора от Об | 5.04.2018 12: | 18:30 | | |
|---|--------------------------|--------------------------|-------------------------|---------------------|--------------------------------|
| | | | | | |
| Организация: Test | | | | | |
| Проверка механизмов очистки | Поиск по ключевым словам | Контрольное суммировани | те Системный аудит Про | оверка прав доступа | Журнал выполнения |
| Параметры поиска | | | | | |
| Выбранные диски/устройств | a: | | | | |
| • D: | | | | | |
| Слова для поиска: | | | | | |
| passwordsecurity | | | | | |
| Кодировки: | | | | | |
| CP1251 UTF-8 | | | | | |
| Поиск с учетом регистра: да | | | | | |
| Результаты поиска | | | | | |
| № Найденное ключевое слово | Кодировка Тип | Локация | Смещение относительно р | оаздела Смещение | относительно физического диска |
| 1 password | СР1251 RAW D:/Новый | і текстовый документ.txt | 2083840 | 3132416 | |
| 2 security | СР1251 RAW D:/Новый | і текстовый документ.txt | 2083850 | 3132426 | |
| 3 security | CP1251 RAW D: | | 33706584 | 34755160 | |
| 4 security | CP1251 RAW D: | | 33707913 | 34756489 | |
| 5 security | CP1251 RAW D: | | 33708177 | 34756753 | |
| 6 security | CP1251 RAW D: | | 66614911 | 67663487 | |
| 7 security | CP1251 RAW D: | | 66616402 | 67664978 | |
| 8 security | CP1251 RAW D: | | 66617165 | 67665741 | |
| 9 security | CP1251 RAW D: | | 66617928 | 67666504 | |
| 10 security | CP1251 RAW D: | | 66618690 | 67667266 | |
| 11 security | CP1251 RAW D: | | 66619455 | 67668031 | |
| 12 security | CP1251 RAW D: | | 66619992 | 67668568 | |
| 13 security | CP1251 RAW D: | | 66620769 | 67669345 | |
| 14 security | CP1251 RAW D: | | 66621779 | 67670355 | |
| | | | | | |

Рисунок 307 – Отчет поиска по ключевым словам

3.11.3.5.2 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. 308).

| 07 | чет работы Инспе | ктора от | т 06.04.20 | 18 12:18 | 30 | | | | |
|-----------|---|--|---|--|--|-------------------|------------------|--|----------------|
| Ŀ | Название проекта: Test Организация: Test | | | | | | | | |
| Пр | оверка механизмов очистки Поиск п | то ключевым сло | овам Контрольное | суммирование | Системный аудит | Проверк | а прав доступа | Журнал выполнения | |
| Кс Инс | онтрольное суммиров рормация о контрольных суммах вы Имя каталога или файла | ание бранных объен Размер, байт | стов. Время создания | Время изменени | я Алгорит | м | | Контрольная сумма | |
| 1 | C:\Users\Olga\Desktop\Tect | - | 29-03-2018 13:39:55 | 04-04-2018 10:28:30 | FOCT 34.11-94 CryptoPr | (S-блок р) | bdf46d8761803 | 81fd77bd64824a193f0 b80776ea3c9d343c93 | fc76c8f7d76c00 |
| 2 | Тест.bmp | 0 | 29-03-2018 13:40:15 | 29-03-2018 13:40:15 | FOCT 34.11-94 CryptoPr | (S-блок c) | 981e5f3ca30c8 | 41487830f84fb433e13 3584ac483234cd656c0 | ac1101569b9c1 |
| 3 | Tест.txt | 0 | 29-03-2018 13:40:07 | 29-03-2018 13:40:07 | FOCT 34.11-94 CryptoPr | (S-блок b) | 981e5f3ca30c8 | 41487830f84fb433e13 3584ac483234cd656c0 | ac1101569b9c1 |
| 4 | C:\Users\Olga\Desktop\Tect\Tect.txl | 0 | 29-03-2018 13:40:07 | 29-03-2018 13:40:07 | CRC-8 | | | ff | |
| | Владелец л Инспектор Инспектор Контакты те | ицензии: Echel Версия: 2.3 Пр ехнической под | on №2. Срок дейст ограммное обеспеч цдержки продукта: | вия лицензии с 27 ение © АО "НПО " support.sca@cnpo. | .11.2016 до 01.06. Эшелон" <u>http://wv</u> ru | 2018 /w.npo-ec | <u>chelon.ru</u> | | |

Рисунок 308 – Отчет о контрольном суммировании

3.11.3.5.3 Отчет инструмента «Системный аудит»

Отчет оформлен в виде таблиц и состоит из двух вкладок «Программная часть» и «Аппаратная часть» (рис. 309). Во вкладке «Программная часть» перечислены версия операционной системы, информация об установленных программах и пакетах, лицензионные номера установленных продуктов (рис. 309).

| тчет ра | боты Иі | нспектора от О | 5.04.2018 12:18 | 8:30 | | |
|--|--|---|---|--|---|--|
| Название Организа | е проекта: Test ация: Test | | | | | |
| роверка механ | измов очистки | Поиск по ключевым словам | Контрольное суммирование | Системный аудит | Проверка прав доступа | Журнал выполнения |
| истемны | ій аудит | | | | | |
| нформация о е тройств, сетее ючей. | зерсии операці зых адаптеров | ионной системы, перечень ус , принтеров, устройств ввода | тановленного программного (информации (клавиатура, мі | обеспечения, парам ышь), перечень под | етры мониторов, централ ключенных USB-накопит | ьного процессора, дисковых елей, перечень лицензионных |
| Программная ч | асть Аппара | тная часть | | | | |
| Прогр Информация о | аммы 6 установленн | | | | | |
| Nº 🔶 | | ых програннах или накстах. | | | | |
| 1 | | вх програнных или пакетах. | мя | | Версия | Дата установки |
| | 64 Bit HP C | IO Components Installer | мя | 8.2.4 | Версия | Дата установки 15.05.2017 |
| 2 | 7-Zip 16.04 | IO Components Installer (x64) | мя | 8.2.4 16.04 | Версия | Дата установки 15.05.2017 12.01.2018 |
| 3 | 7-Zip 16.04 Adobe Acrol | IO Components Installer (x64) bat DC | мя | 8.2.4 16.04 15.020 | Версия .20042 | Дата установки 15.05.2017 12.01.2018 01.02.2018 |
| 2 3 4 | 7-Zip 16.04 Adobe Acrol | IO Components Installer (X64) bat DC bat Reader DC - Russian | мя | 8.2.4 16.04 15.020 18.011 | Версия .20042 .20038 | Дата установки 15.05.2017 12.01.2018 01.02.2018 01.03.2018 |
| 2 3 4 5 | 64 Bit HP Cl 7-Zlp 16.04 Adobe Acrol Adobe Acrol Adobe Refre | IO Components Installer (X64) Dat DC Dat Reader DC - Russian ISM Manager | мя | 8.2.4 16.04 15.020 18.011 1.8.0 | Версия .20042 .20038 | Дата установки 15.05.2017 12.01.2018 01.02.2018 01.03.2018 |
| 2 3 4 5 6 | 64 Bit HP C 7-ZIp 16.04 Adobe Acrol Adobe Acrol Adobe Refre Backup and | IO Components Installer (x64) bat DC bat Reader DC - Russian ssM Manager Sync from Google | мя | 8.2.4 16.04 15.02(18.01) 1.8.0 3.40.8 | Версия .20042 .20038 921.5350 | Дата установки 15.05.2017 12.01.2018 01.02.2018 01.03.2018 01.03.2018 25.03.2018 |
| 2 3 4 5 6 7 | 64 Bit HP C 7-Zlp 16.04 Adobe Acrol Adobe Acrol Adobe Refre Backup and CDBurnerXF | IO Components Installer (X64) baat Reader DC - Russian shi Manager Sync from Google | мя | 8.2.4 16.04 15.02(18.01) 1.8.0 3.40.8 4.5.7. | Версия .20042 .20038 921.5350 6623 | Дата установки 15.05.2017 12.01.2018 01.02.2018 01.03.2018 01.03.2018 25.03.2018 11.09.2017 |
| 2 3 4 5 6 7 8 | 64 Bit HP C 7-Zip 16.04 Adobe Acrol Adobe Acrol Adobe Refre Backup and CDBurnerXF CodeMeter | IO Components Installer (x64) Dat DC Dat Reader DC - Russian Ish Manager Sync from Google O Runtime Kit v6.50b | мя | 8.2.4 16.04 15.02(18.01) 1.8.0 3.40.8 4.5.7.4 6.50.2 | Версия .20042 .20038 921.5350 6623 651.502 | Дата установки 15.05.2017 12.01.2018 01.02.2018 01.03.2018 25.03.2018 25.03.2018 11.09.2017 27.11.2017 |
| 2 3 4 5 6 7 8 9 | 64 Bit HP C 7-Zip 16.04 Adobe Acrol Adobe Acrol Adobe Refre Backup and CDBurnerXF CodeMeter I Definition U | Knop particle for the formation for the formation of | мя 5 (КВ3115407) 32-Bit Edition | 8.2.4 16.04 15.02(18.01) 1.8.0 3.40.8 4.5.7.(6.50.2 - | Версия .20042 .20038 921.5350 6623 531.502 | Дата установки 15.05.2017 12.01.2018 01.02.2018 01.03.2018 25.03.2018 25.03.2018 11.09.2017 27.11.2017 12.01.2018 |
| 2 3 4 5 6 7 7 8 9 9 10 | 64 Bit HP C. 7-Zip 16.04 Adobe Acrol Adobe Acrol Adobe Refre Backup and CDBurnerXF CodeMeter I Definition U doPDF 8 | IO Components Installer (X64) bat DC and the staller bat DC and the staller bat Reader DC - Russian shi Manager Sync from Google Runtime Kit v6.50b pdate for Microsoft Office 2011 | мя 5 (КВ3115407) 32-Bit Edition | 8.2.4 16.04 15.02(18.01) 1.8.0 3.40.8 4.5.7. 6.50.2 - 8.9.95 | Версия .20042 .20038 921.5350 6623 531.502 | Дата установки 15.05.2017 12.01.2018 01.02.2018 01.03.2018 01.03.2018 25.03.2018 11.09.2017 27.11.2017 12.01.2018 12.01.2018 |

Рисунок 309 – Отчет с результатами аудита рабочей станции

Во вкладке «Аппаратная часть» перечислены данные о процессоре, дисковых устройствах, сетевых адаптерах, параметрах монитора, принтерах, устройствах ввода и USB-накопителях (рис. 310).

Примечание. Информация об USB-накопителе, который подключен к рабочей станции, содержится в таблице со статусом «Да» в графе «Подключен» (рис. 311).

| Отчет работы Ин | спектора от Об | 5.04.2018 12:18 | 3:30 | | |
|--|--|---|--|--|---|
| Название проекта: Test Организация: Test | | | | | |
| Проверка механизмов очистки | Поиск по ключевым словам | Контрольное суммирование | Системный аудит | Проверка прав доступа | Журнал выполнения |
| Системный аудит | | | | | |
| Информация о версии операцис устройств, сетевых адаптеров, н слючей. | онной системы, перечень ус принтеров, устройств ввода | тановленного программного (информации (клавиатура, мі | обеспечения, парам ышь), перечень под | етры мониторов, централ ключенных USB-накопит | ьного процессора, дисковых елей, перечень лицензионных |
| Программная часть Аппарати | ная часть | | | | |
| | | | | | |
| 🃒 Информация о | процессоре | | | | |
| Название: Intel(R) Core(T) Архитектура: x64 | 4) 13-3240 CPU @ 3.40GHz | | | | |
| | | | | | |
| 🗵 Дисковые устро | йства | | | | |
| Nº | Модель | Серийн | ый номер | Версия | Размер (байты) |
| 1 WDC W | D5000AAKX-08U6AA0 | WD-WC0 | 2EJP46338 | 19.01H19 | 500 105 249 280 |
| Ceтевые адапте Realtek PCIe GBE Family Статус: Физический адрес: | ры / Controller включен 00-25-АВ-3F-71-F7 | | | | |
| IPv4: | 192.168.5.134 | | | | |
| IPv6: | fe80::459a:188d:14ab:4 | l41f%9 | | | |
| GUID: | {54AC3353-F07B-4C30- | 902B-C98C60781E46} | | | |
| DNS-суффикс: | echelon.lan | | | | |
| соединение: | Ethernet 453 | | | | |

Рисунок 310 – Информация об аппаратной части рабочей станции

| Інформация о когда-либо подклю | ченных USB-накопителях. | | | |
|---------------------------------|--------------------------|----------------------------------|-------------------------------------|-----------|
| № Имя | Серийный номер | Дата и время первого подключения | Дата и время последнего подключения | Подключен |
| 1 Generic Flash Disk USB Device | BFA37B03 | 05.04.2018 16:59:57 | 10.04.2018 14:02:59 | Да |
| 2 USB DISK 2.0 | 07073C14EAB2A129 | 25.04.2017 09:22:38 | 25.04.2017 09:22:38 | Нет |
| 3 JetFlash Transcend 32GB | 70FQ7S7Q9F09NN0Z | 12.05.2017 12:57:11 | 12.05.2017 12:57:11 | Нет |
| 4 Multiple Card Reader | 058F63666433 | 12.05.2017 15:22:05 | 12.05.2017 15:22:05 | Нет |
| 5 USB FLASH DRIVE | 90007125A6EA3276 | 15.06.2017 09:56:43 | 15.06.2017 09:56:43 | Нет |
| USB FLASH DRIVE | 0708482AA61C1621 | 15.06.2017 15:06:15 | 15.06.2017 15:06:15 | Нет |
| 7 ADATA USB Flash Drive | 26C0322000080016 | 18.07.2017 15:58:33 | 18.07.2017 15:58:33 | Нет |
| 8 Kingston DataTraveler 3.0 | 6CF049E16B59BFA0C951912F | 19.07.2017 17:39:57 | 19.07.2017 17:39:57 | Нет |
| USB FLASH DRIVE | 9000712580EA3201 | 31.07.2017 10:46:28 | 31.07.2017 10:46:28 | Нет |
| 0 USB FLASH DRIVE | 900071BD203A9B42 | 31.07.2017 10:47:19 | 31.07.2017 10:47:19 | Нет |
| 1 USB FLASH DRIVE | AP06701BA62AA1EF | 31.07.2017 16:16:14 | 31.07.2017 16:16:14 | Нет |
| 2 USB DISK 3.0 | 90007341DBFF9E45 | 08.08.2017 11:04:26 | 08.08.2017 11:04:26 | Нет |
| 3 USB DISK 3.0 | 90007343F2484737 | 04.10.2017 12:37:03 | 04.10.2017 12:37:03 | Нет |
| 4 Kingmax USB2.0 FlashDisk | C07000000008874 | 03.11.2017 14:23:35 | 03.11.2017 14:23:35 | Нет |

Рисунок 311 – Фрагмент отчета об аппаратной части рабочей станции

3.11.3.5.4 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. 312).

Примечание. Если в процессе проверки прав доступа произошла ошибка (например, файл был удален), то в соответствующей ячейке будет знак «?».

| 0 | Название проекта: Те Организация: Test | est | | | | | | |
|--------------------------------|---|---|---|---------------------|-----------------------|--|--|---|
| Ірове | ерка механизмов очистки | Поиск по ключевым словам | Контрольное суммирование | Системный аудит | Проверка прав доступа | Журнал вы | полнения | |
| 1ро нфор | рмация о проверенных | оступа правах доступа к объектам. | | | | | | |
| Hec | секретная Секретная | Совершенно секретная | | | | | | |
| | | | | | | | | |
| Ce | ссия: Несекре | етная | Пользовател | L: licar | | | | |
| Ce | ссия: Несекре | тная | Пользовател | ь: User | | | | |
| Nº | ссия: Несекре | етная | Пользовател Путь к объекту | ь: User | | Провер | енные пр | ава доступа Выполнені |
| Nº 1 | ссия: Несекре | р/Тест | Пользовател Путь к объекту | ь: User | | Провер Чтение + | енные пр Запись + | ава доступа Выполнені + |
| N9 1 2 | ссия: Несекре C:/Users/Olga/Deskto C:/Users/Olga/Deskto | р/Тест р/Тест.bmp | Пользовател Путь к объекту | ь: User | | Провер Чтение + + | енные пр. Запись + + | ава доступа Выполнені + + |
| Nº 1 2 3 | ссия: Несекре C:/Users/Olga/Deskto C:/Users/Olga/Deskto C:/Users/Olga/Deskto | р/Тест р/Тест /Тест/Тест.bmp р/Тест/Тест.txt | Пользовател Путь к объекту | ь: User | | Провер Чтение + + + | енные пр Запись + + | ава доступа Выполнени + + + |
| Nº 1 2 3 | ссия: Несекре C:/Users/Olga/Deskto C:/Users/Olga/Deskto C:/Users/Olga/Deskto | р/Тест p/Tecr/Tecr.hmp p/Tecr/Tecr.txt | Пользовател Путь к объекту Пользовател | b: User | | Провер Чтение + + + | енные пр Запись + + + | ава доступа Выполнени + + + |
| Nº 1 2 3 | ссия: Несекре C:/Users/Olga/Deskto C:/Users/Olga/Deskto | P/Tecr p/Tecr/Tecr.bmp p/Tecr/Tecr.bx | Пользовател Путь к объекту Пользователя | ь: User s: User2 | | Провер Чтение + + + | енные пра Запись + + + + | ава доступа Выполнени + + + + ава доступа |
| Nº 1 2 3 | ссия: Несекре C:/Users/Olga/Deskto C:/Users/Olga/Deskto | р/Тест p/Tecr p/Tecr/Tecr.bmp p/Tecr/Tecr.txt | Пользовател Путь к объекту Пользовател Путь к объекту | b: User 5: User2 | | Провер Чтение + + + + т | енные пр Запись + + + + Запись | ава доступа Выполнені + + + ава доступа Выполнені |
| Nº 1 2 3 Nº 1 | ссия: Несекре C:/Users/Olga/Deskto C:/Users/Olga/Deskto C:/Users/Olga/Deskto | p/Tecr p/Tecr/Tecr.bmp p/Tecr/Tecr.txt p/Tecr | Пользовател Путь к объекту Пользователя Путь к объекту | b: User s: User2 | | Провер Чтение + + + + - - | енные пр. Запись + + + + - - | ава доступа Выполнени + + + ава доступа Выполнени |
| Nº 1 2 3 Nº 1 2 | ссия: Несекре C:/Users/Olga/Deskto C:/Users/Olga/Deskto C:/Users/Olga/Deskto C:/Users/Olga/Deskto | р/Тест p/Tecr/Tecr.bmp p/Tecr/Tecr.bt p/Tecr p/Tecr | Пользовател Путь к объекту Пользовател Путь к объекту | ь: User s: User2 | | Провер Чтение + + + + - | енные пр. Запись + + + + 3апись - | ава доступа Выполнени + + + Выполнени - |

Рисунок 312 – Отчет с результатами проверки прав доступа

3.11.3.5.5 Журналирование

Во вкладке «Журнал выполнения» содержится информация о ходе проведения тестирования (рис. 313).

| Отчет работы Инспектора от 06.04.2018 12:48:02 | | | | | | | | |
|---|--|--|--|--|-------------------|--|--|--|
| Название проекта: Test Организация: Test | t | | | | | | | |
| Проверка механизмов очистки | Поиск по ключевым словам | Контрольное суммирование | Системный аудит | Проверка прав доступа | Журнал выполнения | | | |
| Журнал выполнен 66.94.2018 12:47:19 Запуск пр 66.94.2018 12:47:16 Завериен 66.94.2018 12:47:16 Завериен 66.94.2018 12:47:55 Завериен 66.94.2018 12:48:80 Запуск сб 66.94.2018 12:48:80 Зоринрова 66.94.2018 12:48:80 Зоринрова | ния роверки механизма очистки жес ме проверки механизма очистки риска по ключевничения по ключевничения риска и по ключевника, по ме проверки механизма очистки опредки механизма очистки ме проверки механизма очистки не проперки суменрования, по не контрольного суменрования, клемного аусича. вне итогового отчета заверше | ткого диска D:. и жесткого диска. пративной памяти. и оперативной памяти. ация: C:/Users/Olga/Desktop ация: C:/Users/Olga/Desktop | /Тест, алгоритм: ГОО /Тест/Тест.txt, алго | СТ 34.11-94 (S-блок Crypt Оритм: CRC-8. | toPro). | | | |
| вл | но. ∣аделец лицензии: Echelon № | 2. Срок действия лицензии с | 27.11.2016 до 01.06 | 5.2018 | | | | |
| В Эшелон Ин Ко | спектор Версия: 2.3 Програм онтакты технической поддерж | мное обеспечение © АО "НП ки продукта: <u>support.sca@cn</u> | 0 "Эшелон" <u>http://w</u> <u>po.ru</u> | ww.npo-echelon.ru | | | | |

Рисунок 313 – Вкладка «Журнал выполнения»

3.11.3.5.6 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. 249). Откроется окно «Инспектор – сравнение отчетов» (рис. 314).

| 🖳 Инспектор - сравнение отчетов | × |
|--|-------|
| Сравнение отчетов | |
| высерите первый отчет (файл general.xmi) | Обзор |
| Выберите второй отчет (файл general.xml) | Обзор |
| Сравнить | |

Рисунок 314 - Окно «Инспектор - сравнение отчетов»

Далее необходимо указать отчеты для сравнения и нажать кнопку «Сравнить» (рис. 315).

| 💞 Инспектор - сравнение отчетов | × |
|--|-------|
| Сравнение отчетов | |
| Выберите первый отчет (файл general.xml) | |
| C:/InspectorProject/report-2017-06-06-13-53-42/general/general.xml | Обзор |
| Выберите второй отчет (файл general.xml) | |
| C:/InspectorProject/report-2017-06-06-17-19-50/general/general.xml | Обзор |
| Сравнить | |

Рисунок 315 – Выбор отчетов для сравнения

В результате успешного сравнения отчетов откроется окно с соответствующим сообщением (рис. 316).



Рисунок 316 – Сообщение

После нажатия кнопки «Открыть отчет» (рис. 316) откроется отчет с результатами сравнения (рис. 317).

| Инспектор - сравнение отчетов | | |
|--|---|----------------|
| Название проекта: Test Организация: Test | | |
| Контрольное суммирование Системный аудит | | |
| Системный аудит | | |
| Программная часть Аппаратная часть | | |
| Операционная система Операционная система не изменилась. Новые установленные программы | | |
| № Название | Версия | Дата установки |
| 1 СоdеМеter Runtime Kit v6.50b Удаленные программы Удаленных программ не обнаружено. | 6.50.2631.502 | 27.11.2017 |
| Владелец лицензии: Echelon №2. Лицензия д инспектор Версия: 2.3 Программная часть © Контакты технической поддержки продукта: | действует от 27.11.2016 до 01.06.2018 AO "НПО "Эшелон" <u>http://www.npo-echelon.ru/</u> : <u>support.sca@cnpo.ru</u> | |

Рисунок 317 – Сравнение отчетов

3.11.3.6. 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.

3.12. Сохранение результатов сканирования на внешние носители

Для сохранения результатов сканирования на внешние носители предназначен «Файловый менеджер».

В ПК «Сканер-ВС» USB-накопители монтируются автоматически (рис. 318).



Рисунок 318 – Подключенный USB-накопитель

Чтобы сохранить данные на внешний жесткий диск, необходимо его смонтировать. Для этого нужно подключить жесткий диск к рабочей станции и открыть проводник (рис. 319).

| a | | r | oot | | | | . o * |
|---------------------------|-------|-------------------|-----------------|---------------|-----------------|---------------|--------|
| Файл Правка Вид Закладки | Пер | ейти Инструм | енты Спра | вка | | | |
| 🔺 🔍 🐨 👻 🐵 🙆 | /root | t . | | | | |) °\$- |
| Точки входа | ~ | | | | | | |
| 🛅 Домашняя папка | | | | ÷ | | 99 | |
| 📷 Рабочий стол | | Видео | Документы | Загрузки | Изображени я | Музыка | |
| 🎬 Корзина | | | - | | | | |
| 🚔 Приложения | | *o7 | (<u>ם</u>) | | | | |
| Seagate Backup Plus Drive | | Общедоступ ные | Рабочий стол | Шаблоны | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| 8 элементов(18 скрыто) | | | | Своболькое ме | сто: 959 3 МиБ | (Bcero: 2.1 F | WE) |

Рисунок 319 – Монтирование внешнего жесткого диска

Далее необходимо нажать левой кнопкой мыши по названию жесткого диска. После этого диск будет смонтирован автоматически (рис. 320).



Рисунок 320 – Подключенный внешний жесткий диск

4. СООБЩЕНИЕ ОПЕРАТОРУ

Тексты сообщений, выдаваемых в ходе выполнения программы, представлены в таблице (см. Таблица 15).

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

ПРИЛОЖЕНИЕ 1

ПРИМЕРЫ НЕОБХОДИМЫХ НАСТРОЕК ДЛЯ ИЗМЕНЕНИЯ ПОРЯДКА ЗАГРУЗКИ В UEFI И РАЗЛИЧНЫХ ТИПАХ BIOS

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

1.1 BIOS типа AMI

Для настройки BIOS типа AMI необходимо выполнить следующие действия: – перейти в раздел «Boot» (рис. 1.1);

| Aptio Setup Utility – Copyright (C) 2011 American Megatrends, Inc. Main Advanced <mark>Boot</mark> Security Save & Exit | | | |
|--|--|---|--|
| Boot Configuration Launch PXE OpROM | [Disabled] | Sets the system boot order | |
| Boot Option Priorities Boot Option #1 Boot Option #2 Boot Option #3 CD/DVD ROM Drive BBS Prioritie | [UEFI: KingstonDT 1] [PO: WDC WD7500BPKT] [P2: MATSHITABD-CMB] 25 | | |
| Hard Drive BBS Priorities Add New Boot Option ▶ Delete Boot Option | Boot Option #1 P2: MATSHITABD-CMB UJ141AF P0: WDC WD7500BPKT-80PK4T0 UEFI: KingstonDT 101 II PMAP Disabled | : Select Screen : Select Item ter: Select +/- : Change Opt. F1 : General Help F9 : Optimized Defaults F10 : Save & Exit ESC : Exit | |
| Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc. | | | |

Рисунок 1.1 – Раздел «Boot»

- в пункте «Boot Option Priorities», в поле «Boot Option #1» указать дисковод или внешний носитель, с которого планируется загрузка ПК «Сканер-ВС» (рис. 1.1);
- перейти в раздел «Save & Exit» и выбрать пункт «Save Changes & Exit» (рис. 1.2);
253 НПЭШ.00606-01 34

| Aptio Setup Utility – Conuright (C) 2011 American Main Advanced Boot Security <mark>Save & Exit</mark> | Megatrends, Inc. |
|--|--|
| Save Changes and Exit Discard Changes and Exit Save Options Save Changes Discard Changes Restore Defaults Boot Override P2: MATSHITABD-CMB UJ141AF P0: WDC WD7500BPKT-80PK4T0 UEFI: KingstonDT 101 II PMAP Launch EFI Shell from filesystem device | Attempts to Launch EFI Shell application (Shellx64.efi) from one of the available filesystem devices ++ : Select Screen t↓ : Select Item Enter: Select +/- : Change Opt. F1 : General Help F9 : Optimized Defaults F10 : Save & Exit ESC : Exit |
| Version 2.14.1219. Copyright (C) 2011 American Ma | egatrends, Inc. |

Рисунок 1.2 – Раздел «Boot»

- после перезагрузки рабочей станции войти в BIOS и произвести дополнительные настройки;
- перейти в раздел «Security», выбрать пункт «Secure Boot menu» и нажать клавишу «Enter» (рис. 1.3);

254 НПЭШ.00606-01 34

| Aptio Setup Utility – Main Advanced Boot <mark>Security</mark> Sav | Copyright (C) 2012 American e & Exit | Megatrends, Inc. |
|---|---|---|
| Password Description If ONLY the Administrator's password access to Setup and is only asked fo If ONLY the User's password is set, password and must be entered to boot In Setup the User will have Administ Administrator Password Status User Password Status Administrator Password User Password | is set, this only r when entering Setup. this is a power on to enter Setup. rator rights. NOT INSTALLED NOT INSTALLED | Customizable Secure Boot settings |
| HDD Password Status : ▶ I/O Interface Security ▶ Secure Boot menu | NOT INSTALLED | <pre>++ : Select Screen 11 : Select Item Enter: Select +/- : Change Opt. F1 : General Help F9 : Optimized Defaults F10 : Save & Exit ESC : Exit</pre> |
| Version 2.15.1236. Co | pyright (C) 2012 American M | egatrends, Inc. |

Рисунок 1.3 – Раздел «Security»

– для отключения функции «Secure Boot Control» в выпадающем списке выбрать «Disabled» (рис. 1.4);

| Aptio Set | up Utility – Copyright Security | (C) 2012 American | Megatrends, Inc. |
|---|------------------------------------|--------------------|--|
| Platform Mode Secure Boot Secure Boot Control | User Disabled [Disabled | | Secure Boot flow control. Secure Boot can be enabled only when 1.Platform Key(PK) is enrolled and Platform is operating in User mode and 2.CSM function is disabled in Setup |
| | | | <pre>++ : Select Screen t↓ : Select Item Enter: Select +/- : Change Opt. F1 : General Help F9 : Optimized Defaults F10 : Save & Exit ESC : Exit</pre> |
| Version | 2.15.1236. Copyright (C |) 2012 American Me | egatrends, Inc. |

Рисунок 1.4 – Раздел «Security»

- перейти во вкладку «Boot» и включить функцию «Launch CSM» в состояние «Enabled» (рис. 1.5);



Рисунок 1.5 – Раздел «Boot»

- перейти в раздел «Save & Exit»;
- выбрать пункт «Save Changes & Exit» (рис. 1.2) для сохранения изменений.

1.2 BIOS типа AWARD, PHOENIX

Для настройки необходимо выполнить следующие действия:

- выбрать пункт меню «Advanced BIOS Features» (рис. 1.6);
- перейти к редактированию «First boot device»;
- указать дисковод или внешний носитель, с которого планируется загрузка ПК «Сканер-ВС» (рис. 1.7);

| Phoenix - AwardBIOS CMOS Setup Utility | | | | | |
|---|---|--|--|--|--|
| Standard CMOS Features Advanced BIOS Features Advanced Chipset Features Integrated Peripherals Power Management Setup PnP/PCI Configurations PC Health Status | Frequency-Voltage Control Load Fail-Safe Defaults Load Optimized Defaults Set Supervisor Password Set User Password Save & Exit Setup Exit Without Saving | | | | |
| Esc : Quit F10 : Save & Exit Setup | | | | | |
| Time, Date, Hard Disk Type | | | | | |

Рисунок 1.6 – Раздел «Advanced BIOS Features»



Рисунок 1.7 – Раздел «First Boot Device»

– перейти в раздел меню «Save & Exit Setup» (рис. 1.7) для сохранения изменений.

1.3 BIOS типа INSYDE H20

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». Если для загрузки ПК «Сканер-ВС» используется DVD-диск, то первым в списке должен быть указан «Internal Optic Disc Drive». Если для загрузки ПК «Сканер-ВС» используется USB-накопитель, то первым в списке необходимо указать «External Device»;
- перейти в раздел «Exit» и выбрать «Save and Exit Setup» для сохранения изменений.

1.4 BIOS C UEFI BOOT

Для успешной загрузки ПК «Сканер-ВС» с внешнего носителя необходимо отключить функцию «Secure Boot». Для этого необходимо выполнить следующие действия:

 – перейти во вкладку «Security» и отключить функцию «Secure Boot», выбрав в выпадающем списке «Disabled» (рис. 1.8);



Рисунок 1.8 – Раздел «Security»

– перейти во вкладку «Boot» и установить у функции «Boot Mode» значение «Legacy Support», а у функции «Boot Priority» – «Legacy First» (рис. 1.9);

- в списке «Legacy» перенести в начало списка наименование носителя, с которого будет произведена загрузка ПК «Сканер-ВС»;
- перейти в раздел «Exit» и выбрать «Exit Saving Changes» (рис. 1.10) для сохранения изменений.

| Information Configuration Security | InsydeH20 Setup Utility |
|---|--|
| Boot Hode Boot Priority USB Boot PXE Boot to LAN | [Legacy Support] [Legacy First] [Enabled] [Enabled] |
| EFI Legacy SATA HDD : TOSHIBA MQ01ABF050 Network Boot: Realtek PXE B03 D00 | Появился выбор устройств загрузки |
| | |

Рисунок 1.9 – Раздел «Boot»

Если USB-накопитель отсутствует в списке «Legacy», необходимо перезагрузить рабочую станцию.



Рисунок 1.10 – Раздел «Exit»

1.5 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 (рис. 1.11) и при выходе из UEFI сохранить настройки.

| ASUS EFI BIOS Util | lity - EZ Mo | de | | | | C | 🚺 Exit/Advance | d Mode |
|---------------------------|-------------------|------------|--------------|----------------|----------------|-------------|----------------|--------|
| 00.00 | P8H67-V | | | | | | English | n 🔻 |
| - C - C - H | BIOS Versio | n : 0712 | | | | Build Date | : 05/09/2011 | |
| | CPU Type : | Intel(R) C | ore(TM) 13-2 | 2125 CPU @ 3.3 | 0GHz | Speed : 333 | 6 MHz | |
| Tuesday (8/21/2012) | Total Memor | y : 4096 M | 8 (DDR3 133 | (MHZ) | | | | |
| I Temperature | 🗲 Voltage | | | | Fan Spe | ed | | |
| CPU +125.6"F7+52.0"C | CPU | 1,1369 | 5V | 5.0407 | CPU_FAN | 1295RPH | PHR_FAN | |
| MB +91.4 F7+33.0 C | 3.3V | 3.296V | 12V | | CHA_FAN1 | NZA. | CHA_FAN2 | |
| | | | - | | | | | |
| System Performance | | | | | | | | |
| Quiet | | | 0 | | 0 | | - | |
| | | | (| | () | | | 1 |
| | | | 10 1 | | 6.9 | | 1 1 | |
| Perfermance | Eller 83. 29A tuš | The a | dvanced opt | ions or the ha | ndware setup h | ave been ch | anged | |
| U Boot Priority | | | | | | | | |
| | N Con | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| Use he mouse to drag or k | eyboard to ray | igate to d | ecide the b | oot priority. | | | | |
| 1 | | | | | Boot | Menu(F8) | Default | (F5) |
| | | | | | | | | |

Рисунок 1.11 – Интерфейс UEFI

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 (рис. 1.11);
- перейти в раздел «Boot»;
- в пункте «Boot Option Priorities» указать в «Boot Option #1» вид и наименование загрузочного устройства (рис. 1.12);

| I | | ⊑₀ | C. | U V |
|---|--------------------------------------|--|--|--|
| Main | Ai Tweaker | Advanced | Monitor | Boot |
| | | | | |
| Bootup NumLock S Full Screen Logo Wait For 'F1' If Post Report Option ROM Messa | State 9 F Error 19ges | Boot D | On Disabled Enabled 1 sec ption #1 | Sets the syst |
| Setup Mode Boot Option Pric Boot Option #1 | mities | P1: WDC WD1002 P6: ATAPI iH Windows Boot M Disabled | FAEX-00Z3A0 AS424 Y anager | |
| Boot Option #2 Boot Option #3 | | | P6: ATAPI P1: WDC WD | ++: Select Sc tl: Select It Enter: Select +/-: Change D |
| ► Hard Drive BE | 3S Priorities rive BBS Priorities | | | F1: General H F2: Previous F5: Optimized F10: Save ES |

Рисунок 1.12 – Раздел «Boot»

– при выходе из UEFI необходимо сохранить настройки.

ПРИЛОЖЕНИЕ 2

СПИСОК ПОДДЕРЖИВАЕМЫХ АДАПТЕРОВ

Список поддерживаемых адаптеров представлен в таблице (см. Таблица 2.1).

Таблица 2.1 – Список поддерживаемых адаптеров

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

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|-----------------|-------------|-----------------|------------|
| Airlink101 | AWLC-3026 | Cardbus | Ralink | rt61 |
| Airlink101 | AWLL5088 | USB | RealTek | rt18192cu |
| Airlink101 | AWLL3025 | USB | Zydas | ZD1211 |
| Airlink101 | AWLL3025 v. 2 | USB | Zydas | ZD1211 |
| Airlink101 | AWLL3026 | USB | Zydas | ZD1211 |
| Airlink101 | AWLL3026 | USB | Zydas | ZD1211 |
| Airnet | AWN108 | Cardbus | Atheros | Mad WiFi |
| Airvast | XN-100 | Cardbus | Atheros | Mad WiFi |
| Airvast | XN-200 | Mini-PCI | Atheros | Mad WiFi |
| Alfa | GWPC005 | Cardbus | Cardbus Atheros | |
| Alfa | GWPC006G | Cardbus | Atheros | Mad WiFi |
| Alfa | GWPC007 | Cardbus | Atheros | Mad WiFi |
| Allnet | ALL0281 | PCI | PCI Atheros | |
| Alloy | WLF245401 | Cardbus | Broadcom | Bcm43xx |
| Alloy | WLF2454USB | USB | Broadcom | Bcm43xx |
| Alloy | WLF2454VP | PCI | Broadcom | Bcm43xx |
| Ambit | Т60Н906 | Mini-PCI | Broadcom | Bcm43xx |
| Aopen | AOI-811 | Cardbus | Atheros | Mad WiFi |
| Aopen | WL54 | USB | Zydas | ZD1211 |
| Apple | Airport extreme | Mini-PCI | Broadcom | Bcm43xx |
| Apple | Airport extreme | Mini-PCI | Broadcom | Bcm43xx |
| Apple | Airport extreme | Mini-PCI | Atheros | madwifi-ng |

| Производитель | Модель | Форм-фактор | Форм-фактор Чипсет | |
|---------------|------------------|-------------|--------------------|----------|
| Approx | appPCI300 | PCI | PCI Atheros | |
| Arcadyan | WN4401C1-ZZ | Mini-PCI | Atheros | Mad WiFi |
| Asante | AL 5402-XG | Cardbus | Broadcom | Bcm43xx |
| Askey | WLL220 | Mini-PCI | Atheros | ath5k |
| Askey | WLC3010 | Cardbus | Broadcom | Bcm43xx |
| Askey | WLH3010 | PCI | Broadcom | Bcm43xx |
| Askey | WLL3010 | Mini-PCI | Broadcom | Bcm43xx |
| Askey | WLL220 | Cardbus | Atheros | Mad WiFi |
| Askey | WLL3020 | Mini-PCI | Atheros | Mad WiFi |
| Askey | WLL4070-D50 | Mini-PCI | Mini-PCI Atheros | |
| Asus | WL-100G | Cardbus | Broadcom | Bcm43xx |
| Asus | WL-100G | Cardbus | Broadcom | Bcm43xx |
| Asus | WL-103b | Cardbus | Broadcom | Bcm43xx |
| Asus | WL-138G v.2 | PCI | Broadcom | Bcm43xx |
| Asus | WL-200 | Cardbus | Atheros | Mad WiFi |
| Asus | PCI-G31 | PCI | Ralink | rt61 |
| Asus | WL-167G v.2 | USB | Ralink | rt73 |
| Ativa | AWGNA54 | Cardbus | Atheros | Mad WiFi |
| Ativa | AWGUA54 | USB | Zydas | ZD1211 |
| Atlantis | A02-PCI-W54 v1.3 | PCI | Ralink | rt61 |
| Azio | AWU254 | USB | Ralink | rt73 |
| Azurewave | AW-NE771 | Mini-PCIe | Atheros | ath9k |
| Belkin | F5D8011 v. 1000 | Cardbus | Atheros | ath9k |

| Производитель | Модель | Форм-фактор | Форм-фактор Чипсет | |
|---------------|-----------------|-------------|--------------------|-----------|
| Belkin | F5D7000 | PCI | PCI Broadcom | |
| Belkin | F5D7001 | PCI | Broadcom | Bcm43xx |
| Belkin | F5D7010 | Cardbus | Broadcom | Bcm43xx |
| Belkin | F5D7011 | Cardbus | Broadcom | Bcm43xx |
| Belkin | F5D7051 | USB | Broadcom | Bcm43xx |
| Belkin | F5D7000 v.5000 | PCI | Atheros | Mad WiFi |
| Belkin | F5D7010 v.5100 | Cardbus | Atheros | Mad WiFi |
| Belkin | F5D7000 v.6000 | PCI | PCI Ralink | |
| Belkin | F5D7050 v. 5000 | USB | RealTek | rt18187 |
| Belkin | F9L1001 | USB | RealTek | RTL8188SU |
| Belkin | F9L1004 | USB | RealTek | RTL8192CU |
| Belkin | F5D7050 v. 4000 | USB | Zydas | ZD1211 |
| Blitz | BWI-715 rev.1 | PCI | Atheros | Mad WiFi |
| Bromax | WE602B | Cardbus | Broadcom | Bcm43xx |
| Buffalo | WLI-CB-G54 | Cardbus | Broadcom | Bcm43xx |
| Buffalo | WLI-PCI-G54 | PCI | Broadcom | Bcm43xx |
| Buffalo | WLI-USB-G54 | USB | Broadcom | Bcm43xx |
| Buffalo | WLI-U2-SG54HG | USB | Ralink | rt73 |
| Buffalo | WLI-U2-KG54L | USB | Zydas | ZD1211 |
| Canyon Tech | CN-WF518 | USB | Zydas | ZD1211 |
| CC&C | WL-2100 | Cardbus | Broadcom | Bcm43xx |

| Производитель | Модель | Форм-фактор | Форм-фактор Чипсет | |
|---------------------------|-----------------|-------------|--------------------|----------|
| CC&C | WL-2400 | Mini-PCI | Broadcom | Bcm43xx |
| Cisco | Air-CB21AG | Cardbus | Atheros | Mad WiFi |
| Cnet | CWP-903 | PCI | Ralink | rt61 |
| Compex | WLM200NX | Mini-PCI | Atheros | ath9k |
| Compex | WLU108g | USB | Atheros | Mad WiFi |
| CompuShack | CS-23-543-84 | Cardbus | Atheros | Mad WiFi |
| Conceptronic | C54C | Cardbus | Atheros | Mad WiFi |
| Conceptronic | C54I | PCI | Atheros | Mad WiFi |
| Conceptronic | C54WIFIU | USB | Zydas | ZD1211 |
| Contec Flexscan | FX-DS540-PCC | Cardbus | Atheros | Mad WiFi |
| Dell | TrueMobile 1180 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | TrueMobile 1300 | Cardbus | Broadcom | Bcm43xx |
| Dell | TrueMobile 1300 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | TrueMobile 1350 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | TrueMobile 1370 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | TrueMobile 1400 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | TrueMobile 1450 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | Wireless 1390 | Mini-PCI | Broadcom | Bcm43xx |
| Dell | Wireless 1395 | Mini-PCI | Broadcom | Bcm43xx |
| Delta Networks | LM-WB521 | Cardbus | Atheros | Mad WiFi |
| Dick Smith Electronics | XH9946 | PCI | Atheros | Mad WiFi |
| Digicom | 8E4213 | USB | Zydas | ZD1211 |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|-----------------|--------------------|-------------|---------|---------------|
| Digitus Network | DN-7031 | Cardbus | Atheros | Mad WiFi |
| Digitus Network | DN-7036 | PCI | Atheros | Mad WiFi |
| Digitus Network | DN-7003GV | USB | Zydas | ZD1211 |
| D-Link | WNA-1330 | Cardbus | Atheros | ath5k |
| D-Link | DWA-547 | PCI | Atheros | ath5k / ath9k |
| D-Link | DWA-522 rev. A1 | PCI | Atheros | ath9k |
| D-Link | DWA-522 rev. A2 | PCI | Atheros | ath9k |
| D-Link | DWA-547 | PCI | Atheros | ath9k |
| D-Link | DWA-642 | Cardbus | Atheros | ath9k |
| D-Link | DWA-652 | Cardbus | Atheros | ath9k |
| D-Link | DWL-650+ | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-A520 | PCI | Atheros | Mad WiFi |
| D-Link | DWL-A650 | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-A650 | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-AB520 | PCI | Atheros | Mad WiFi |
| D-Link | DWL-AB650 | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-AG520 | PCI | Atheros | Mad WiFi |
| D-Link | DWL-AG650 | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-AG660 (rev. 1) | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-G510 | PCI | Atheros | Mad WiFi |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|-----------------------|-------------|---------|---------------------|
| D-Link | DWL-G520 | PCI | Atheros | Mad WiFi |
| D-Link | DWL-G550 | PCI | Atheros | Mad WiFi |
| D-Link | DWL-G650 | Cardbus | Atheros | Mad WiFi |
| D-Link | DWL-G650M | Cardbus | Atheros | Mad WiFi |
| D-Link | WDA-1320 | PCI | Atheros | Mad WiFi |
| D-Link | WDA-2320 | PCI | Atheros | Mad WiFi |
| D-Link | DWA-520 | PCI | Atheros | Mad WiFi / ath5k |
| D-Link | DWL-G520M | PCI | Atheros | Mad WiFi / ath5k |
| D-Link | DWL-G630 (rev. C1) | Cardbus | Atheros | Mad WiFi / ath5k |
| D-Link | DWL-G630 (rev. D) | Cardbus | Atheros | Mad WiFi / ath5k |
| D-Link | WDA-2320 v. 1 | PCI | Atheros | Mad WiFi / ath5k |
| D-Link | WNA-2330 | Cardbus | Atheros | Mad WiFi / ath5k |
| D-Link | DWL-AG530 | PCI | Atheros | Madi WiFi |
| D-Link | DWA-525 | PCI | Ralink | rt2800pci |
| D-Link | DWA-525 rev. A2 | PCI | Ralink | rt2800pci |
| D-Link | DWA-125 rev. A2 | USB | Ralink | rt2800usb |
| D-Link | DWA-130 rev. B | USB | Ralink | rt2800usb |
| D-Link | DWA-510 | PCI | Ralink | rt61 |
| D-Link | DWL-G510 rev. C2 | PCI | Ralink | rt61 |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|-----------------------|-------------|---------|---------------------|
| D-Link | DWL-G510 rev.C1 | PCI | Ralink | rt61 |
| D-Link | DWL-G520+A v.C1 | PCI | Ralink | rt61 |
| D-Link | DWL-G630 (rev. E1) | Cardbus | Ralink | RT61 |
| D-Link | DWL-G630 (rev. E2) | Cardbus | Ralink | rt61 |
| D-Link | DWA-110 | USB | Ralink | rt73 |
| D-Link | DWA-111 | USB | Ralink | rt73 |
| D-Link | WUA-1340 | USB | Ralink | rt73 |
| D-Link | DWA-121 rev. A | USB | RealTek | RTL8192CU |
| D-Link | DWA-120 | USB | Atheros | ar5523 |
| Edimax | EW-7325IG | PCI | Atheros | Mad WiFi |
| Edimax | EW-7108PCG | Cardbus | Ralink | rt61 |
| Edimax | EW-7318USg | USB | Ralink | rt73 |
| Edimax | EW-7318Ug | USB | Ralink | rt73 |
| Edimax | EW-7811Un | USB | RealTek | RTL8192CU |
| Edimax | EW-7317Ug | USB | Zydas | zd1211 |
| EDUP | EP-MS8511 | USB | RealTek | RTL8188CUS |
| Eminent | EM4056 v. 1.0 | Cardbus | Atheros | Mad WiFi / ath5k |
| Eminent | EM4454 | USB | Ralink | rt73 |
| Enterasys | RBTBG-AW | Cardbus | Atheros | Mad WiFi |
| Eusso | GL 2454-01 | Cardbus | Atheros | Mad WiFi |
| Eusso | GL 2454-01 | PCI | Atheros | Mad WiFi |
| Farallon | PN4030 | Cardbus | Atheros | Mad WiFi |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|-----------------|--------------|-------------|----------|---------------------|
| Farallon | PN4032 | PCI | Atheros | Mad WiFi |
| Fujitsu-Siemens | E-5454 | Cardbus | Atheros | Mad WiFi |
| Gemtek | WL-352BW | Mini-PCI | Broadcom | Bcm43xx |
| Gemtek | WL-360G | PCI | Broadcom | Bcm43xx |
| Gemtek | WPI-100G | PCI | Broadcom | Bcm43xx |
| Gemtek | WL-511 | Cardbus | Atheros | Mad WiFi |
| Gemtek | WL-550 | Mini-PCI | Atheros | Mad WiFi |
| Gemtek | WL-571 | Cardbus | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WIAG01 | Mini-PCI | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WIAG02 | Mini-PCI | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WLMA101 | Cardbus | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WLMA102 | Cardbus | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WLMAG | Cardbus | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WMAG01 | Cardbus | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WP01GT | PCI | Atheros | Mad WiFi |
| Gigabyte Tech | GN-WI01HT | Mini-PCI | Atheros | Mad WiFi / ath5k |
| Gigabyte Tech | GN-WPKG | PCI | Ralink | rt2500pci |
| Gigabyte Tech | GN-WI01GS | Mini-PCI | Ralink | rt61 |
| Gigabyte Tech | GN-WB01GS | USB | Ralink | rt73 |
| Gigafast | WF748-CUI | USB | Zydas | ZD1211 |
| GlobalSun Tech | GL 245401-OA | Cardbus | Atheros | Mad WiFi |
| GlobalSun Tech | GL 2454MP | Mini-PCI | Atheros | Mad WiFi |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|----------------|--------------------------|-------------|----------|---------------------|
| GlobalSun Tech | GL 505401 | Cardbus | Atheros | Mad WiFi |
| GlobalSun Tech | GL 505402 | Cardbus | Atheros | Mad WiFi |
| GlobalSun Tech | GL 5054MP | Mini-PCI | Atheros | Mad WiFi |
| GlobalSun Tech | GL 5054VP | PCI | Atheros | Mad WiFi |
| GlobalSun Tech | GL 5254MP | Mini-PCI | Atheros | Mad WiFi |
| Hama | 62764 | USB | Ralink | rt73 |
| Hama | 39741 | USB | Zydas | ZD1211 |
| Hamlet | HNWU254G | USB | Ralink | rt73 |
| Hawking Tech | HWUG1 | USB | Ralink | rt73 |
| Hawking Tech | HWU54G | USB | Zydas | ZD1211 |
| Hawking Tech | HWU8DD rev. B | USB | Zydas | ZD1211 |
| Hercules | HWGPCI-54 v. 2 | PCI | Ralink | rt61 |
| HP | AR242x | PCI-E | Atheros | ath5k |
| HP | Wireless | Mini-PCI | Broadcom | Bcm43xx |
| HP | AR5007 | Mini-PCI | Atheros | Mad WiFi |
| IBM | 22P7501 | Cardbus | Atheros | Mad WiFi |
| ICIDU | Wireless 11G PCI Card | PCI | Atheros | Mad WiFi / ath5k |
| Icom | SL-5000 | Cardbus | Atheros | Mad WiFi |
| Icom | SR-21BB | Cardbus | Atheros | Mad WiFi |
| Inexq | UR055g | USB | Zydas | ZD1211 |
| Intel | 3160ac rev. 83 | Mini-PCIe | Intel | iwlwifi |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|----------------|-------------|----------|----------|
| Intel | 3160ac rev. 84 | Mini-PCIe | Intel | iwlwifi |
| Intel | 7260ac rev. 83 | Mini-PCIe | Intel | iwlwifi |
| Intel | 7260ac rev. 84 | Mini-PCIe | Intel | iwlwifi |
| Intel | N6200 | Mini-PCIe | Intel | iwlwifi |
| Intel | WCB5000 | Cardbus | Atheros | Mad WiFi |
| Intel | WPCI5000 | PCI | Atheros | Mad WiFi |
| I-O Data | WN-A54 / PCM | Cardbus | Atheros | Mad WiFi |
| IOGear | GWU523 | USB | Zydas | ZD1211 |
| JAHT | WN-5054CB | Cardbus | Atheros? | Mad WiFi |
| Lancom | MC-54a / g | Cardbus | Atheros | Mad WiFi |
| Lancom | MC-54ab | Cardbus | Atheros | Mad WiFi |
| Lancom | MC-54g | Cardbus | Atheros | Mad WiFi |
| Lancom | PCI-54a | PCI | Atheros | Mad WiFi |
| Lancom | PCI-54a / g | PCI | Atheros | Mad WiFi |
| LevelOne | WNC-0300 | PCI | Atheros | Mad WiFi |
| LevelOne | WPC-0300 | Cardbus | Atheros | Mad WiFi |
| LevelOne | WNC-0301 v.3 | PCI | Ralink | rt61 |
| LevelOne | WNC-0301 v.3 | USB | Ralink | rt73 |
| Linksys | WPC300N v. 2 | Cardbus | Atheros | ath9k |
| Linksys | WEC600N | PCI-E | Broadcom | Bcm43xx |
| Linksys | WMP11 v. 2.7 | PCI | Broadcom | Bcm43xx |
| Linksys | WMP300N | PCI | Broadcom | Bcm43xx |
| Linksys | WMP300N v. 1 | PCI | Broadcom | Bcm43xx |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|---------------|-------------|--------------------|---------------------|
| Linksys | WMP54G | PCI | Broadcom | Bcm43xx |
| Linksys | WMP54G v. 3 | PCI | Broadcom | Bcm43xx |
| Linksys | WMP54G v.2 | PCI | Broadcom | Bcm43xx |
| Linksys | WPC300N v. 1 | Cardbus | Broadcom | Bcm43xx |
| Linksys | WPC54G v. 1 | Cardbus | Broadcom | Bcm43xx |
| Linksys | WPC54G v. 3 | Cardbus | Broadcom | Bcm43xx |
| Linksys | WPC54GS | Cardbus | Broadcom | Bcm43xx |
| Linksys | WPM54G v.2 | PCI | Broadcom | Bcm43xx |
| Linksys | WMP300N v. 2 | PCI | Atheros | Mad WiFi |
| Linksys | WMP55AG | PCI | Atheros | Mad WiFi |
| Linksys | WPC51AB | Cardbus | Atheros | Mad WiFi |
| Linksys | WPC54A | Cardbus | Atheros | Mad WiFi |
| Linksys | WPC55AG | Cardbus | Atheros | Mad WiFi |
| Linksys | WMP110 v.1 | PCI | Atheros | Mad WiFi / ath9k |
| Linksys | WPC11 v.3 | PCMCIA | Prism 1 | orinoco |
| Linksys | WUSB54AG | USB | Intersil / Frisbee | p54usb |
| Linksys | WUSB54G v. 1 | USB | Intersil / Frisbee | p54usb |
| Linksys | WUSB54G v. 2 | USB | Intersil / Frisbee | p54usb |
| Linksys | WUSB54GP v. 1 | USB | Intersil / Frisbee | p54usb |
| Linksys | WUSB54G v. 4 | USB | Ralink | rt2500usb |
| Linksys | WUSB54GP v. 4 | USB | Ralink | rt2500usb |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|---------------|---------------|-------------|----------|----------|
| Linksys | WMP54G v. 4.1 | PCI | Ralink | RT61 |
| Linksys | WUSB54GC | USB | Ralink | rt73 |
| Longshine | LCS8131G3 | USB | Zydas | ZD1211 |
| Macromate | MWN-754 | Cardbus | Atheros | Mad WiFi |
| Macsense | WPE-800 | Cardbus | Broadcom | Bcm43xx |
| Micradigital | F5D7000eaE | PCI | Atheros | Mad WiFi |
| Microsoft | MN-720 | Cardbus | Broadcom | Bcm43xx |
| Microsoft | MN-730 | PCI | Broadcom | Bcm43xx |
| Microtik | 5G / ABG | PCI | Atheros | Mad WiFi |
| Microtik | 5G / ABM | PCI | Atheros | Mad WiFi |
| Minitar | MN54GCB | Cardbus | Broadcom | Bcm43xx |
| Minitar | MN54GPC | PCI | Broadcom | Bcm43xx |
| Minitar | MWGUHA | USB | Zydas | ZD1211 |
| Motorola | WN825Gv2 | Cardbus | Broadcom | b43 |
| Motorola | WN825G | Cardbus | Broadcom | Bcm43xx |
| Motorola | WPCI810G | PCI | Broadcom | Bcm43xx |
| MSI | UB11B | USB | Broadcom | Bcm43xx |
| MSI | US54SE II | USB | Ralink | rt73 |
| MSI | US54SE | USB | Zydas | ZD1211 |
| NDC | NWH1054 | Cardbus | Atheros | Mad WiFi |
| NEC | WL-54AC | Cardbus | Atheros | Mad WiFi |
| NEC | WL54AG | Cardbus | Atheros | Mad WiFi |
| Netegriti | EM-500AG | Mini-PCI | Atheros | Mad WiFi |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|-------------------------|-----------------|-------------|--------------------|----------|
| Netgear | WPN511 (rev. 1) | Cardbus | Atheros | ath5k |
| Netgear | WNA-1100 | USB | atheros | ath9k |
| Netgear | WN511B | Cardbus | Broadcom | Bcm43xx |
| Netgear | HA 311 | PCI | Atheros | Mad WiFi |
| Netgear | HA 501 | Cardbus | Atheros | Mad WiFi |
| Netgear | WAB501 | Cardbus | Atheros | Mad WiFi |
| Netgear | WAG311 | PCI | Atheros | Mad WiFi |
| Netgear | WAG511 | Cardbus | Atheros | Mad WiFi |
| Netgear | WG 311 | PCI | Atheros | Mad WiFi |
| Netgear | WG 311T | PCI | Atheros | Mad WiFi |
| Netgear | WG111T | USB | Atheros | Mad WiFi |
| Netgear | WG511T | Cardbus | Atheros | Mad WiFi |
| Netgear | WG511U | Cardbus | Atheros | Mad WiFi |
| Netgear | WPN111 | USB | Atheros | Mad WiFi |
| Netgear | WPN311 | PCI | Atheros | Mad WiFi |
| Netgear | WG511 v. 3 | Cardbus | Intersil / Frisbee | p54pci |
| Netgear | WG111 v. 1 | USB | Intersil / Frisbee | p54usb |
| Netgear | WG111 v. 2 | USB | Realtek | rt18187 |
| Netgear | WG111 v. 3 | USB | RealTek | rtl8187 |
| Nortel / E- mobility | 2201 | Cardbus | Atheros | Mad WiFi |
| Nortel / E- mobility | 2202 | Cardbus | Atheros | Mad WiFi |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|----------------------|--------------|-------------|----------|---------------------|
| Ovislink | W542USB | USB | Ralink | rt73 |
| Ovislink | W54USB v. 2 | USB | Ralink | rt73 |
| Ovislink | WT-2000USB | USB | Ralink | rt73 |
| Passys | ipw4965 | PCI-E | ipw4965 | iwlwifi |
| Passys | ipw5100 | PCI-E | ipw5100 | iwlwifi |
| Passys | ipw5150 | PCI-E | ipw5100 | iwlwifi |
| Passys | ipw5300 | PCI-E | ipw5300 | iwlwifi |
| Passys | ipw5350 | PCI-E | ipw5300 | iwlwifi |
| Philips | PH 10819 | Cardbus | Atheros | Mad WiFi |
| Philips | PH 11107 | Mini-PCI | Atheros | Mad WiFi |
| Philips | PH 11840 | Mini-PCI | Atheros | Mad WiFi |
| Philips | SNN6500 | Cardbus | Atheros | Mad WiFi |
| Philips | РН 12127Е | Mini-PCI | Atheros | Mad WiFi / ath5k |
| Philips | SNU5600 | USB | Zydas | ZD1211 |
| Phoebe | PHWL54 | Cardbus | Broadcom | Bcm43xx |
| Phoebe | PHWL54-PCI | PCI | Broadcom | Bcm43xx |
| Planet Technology | WL-3560 | Cardbus | Atheros | Mad WiFi |
| Planet Technology | WL-8310 | PCI | Atheros | Mad Wifi / ath5k |
| Planet Technology | WL-U356 | USB | Zydas | ZD1211 |
| Planex | GW-NS540a | Cardbus | Atheros | Mad WiFi |
| Pluscom | WP-AR2413 | PCI | Atheros | ath5k |
| Pluscom | WMP-RT2561ST | Mini-PCI | Ralink | rt61 |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|------------------|--------------|-------------|---------|----------|
| Pluscom | WP-RT2561T | PCI | Ralink | rt61 |
| Pluscom | WU-RT2571 | USB | Ralink | rt73 |
| Pluscom | WU-TR2571W | USB | Ralink | rt73 |
| Pluscom | WU-RTL8187 | USB | RealTek | rt18187 |
| Pluscom | WU-ZD1211B | USB | Zydas | ZD1211 |
| Proxim | 8450 | Cardbus | Atheros | Mad WiFi |
| Proxim | 8451 | Cardbus | Atheros | Mad WiFi |
| Proxim | 846005 | Cardbus | Atheros | Mad WiFi |
| Proxim | 846105 | Cardbus | Atheros | Mad WiFi |
| Proxim | 8470 | Cardbus | Atheros | Mad WiFi |
| Proxim | 8470 WD | Cardbus | Atheros | Mad WiFi |
| Proxim | 8471 | Cardbus | Atheros | Mad WiFi |
| Proxim | 8480 | Cardbus | Atheros | Mad WiFi |
| Proxim | 8480 WD | Cardbus | Atheros | Mad WiFi |
| Proxim | 8481 | Cardbus | Atheros | Mad WiFi |
| Proxim | 8482 | PCI | Atheros | Mad WiFi |
| Roper | RO80211GA-CB | Cardbus | Atheros | Mad WiFi |
| Rosewill | RNX-G300EX | PCI | Ralink | rt61 |
| Safecom | SWLU-5400 | USB | Zydas | ZD1211 |
| Sceptre | SC254g | Cardbus | Atheros | Mad WiFi |
| Senao / Engenius | 3054pcia | PCI | Atheros | Mad WiFi |
| Senao / Engenius | 5354cba | Cardbus | Atheros | Mad WiFi |
| Senao / Engenius | SL-3054CB | Cardbus | Atheros | Mad WiFi |
| Senao / Engenius | SL-3054MP | Mini-PCI | Atheros | Mad WiFi |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер |
|------------------------|-----------------|-------------|----------|---------------------|
| Senao / Engenius | SL-5054CB | Cardbus | Atheros | Mad WiFi |
| Senao / Engenius | SL-5054CB Dual | Cardbus | Atheros | Mad WiFi |
| Senao / Engenius | SL-5354CB | Cardbus | Atheros | Mad WiFi |
| Senao / Engenius | SL-5354MP | Mini-PCI | Atheros | Mad WiFi |
| Senao / Engenius | SL-NMP 8602 | Mini-PCI | Atheros | Mad WiFi |
| Siemens Speedstream | 1024 ver.2 | PCI | Broadcom | Bcm43xx |
| Siemens-Gigaset | usb 108 | USB | Atheros | Mad WiFi / ath5k |
| Sitecom | WL-100b | Cardbus | Broadcom | Bcm43xx |
| Sitecom | WL-110b | PCI | Broadcom | Bcm43xx |
| Sitecom | WL-170 v. 1 | Cardbus | Ralink | rt61 |
| Sitecom | WL-171 | PCI | Ralink | rt61 |
| Sitecom | WL-113 v. 1.002 | USB | Ralink | rt73 |
| Sitecom | WL-172 | USB | Ralink | rt73 |
| Sitecom | WL-113 | USB | Zydas | ZD1211 |
| SMC | 2335W | Cardbus | Atheros | Mad WiFi |
| SMC | 2336W-AG | Cardbus | Atheros | Mad WiFi |
| SMC | 2536W-AG | Cardbusp | Atheros | Mad WiFi |
| SMC | 2735W | Cardbus | Atheros | Mad WiFi |
| SMC | SMCWPCI-G | PCI | Atheros | Mad WiFi |
| SMC | SMCWPCIT-G EU | PCI | Atheros | Mad WiFi |
| SMC | SMCWBCT | Cardbus | Atheros | Mad WiFi / ath5k |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер | |
|---------------|------------------------|------------------|-------------|----------|--|
| SMC | SMCWUSB-G | USB | Zydas | ZD1211 | |
| Sony | PCWA-C300S | Cardbus | Atheros | Mad WiFi | |
| Sony | PCWA-C500 | Cardbus | Atheros | Mad WiFi | |
| Sony | PCWAC700 | Cardbus | Atheros | Mad WiFi | |
| Sony | IFU-WLM2 | USB | Zydas | ZD1211 | |
| Sparklan | WL-352 | Mini-PCI | Broadcom | Bcm43xx | |
| Sparklan | WL-660GT | PCI | Broadcom | Bcm43xx | |
| Sparklan | WL-555 | Mini-PCI | Atheros | Mad WiFi | |
| Sparklan | WL-558 | Mini-PCI | Atheros | Mad WiFi | |
| Sweex | LW051 v. 1.0 | Cardbus | Atheros | Mad WiFi | |
| Sweex | LW052 | PCI | Atheros | Mad WiFi | |
| Sweex | LW053 | USB | Ralink | rt73 | |
| TDK | WN-5CB01 | Cardbus | Atheros | Mad WiFi | |
| TDK | WN-5MP01 | Mini-PCI | Atheros | Mad WiFi | |
| Tecom | WL5021 | Cardbus | Broadcom | Bcm43xx | |
| Tellus | s C6100 Cardbus | | Atheros | Mad WiFi | |
| Tellus | M6100 | Mini-PCI | Atheros | Mad WiFi | |
| Topcom | 4001g | USB | Ralink | rt73 | |
| Toshiba | AR2413 | Mini-PCI Atheros | | ath5k | |
| Toshiba | Toshiba Atheros AR5001 | | PCI Atheros | | |
| Totolink | Totolink N200UP | | USB Ralink | | |
| TP-Link | TL-WN350GD | PCI | Atheros | ath5k | |
| TP-Link | TP-Link TL-WN851ND | | Atheros | ath9k | |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер | |
|---------------|------------------------|-------------|------------|---------------------|--|
| TP-Link | TL-WN861N v1.1 | Mini-PCI | Atheros | ath9k | |
| TP-Link | TL-WN861N v2 | Mini-PCI | Atheros | ath9k | |
| TP-Link | TL-WN881ND v.1.1 | PCI | Atheros at | | |
| TP-Link | WN721N | USB | Atheros | ath9k | |
| TP-Link | WN751ND | PCI-E | Atheros | ath9k | |
| TP-Link | WN781ND | PCI-E | Atheros | ath9k | |
| TP-Link | WN951N | PCI | Atheros | ath9k | |
| TP-Link | WN322G v. 3.0 | USB | Atheros | ath9k_htc | |
| TP-Link | WN422G v. 2 | USB | Atheros | ath9k_htc | |
| TP-Link | WN722N | USB | Atheros | ath9k_htc | |
| TP-Link | WN822N v.2 | USB | Atheros | ath9k_htc | |
| TP-Link | WN550G | PCI | Atheros | Mad WiFi | |
| TP-Link | WN551G | PCI | Atheros | Mad WiFi | |
| TP-Link | WN560G | Mini-PCI | Atheros | Mad WiFi | |
| TP-Link | WN610G | Cardbus | Atheros | Mad WiFi | |
| TP-Link | WN620g | USB | Atheros | Mad WiFi | |
| TP-Link | WN651G | PCI | Atheros | Mad WiFi | |
| TP-Link | WN510G | Cardbus | Atheros | Mad WiFi / ath5k | |
| TP-Link | TL-WDN3200 rev. 1.2 | USB | Ralink | rt2800usb | |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер | |
|---------------|----------------|-------------|----------|-----------|--|
| TP-Link | WN321G | USB | Ralink | rt73 | |
| TP-Link | TL-WN8200ND | USB | RealTek | RTL8192CU | |
| TP-Link | TL_WN823N | USB | RealTek | RTL8192CU | |
| TP-Link | Tl-wn821 v.4 | USB | RealTek | RTL8192CU | |
| TP-Link | WN322G | USB | Zydas | ZD1211 | |
| TP-Link | WN422G v. 1 | USB | Zydas | ZD1211 | |
| TP-Link | WN442G | USB | Zydas | ZD1211 | |
| TRENDware | TEW-401PC | Cardbus | Broadcom | Bcm43xx | |
| TRENDware | TEW-403PCI | PCI | Broadcom | Bcm43xx | |
| TRENDware | TEW-441PC | Cardbus | Atheros | Mad WiFi | |
| TRENDware | TEW-443PI | PCI | Atheros | Mad WiFi | |
| TRENDware | TEW-424UB v.1 | USB | Zydas | ZD1211 | |
| Trust | 13645 | PCI | Atheros | Mad WiFi | |
| Trust | 13647 | Cardbus | Atheros | Mad WiFi | |
| TwinMOS | G240 | USB | Zydas | ZD1211 | |
| Ubiquiti | RC-UBI-SRC | Cardbus | Atheros | Mad WiFi | |
| US Robotics | USR5417A | PCI | Broadcom | Bcm43xx | |
| US Robotics | USR5421 | USB | Broadcom | Bcm43xx | |
| US Robotics | USR805423 | USB | Zydas | ZD1211 | |
| USI | MP-G-BR-01(3A) | Mini-PCI | Broadcom | Bcm43xx | |
| USI | CB-AG-AT-01 | Cardbus | Atheros | Mad WiFi | |

| Производитель | Модель | Форм-фактор | Чипсет | Драйвер | |
|---------------|-----------------|-------------------|----------|---------------------|--|
| USI | MP-AG-AT-01(3B) | Mini-PCI | Atheros | Mad WiFi | |
| Wistron | CB-300G | Cardbus | Broadcom | Bcm43xx | |
| Wistron | EM-300G | Mini-PCI | Broadcom | Bcm43xx | |
| Wistron | CB-100AB | Cardbus | Atheros | Mad WiFi | |
| Wistron | CB-500AG | Cardbus | Atheros | Mad WiFi | |
| Wistron | EM-500AG | Mini-PCI | Atheros | Mad WiFi | |
| Wistron | EM9-AB (VM4) | Mini-PCI | Atheros | Mad WiFi | |
| W-Link | WEN-2091 | PCI | Broadcom | Bcm43xx | |
| W-Link | WEN-2200 | Mini-PCI Broadcom | | Bcm43xx | |
| X-Micro | XWL-11GPAG | Cardbus Atheros | | Mad WiFi | |
| X-Micro | XWL-11GUZX | USB | Zydas | zd1211 | |
| Z-Com | AG-320 | Cardbus | Atheros | Mad WiFi | |
| Z-Com | XV5300 | Cardbus | Atheros | Mad WiFi | |
| Z-Com | XV5350 | Cardbus | Atheros | Mad WiFi | |
| Zonet | ZEW 1500S | Cardbus | Atheros | Mad WiFi | |
| Zonet | ZEW 2501 | USB Zydas | | ZD1211 | |
| Zyxel Zyair | G-102 | Cardbus Atheros | | Mad WiFi | |
| Zyxel Zyair | M-102 | Cardbus | Atheros | Mad WiFi / ath5k | |
| Zyxel Zyair | M-302 | PCI | Atheros | Mad WiFi / ath5k | |
| Zyxel Zyair | G-220 | USB | Zydas | ZD1211 | |
| Zyxel Zyair | ag-225h | USB | Zydas | ZD1211 | |

ПРИЛОЖЕНИЕ 3

КОМБИНАЦИИ КЛАВИШ ДЛЯ УПРАВЛЕНИЯ КОМПОНЕНТОМ «ИНСПЕКТОР»

Комбинации клавиш для клавиатурного режима работы с компонентом «Инспектор» представлены в таблице (см. Таблица 3.1).

Таблица 3.1 – Комбинации клавиш

| Клавиша / комбинации клавиш | Действие | | | | |
|--|---|--|--|--|--|
| Общие комбинации 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 | | | | |
| Комбинации управления стартовой страницы | | | | | |
| Tab | Переход между областью «Выбор утилит» и кнопками «Обзор (путь до отчета)», «Вперед», «Отмена» | | | | |
| Область выбора утилит | | | | | |
| Стрелки вверх / вниз | Навигация | | | | |
| Пробел / Enter | Смена состояния | | | | |
| Комбинации управления утилить | і поиска остаточной информации | | | | |
| Tab | Переход между областью «Выбор диска» и кнопками «Назад», «Вперед» и «Отмена» | | | | |
| Область выбора диска | | | | | |
| Стрелки вправо / влево | Навигация | | | | |
| Пробел / Enter | Смена состояния | | | | |

| Клавиша / комбинации клавиш | Действие | | | | | |
|---|---|--|--|--|--|--|
| Комбинации управления утилиты контрольного суммирования | | | | | | |
| Tab | Переход между областями «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 - то переход в ее подпапку | | | | | |
| Стрелка влево | Скрытие папки, если уже скрыта - то переход на уровень выше | | | | | |
| Пробел | Раскрытие / скрытие папки | | | | | |
| Enter | Добавление выбранной папки | | | | | |
| Область настро | ойки алгоритмов | | | | | |
| Стрелки вверх / вниз и вправо / влево | Навигация по таблице | | | | | |
| Enter на ячейках с выбором | Просмотр вариантов | | | | | |
| Delete | Удаление | | | | | |
| Комбинации управления ути | Комбинации управления утилиты проверки прав доступа | | | | | |
| Tab | Переход между областями «Выбор целей», «Директории», «Пользователи», «Модель прав», «Массовая работа» и кнопками «Назад», «Вперед», «Отмена» | | | | | |
| Область в | ыбора целей | | | | | |
| Стрелки вверх / вниз | Навигация | | | | | |
| Стрелка вправо | Раскрытие папки, если папка уже раскрыта - то переход в ее подпапку | | | | | |
| Стрелка влево | Скрытие папки, если уже скрыта - то перехо на уровень выше | | | | | |
| Пробел | Раскрытие / скрытие папки | | | | | |
| Enter | Добавление выбранной папки | | | | | |
| Область «Д | Іиректории» | | | | | |
| Delete | Удаление | | | | | |
| Стрелки вправо / влево | Навигация | | | | | |
| Пробел / Enter на ячейке с уровнем секретности | Смена состояния | | | | | |

| Клавиша / комбинации клавиш | Действие | | | | |
|---------------------------------------|---------------------------------|--|--|--|--|
| Область «Пользователи» | | | | | |
| Delete | Удаление | | | | |
| Стрелки вверх / вниз | Навигация | | | | |
| 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 | | | | |

Перечень сокращений

| Сокращение | Расшифровка |
|---|--|
| BIOS | (от англ. <i>Basic input/output system</i>) – Базовая система ввода / вывода |
| ID | (от англ. Identification data) – Идентификатор |
| SVGA | (от англ. Super video graphics array) – Графический видеоадаптер |
| UEFI | (от англ. Unified extensible firmware interface) – Унифицированный расширяемый интерфейс встроенного (базового) программного обеспечения |
| USB | (от англ. Universal serial bus) – Универсальная последовательная шина |
| WEP | (от англ. Wired equivalent privacy) – Алгоритм для обеспечения безопасности беспроводных сетей |
| Wi-Fi | (от англ. Wireless fidelity) – Беспроводная сеть |
| WPA | (от англ. <i>Wi-Fi protected access</i>) – Алгоритм для обеспечения безопасности беспроводных сетей |
| АО «НПО Эшелон» | Акционерное общество «Научно-производственное объединение «Эшелон» |
| OC | Операционная система |
| ПО | Программное обеспечение |
| ПК «Сканер-ВС», программный комплекс | Программный комплекс «Средство анализа защищенности «Сканер-ВС» |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю |

| Лист регистрации изменений | | | | | | | | | |
|----------------------------|---|------------|-------|----------------|--|----------------|--|---------|------|
| Изм. | Иомера листов (страниц) | | | ов | | | | | |
| | измененных | замененных | НОВЫХ | аннулированных | Всего листов (страниц) в докум. | № документа | Входящий № сопроводит. документа и дата | Подпись | Дата |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |