

УТВЕРЖДЕН
НПЕШ.00606-01 91-ЛУ

Экз. №__

ПРОГРАММНЫЙ КОМПЛЕКС
«СРЕДСТВО АНАЛИЗА ЗАЩИЩЕННОСТИ «СКАНЕР-ВС»

Руководство администратора**Часть 2****НПЕШ.00606-01 91-1****Листов 61**

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

Литера «__»

АННОТАЦИЯ

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

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

В документе содержатся следующие сведения:

- назначение программы (п. 1 настоящего руководства);
- условия выполнения программы (п. 2 и 3 настоящего руководства);
- описание функций и особенностей эксплуатации изделия для пользователя с ролью «Администратор» (п. 4 настоящего руководства);
- конфигурирование ПК «Сканер-ВС» (п. 4 настоящего руководства);
- удаление ПК «Сканер-ВС» (п. 6 настоящего руководства);
- сообщения пользователю (п. 6 настоящего руководства);
- инструкция подключения к узлу исследуемой сети по протоколу WinRM (Приложение 1 настоящего документа);
- инструкция подключения к узлу исследуемой сети, работающему на ОС Windows, по протоколу SSH (Приложение 2 настоящего документа).

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

Таблица 1 – Состав ПК «Сканер-ВС»

№ исполнения Компонент	1	2	3	4	5	6	7	8	9
Программное обеспечение «Сканер-ВС» версии 5	+	+	–	–	+	–	–	–	–
Программное обеспечение «Сканер-ВС» версии 6	–	–	+	+	+	–	–	–	–

№ исполнения Компонент	1	2	3	4	5	6	7	8	9
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, установке, конфигурировании и особенностях эксплуатации ПК «Сканер-ВС» в 6, 7, 8 и 9 вариантах исполнения.

Сведения о назначении, установке, конфигурировании и особенностях эксплуатации изделия в 3, 4 и 5 вариантах исполнения содержатся в документе НПЕШ.00606-01 91-1 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Руководство администратора. Часть 1».

Функциональные отличия Сканер-ВС версии 7 редакций «Base» и «Enterprise» представлены в разделе 2 документа «НПЕШ.00606-01 90-2 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Руководство пользователя. Часть 3».

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

Под администратором понимается любое лицо, допущенное до эксплуатации и конфигурировании изделия с ролью «Администратор».

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

СОДЕРЖАНИЕ

1. Назначение программы.....	6
2. Условия выполнения программы	13
2.1 Требования к аппаратному обеспечению.....	13
2.2 Требования к среде функционирования	14
3. Выполнение программы	16
3.1 Подготовка к установке.....	16
3.1.1 Проверка комплектности.....	16
3.1.2 Проверка контрольных сумм	16
3.2 Установка и первичная настройка Сканер-ВС	17
3.2.1 Установка и запуск Сканер-ВС в стандартном режиме.....	17
3.2.2 Установка и запуск Сканер-ВС на RPM-based ОС	22
4. Конфигурирование Сканер-ВС	24
4.1 Описание конфигурационного файла «scanner.yml»	24
4.2 Настройка интеграции Сканер-ВС с LDAP сервером.....	32
4.3 Настройка интеграции доменной зоны kerberos.....	34
4.4 Назначение параметров окружения службы «Scanner».....	35
4.5 Настройка сложности пароля для аутентификации операторов.....	36
4.6 Создание нового администратора	37
4.7 Смена паролей системных учетных записей	39

4.8 Управление сертификатами	41
4.8.1 Генерация пользовательских сертификатов	42
5. Удаление Сканер-ВС.....	43
6. Сообщения оператору	44
Перечень сокращений	46
ПРИЛОЖЕНИЕ 1. (ОБЯЗАТЕЛЬНОЕ) ИНСТРУКЦИЯ ПОДКЛЮЧЕНИЯ К УЗЛУ ИССЛЕДУЕМОЙ СЕТИ ПО ПРОТОКОЛУ WINRM	47
1.1. Настройка подключения по протоколу WinRM с помощью поставляемого скрипта	47
1.2. Ручная настройка подключения по протоколу WinRM для Windows Server 2008 и Windows 7	48
1.3. Удаление внесенных во время настройки подключения по протоколу WinRM изменений с помощью поставляемого скрипта	52
ПРИЛОЖЕНИЕ 2. (ОБЯЗАТЕЛЬНОЕ) ИНСТРУКЦИЯ ПОДКЛЮЧЕНИЯ К УЗЛУ ИССЛЕДУЕМОЙ СЕТИ, РАБОТАЮЩЕМУ НА ОС WINDOWS, ПО ПРОТОКОЛУ SSH.....	53
2.1. Подключение к узлу исследуемой сети.....	53
2.2. Настройка сервисов SSH с помощью встроенного приложения «Параметры»	58
2.3. Настройка сервисов SSH с помощью Windows PowerShell	59
2.4. Запуск и настройка OpenSSH Server.....	59

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- а) управление учетными записями операторов Сканер-ВС;
- б) управление учетными записями, используемыми для осуществления активного подключения к узлам исследуемой сети, и привязанными к ним секретами;
- в) обновление базы уязвимостей Сканер-ВС. Пользователю с ролью «Пользователь» доступен только просмотр истории обновлений;
- г) конфигурирование Сканер-ВС и его компонентов. Запрет конфигурирования осуществляется средствами среды функционирования Сканер-ВС.

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

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

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

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

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

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

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

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

- обеспечение контроля реализации правил разграничения доступа (АНЗ.5 в части контроля реализации правил разграничения доступа и полномочий операторов в информационной системе). Компонент «Инспектор» обеспечивает формирование и контроль дискреционных и мандатных полномочий доступа операторов (локальных и доменных) к выбранным сетевым папкам и объектам файловой системы ОС семейства

Microsoft Windows, в том числе с учетом настроек СЗИ Secret Net Studio, СЗИ Secret Net Studio-C, СЗИ Secret Net 7, СЗИ НСД Dallas Lock 8.0-К, СЗИ Dallas Lock 8.0-С;

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

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

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

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

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

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

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

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

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

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

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

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

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

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Требования к аппаратному обеспечению

Изделие устанавливается на рабочие станции, удовлетворяющие минимальным аппаратным и программным требованиям, представленным в таблице 2.

Т а б л и ц а 2 – Минимальные требования к аппаратной платформе Сканер-ВС

Параметр	Значение
Операционная система	Astra Linux Special Edition: 1.7.4
Процессор	Количество ядер – 4, Базовая тактовая частота процессора – 2 ГГц
Оперативная память	DDR3 8 Гб, частота – 1600 МГц
SSD	Один накопитель SSD, объемом 100 Гб
Дополнительные требования к аппаратуре	1) интерфейс для подключения монитора; 2) разрешение монитора – 1280x1024 пикселей.

Приведённые в таблице 2 требования достаточны для установки и работы системы, однако для более масштабных инфраструктур могут потребоваться дополнительные аппаратные ресурсы.

Для штатной работы Сканер-ВС и просмотра отчетов требуется установка на рабочую станцию одного из типов браузеров, представленных в таблице 3.

Т а б л и ц а 3 – Поддерживаемые веб-браузеры

№	Тип браузера	Минимальная рекомендуемая версия
1	Google Chrome	Google Chrome 84
2	Safari	Safari 13.0
3	Mozilla Firefox	Mozilla Firefox 78
4	Microsoft Edge	Microsoft Edge 83
5	Opera	Opera 69
6	Yandex Browser	Yandex Browser 20.7.2
7	Chromium	Chromium 81
8	Internet Explorer	Internet Explorer 11

2.2 Требования к среде функционирования

Перед эксплуатацией изделия необходимо внимательно ознакомиться с эксплуатационной документацией, входящей в состав поставки Сканер-ВС в соответствии с НПЕШ.00606-01 30 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Формуляр».

Для программного обеспечения среды функционирования Сканер-ВС должны быть установлены все актуальные обновления, выпущенные предприятием-изготовителем, а также выполнены рекомендации предприятия-изготовителя по безопасному конфигурированию.

При эксплуатации изделия на объектах информатизации, где производится обработка конфиденциальной информации, необходимо выполнение следующих условий:

- наличие администратора безопасности, отвечающего за правильную эксплуатацию (включая рекомендации по безопасному конфигурированию комплекса) Сканер-ВС;
- обеспечение физической сохранности рабочей станции с установленным Сканер-ВС и исключение возможности доступа к ней/ним посторонних лиц;
- проведение периодического контроля целостности, установленного Сканер-ВС с помощью программ контроля целостности (не реже одного раза в месяц);
- проведение периодической проверки на наличие актуальных уязвимостей в Сканер-ВС и среде его функционирования с использованием средств анализа защищенности (не реже одного раза в месяц);
- проведение периодической проверки Сканер-ВС и среды его функционирования на наличие компьютерных вирусов с использованием средств антивирусной защиты (не реже одного раза в месяц);
- наличие организационных и технических мер, направленных на исключение несанкционированного доступа к объекту функционирования Сканер-ВС.

Для защиты каналов передачи данных 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 Сканер-ВС по незащищенным каналам связи.

При эксплуатации Сканер-ВС оператором информационной системы должно быть обеспечено выполнение всех необходимых усиленных мер защиты информации.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1 Подготовка к установке

Перед проведением установки Сканер-ВС необходимо выполнить следующие действия:

- получить комплект Сканер-ВС установленным порядком;
- получить доступ к автоматизированному рабочему месту (далее – АРМ) установленным порядком;
- включить АРМ в соответствии с эксплуатационной документацией на него;
- подключить к АРМ компакт-диск с Сканер-ВС в соответствии с эксплуатационной документацией на него;
- произвести проверки в соответствии с п. 3.1.1 и 3.1.2 настоящего документа;
- после успешного проведения проверок необходимо перейти к установке Сканер-ВС (п. 3.2 настоящего документа).

3.1.1 Проверка комплектности

Проверка комплектности Сканер-ВС производится сравнением комплектности предъявленного оператору экземпляра Сканер-ВС с комплектностью, указанной в НПЕШ.00606-01 30 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Формуляр».

Сканер-ВС считается прошедшим проверку, если его комплектность соответствует комплектности, указанной в НПЕШ.00606-01 30 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Формуляр».

3.1.2 Проверка контрольных сумм

Проверка соответствия контрольных сумм дистрибутива Сканер-ВС производится сравнением контрольных сумм, указанных в НПЕШ.00606-01 30 «Программный комплекс «Средство анализа защищенности «Сканер-ВС». Формуляр», контрольным суммам, вычисленным оператором.

Результаты проверки считаются положительными в случае, если полученная контрольная сумма установочного носителя изделия соответствует контрольной сумме установочного носителя Сканер-ВС, представленной в документе НПЕШ.00023-01 30 «Сканер-ВС. Формуляр».

Контрольные суммы, указанные в НПЕШ.00023-01 30 «Сканер-ВС. Формуляр», фиксируются с помощью программы фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.2), сертификат № 1548 выдан ФСТЭК России 15.01.2008, по алгоритму «Уровень-1, программно».

3.2 Установка и первичная настройка Сканер-ВС

3.2.1 Установка и запуск Сканер-ВС в стандартном режиме

Установка Сканер-ВС в стандартном режиме происходит при помощи встроенного системного терминала «Fly» ОС типа Astra Linux.

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

- скопировать полученный архив, содержащий необходимые для установки Сканер-ВС компоненты, в любую удобную папку системы;
- запустить терминал «Fly» (рис. 1);

Запуск терминала «Fly»

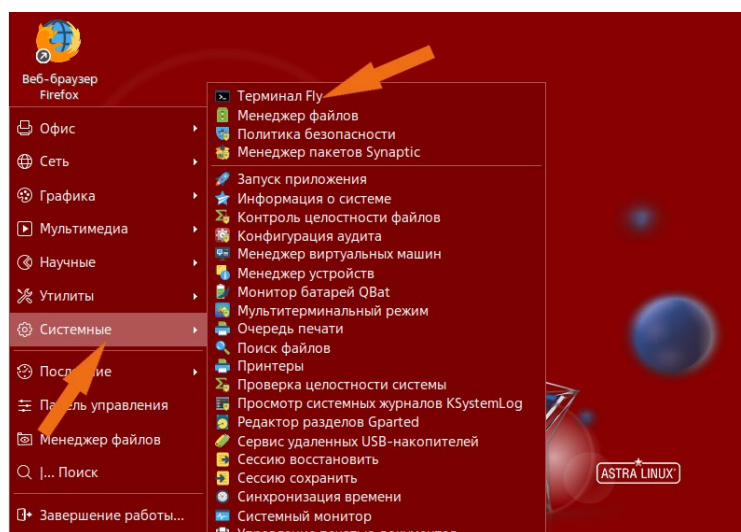


Рис. 1

– войти в учетную запись «root» рабочей станции, для чего в командной строке ввести следующую команду и нажать ввод:

```
sudo su
```

– ввести пароль для учетной записи «root» (рис. 2);

Запрос пароля от учетной записи «root»

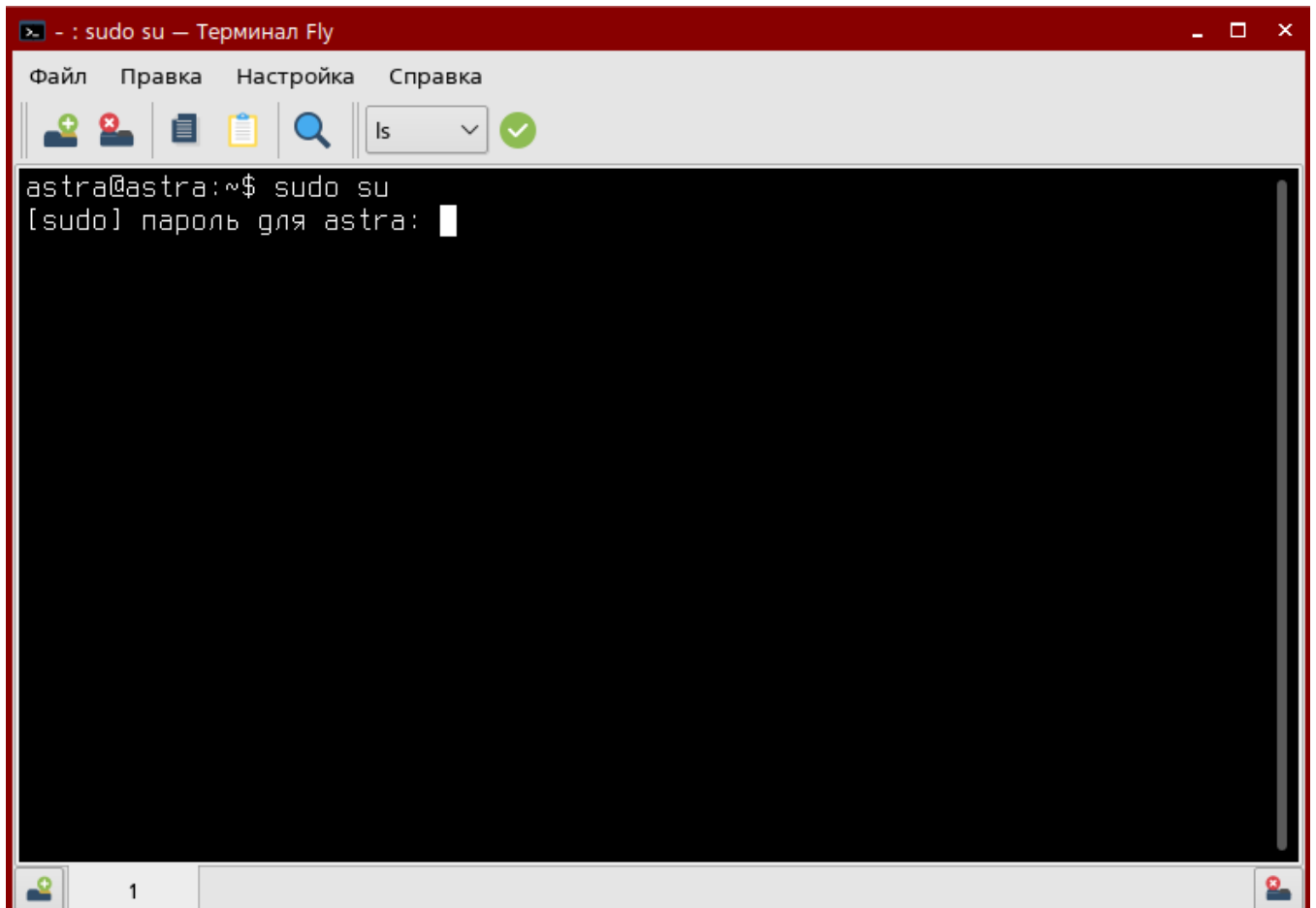


Рис. 2

– после ввода пароля и успешной авторизации с учетной записью «root» в окне терминала «Fly» отобразятся изменения, связанные с тем, от лица какой учетной записи подаются команды (рис. 3);

Успешная авторизация для учетной записи «root»

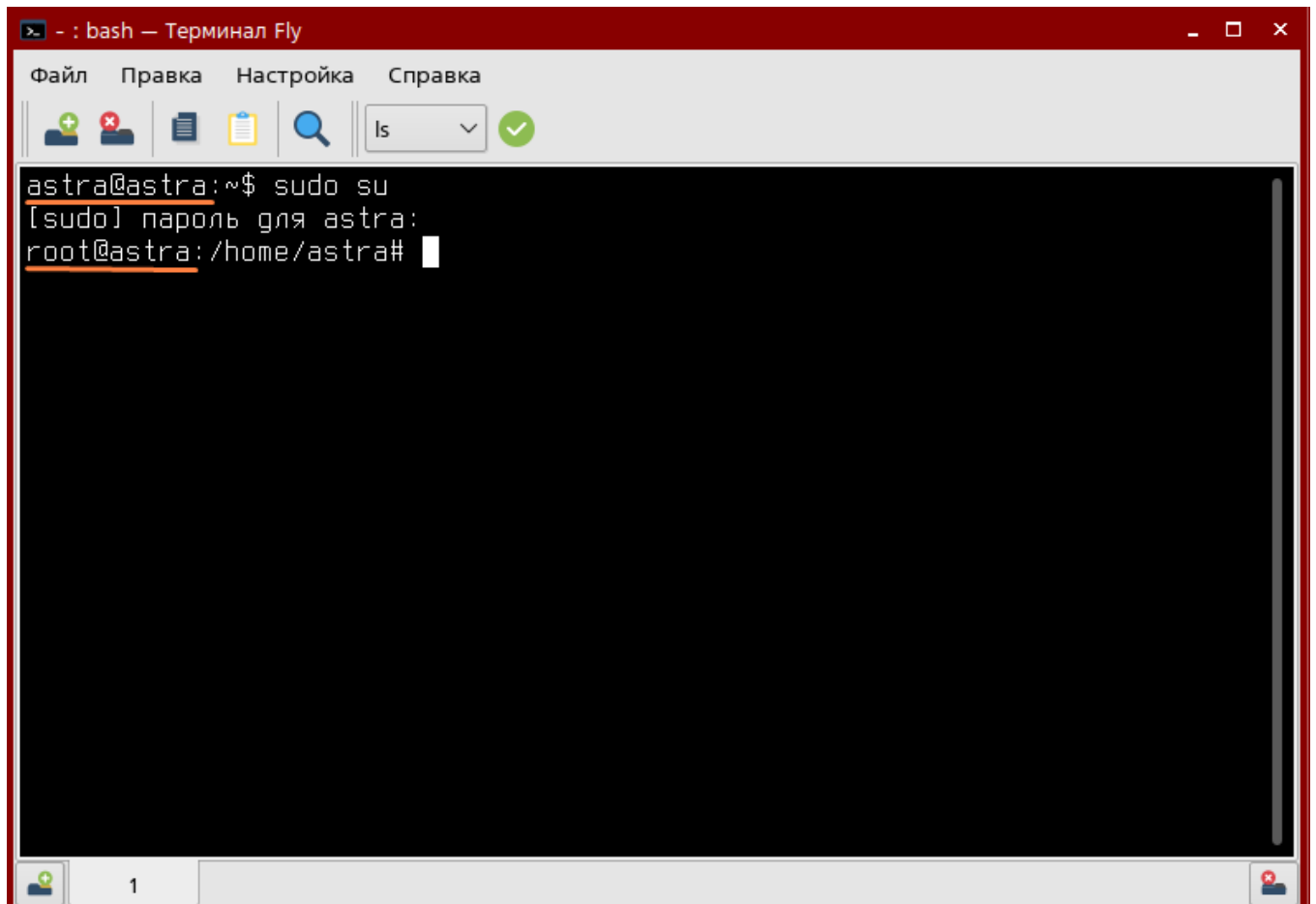


Рис. 3

В случае ввода неверного пароля в окне терминала «Fly» отобразится сообщение «Попробуйте еще раз.». После третьей неудачной попытки авторизации в учетной записи «root» в окне терминала снова отобразится учетная запись пользователя и сообщение «3 incorrect password attempts» (рис. 4).

Авторизация для учетной записи «root» не пройдена

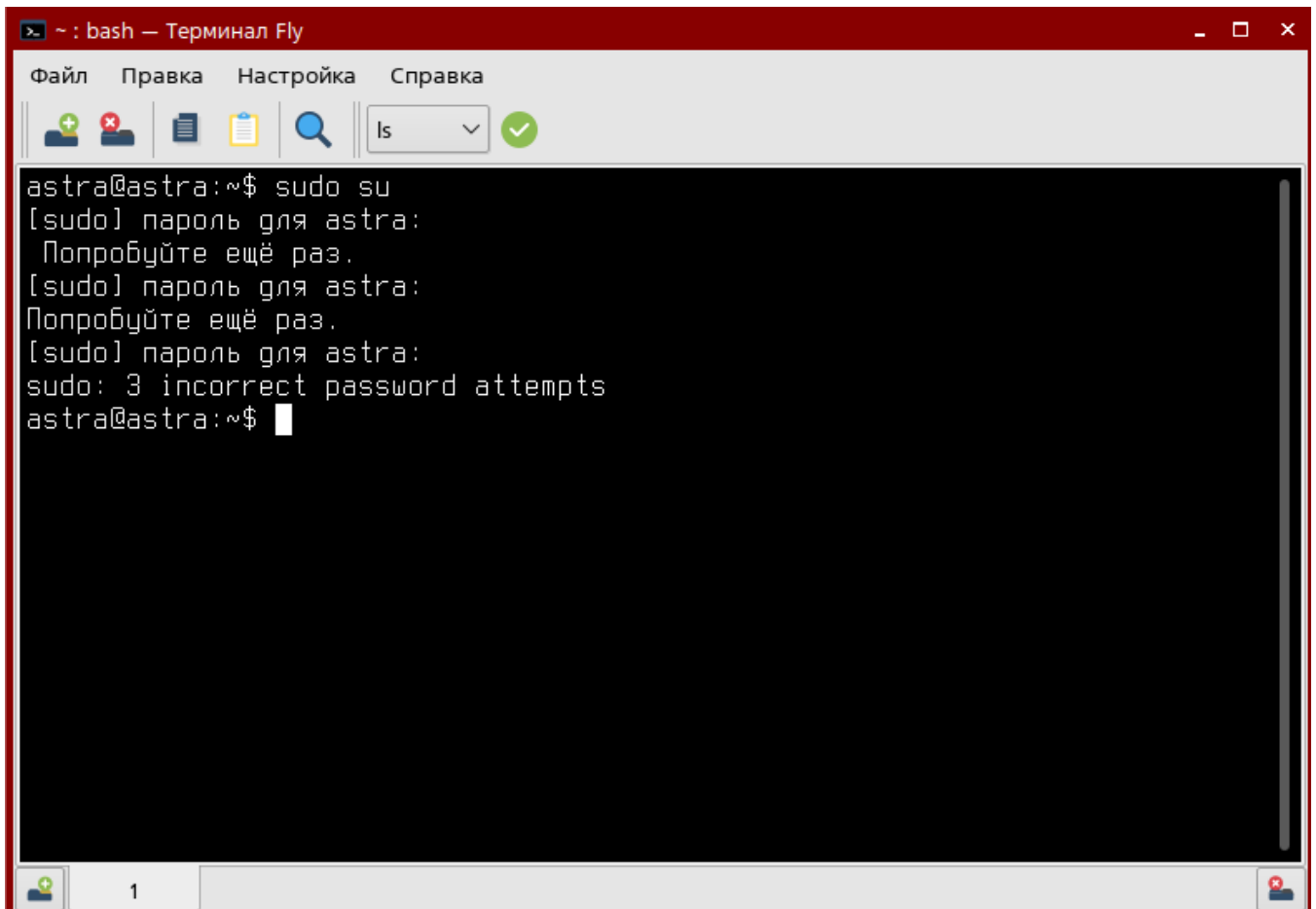


Рис. 4

– перейти в каталог, в который был скопирован архив с файлами Сканер-ВС, для чего необходимо использовать следующую команду:

```
cd /home/astra/Scanner
```

где `cd` – команда перехода к каталогу,

`/home/astra/scanner` – путь к каталогу, в который был скопирован архив с файлами Сканер-ВС;

– распаковать архив с необходимыми для установки компонентами с помощью следующей команды:

```
sh scanner.run
```

– дождаться завершения распаковки архива;

- перейти в созданную папку «pkg»;
- убедиться в наличии пакетов для установки Сканер-ВС и файла лицензии в данном каталоге с помощью команды `ls`. После ввода команды, на экране терминала «Fly» должны отобразиться файлы, которые были распакованы из архива Сканер-ВС (рис. 5);

Проверка наличия необходимых пакетов

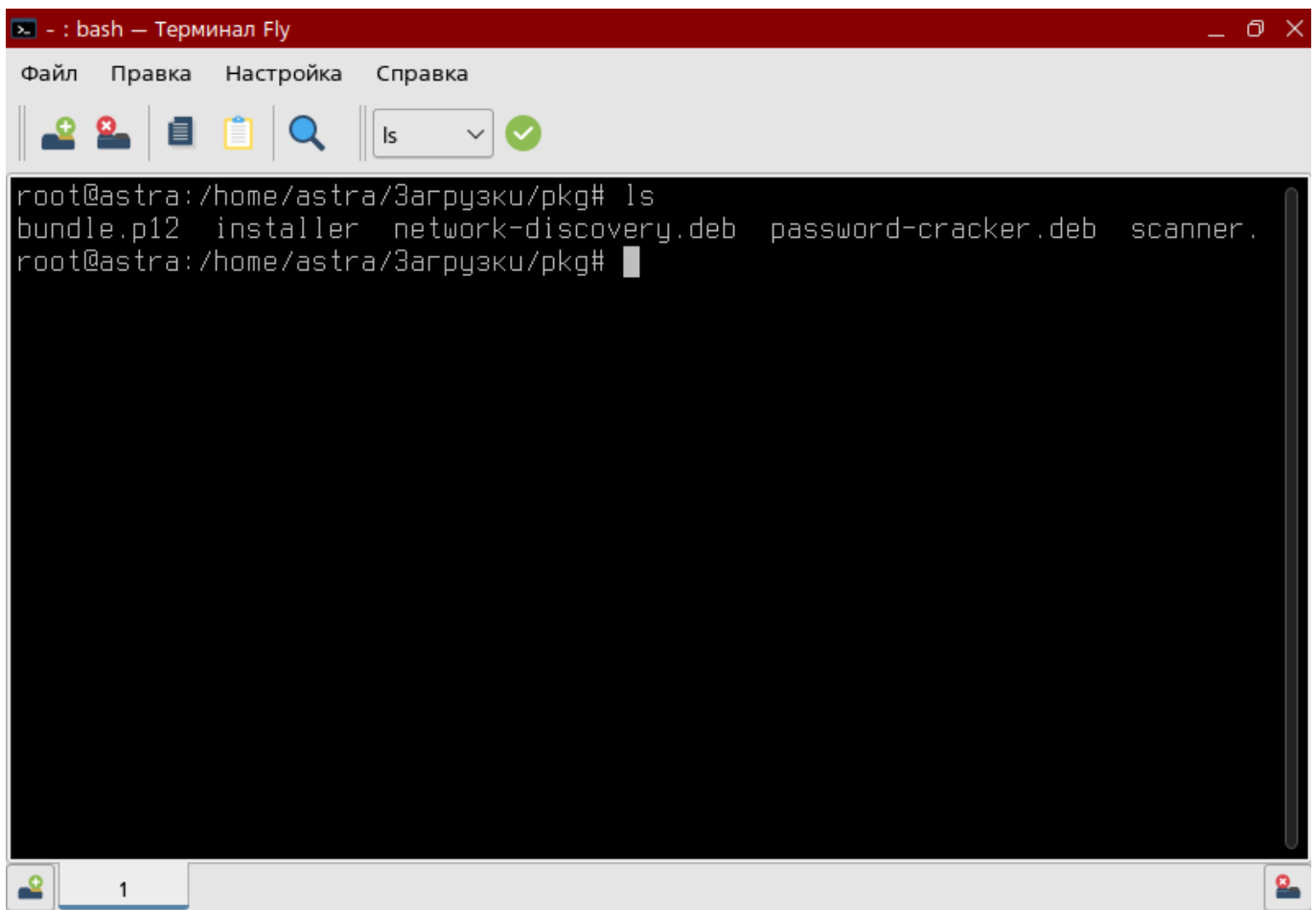


Рис. 5

- запустить установку Сканер-ВС с помощью следующей команды:

```
./installer install
```

- дождаться завершения установки Сканер-ВС.

3.2.2 Установка и запуск Сканер-ВС на RPM-based ОС

Установка Сканер-ВС на RPM-based ОС происходит при помощи встроенного системного терминала.

Для установки и запуска Сканер-ВС на RPM-based ОС необходимо выполнить следующие действия:

- 1) скопировать установочный архив с расширением «.run» с установочного носителя в файловую систему ОС;
- 2) перейти в папку, в которую был скопирован архив и установить права на выполнение с помощью следующей команды:

```
sudo chmod +x scanner.run
```

- 3) распаковать установочный архив с Сканер-ВС. Команды должны выполняться от имени учетной записи суперпользователя ОС:

```
sudo bash scanner.run -noexec
```

- 4) далее необходимо перейти в каталог с распакованным ранее установочным архивом с помощью команды `cd pkg` и скопировать полученный файл лицензии с названием «license.lic» в каталог «var/lib/echelon/0/scanner/license.lic»;

- 5) далее в каталоге с распакованным ранее установочным архивом запустить установку RPM-пакета с помощью команды:

```
sudo dnf install -y *.rpm # Для RedOS  
# ИЛИ  
sudo rpm -i *.rpm # Для ALT Server
```

Примечание. При существовании программных зависимостей может потребоваться установка дополнительного пакета «libsmbclient». Данный пакет можно установить с помощью следующей команды:

```
sudo apt-get update && sudo apt-get install libsmbclient -y
```

- 6) после завершения установки Сканер-ВС необходимо проверить статус службы Сканер-ВС с помощью команды:

```
sudo systemctl status scanner
```

7) по умолчанию для пользователя «**root**» пароль «**admin**» но если данный пароль не подходит необходимо скопировать строку после = и использовать как пароль:

```
sudo cat /var/lib/echelon/0/scanner/secrets.env | grep  
PAUTH_SERVER_ROOT_PASSWORD
```

Примечание. При необходимости смены пароля необходимо удалить файл «`pauth.*`» командой `sudo rm -rf /var/lib/echelon/0/scanner/pauth.*` и перезапустить сервис используя команду `sudo systemctl restart scanner.service`.

8) далее необходимо перезапустить систему с помощью команды:

```
sudo reboot
```

После успешной установки веб-интерфейс Сканер-ВС должен стать доступен по следующим адресам:

- `https://localhost` – если настроен локальный доступ;
- `https://your-hostname` – если настроен *hostname*;
- `https://IP-адрес`.

4. КОНФИГУРИРОВАНИЕ СКАНЕР-ВС

ВНИМАНИЕ! После внесения любых изменений в конфигурационный файл Сканер-ВС необходимо выполнить перезапуск его сервиса с помощью команды `systemctl restart scanner`

В процессе установки Сканер-ВС в файловой системе АРМ создается необходимый для его функционирования конфигурационный файл «scanner.yml». Конфигурационный файл «scanner.yml» сохраняется в каталоге /var/lib/echelon/0/scanner.

Примечания:

1. При установке Сканер-ВС с возможностью его использования под разными уровнями конфиденциальности дополнительно создается еще три конфигурационных файла «scanner.yml» для уровней конфиденциальности от 1 до 3, расположенных в каталогах /var/lib/echelon/1/scanner, /var/lib/echelon/2/scanner и /var/lib/echelon/3/scanner соответственно.

2. Конфигурирование Сканер-ВС при функционировании под разными уровнями конфиденциальности однотипно, однако, стоит учитывать, что изменения в одном из конфигурационных файлов «scanner.yml» **не приводят** к изменениям в остальных подобных файлах.

4.1 Описание конфигурационного файла «scanner.yml»

Конфигурационный файл «scanner.yml» состоит из следующих секций, описание параметров которых приведено в таблице 4:

- license – путь к файлу лицензии;
- logger – секция параметров, отвечающая за запись регистрируемых событий информационной безопасности во внутренние ресурсы рабочей станции, на базе которой функционирует Сканер-ВС;
- sysloger – секция параметров, отвечающая за отправку регистрируемых событий информационной безопасности в SIEM системы;
- http – секция параметров, отвечающая за настройки http-сервера Сканер-ВС;

- databases – секция параметров, содержащая настройки, связанные с используемыми Сканер-ВС базами данных;
- connection-policy – секция параметров, отвечающих за настройки политик проведения попыток повторного подключения к сервисам;
- services – секция параметров, отвечающая за настройки, определяющие взаимодействие http-сервера Сканер-ВС с внутренними сервисами;
- audit-params – секция параметров, отвечающая за множественный сетевой запуск правил аудита и указание языковой настройки целевой машины;
- crack-params – секция параметров, отвечающих за настройки запуска задачи типа «Подбор паролей», описанной в НПЕШ.00023-01 34 «Сканер-ВС. Руководство оператора»;
- exec-retry – секция параметров, отвечающих за настройку политик отправки команд, выполняемых на активах исследуемой сети при проведении задач Сканер-ВС, описанных в НПЕШ.00023-01 34 «Сканер-ВС. Руководство оператора»;
- secrets – секция параметров, отвечающих за настройку мастер ключа, на основании которого генерируются пары ключей для секретов, описанных в НПЕШ.00023-01 34 «Сканер-ВС. Руководство оператора»;
- kerberos – секция, содержащая один параметр, отвечающий за месторасположение конфигурационного файла, используемого для настройки удаленного подключения к узлам исследуемой сети, находящихся в доменной зоне с использованием сервера аутентификации Kerberos;
- parallelism – секция, содержащая один параметр, определяющий коэффициент параллелизма выполнения задач;
- vulns-impact-score – секция параметров, отвечающая за формулу расчета влияния уязвимостей на ИС;
- tuning – секция параметров, отвечающая за добавление/удаление предустановленных пакетов iso-образа, переменных запуска системы iso.

Т а б л и ц а 4 – Параметры конфигурационного файла «scanner.yml»

Секция	Подсекция	Параметр (строка)	Значение по умолчанию	Описание подсекции/параметра
license	—		/var/lib/echelon/0/scanner /license.lic	Указывает путь к файлу лицензии
logger	sink		stdout	Указывает адресат отправки регистрируемых событий
	format		color	Формат передачи регистрируемых событий
	levels		-info -warn -error -panic -fatal	Типы регистрируемых событий
syslogger	sink		"syslog:tcp://localhost:49000"	Указывает адресат отправки регистрируемых событий
	levels		all	Типы регистрируемых событий
http	url		0.0.0.0	Адрес, на котором запускается http сервер Сканер-ВС
	ttl		24h0m0s	Время, в течении которого хранятся данные cookie текущей сессии. По истечении данного времени произойдет автоматический разрыв текущей сессии.
	cookiesecure		false	Включение/Отключение атрибута secure для хранящихся данных cookie
	cors	Проверка адресов, по которым обращаются к http серверу Сканер-ВС		
		enabled	true	Включение/Отключение проверки адресов
	cors	allowedorigins	https://IP-адрес рабочей станции http://IP-адрес рабочей станции https://localhost http://localhost	Список адресов, по которым доступен Сканер-ВС

Секция	Подсекция	Параметр (строка)	Значение по умолчанию	Описание подсекции/параметра
http	tls	Настройки шифрования для http-сервера Сканер-ВС		
		disable	false	Включение/Отключение шифрования
		serverName	scanner-server	Имя сервера
		trustedCa	/var/lib/echelon/0/scanner/certs/ca.pem	Путь к корневому сертификату Сканер-ВС
		cert	/var/lib/echelon/0/scanner/certs/server.pem	Путь к сертификату сервера
		certKey	/var/lib/echelon/0/scanner/certs/server-key.pem	Путь к закрытому ключу RSA сертификата сервера
		systemPool	false	Включение/Отключение опции добавления системных сертификатов к корневому сертификату Сканер-ВС
		minVersion	"1.3"	Минимальная версия tls
	clientAuth		false	Включение/Отключение проверки сертификата авторизации клиента
databases	scannerdb	Основная база данных, содержащая генерируемую в процессе функционирования Сканер-ВС информацию		
		path	/var/lib/echelon/0/scanner/scanner.db	Путь к основной базе данных Сканер-ВС
		backup-path	/var/lib/echelon/0/scanner/scanner.db.backup	Путь к резервной копии основной базы данных Сканер-ВС
		wal-version	wal2	Параметр журнала, в который изменения в базе пишутся до их применения, чтобы обеспечить восстановление после сбоев. Режим «wal1»- базовый, поддерживает одного писателя и читателя, а wal2 – улучшенная версия без -shm файла, позволяющая больше параллелизма и стабильности в сетевых средах

Секция	Подсекция	Параметр (строка)	Значение по умолчанию	Описание подсекции/параметра
databases	vulndb	База данных, представляющая собой встроенную базу уязвимостей Сканер-ВС		
		path	/var/lib/echelon/0/scanner/vuln.db	Путь к базе уязвимостей Сканер-ВС
		backup-path	/var/lib/echelon/0/scanner/vuln_old.db	Путь к резервной копии базы уязвимостей Сканер-ВС
	customvuln db	База данных, представляющая собой пользовательскую базу уязвимостей Сканер-ВС		
		path	/var/lib/echelon/0/scanner/customvuln.db	Путь к пользовательской базе уязвимостей Сканер-ВС
		backup-path	/var/lib/echelon/0/scanner/customvuln.db.backup	Путь к резервной копии пользовательской базы уязвимостей Сканер-ВС
connection-policy	attempts		3	Количество попыток
	duration		20s	Длительность попытки
services	pauth-server	Подсекция настроек сервера аутентификации		
		id	"da62d3bb-9dfb-4dcd-b9d8-704bf887b29e"	Идентификатор сервера аутентификации
		database	file:/var/lib/echelon/0/scanner/pauth.sqlite	Путь к базе данных зарегистрированных операторов Сканер-ВС
		session-ttl	24h	Продолжительность сессии
		default-role	"user"	Роль оператора по умолчанию
		min-password-entropy-bits	"70"	Минимальная энтропия задаваемого пароля (см. п. 4.2 настоящего руководства)
		root-password	"mn9NRmcJakbfZRYhTMieb7nNRF9hJ9qFwg5jCkm iudLpiNJ5pNhqgLC7LzDv5d9jT5mbT4Vo "	Хэш-сумма пароля учетной записи «root»
		roles	– admin – user	Роли операторов Сканер-ВС
		Подсекция настроек правил доступа для операторов с разными ролями		
		rules	"user": - "/app/*.*" - "/echelon.pauth_server.user.v1.UserService/*.*" - "/api/*.*" - "/echelon.scanner.*"	Правила доступа для оператора с ролью «Пользователь»

Секция	Подсекция	Параметр (строка)	Значение по умолчанию	Описание подсекции/параметра
services	pauth-server	"admin"	– "/".*"	Правила доступа для оператора с ролью «Администратор»
	update-service	Обновление БД уязвимостей		
		max-update-memory-mi-byte	60	Максимальный объем оперативной памяти (в МБ), используемой для обработки части файла при ручном обновлении без записи на диск. Увеличение значения может ускорить обновление, но повысит нагрузку на память
	connector	url	https://updates.etecs.ru	Путь к базе данных уязвимостей для обновлений
audit-params	local-sessions-per-account		5	Максимальное количество одновременно выполняемых локальных сессий аудита
	remote-sessions-per-account		1	Максимальное количество одновременно выполняемых удалённых сессий аудита
	target-locale		C.UTF-8	Параметр для заданной локализации (языковые и региональные настройки), используемой в процессе аудита (особенно необходимо для корректной обработки текстов)
crack-params	time-per-login		0	Время ожидания на попытку входа во все потоки
	disable-redo-on-failed-attempts		false	Флаг повторения запроса при неудачной попытке
exec-retry	initial-interval		100s	Длительность первой попытки подключения к узлу исследуемой сети

30
НПЕШ.00606-01 91-1

Секция	Подсекция	Параметр (строка)	Значение по умолчанию	Описание подсекции/параметра
exec-retry	max-interval		200s	Максимальное значение, до которого может увеличиться длительность попытки подключения к узлу исследуемой сети
	max-elapsed-time		600s	Максимальное время, выделяемое на все попытки подключения к узлу исследуемой сети
	max-retry		3	Максимальное количество попыток подключения
	max-exec-time		10m	Максимальное значение времени, за которое Сканер-ВС должно получить ответ о выполнении команд от узла исследуемой сети
secrets	salt		age1fsyarstxhcy2uxv40524a6944kjufnpnqmdsa40pfsqfnht9sksxqglx	Дополнительное значение, участвующее в формировании защищённого пароля, повышающее устойчивость к подбору
	password		AGE-SECRET-KEY-1DJZL0AFG6HS5JDHZCYM2FVRM80C9VTLNWTV65DHVJ8XMRFUTAK0SPNUMAN	Зашифрованное значение, используемое в системе для защиты конфиденциальных данных
kerberos	path		/var/lib/echelon/0/scanner/krb	Путь к конфигурационному файлу с настройками аутентификации kerberos
parallelism	coeff		40	Параметр, определяющий коэффициент параллельности выполнения задач (параллелизм)
	adaptive-concurrency		Параметры, определяющие настройки адаптивного управления параллельности выполнения задач	
	adaptive-concurrency	enabled	true	Включение/отключение адаптивного управления параллельности выполнения задач

Секция	Подсекция	Параметр (строка)	Значение по умолчанию	Описание подсекции/параметра
parallelism	adaptive-concurrency	min-cpu-threshold	40.0	Минимальное пороговое значение (CPU), на которое опирается алгоритм адаптивного управления параллелизмом
		max-cpu-threshold	60.0	Максимальное пороговое значение (CPU), на которое опирается алгоритм адаптивного управления параллелизмом
		max-ram-threshold	80.0	Максимальное пороговое значение (RAM), на которое опирается алгоритм адаптивного управления параллелизмом
		proportional-coefficient	0.25	Пропорциональный коэффициент, влияющий на реагирование выхода значения целевого показателя (CPU) из окна
		integral-coefficient	0.01	Интегральный коэффициент, позволяющий накапливать отклонения показателя (выход из окна) и влиять на корректирующие действия алгоритма
		derivative-coefficient	0.05	Производный коэффициент, позволяющий оценивать скорость изменения (роста/упадка) показателя и влиять на корректирующие действия алгоритма
vulns-impact-score	weights	Весовые коэффициенты		
		k	0.4	Вес для компонента K
		l	0.2	Вес для компонента L
		p	0.4	Вес для компонента P
vulns-impact-score	scores	Оценки показателей		
		k-score	critical-processes-value: "1.0"	Критические процессы (бизнес-процессы, функции)
			servers-value: "0.8"	Серверы
			telecommunication-value: "0.8"	Телекоммуникационное оборудование

Секция	Подсекция	Параметр (строка)	Значение по умолчанию	Описание подсекции/параметра
vulns-impact-score	scores	k-score	automated-workplaces-value: "0.5"	Автоматизированные рабочие места
			other-value: "0.5"	Другие компоненты
		l-score	gt70-value: "1.0"	Более 70% компонентов подвержены уязвимости
			gte50-value: "0.8"	50-70% компонентов подвержены уязвимости
			gte10-value: "0.6"	10-50% компонентов подвержены уязвимости
			lt10-value: "0.5"	Менее 10% компонентов подвержены уязвимости
		p-score	available-from-net-value: "1.0"	Доступно из сети Интернет
			unavailable-from-net-value: "0.5"	Недоступно из сети Интернет
tuning	usb-since-flag		"1 day ago"	Настройка интервала просмотра истории подключения (и т.д.) устройств USB

4.2 Настройка интеграции Сканер-ВС с LDAP сервером

В Сканер-ВС предусмотрена возможность интеграции сервера аутентификации LDAP. Настройка взаимодействия Сканер-ВС с LDAP сервером производится путем внесения изменений в основной конфигурационный файл «scanner.yml», а именно внесением следующего блока настроек в подсекцию «pauth-server» секции «services»:

```
auth-providers:
  - kind: internal
    priority: 10
    enabled: true
  - kind: ldap
    priority: 20
    enabled: true
    ldap:
      url: ldap://url-адрес сервера LDAP
      search-dn:
      search-password:
```

```

base-dn:
uid:
scope: 2
connection-timeout: 30
tls:
    enabled: false
group-conf:
    filter: objectclass=Group
    membership-attribute: memberof
group-roles:
    - group-to-org-role:
        group-dn:
        org-role: admin

```

Описание добавляемых параметров приведено в таблице 5.

Т а б л и ц а 5 – Параметры интеграции с LDAP сервером

Параметр (строка)	Описание подсекции/параметра
auth-providers	Указывает адресат отправки регистрируемых событий
kind	Вид используемого сервера аутентификации
priority	Приоритет проверки данных аутентификации, введенных оператором
enabled	Включение/выключение интеграции с указанным сервером аутентификации
ldap	Настройки интеграции LDAP сервера
url	Url-адрес для подключения к LDAP серверу
search-dn	Логин учётной записи, используемой для выполнения поисковых запросов на сервере LDAP
search-password	Пароль учётной записи, используемой для выполнения поисковых запросов на сервере LDAP
base-dn	Базовый элемент, с которого начинается поиск пользователей и групп
uid	Атрибут, используемый для уникальной идентификации пользователя в LDAP
scope	Уровень охвата поиска: 0 – поиск только на уровне базового элемента, 1 – поиск на уровне базового элемента и на уровне ниже, 2 – рекурсивный поиск по всем уровням ниже уровня базового элемента
connection-timeout	Время ожидания подключения к LDAP-серверу в секундах
tls	Настройки шифрования подключения к серверу
enabled	Включение/выключение шифрования
group-conf	Настройки для работы с группами в LDAP
filter	Фильтр для определения LDAP-групп

Параметр (строка)	Описание подсекции/параметра
membership-attribute	Атрибут, указывающий на принадлежность пользователя к группе
group-roles	Настройки ролей, которые назначаются пользователям на основе их принадлежности к LDAP-группам
group-to-org-role	Отображение LDAP-группы на роль в организации
group-dn	Наименование группы в LDAP, которое используется для определения принадлежности пользователя к определённой группе
org-role	Роль в организации, которая будет назначена пользователям, являющимся членами указанной группы
Примечание. Для различных серверов аутентификации LDAP может потребоваться указание дополнительных параметров в подсекции «auth-providers» для используемого LDAP сервера.	

4.3 Настройка интеграции доменной зоны kerberos

Для осуществления удаленного подключения к узлам исследуемой сети, находящимся в доменной зоне, настроенной с использованием сервера аутентификации Kerberos необходимо создать дополнительный конфигурационный файл «krb5.conf» в каталоге /var/lib/echelon/0/scanner/krb.

Пример создаваемого конфигурационного файла:

```
[realms]
EHELON.NET = {
    kdc =
    kdc =
    admin_server =
}

[domain_realm]
.ehelon.net =
ehelon.net =
```

Описание параметров конфигурационного файла «krb5.conf» приведено в таблице 6.

Т а б л и ц а 6 – Параметры интеграции доменной зоны Kerberos

Параметр (строка)	Описание подсекции/параметра
[realms]	Секция, описывающая области аутентификации сервера Kerberos

Параметр (строка)	Описание подсекции/параметра
EHELON.NET	Имя области аутентификации (имя домена заглавными буквами). Необходимо указать актуальное имя
kdc	Основной сервер центра рассылки ключей для указанного домена
kdc	Резервный сервер центра рассылки ключей для указанного домена
admin_server	Сервер, предоставляющий административный доступ к указанному домену
[domain_realm]	Секция, обеспечивающая перевод с доменного имени или имени хоста в имя области Kerberos
ehelon.net	Параметр указывает какую область аутентификации использовать дочерним доменам ehelon.net
ehelon.net	Параметр указывает какую область аутентификации использовать домену ehelon.net

4.4 Назначение параметров окружения службы «Scanner»

Для назначения параметров окружения службы «Scanner» необходимо воспользоваться следующими командами:

– `SCANNER_RESTART_TIMEOUT` – определяет интервал времени, по истечении которого служба «Scanner» может быть автоматически перезапущена при необходимости. Значение задаётся в формате длительности, например: 5m (5 минут), 1h (1 час);

– `SCANNER_RESTART_DISK_SPACE_THRESHOLD` – устанавливает порог использования дискового пространства (в процентах), при превышении которого служба «Scanner» может быть автоматически перезапущена. Это обеспечивает своевременное освобождение ресурсов и предотвращение возможных сбоев, связанных с нехваткой дискового пространства.

4.5 Настройка сложности пароля для аутентификации операторов

При добавлении новых операторов Сканер-ВС с ролью «Пользователь» необходимым является создание пароля для аутентификации этого оператора. Помимо создания операторов с ролью «Пользователь», необходимым условием безопасного функционирования Сканер-ВС является смена предустановленного пароля оператора с ролью «Администратор».

В Сканер-ВС предусмотрена настройка сложности задаваемого пароля для аутентификации операторов.

Для настройки сложности задаваемого пароля необходимо воспользоваться встроенной утилитой «Midnight Commander» ОС типа AstraLinux. Далее в «Midnight Commander» необходимо перейти к каталогу, в котором находится конфигурационный файл «config.yaml». При установке данный файл сохраняется в каталоге /var/lib/echelon/0/scanner/scanner.yaml.

Необходимо открыть данный файл для редактирования и найти в нем строку «MinPasswordEntropyBits». Значение в данной строке и отвечает за уровень сложности задаваемых для операторов паролей.

Сила пароля характеризуется энтропией – числовым представлением количества случайности, которая содержится в пароле.

По своей сути переменная «MinPasswordEntropyBits», которая принимает заданное оператором значение, является мерой энтропии пароля и измеряется в битах. Чем выше значение указывает оператор, тем выше энтропия пароля, и, соответственно, сама его сложность.

Энтропия пароля рассчитывается по формуле:

$$\log_2(\text{'количество разных символов'}^{\text{'длина пароля'}})$$

или

$$\text{'длина пароля'} \cdot \log_2(\text{'количество разных символов'})$$

где 'длина пароля' – количество символов в задаваемом пароле;

– $\log_2(\text{'количество разных символов'})$ – удельная энтропия используемого класса символов;

– 'количество разных символов' – количество разных символов в используемом алфавите (например, для алфавита прописных букв латиницы – 26).

Для настройки на минимальную рекомендуемую сложность задаваемого пароля необходимо задать значение энтропии пароля в пределах 47-51 бит энтропии в зависимости от используемых классов символов.

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

- пароль должен содержать латинские буквы обоих регистров: как заглавные (A-Z), так и строчные (a-z);
- в пароле обязательно должна присутствовать хотя бы одна цифра (0-9);
- пароль должен содержать минимум один специальный символ, например: !, @, #, \$, %, ^, &, *, и т. д.;
- минимальная длина пароля – не менее 9 символов;
- рекомендуется избегать последовательностей одинаковых символов подряд;
- запрещается использовать пробелы и управляющие символы;
- рекомендуется не использовать легко угадываемые слова, такие как «password», «123456», имя пользователя и т.д.

4.6 Создание нового администратора

Для создания нового администратора в Сканер-ВС необходимо выполнить следующее:

- 1) перейти в рабочий каталог сканера:

```
cd /var/lib/echelon/0/scanner/
```

- 2) проверить наличие ПО sqlite3. Если программа не установлена, выполните следующие действия для установки её с диска:

- a) откройте файл `/etc/apt/sources.list` с правами суперпользователя;

б) раскомментируйте строку с **deb cdrom:...**;

в) вставьте установочный диск Astra Linux и выполните команды:

```
sudo apt update
sudo apt install sqlite3
```

3) сгенерировать хеш-пароль, используя следующие параметры:

- Алгоритм: Bcrypt;
- Фактор стоимости (Rounds/Cost Factor): 10 или 12.

Для генерации хеша можно воспользоваться **любым** доступным и доверенным сторонним решением (включая онлайн-сервисы, пакеты из удалённых репозиторий), поддерживающим «bcrypt». В итоге вы должны получить строку хеша, похожую на данный пример: \$2a\$10\$QCSBZniZ1/ynLKHkBmE9EuwZzEWZHiAFs/GdygaAUOPC6fTEtVCYu. Скопируйте её.

4) далее подключиться к базе данных:

```
sqlite3 'pauth.sqlite?_pragma=busy_timeout(10000)&_pragma=journal_mode(wal)'
```

5) выполнить следующий SQL-запрос, чтобы создать нового пользователя с обязательными полями (важно – **заменить хеш на свой**):

```
-- Добавляем пользователя superadmin
INSERT INTO users (
    id, login, password_hash, name, surname, patronymic, phone, email,
    state, provider
) VALUES (
    lower(hex(randomblob(4)) || '-' ||
        hex(randomblob(2)) || '-' ||
        '4' || substr(hex(randomblob(2)),2) || '-' ||
        substr('AB89',abs(random()) % 4 + 1,1) ||
        substr(hex(randomblob(2)),2) || '-' ||
        hex(randomblob(6))),
    'superadmin',
    '$2a$12$u3PUEtXAjNLl00hNHBX9Qe0oaZEJDZxveaJBYaqZl07f3hTgBs1Xe', --
    хеш для "superadmin"
    'Иван', -- имя
```

```
'Иванов',          -- фамилия
'Иванович',        -- отчество
'+79990000000',    -- телефон
'admin@example.com', -- email
'STATE_ACTIVE',    -- статус
'internal'         -- тип пользователя
);

-- Назначаем роль администратора (role_id = 1)
INSERT INTO user_roles (user_id, role_id)
SELECT id, 1
FROM users
WHERE login='superadmin';
```

б) для проверки выполнения воспользуйтесь следующим:

```
SELECT u.id, u.login, u.name, u.surname, u.email, r.name AS role
FROM users u
JOIN user_roles ur ON u.id = ur.user_id
JOIN roles r ON ur.role_id = r.id
WHERE u.login='superadmin';
```

7) после вы должны увидеть нового пользователя с ролью admin;

8) далее необходимо выйти из sqlite3, используя команду `.quit`;

9) чтобы изменения вступили в силу, перезапустите сервис Сканера-ВС:

```
systemctl restart scanner
```

После выполнения данной инструкции пользователь «superadmin» с паролем «superadmin» создан и имеет роль администратора.

4.7 Смена паролей системных учетных записей

Необходимым условием безопасного функционирования Сканер-ВС является смена предустановленных паролей системных учетных записей.

Учетные записи Сканер-ВС, относящиеся к системным:

- RootPassword;
- пароли учетных записей баз данных;

– пароль, используемый для шифрования паролей.

Для смены перечисленных паролей необходимо воспользоваться встроенной утилитой «Midnight Commander» ОС типа AstraLinux. В «Midnight Commander» необходимо перейти к каталогу, в котором находятся соответствующие конфигурационные файлы. Соответствие изменяемых паролей, место расположение конфигурационных файлов и их описание приведено в таблице 7.

Т а б л и ц а 7 – Описание паролей системных учетных записей

Наименование	Конфигурационный файл	Раздел конфигурационного файла	Расположение конфигурационного файла	Описание
RootPassword	config.yaml	RootPassword	/var/lib/echelon/0/scanner/scanner.yaml	Пароль суперпользователя Сканер-ВС
pub	scanner.yaml	secrets	etc/echelon/scanner	Пароль, используемый для шифрования паролей системных учетных записей

Для смены пароля суперпользователя Сканер-ВС (RootPassword) необходимо выполнить следующие действия:

1) подготовить и проверить зависимости следующим способом:

а) необходимо перейти в рабочий каталог: `cd /var/lib/echelon/0/scanner;`

б) проверить наличие ПО sqlite3. Если программа не установлена, выполните следующие действия для установки её с диска:

– откройте файл `/etc/apt/sources.list` с правами суперпользователя;

– раскомментируйте строку с **deb cdrom:...**;

– вставьте установочный диск Astra Linux и выполните команды:

```
sudo apt update
sudo apt install sqlite3
```

2) сгенерировать хеш-пароль. Для обновления пароля в базе данных вам потребуется предварительно сгенерировать его хеш, используя следующие параметры:

– Алгоритм: Vcrypt;

– Фактор стоимости (Rounds/Cost Factor): 10.

Для генерации хеша можно воспользоваться **любым** доступным и доверенным сторонним решением (включая онлайн-сервисы, пакеты из удалённых репозиторий), поддерживающим «bcrypt». В итоге вы должны получить строку хеша, похожую на данный пример: \$2a\$10\$QCSBZniZ1/ynLKHkBmE9EuwZzEWZHiAFs/GdygaAUOPC6fTEtVCYu. Скопируйте её.

3) обновить пароль в базе данных следующим способом:

а) подключитесь к базе данных, выполнив следующую команду:

```
sqlite3 'pauth.sqlite?_pragma=busy_timeout(10000)&_pragma=journal_mode(wal)'
```

б) выполните SQL-запрос, подставив ваш сгенерированный хеш вместо «ВАШ_НОВЫЙ_ХЕШ»:

```
update users set password_hash = 'ВАШ_НОВЫЙ_ХЕШ' where login = 'admin';
```

4) чтобы внесённые изменения вступили в силу, перезапустите службу Сканера следующим образом:

```
systemctl restart scanner
```

4.8 Управление сертификатами

Сканер-ВС для своего функционирования использует сертификаты. Во время установки заводские сертификаты распаковываются в папку /var/lib/echelon/0/scanner/certs. В данной папке должны находиться следующие файлы:

- ca-key.pem – закрытый ключ RSA корневого сертификата;
- ca.pem – корневой сертификат;
- client-key.pem – закрытый ключ RSA сертификата клиента;
- client.pem – сертификат клиента;
- server-key.pem – закрытый ключ RSA сертификата сервера;
- server.pem – сертификат сервера.

4.8.1 Генерация пользовательских сертификатов

В Сканер-ВС предусмотрена возможность использования пользовательских сертификатов. Для генерации пользовательских сертификатов необходимо создать конфигурационные файлы для них. В процессе установки Сканер-ВС примеры конфигурационных файлов для сертификатов распаковываются в папку `/usr/share/scanner/certconf`.

В конфигурационных файлах необходимо указать соответствующие типу сертификата секции расширений и указать имя данной секции в поле «`x509_extensions`», заполнить секцию «`dn`» конфигурационного файла данными эксплуатирующей организации. А также указать IP- или DNS-адрес в поле «`subjectAltName`» секций «`v3_ca`» и «`alt_names`». После создания конфигурационных файлов необходимо сгенерировать сертификаты.

Генерация пользовательских сертификатов происходит следующим образом:

- сгенерировать закрытый ключ с помощью команды:

```
openssl genrsa -out ca-key.pem 2048
```

- сгенерировать сертификат для созданного на предыдущем шаге закрытого ключа, используя следующую команду:

```
openssl req -new -x509 -days 365 -config ca.conf -key ca-key.pem -out ca.pem
```

- повторить генерацию закрытого ключа и сертификата для сертификатов клиента и сервиса;

- привести конфигурационные файлы, расположенные в папке **`/var/lib/echelon/0/scanner`** в соответствие новым созданным сертификатам (указать имена и расположение сертификатов);

- перезагрузить сервисы Сканер-ВС, используя следующие команды:

```
systemctl restart scanner
```

5. УДАЛЕНИЕ СКАНЕР-ВС

Для удаления Сканер-ВС с рабочей станции необходимо удалить описанные в п. 3.2.1 настоящего руководства пакеты. Процедура удаления пакетов аналогична процедуре их установки.

Для удаления пакетов необходимо выполнить следующее:

1) остановить службу Сканер-ВС:

```
sudo systemctl stop scanner
```

2) удалить установленный ранее Сканер-ВС:

```
sudo apt remove scanner --purge
```

3) удалить создаваемые при установке каталоги:

```
sudo rm -rf /opt/echelon /etc/echelon /var/lib/echelon
```

4) удалить создаваемый при распаковке архива с установочными файлами каталог:

```
sudo rm -rf /home/astra/pkg, где /home/astra - путь к скопированному архиву с установочными файлами.
```

6. СООБЩЕНИЯ ОПЕРАТОРУ

Тексты сообщений, выдаваемых в ходе функционирования ПК «Сканер-ВС», представлены в таблице 8.

Т а б л и ц а 8 – Сообщения Оператору

Сообщение	Описание
«Доступ запрещен»	Данное сообщение появляется в случае, если учетная запись, с помощью которой оператор пытается пройти авторизацию, не существует либо заблокирована (не активна), а также в случае ввода неверных данных аутентификации
«Пароль не может быть пустым»	Данное сообщение появляется при попытке авторизации в Сканер-ВС с пустым полем «Пароль»
«Логин не может быть пустым»	Данное сообщение появляется при попытке авторизации в Сканер-ВС с пустым полем «Логин»
«Логин не может быть пустым. Пароль не может быть пустым»	Данное сообщение появляется при попытке авторизации в Сканер-ВС с пустыми полями «Логин» и «Пароль» одновременно
«Отчет создан успешно»	Данное сообщение появляется при генерировании нового отчета и сигнализирует об успешном завершении процесса его создания
«Карта сети создана успешно»	Данное сообщение появляется при создании новой карты сети и сигнализирует об успешном завершении процесса ее создания
«Словарь создан успешно»	Данное сообщение появляется при создании нового пользовательского словаря и сигнализирует об успешном завершении процесса его создания
«Удалено успешно»	Данное сообщение появляется в случае успешного создания какого-либо объекта Сканер-ВС
«Обязательное поле»	Сообщение в форме заполнения данных, сигнализирующее о том, что оно обязательно для заполнения
«Ошибка парсинга»	Сообщение в форме заполнения данных, сигнализирующее о том, что данные в нем не соответствуют требуемому формату
«Введенные пароли не совпадают»	Сообщение в форме заполнения данных, сигнализирующее о том, что пароли, введенные в полях «Пароль» и «Повтор пароля» не совпадают

Сообщение	Описание
«Network error»	Данное сообщение появляется в случае разрыва сетевого соединения
«permission denied»	Данное сообщение появляется в том случае, если пользователь Сканер-ВС обращается к функции, недоступной ему настройками ролевой модели разграничения доступа
«Что-то пошло не так»	Данное сообщение появляется в том случае, если по какой-либо причине произошла критическая ошибка в работе Сканер-ВС

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Расшифровка
BIOS	(англ. Basic Input/Output System) – базовая система ввода / вывода
CSV	(англ. <i>Comma-Separated Values</i>) – текстовый формат, предназначенный для представления табличных данных
HTML	(англ. HyperText Markup Language) – стандартизированный язык разметки документов в сети Интернет
ID	(англ. Identification Data) – идентификатор
PDF	(англ. <i>Portable Document Format</i>) – межплатформенный формат электронных документов, разработанный фирмой Adobe Systems с использованием ряда возможностей языка PostScript
TCP	(англ. <i>Transmission Control Protocol</i>) – один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных
UDP	(англ. <i>User Datagram Protocol</i> – протокол пользовательских датаграмм) – один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета
UEFI	(англ. Unified extensible Firmware Interface) – унифицированный расширяемый интерфейс встроенного (базового) программного обеспечения
USB	(англ. <i>Universal Serial Bus</i> – универсальная последовательная шина) – последовательный интерфейс для подключения периферийных устройств к вычислительной технике
АО «НПО Эшелон»	Акционерное общество «Научно-производственное объединение «Эшелон»
АРМ	Автоматизированное рабочее место
ОС	Операционная система
ПО	Программное обеспечение
Сканер-ВС	Программное обеспечение Сканер-ВС
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

ПРИЛОЖЕНИЕ 1.
(ОБЯЗАТЕЛЬНОЕ)

ИНСТРУКЦИЯ ПОДКЛЮЧЕНИЯ К УЗЛУ ИССЛЕДУЕМОЙ СЕТИ
ПО ПРОТОКОЛУ WINRM

Для проведения задач «Инвентаризация» и «Аудит» необходимо активное подключение к узлам исследуемой сети с заведенными учетными записями для этих узлов.

Для корректного подключения к узлу исследуемой сети по протоколу WinRM необходимо произвести предварительную настройку узла исследуемой сети.

1.1. Настройка подключения по протоколу WinRM с помощью поставляемого скрипта

Для настройки необходимо выполнить следующие действия:

- убедиться, что на узле, к которому планируется подключение, установлены powershell 5.1 и .Net framework 4;
- запустить Windows PowerShell от имени администратора;
- выполнить скрипт изначальной настройки WinRM:

```
Powershell.exe -ExecutionPolicy Bypass -File winrm.ps1;
```

– после успешного выполнения данного скрипта становится возможным подключение к узлу исследуемой сети по протоколу WinRM через basic аутентификацию;

Для работы с парами ключей (WinRM KeyPair) необходимо дополнительно выполнить следующие действия:

- скопировать на АРМ оператора, с которого производится управление Сканер-ВС, публичный ключ в формате CER или PEM в файл;

– выполнить скрипт:

```
Powershell.exe -ExecutionPolicy Bypass -File clientCert.ps1 <путь к файлу с ключом> <имя пользователя> <пароль>
```

где <путь к файлу с ключом> – путь к сохраненному файлу, содержащему публичный ключ в формате CER или PEM;

<имя пользователя> и <пароль> –аутентификационные данные, которые будут использоваться для подключения к узлу исследуемой сети по протоколу WinRM;

– после успешного выполнения данного скрипта становится возможным подключение к узлу исследуемой сети по протоколу WinRM с использованием пары ключей WinRM KeyPair.

Примечания:

1. Необходимые для настройки подключения по протоколу WinRM, а также отмены внесенных изменений файлы при установке Сканер-ВС по умолчанию сохраняются в папке `/var/lib/echelon/0/scanner/scripts`.

2. Для установки подключения по протоколу WinRM с использованием пары ключей типа «ЕС P521» в командной строке Windows PowerShell необходимо выполнить следующую команду:

```
Enable-TlsEccCurve nistp521
```

1.2. Ручная настройка подключения по протоколу WinRM для Windows Server 2008 и Windows 7

Для подключения к узлам исследуемой сети, функционирующим на базе старых версий ОС семейства Windows (Windows 7 и Windows Server 2008) по протоколу WinRM необходима их дополнительная настройка.

Для настройки таких узлов исследуемой сети необходимо выполнить следующие действия:

1. Установить обновления для Windows Server 2008 <https://support.microsoft.com/en-us/topic/update-to-add-support-for-tls-1-1-and-tls-1-2-in-windows-server-2008-sp2-windows-embedded-posready-2009-and-windows-embedded-standard-2009-b6ab553a-fa8f-3f5e-287c-e752eb3ce5f4>, для Windows 7 –

<https://support.microsoft.com/en-us/topic/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-winhttp-in-windows-c4bd73d2-31d7-761e-0178-11268bb10392>.

2. Перейти в редактор реестра нажав сочетание клавиш Win+R и введя «regedit».

3. В редакторе реестра перейти по пути HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SC HANNEL\Protocols\

4. Нажать правую кнопку мыши в любом месте в правой части окна редактора реестра и нажать «Создать» и выбрать в открывшемся списке «Раздел» и назвать его «TLS 1.2».

5. В созданном разделе «TLS 1.2» аналогично создать два раздела с именами «Server» и «Client».

6. В разделе «Server» нажать правую кнопку мыши, нажать «Создать» и в открывшемся списке выбрать «параметр DWORD (32 бита)».

7. Переименовать созданный параметр в «DisabledByDefault» и присвоить ему значение «0».

8. Аналогично создать параметр с именем «Enabled» и присвоить ему значение «1».

9. Перейти в созданный на 5 раздел с именем «Client».

10. Создать в этом разделе такие же два параметра, как и в разделе «Server».

11. Перезагрузить настраиваемый узел исследуемой сети.

12. Запустить от имени администратора Windows PowerShell.

13. Ввести команду:

```
Enable-Psremoting -force
```

14. Запустить скрипт «winrm.ps1» с помощью команды:

```
Powershell.exe -ExecutionPolicy Bypass -File путь\до\файла\winrm.ps1
```

После выполнения скрипта «winrm.ps1» станет доступным подключение по протоколу WinRM методом Basic.

Для установки подключения методом KeyPair помимо настройки описанной ранее необходимо выполнить следующие дополнительные действия:

1. Для настройки подключения необходимо скопировать сгенерированный с помощью Сканер-ВС публичный ключ и поместить его в файл с расширением «.cer» на узле исследуемой сети.

2. Нажать комбинацию клавиш Win+R, ввести «mmc.exe» и нажать клавишу ввод.

3. В открывшейся консоли управления нажать «Файл» и в открывшемся списке выбрать «Добавить или удалить оснастку...».

4. В левой части открывшегося окна «Добавление и удаление оснасток» в разделе «Доступные оснастки» выбрать «Сертификаты» и нажать кнопку «Добавить >».

5. В открывшемся окне «Оснастка диспетчера сертификатов» выбрать «учетной записи компьютера» и нажать кнопку «Далее >».

6. В отобразившемся окне «Выбор компьютера» необходимо выбрать «локальным компьютером (тем, на котором выполняется эта консоль)» и нажать кнопку «Готово».

7. В правой части окна «Добавление и удаление оснасток» в поле «Выбранные оснастки» появились «Сертификаты (локальный компьютер)».

8. Необходимо выбрать данную оснастку путем нажатия на нее левой кнопкой мыши и нажать кнопку «ОК».

9. Далее в левой части консоли управления необходимо нажать на «Сертификаты (локальный компьютер)» после чего отобразится список локальных хранилищ, соответствующих добавленной оснастке, в средней части окна консоли управления.

10. В списке логических хранилищ необходимо найти «Личное», нажать на данное хранилище правой кнопкой мыши, выбрать «все задачи» и в открывшемся списке нажать на «Импорт...», после чего откроется мастер импорта сертификатов.

11. В окне мастера импорта сертификатов необходимо нажать кнопку «Далее» и в отобразившемся интерфейсе импорта файлов добавить файл со скопированным на шаге 1 публичным ключом и нажать кнопку «Далее».

12. Повторить добавление сертификата в хранилища с именами «Доверенные лица» и «Доверенные корневые центры сертификации».

13. В окне консоли управления открыть импортированный сертификат, перейти к вкладке «Состав» и скопировать значение в поле «Отпечаток».

ВАЖНО!

Отпечаток сертификата не должен иметь никаких пробелов ни в начале, ни в конце!

14. Открыть скрипт с именем «clientCertOld.ps1», который распаковывается при установке Сканер-ВС в папку /var/lib/echelon/0/scanner/scripts.

15. Скрипт должен иметь следующее содержание:

```
param($thumbprint, $username, $password)

if (!$thumbprint -or !$username -or !$password){
write-host "need 3 arguments: certificate thumbprint, local username
and password"
return
}

$passwordseq= "$password" | ConvertTo-SecureString -AsPlainText -Force
$thumbprint = "$thumbprint"

# Создание маппинга сертификата
$credential = New-Object -TypeName
System.Management.Automation.PSCredential -ArgumentList $username,
$passwordseq
New-Item -Path WSMAN:\localhost\ClientCertificate `
-Subject "*" `
-URI * `
-Issuer $thumbprint `
-Credential $credential `
```

-Force

16. В данном скрипте необходимо заполнить поля «\$passwordseq» и «\$thumbprint» валидными паролем и отпечатком сертификата соответственно.

17. Запустить Windows PowerShell от имени администратора.

18. Запустить выполнение скрипта следующей командой:

```
Powershell.exe -ExecutionPolicy Bypass -File  
путь\до\файла\clientCertOld.ps1
```

1.3. Удаление внесенных во время настройки подключения по протоколу WinRM изменений с помощью поставляемого скрипта

После завершения исследования узла необходимо отменить внесенные в узел исследуемой сети во время настройки подключения по протоколу WinRM изменений.

Для отмены внесенных изменений необходимо выполнить следующие действия:

- перейти в командную строку от имени администратора;
- выполнить команду:

```
Powershell.exe -ExecutionPolicy Bypass -File remove.ps1;
```

- выполнить команду:

```
Disable-PSRemoting -Force.
```

Примечание. Последняя команда отключает удаленное управление не только с помощью WinRM через PowerShell, но и по всем остальным протоколам и утилитам также.

ПРИЛОЖЕНИЕ 2. (ОБЯЗАТЕЛЬНОЕ)

ИНСТРУКЦИЯ ПОДКЛЮЧЕНИЯ К УЗЛУ ИССЛЕДУЕМОЙ СЕТИ, РАБОТАЮЩЕМУ НА ОС WINDOWS, ПО ПРОТОКОЛУ SSH

2.1. Подключение к узлу исследуемой сети

Для подключения к узлу исследуемой сети, функционирующему на базе ОС семейства Windows, необходима предварительная настройка сервисов SSH. Настройка сервисов описана в п. 2.2 – 2.4 настоящего приложения.

Для подключения к узлу исследуемой сети, функционирующему на базе ОС семейства Windows необходимо выполнить следующие действия:

1. Запустить Windows PowerShell от имени администратора.
2. Проверить статус компонента «Сервер OpenSSH» с помощью команды:

```
Get-WindowsCapability -Online | ? Name -like 'OpenSSH.Ser*'
```

3. В результате выполнения команды должно быть отображено «Installed» в поле «State» (State : Installed).

4. Изменить тип запуска службы sshd на автоматический и запустить ее с помощью следующих команд:

```
Set-Service -Name sshd -StartupType 'Automatic'  
Start-Service sshd
```

5. Убедиться в том, что Сервер OpenSSH запущен и разрешены подключения через порт 22 с помощью следующей команды:

```
netstat -na| find ":22"
```

6. В результате выполнения команды должна отобразиться следующая строка:

```
TCP 0.0.0.0.22 0.0.0.0 LISTENING
```

7. Проверить статус правила Windows Defender Firewall, разрешающее подключения по порту TCP/22 с помощью команды:

```
Get-NetFirewallRule -Name *OpenSSH-Server* |select Name, DisplayName, Description, Enabled
```

8. В том случае, если правило по каким-либо причинам отключено (состояние Enabled=False) или отсутствует, необходимо добавить новое правило используя команду:

```
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' - Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
```

9. Настроить конфигурационный файл sshd_config и перезапустить сервис sshd с помощью команды:

```
restart-service sshd
```

10. Конфигурационный файл после внесения изменений должен выглядеть следующим образом:

```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# The strategy used for options in the default sshd_config shipped
with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override
the
# default value.
```

Port 22

AddressFamily any

ListenAddress 0.0.0.0

```
#ListenAddress ::
```

```
#HostKey __PROGRAMDATA__/ssh/ssh_host_rsa_key
```

```
#HostKey __PROGRAMDATA__/ssh/ssh_host_dsa_key
```

```
#HostKey __PROGRAMDATA__/ssh/ssh_host_ecdsa_key
```

```
#HostKey __PROGRAMDATA__/ssh/ssh_host_ed25519_key
```

```
# Ciphers and keying
```

```
#RekeyLimit default none
```

```
# Logging
```

```
#SyslogFacility AUTH
```

```
#LogLevel INFO
```

```
# Authentication:
```

```
#LoginGraceTime 2m
```

```
#PermitRootLogin prohibit-password
```

```
StrictModes no
```

```
#MaxAuthTries 6
```

```
#MaxSessions 10
```

```
PubkeyAuthentication yes
```

```
# The default is to check both .ssh/authorized_keys and  
.ssh/authorized_keys2
```

```
# but this is overridden so installations will only check  
.ssh/authorized_keys
```

```
AuthorizedKeysFile .ssh/authorized_keys
```

```
#AuthorizedPrincipalsFile none
```

```
# For this to work you will also need host keys in  
%programData%/ssh/ssh_known_hosts
```

```
#HostbasedAuthentication no
```

```
# Change to yes if you don't trust ~/.ssh/known_hosts for
```

```
# HostbasedAuthentication
```

```
#IgnoreUserKnownHosts no
```

```
# Don't read the user's ~/.rhosts and ~/.shosts files
```

```
#IgnoreRhosts yes
```

```
# To disable tunneled clear text passwords, change to no here!
```

```
PasswordAuthentication yes
```

```
#PermitEmptyPasswords no
```

```
# GSSAPI options
```

```
#GSSAPIAuthentication no
```

```
#AllowAgentForwarding yes
```

```
#AllowTcpForwarding yes
```

```
#GatewayPorts no
```

```
#PermitTTY yes
```

```
#PrintMotd yes
```

```
#PrintLastLog yes
```

```
#TCPKeepAlive yes
```

```
#UseLogin no
```

```
#PermitUserEnvironment no
```

```
#ClientAliveInterval 0
```

```
#ClientAliveCountMax 3
```

```
#UseDNS no
```

```
#PidFile /var/run/sshd.pid
```

```
#MaxStartups 10:30:100
```

```
#PermitTunnel no
```

```
#ChrootDirectory none
```

```
#VersionAddendum none
```

```
# no default banner path
```

```
#Banner none
```

```
# override default of no subsystems
```

```
Subsystem      sftp      sftp-server.exe
```

```
# Example of overriding settings on a per-user basis
```

```
#Match User anoncvs
```

```
#      AllowTcpForwarding no
```

```
# PermitTTY no
# ForceCommand cvs server
```

#Match Group administrators

AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys

Примечание. Красным цветом выделены внесенные в конфигурационный файл изменения.

11. Запустить командную строку от имени администратора и сгенерировать пару ключей используя команду:

```
ssh-keygen
```

12. В папке, в которой была создана пара ключей (C:\Users\ %User%\ssh) создать файл authorized_keys.CRLF.

13. В папке C:\ProgramData\ssh\ создать файл administrators_authorized_keys.CRLF.

14. Изменить права доступа на созданные файлы (удалить всех пользователей кроме «Система» и текущего пользователя) и сохранить изменения.

15. В Windows PowerShell поочередно выполнить следующие, скрипты из состава OpenSSH для ОС семейства Windows:

```
powershell.exe -ExecutionPolicy Bypass -File
fixhostfilepermissions.ps1
powershell.exe -ExecutionPolicy Bypass -File
fixuserfilepermissions.ps1
```

16. Перезапустить сервис sshd с помощью следующей команды:

```
Restart-Service sshd
```

Примечание. Необходимые для настройки подключения по протоколу SSH, а также отмены внесенных изменений скрипты при установке Сканер-ВС по умолчанию сохраняются в папке /opt/echelon/scanner/scripts.

2.2. Настройка сервисов SSH с помощью встроенного приложения «Параметры»

Для настройки подключения по протоколу SSH с помощью встроенного приложения «Параметры» необходимо выполнить следующие действия:

1. Открыть встроенное приложение «Параметры» и выбрать элемент «Приложения».

2. Перейти в раздел «Приложения и возможности» и нажать на «Дополнительные компоненты».

3. В списке установленных компонентов необходимо убедиться в наличии компонентов «Клиент OpenSSH» на рабочей станции, с которой будет производиться подключение, и «Сервер OpenSSH» на узле исследуемой сети. В том случае, если данные компоненты не установлены, необходимо нажать на «Добавить компонент», в открывшемся интерфейсе «Добавление дополнительного компонента» выбрать указанные компоненты и нажать «Установить».

4. При установке серверного компонента OpenSSH автоматически создается и включается правило Windows Defender Firewall с именем «OpenSSH-Server-In-TCP», которое разрешает входящий трафик по протоколу SSH через порт 22. В том случае, если данное правило выключено и порт 22 закрыт, то подключения будут отклонены и сброшены.

5. Запустить Windows PowerShell от имени администратора.

6. Проверить статус правила можно с помощью следующей команды:

```
Get-NetFirewallRule -Name *OpenSSH-Server* |select Name, DisplayName, Description, Enabled
```

7. В том случае, если правило по каким-либо причинам отключено (состояние Enabled=False) или отсутствует, необходимо добавить новое правило используя команду:

```
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' - Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
```

2.3. Настройка сервисов SSH с помощью Windows PowerShell

Для настройки подключения по протоколу SSH с помощью Windows PowerShell необходимо выполнить следующие действия:

1. Запустить Windows PowerShell от имени администратора.
2. Проверить доступность сервисов OpenSSH с помощью следующей команды:

```
Get-WindowsCapability -Online | Where-Object Name -like 'OpenSSH*'
```

3. В том случае, если ни один из описанных в п. 2.1 настоящего приложения компонентов не установлен, в результате выполнения команды отобразится следующее сообщение:

```
Name : OpenSSH.Client~~~~0.0.1.0
State : NotPresent

Name : OpenSSH.Server~~~~0.0.1.0
State : NotPresent
```

4. Установить на рабочей станции и узле исследуемой сети компонент «Клиент OpenSSH» и «Сервер OpenSSH» соответственно с помощью следующих команд:

```
# Install the OpenSSH Client
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0

# Install the OpenSSH Server
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```

5. Результатом выполнения обеих команд должен быть:

```
Path :
Online : True
RestartNeeded : False
```

2.4. Запуск и настройка OpenSSH Server

Для запуска и настройки OpenSSH Server для первого использования необходимо выполнить следующие действия:

1. Запустить Windows PowerShell от имени администратора.

2. Запустить службу sshd service путем выполнения следующих команд:

```
# Start the sshd service
Start-Service sshd

# OPTIONAL but recommended:
Set-Service -Name sshd -StartupType 'Automatic'

# Confirm the Firewall rule is configured. It should be created
automatically by setup. Run the following to verify
if (!(Get-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -ErrorAction
SilentlyContinue | Select-Object Name, Enabled)) {
    Write-Output "Firewall Rule 'OpenSSH-Server-In-TCP' does not
exist, creating it..."
    New-NetFirewallRule -Name 'OpenSSH-Server-In-TCP' -DisplayName
'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP
-Action Allow -LocalPort 22
} else {
    Write-Output "Firewall rule 'OpenSSH-Server-In-TCP' has been
created and exists."
}
```

Лист регистрации изменений

[illegible]