АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «ЭШЕЛОН»

УТВЕРЖДЕН
НПЕШ.00606-01 31-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВО АНАЛИЗА ЗАЩИЩЕННОСТИ «СКАНЕР-ВС»

Описание применения

НПЕШ.00606-01 31-2

Часть 3

Листов 21

2025

Инв. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата

АННОТАЦИЯ

ПК «Сканер-ВС» состоит из нескольких (в зависимости от исполнения) функционально независимых составных частей, как указано в таблице 1.

Т а б л и ц а 1 – Состав ПК «Сканер-ВС»

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

В документе содержатся сведения о назначении программного комплекса «Средство анализа защищенности «Сканер-ВС» НПЕШ.00606-01 исполнений № 6, 7, 8 и 9 (далее — ПК «Сканер-ВС»), области и ограничениях его применения, классе решаемых задач, минимальной конфигурации технических средств, на которых ПК «Сканер-ВС» эксплуатируется.

Сведения о назначении программного комплекса «Средство анализа защищенности «Сканер-ВС» НПЕШ.00606-01 исполнений № 1 и 2 приведены в НПЕШ.00606-01 31 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Описание применения. Часть 1».

Сведения о назначении программного комплекса «Средство анализа защищенности «Сканер-ВС» НПЕШ.00606-01 исполнений № 3 и 4 приведены в НПЕШ.00606-01 31-1 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Описание применения. Часть 2».

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение программы

Сканер-ВС предназначен для поиска уязвимостей программного обеспечения, сканирования сетевых узлов и сервисов, идентификации ОС и приложений, трассировки сетевых маршрутов для построения топологии сети, сбора информации при помощи активного подключения к исследуемому узлу, проверки стойкости сетевых паролей и настроек программного обеспечения на соответствие требованиям безопасности.

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

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

Компонент «Инспектор» предназначен для тестирования функций безопасности при проведении аттестации ИС (АС).

1.2. Основные функции и параметры

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

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

Сканер-ВС осуществляет обновление базы данных уязвимостей через центр обновлений Сканер-ВС.

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

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

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

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

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

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

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

2. УСЛОВИЯ ПРИМЕНЕНИЯ

ПК «Сканер-ВС» эксплуатируется на рабочих станциях, удовлетворяющих минимальным аппаратным и программным требованиям, представленным в таблице 2.

Таблица 2 — Минимальные требования к среде функционирования ПК «Сканер-ВС»

Параметр	Значение
Операционная система	Astra Linux Special Edition: 1.6, 1.7 и 1.8 ОС семейства Windows (WSL) Операционная система Альт СП: 10.2 Операционная система «РЕД ОС»: 8
Процессор	количество ядер – 4; базовая тактовая частота процессора – 2 ГГц
Оперативная память	не хуже DDR3 8 Гб, частота – 1600 МГц
Свободное дисковое пространство	один накопитель SSD, объем – 100 Гб
Дополнительные требования к аппаратуре	интерфейс для подключения монитора 1) разрешение монитора – 1920x1080 пикселей

3. ОПИСАНИЕ ЗАДАЧИ

Сканер-ВС выполняет следующие задачи:

– управление активами;

– управление проектами;

– исследование сети;

– инвентаризация;

– поиск уязвимостей;

– подбор паролей;

– аудит;

– формирование отчетов;

– построение карты сети.

Компонент «Инспектор» выполняет следующие задачи:

– контроль состава технических средств и ПО;

– обеспечение контроля реализации правил разграничения доступа (в части контроля реализации правил разграничения доступа и полномочий пользователей в информационной системе);

– контроль целостности программного обеспечения;

– контроль уничтожения информации и обеспечение поиска остаточной информации на машинных носителях.

3.1. Управление активами

Управление активами позволяет осуществить выборку целей для тестирования последующих задач. Для каждого актива заводится карточка с полной информацией об активе.

В Сканер-ВС реализованы следующие функции управления активами:

– добавление активов;

– удаление активов;

– изменение информации об активе;

– установка метки активу (активам).

3.2. Управление проектами

Проекты в Сканер-ВС созданы для сортировки активов по тому или иному признаку, удобного для пользователя. Проекты предоставляют возможность пользователю отделить для последующего исследования определенные группы активов из более большой сети или, например, активы разных сетей (для каждой отдельно взятой сети можно создать свой проект, в который будут включены только активы из этой сети).

3.3. Исследование сети

Задача «Исследование сети» предназначена для сканирования сетевых узлов и сервисов, идентификации ОС и приложений, трассировки сетевых маршрутов для построения топологии сети.

Исследование сети производится путем сканирования IP-адресов и портов (TCP- и UDP-портов) компьютеров. Найденные в результате поиска действующие подключения с IP-адресами и задействованными TCP- и UDP-портами попадают в «Активы».

3.4. Инвентаризация

Инвентаризация предназначена для активного подключения к исследуемому узлу для сбора информации безагентным способом (подключение к интересующему хосту и получение от него информации, однако, для данного способа необходимы соответствующие полномочия доступа). При инвентаризации происходит заполнение данных в карточке актива, указание портов и прикладного ПО.

3.5. Поиск уязвимостей

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

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 (https://www.bdu.fstec.ru), национальная база данных уязвимостей США «National Vulnerability Database» (https://nvd.nist.gov/), база отслеживания ошибок безопасности ОС на базе Debian GNU/Linux «Debian GNU/Linux Security Bug Tracker» (https://security-tracker.debian.org/tracker/), база данных уязвимостей информационной безопасности ОС на базе Ubuntu «Ubuntu CVE Tracker» (https://ubuntu.com/security/cve), база отслеживания ошибок безопасности ОС на базе RHEL/CentOS «RHEL/CentOS Security Data» (https://access.redhat.com/security/data).

3.6. Подбор паролей

Задача подбора паролей – проверка стойкости паролей сетевых сервисов, а именно выявление возможности получения доступа к ресурсам компьютеров в проверяемой сети путем подбора имени и пароля пользователя. Подбор паролей осуществляется по словарю для следующих сетевых сервисов: ftp, imap, imaps, mssql, mysql, pop3, pop3s, postgres, rdp, redis, smb, smtp, smtps, snmp, ssh, telnet, telnets, vnc.

3.7. Аудит

Аудит – проверка настроек программного обеспечения на соответствие требованиям безопасности. Аудит определяет какие угрозы, связанные с настройками программного обеспечения, представляют опасность для сети и инфраструктуры.

Следуя рекомендациям и исправляя параметры настройки ПО согласно результатам аудита, можно повысить безопасность и управляемость сети.

3.8. Формирование отчетов

Документирование является неотъемлемой частью анализа защищенности информационной системы. Для объединения результатов всех этапов тестирования в Сканер-ВС используются отчеты.

После проведения различных задач по тестированию сети на предмет информационной уязвимости можно сгенерировать отчет, в котором отображаются такие аспекты информационной безопасности, как выявленные уязвимости, типы ОС активов сети, топ-5 уязвимых активов, подобранные пароли.

3.9. Построение карты сети

Связи между активами в сети представлены в виде карты сети. Она строится на основе информации, полученной в ходе выполнения задачи «Исследование сети» с включенной функцией «Трассировка для топологии».

Карта сети представляет собой граф, вершины которого являются узлы сети, а ребра – связи между ними.

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

С помощью карты сети можно узнать:

– связи между узлами;

– отсутствие необходимых связей между узлами;

– проблемы архитектуры сети;

– постороннее оборудование, подключенное к внутренним сетям;

– информацию об активе, подключенном к сети.

3.10. Контроль состава технических средств и ПО

После запуска компонент «Инспектор» читает параметры аппаратного и программного обеспечения ЭВМ, на которой запущен компонент «Инспектор», сохраняет результат чтения и возвращает сообщение о завершении по тому же интерфейсу.

Для каждого IBM PC-совместимого персонального компьютера в используемой локальной сети компонент «Инспектор» читает следующие параметры:

– версия 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.

По результатам чтения вышеуказанных параметров компонент «Инспектор» формирует отчет.

3.11. Обеспечение контроля реализации правил разграничения доступа

После запуска и получения параметров функционирования компонент «Инспектор» выполняет проверки соответствия смоделированной пользователем эталонной модели доступа реальным правилам разграничения доступа, сохраняет результат проверки и возвращает сообщение о завершении по тому же интерфейсу.

Режим функционирования:

Чтение созданной пользователем модели дискреционных и мандатных полномочий доступа пользователей (локальных и доменных) к выбранным сетевым папкам и объектам файловой системы ОС специального назначения «Astra Linux Special Edition».

По результатам проведения проверок компонент «Инспектор» формирует отчет.

3.12. Контроль целостности программного обеспечения

После запуска и получения параметров функционирования компонент «Инспектор» производит подсчет контрольных сумм указанных пользователем объектов по выбранным алгоритмам, сохраняет результат и возвращает сообщение о завершении по тому же интерфейсу.

Контрольное суммирование заданных пользователем файлов, папок, подпапок, съемных носителей осуществляется по следующим алгоритмам (по выбору пользователя):

– ГОСТ 34.11-94 (S-блок CryptoPro);

– ГОСТ 34.11-94 (тестовый S-блок);

– ГОСТ 34.11-2012 (256 бит);

– ГОСТ 34.11-2012 (512 бит);

– CRC-8;

– CRC-16;

– CRC-32;

– MD5;

– SHA-1;

– SHA-224;

– SHA-256;

– SHA-384;

– SHA-512.

По результатам суммирования компонент «Инспектор» формирует отчет.

3.13. Контроль уничтожения информации и обеспечение поиска остаточной информации на машинных носителях

После запуска и получения параметров функционирования по интерфейсу «GUI» компонент «Инспектор» формирует псевдослучайную последовательность для записи на диск, инициирует ее запись на проверяемое устройство, стирание и поиск

этой последовательности. По завершении сохраняет результат поиска и возвращает сообщение о завершении по тому же интерфейсу.

Режимы функционирования:

1. Поиск остаточной информации на машинных носителях информации на основе заданной структуры данных в соответствии с заданными ключевыми словами.

2. Определение директории файла с найденной информацией.

3. Тестирование механизмов очистки оперативной памяти ОС специального назначения «Astra Linux Special Edition» и запоминающих устройств рабочей станции.

По результатам тестирования компонент «Инспектор» формирует отчет.

Подробное описание функциональных возможностей Сканер-ВС и компонента «Инспектор» приведено в НПЕШ.00606-01 90-1 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Руководство пользователя. Часть 2».

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входные и выходные данные Сканер-ВС представлены в таблице 3.

Таблица 3 — Входные и выходные данные Сканер-ВС

Задача	Входные данные	Выходные данные
Управление активами	– Имя актива; – FQDN; – IPv4-адрес; – IPv6-адрес; – MAC-адрес; – Имя хоста; – Тип устройства; – Тип ОС; – Метки; – Уровень критичности; – Дата и время создания; – Дата и время обновления.	– Карточка актива.
	– Сетевой протокол; – Порт; – Логин; – Пароль; – Описание.	– Учетные записи.
Управление проектами	– Количество активов; – Количество обнаруженных уязвимостей; – Количество сгенерированных отчетов.	– Карточка проекта.

Задача	Входные данные	Выходные данные
Исследование сети	– Основные настройки: 1) имя задачи; 2) перечень целей (активов); 3) перечень активов для исключения из исследования; 4) опция предварительного обнаружения хостов; 5) опция трассировки для топологии; 6) опция определения ОС; – Сканирование портов: 1) перечень портов для сканирования (TCP, UDP); 2) перечень портов для исключения из сканирования; 3) опция сканирования наиболее популярных портов; 4) количество наиболее популярных портов; 5) опция определения версий сервисов; 6) Интенсивность определения версий сервисов; – Сетевые настройки: 1) порт, с которого осуществляется сканирование; 2) сетевой интерфейс для сканирования; – Политики сканирования: 1) минимальное число пакетов в секунду; 2) максимальное число пакетов в секунду; – Расписание: 1) не повторять; 2) 1 раз; 3) по расписанию.	– Карточка актива; – Таблица «Хосты»; – Таблица «Порты»; – Карта сети; – Таблица «История».

Задача	Входные данные	Выходные данные
Инвентаризация	– Имя задачи; – Перечень целей (активов); – Учетные записи для целей; – Расписание: 1) не повторять; 2) 1 раз; 3) по расписанию.	– Карточка актива; – Таблица «Хосты»; – Таблица «Прикладное ПО»; – Таблица «История».
Поиск уязвимостей	– Имя задачи; – Перечень целей (активов); – Опция использования NIST NVD; – Опция строгого соответствия версии ПО в NIST NVD; – Опция приоритета данных от вендора; – Опция скрытия неизученных уязвимостей; – Расписание: 1) не повторять; 2) 1 раз; 3) по расписанию.	– Карточка актива; – Таблица «Уязвимое ПО»; – Таблица «Уязвимости»; – Таблица «История».
Подбор паролей	– Имя задачи; – Перечень целей (активов); – Сервис; – Порт; – Опция завершения подбора при первом положительном результате; – Словари и списки логинов и паролей; – Опция проверки пустого пароля; – Опция проверки пароля, совпадающего с логином; – Опция проверки пароля, совпадающего с логином в обратном порядке; – Расписание: 1) не повторять; 2) 1 раз; 3) по расписанию.	– Таблица «Учетные записи»; – Таблица «История».

Задача	Входные данные	Выходные данные
Аудит	– Имя задачи; – Перечень целей (активов); – Учетные записи; – Расписание: 1) не повторять; 2) 1 раз; 3) по расписанию.	– Таблица «Аудит».
Формирование отчетов	– Имя отчета; – Уровень критичности; – Перечень целей (активов); – Опция скрытия паролей; – Тип отчета; – Расширение.	– Таблица «Отчеты»; – Отчет.
Построение карты сети	– Завершенные задачи исследования сети с включенной при этом опцией трассировкой для топологии	– Таблица «Карты сети»; – Карта сети.

Входные и выходные данные компонента «Инспектор» представлены в таблице 4.

Таблица 4 — Входные и выходные данные компонента «Инспектор»

Задача	Входные данные	Выходные данные
Контроль состава технических средств, ПО и СЗИ	– Версия ОС; – Перечень установленного ПО; – Параметры периферийных устройств; – Перечень подключенных USB-накопителей; – Перечень лицензионных ключей.	– Отчет.
Обеспечение контроля реализации правил разграничения доступа	– модель дискреционных и мандатных полномочий доступа пользователей (локальных и доменных) к выбранным сетевым папкам и объектам файловой системы ОС семейства Windows и ОС специального назначения «Astra Linux Special Edition».	– Отчет.

Задача	Входные данные	Выходные данные
Контроль целостности программного обеспечения	– полные адреса объектов контроля (папки, файлы…); – идентификатор алгоритма суммирования.	– Отчет.
Контроль уничтожения информации и обеспечение поиска остаточной информации на машинных носителях	– Полные имена объектов контроля (устройства, разделы/области дисков).	– Отчет.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Расшифровка
API	(англ. Application Programming Interface) – набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением или операционной системой для использования во внешних программных продуктах
ARP	(англ. Address Resolution Protocol – протокол определения адреса) – протокол в компьютерных сетях, предназначенный для определения MAC-адреса по IP-адресу другого компьютера
CLI	(англ. Command Line Interface) – интерфейс командной строки
CSV	(англ. Comma-Separated Values) – текстовый формат, предназначенный для представления табличных данных
CVE	(англ. Common Vulnerabilities and Exposures) - база данных общеизвестных уязвимостей информационной безопасности
HTML	(англ. HyperText Markup Language) – стандартизированный язык разметки документов в сети Интернет
GUI	(англ. Graphical User Interface) — разновидность пользовательского интерфейса, в котором элементы интерфейса (меню, кнопки, значки, списки и т. п.), представленные пользователю на дисплее, исполнены в виде графических изображений
ICMP	(англ. Internet Control Message Protocol – протокол межсетевых управляющих сообщений) – сетевой протокол, входящий в стек протоколов TCP/IP
IP-адрес	(англ. Internet Protocol Address – адрес Интернет-протокола) – уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP
MAC-адрес	(англ. Media Access Control – управление доступом к среде, также Hardware Address, также физический адрес) – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet
MD5	(англ. Message Digest 5) – алгоритм хеширования предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности
PDF	(англ. Portable Document Format) – межплатформенный формат электронных документов, разработанный фирмой Adobe Systems с использованием ряда возможностей языка PostScript
SMB	(англ. Simple Mail Transfer Protocol) – сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SSH	(англ. Secure Shell — безопасная оболочка) – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений

Сокращение	Расшифровка
SVGA	(англ. Super video graphics array) графический видеоадаптер
TCP	(англ. Transmission Control Protocol) – один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных
UDP	(англ. User Datagram Protocol – протокол пользовательских датаграмм) – один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета
USB	(англ. Universal Serial Bus – универсальная последовательная шина) – последовательный интерфейс для подключения периферийных устройств к вычислительной технике
WEP	(англ. Wired Equivalent Privacy) – алгоритм для обеспечения безопасности беспроводных сетей
WPA	(англ. Wi-Fi Protected Access) – обновлённая программа сертификации устройств беспроводной связи
WUI	(англ. Web User Interface) – пользовательский Web-интерфейс
АС	Автоматизированная система
БД	База данных
БДУ	Банк данных угроз
ГОСТ	Государственный стандарт
ИА	Идентификация и аутентификация
ИБ	Информационная безопасность
ИС	Информационная система
Компонент «Инспектор»	Программный компонент «Инспектор»
НЖМД	Накопитель на жестких магнитных дисках
НСД	Несанкционированный доступ
ОС	Операционная система
ПК «Сканер-ВС»	Программный комплекс «Средство анализа защищенности «Сканер-ВС»
ПО	Программное обеспечение
СЗИ	Средство защиты информации
Сканер-ВС	Программное обеспечение «Сканер-ВС»
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЭВМ	Электронно-вычислительная машина

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводит. документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					