Руководство администратора по эксплуатации

версия 10 ред. от 19.05.2025

Листов 116

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем руководстве использованы определения, представленные в таблице (см. Таблица «Термины и сокращения»).

Таблица «Термины и сокращения»

Термины и сокращения	Значение
ИБ	Информационная безопасность
МЭ	Межсетевой экран
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
СОВ	Система обнаружения вторжений
УЗ	Учётная запись
ЦП	Центральный процессор
ARMA Стена	InfoWatch ARMA Стена
CIDR	Classless Inter-Domain Routing – бесклассовая междоменная маршрутизация
DHCP	Dynamic Host Configuration Protocol, протокол динамической настройки узла
DVI	Digital Visual Interface – цифровой видеоинтерфейс
FTP	File Transfer Protocol – протокол передачи файлов по сети
FQDN	Fully Qualified Domain Name, полностью определённое имя домена – имя домена, не имеющее неоднозначностей в определении
HTTP	HyperText Transfer Protocol, протокол передачи гипертекста – протокол прикладного уровня передачи данных
HTTPS	HyperText Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
IP	Internet Protocol, межсетевой протокол – маршрутизируемый протокол сетевого уровня стека TCP/IP
LAN	Local Area Network – локальная вычислительная сеть

Термины и сокращения	Значение
NTP	Network Time Protocol, протокол сетевого времени – сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью
SSD	Solid-State Drive – твердотельный накопитель
SSH	Secure Shell, безопасная оболочка – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
STP	Spanning Tree Protocol, протокол основного дерева – канальный протокол, предназначенный для устранения петель в топологии сети Ethernet
TCP	Transmission Control Protocol, протокол управления передачей – один из основных протоколов передачи данных интернета
USB	Universal Serial Bus – универсальная последовательная шина
VRRP	Virtual Router Redundancy Protocol, протокол резервирования виртуального маршрутизатора – сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
WAN	Wide Area Network – глобальная вычислительная сеть
Zabbix	Свободная система мониторинга статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования

В настоящем руководстве использованы ссылки на документы, представленные в таблице (см. Таблица «Смежные документы»).

Таблица «Смежные документы»

Сокращённое наименование	Полное наименование
Руководство пользователя ARMA Стена	Руководство пользователя по эксплуатации InfoWatch ARMA Стена

АННОТАЦИЯ

Настоящее руководство администратора предназначено для пользователей, производящих установку, запуск и первоначальную настройку конфигурации работы **InfoWatch ARMA Стена v.4.5.0**.

К первоначальным настройкам относятся:

- настройка IP-адресов;
- активация лицензии;
- создание пользовательских учётных записей.

Роль пользователя и администратора может выполнять один сотрудник предприятия.

1 УСТАНОВКА И ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА СИСТЕМЫ

В настоящем разделе представлено описание установки и первоначальной настройки системы **ARMA Стена**.

1.1 Установка

Для установки **ARMA Стена** используется ISO-образ, который представляет собой файл, содержащий все необходимые данные для установки операционной системы в режиме реального времени. Установка **ARMA Стена** производится с USB-накопителя.

Для записи установочного образа **«ARMA Стена»** на USB-накопитель необходимо использовать специализированное программное обеспечение для записи образов на внешние накопители, такое как «Rufus» (https://rufus-usb.ru.uptodown.com/windows). Запись образа производится в соответствии с инструкцией по использованию данного программного обеспечения.

Для установки **ARMA Стена** необходимо выполнить следующие шаги:

1. Загрузить **ARMA Стена** в режиме **«live»**.
2. Выполнить установку образа.

   Примечание:

   После установки системы **ARMA Стена** весь транзитный трафик будет блокироваться.

1.1.1 Загрузка в режиме «live»

Для загрузки **ARMA Стена** в режиме **«live»** необходимо выполнить следующие действия:

1. Подключить подготовленный USB-накопитель с установочным образом в один из доступных USB-портов на аппаратной платформе. Аппаратная платформа во время подключения установочного USB-накопитель должна быть выключена.
2. Включить аппаратную платформу.
3. Выбрать в течение 10 секунд с помощью **клавиш клавиатуры со стрелками вверх и вниз**, в открывшемся меню варианты загрузки (см. Рисунок – Варианты загрузки ОС):
   - **«Live system (amd64–ngfwos)»** – стандартная загрузка, выполняется по умолчанию;
   - **«Live system (amd64–ngfwos fail–safe mode)»** – загрузка в безопасном режиме (Initramfs).

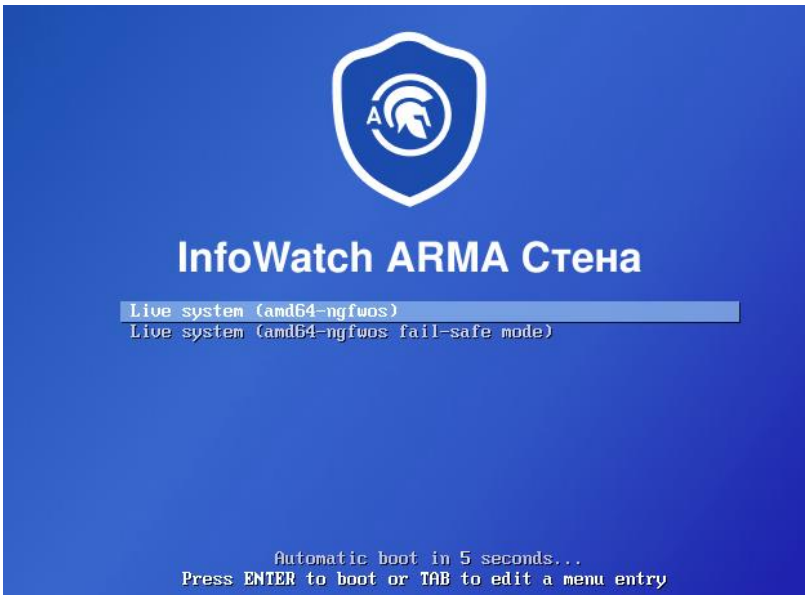


Рисунок – Варианты загрузки ОС

4. Нажать **клавишу «ENTER»** для подтверждения выбранного способа и начала загрузки.

   Примечание:

   Загрузка **ARMA Стена** в режиме **«live»** по умолчанию автоматически выполняется при следующих условиях:

   - в случае бездействия пользователя в меню загрузки в течение 10 секунд;
   - в случае неподтверждённого выбора способа загрузки и последующего бездействия пользователя в течение 5 минут.

5. При появлении приглашения на вход в консольном интерфейсе, указать следующие учётные данные, нажимая **клавишу «ENTER»** после каждого ввода:

   - **«ngfwos login:»** – «admin»;
   - **«Password:»** – «admin».

   Примечание:

   Пароль пользователя не отображается при наборе.

После успешной аутентификации будет отображён интерфейс командной строки в эксплуатационном режиме (см. Рисунок – Интерфейс командной строки).

Рисунок – Интерфейс командной строки

1.1.2 Установка образа

В качестве примера приведено описание установки образа **ARMA Стена** на один жёсткий диск, без деления на несколько разделов. Вводимые команды могут отличаться для каждой конкретной ситуации.

Для запуска процесса установки образа **ARMA Стена** необходимо выполнить следующие действия:

1. Ввести команду **«install image»**:

   ```
   admin@ngfwos:~$ install image
   ```

   и нажать **клавишу «ENTER»**.

   В процессе установки системой будут выводиться запросы, в некоторых случаях содержащие предлагаемый ответ по умолчанию, заключённый в скобки.

   При необходимости отмены выполнения команды, следует нажать комбинацию **клавиш «CTRL»** + **«C»**.

2. Подтвердить запуск процесса установки **ARMA Стена**. Ввести **«y»** и нажать **клавишу «ENTER»**:

   ```
   This command will install NGFWOS to your permanent storage.
   Would you like to continue? [y/N]
   ```

3. Ввести имя образа и нажать **клавишу «ENTER»**:

   ```
   What would you like to name this image? (Default: номер_релизной_версии_ПО)
   ```

4. Ввести новый пароль для УЗ «admin» и нажать **клавишу «ENTER»**:

   ```
   Please enter a password for the "admin" user:
   ```

5. Ввести повторно пароль для УЗ «admin» и нажать **клавишу «ENTER»**:

   ```
   Please confirm password for the "admin" user:
   ```

6. Если требуется создать API-ключ для доступа к веб-интерфейсу системы, следует ввести **«Y»** и нажать **«ENTER»**:

   ```
   Would you like to set API key? [Y/n]
   ```

   6.1. Ввести дополнительный новый пароль, который будет использоваться в качестве API-ключа для УЗ «admin», и нажать **клавишу «ENTER»**:

   ```
   Please enter API key for the "admin" user:
   ```

6.2. Повторно ввести дополнительный пароль для УЗ «admin» и нажать **клавишу «ENTER»**:

```
Please confirm API key for the "admin" user:
```

Примечание:

В системе **ARMA Стена** пароли хранятся в зашифрованном виде.

7. Нажать **клавишу «ENTER»** на следующий запрос:

```
What console should be used by default? (K: KVM, S: Serial)? (Default: K)
```

8. Ввести имя раздела для установки и нажать **клавишу «ENTER»**:

```
Which one should be used for installation? (Default: /dev/sda)
```

Примечание:

В случае, если в ПАК установлено два диска, система предложит настроить конфигурацию RAID-1. Для отказа от настройки RAID-1 необходимо ввести **«n»** и нажать **клавишу «ENTER»**:

```
Probing disks
2 disk(s) found
Would you like to configure RAID-1 mirroring? [Y/n]
```

При подтверждении конфигурации RAID-1 система выведет запрос на добавление перечисленных дисков в массив. Для объединения дисков в RAID-1 необходимо ввести **«Y»** и нажать **клавишу «ENTER»**:

```
The following disks were found:
    /dev/sda (469.0 GB)
    /dev/sda (469.0 GB)
Would you like to configure RAID-1 mirroring on them? [Y/n]
```

Примечание:

В случае выполнения установки с USB-накопителя, система определит его как второй жёсткий диск и предложит настроить конфигурацию RAID-1. Для корректного продолжения установки следует отказаться от настройки RAID. Для этого необходимо ввести **«n»** и подтвердить действие нажатием **клавиши «ENTER»**.

9. Ввести **«y»** и нажать **клавишу «ENTER»** для подтверждения удаления всех данных с устройства:

```
Installation will delete all data on the drive. Continue? [y/N]
```

Примечание:

Все данные на диске будут безвозвратно удалены.

10. Нажать **клавишу «ENTER»** на следующий запрос:

```
Would you like to use all the free space on the drive? [Y/n]
```

11. Программа предложит выбрать следующие доступные конфигурационные файлы для загрузки:

```
Creating partition table...
The following config files are available for boot:
        1: Default live boot config
        2: DHCP client on eth0, SSH
        3: DHCP client on eth0, SSH, 192.168.1.1 on eth1, IPS minimal
Which file would you like as boot config? (Default: 2)
```

Система **ARMA Стена** автоматически устанавливает определённый набор настроек в зависимости от выбранного конфигурационного файла:

- **1 конфигурационный файл** – установка конфигурационного файла с заводскими настройками.
- **2 конфигурационный файл** *(используется по умолчанию)* – установка конфигурационного файла с заводскими настройками, включающие в себя следующие дополнительные настройки:
    - доступа к системе по протоколу SSH (порт 22);
    - автоматическое получение IP-адреса на сетевом интерфейсе «eth0» по протоколу DHCP.
- **3 конфигурационный файл** – установка конфигурационного файла с заводскими настройками, включающие в себя следующие дополнительные настройки:
    - доступа к системе через протокол SSH (порт 22);
    - автоматическое получение IP-адреса на сетевом интерфейсе «eth0» по протоколу DHCP;
    - статический IP-адрес 192.168.1.1 на сетевом интерфейсе «eth1»;
    - настроен DHCP-сервер с диапазоном IP-адресов от 192.168.1.100 до 192.168.1.254;

- включение правил Suricata в режиме захвата «IDS» на сетевом интерфейсе «eth0».

Ввести номер конфигурационного файла и нажать **клавишу «ENTER»**.

12. После завершения процесса установки образа, системой будет выведено сообщение о необходимости выполнить перезагрузку **ARMA Стена**. Извлечь USB-носитель с установочным образом и в командной строке ввести команду **«reboot»**:

```
The image installed successfully; please reboot now.
admin@ngfwos:~$ reboot
```

Подтвердить перезагрузку системы введя **«y»** и нажав **клавишу «ENTER»**:

```
Are you sure you want to reboot this system? [y/N] y
```

После перезагрузки **ARMA Стена** будет отображено приглашение авторизации в локальном консольном интерфейсе:

```
Welcome to NGFWOS – ngfwos tty1

ngfwos login:
```

Для входа в локальный консольный интерфейс необходимо указать учётные данные, нажимая **клавишу «ENTER»** после каждого ввода:

- **«ngfwos login:»** – «admin»;
- **«Password:»** – пароль, заданный на этапе установки образа **ARMA Стена** (пункт 4).

При первоначальной загрузке необходимо произвести активацию лицензии **ARMA Стена**. Процесс активации лицензии подробно описан в разделе «Управление лицензией» настоящего руководства.

Настройка системы производится в режиме конфигурирования. Подробное описание работы в режиме конфигурирования представлено в разделе «Конфигурационный режим» настоящего руководства.

1.2 Первоначальная настройка

1.2.1 Настройка интерфейсов

Просмотр конфигурации интерфейсов возможен с помощью команды **«show interfaces»**. В случае выполнения вышеуказанной команды в режиме конфигурирования дополнительно будет отображена информация о MAC-адресах.

Интерфейсам по умолчанию назначается имя **«ethN»**, где **«N»** – идентификатор, присвоенный интерфейсу системой.

Используемые далее имена интерфейсов и IP-адреса приведены в качестве примера и могут отличаться для каждой конкретной ситуации.

Для назначения IP-адреса на интерфейсе необходимо ввести команду **«set interfaces ethernet eth1 address 192.168.22.1/24»**:

```
[edit]
admin@ngfwos# set interfaces ethernet eth1 address 192.168.22.1/24
```

где:

- **«eth1»** – имя интерфейса;
- **«192.168.22.1/24»** – IP-адрес в формате CIDR.

При необходимости получения IP-адреса на интерфейсе «eth0» по протоколу «DHCP» необходимо ввести команду **«set interfaces ethernet eth0 address dhcp»**:

```
[edit]
admin@ngfwos# set interfaces ethernet eth0 address dhcp
```

Возможно добавление описания интерфейса с помощью команды **«set interfaces ethernet eth1 description LAN»**:

```
[edit]
admin@ngfwos# set interfaces ethernet eth1 description 'LAN'
```

где **«LAN»** – описание для интерфейса.

Пример вывода информации о настроенных интерфейсах:

```
[edit]
admin@ngfwos#    show interfaces
 ethernet eth0 {
        address dhcp
        description WAN
        hw-id 00:50:56:bd:ca:9e
 }
 ethernet eth1 {
        address 192.168.22.1/24
        description LAN
        hw-id 00:50:56:bd:f5:cd
 }
 loopback lo {
 }
```

Процесс настройки сетевых интерфейсов подробно описан в разделе **«Сетевые интерфейсы»** Руководства пользователя **ARMA Стена**.

Примечание:

В случае ошибки в конфигурации сетевых интерфейсов существует возможность потери сетевого доступа к системе ARMA Стена.

1.2.2 Настройка SSH

Сервер SSH обеспечивает безопасный удалённый доступ к управлению функциями локального консольного интерфейса **ARMA Стена**.

Для включения SSH необходимо ввести команду **«set service ssh port 22»**:

```
[edit]
admin@ngfwos# set service ssh port 22
```

где **«22»** – назначаемый порт.

Для указания IP-адреса, прослушиваемого сервисом «SSH», необходимо ввести команду **«set service ssh listen-address 192.168.2.11»**:

```
[edit]
admin@ngfwos# set service ssh listen-address 192.168.2.11
```

где **«192.168.2.11»** – IP-адрес прослушивания сервисом «SSH», приведён в качестве примера. Возможно указать IP-адрес в формате IPv4 или IPv6.

Для указания алгоритма шифрования необходимо ввести команду **«set service ssh ciphers aes128-ctr»**:

```
[edit]
admin@ngfwos# set service ssh ciphers aes128-ctr
```

где **«aes128-ctr»** – алгоритм шифрования, приведён в качестве примера.

Поддерживаются следующие алгоритмы шифрования:

- **3des-cbc**;
- **aes128-cbc**;
- **aes128-ctr**;
- **aes128-gcm@openssh.com**;
- **aes192-cbc**;
- **aes192-ctr**;
- **aes256-cbc**;
- **aes256-ctr**;
- **aes256-gcm@openssh.com**;
- **chacha20-poly1305@openssh.com**;
- **rijndael-cbc@lysator.liu.se**.

1.2.3 Веб-интерфейс

ARMA Стена версии **4.5** поставляется с базовым интерфейсом командной строки (CLI) для управления. Для удобства настройки и контроля работы системы **ARMA Стена** предусмотрена интеграция с ПО **ARMA Management Console (MC)** начиная с версии 1.8 и выше, которая предоставляет полноценный графический интерфейс пользователя (GUI) системы.

Для обеспечения доступа **MC** к системе **ARMA Стена** необходимо выполнить процедуру активации системы (см. Активация системы ARMA Стена) и установить API ключ для HTTP-запросов.

Для создания и установки API ключа необходимо ввести следующую команду в конфигурационном режиме:

```
set service https api keys user <УЗ> key <key>
```

где:

- **<УЗ>** - имя локальной учётной записи в системе **ARMA Стена**;
- **<key>** - пользовательский пароль (API-ключ) для локальной учётной записи **<УЗ>**. Данные параметры будут использоваться для взаимодействия с **MC**.

Примечание:

При использовании API-ключа, созданного для учётной записи с ограниченными привилегиями в системе **ARMA Стена** (см. раздел «Назначение прав доступа пользовательским учётным записям» руководства администратора **ARMA Стена**), доступ к функциональным возможностям веб-интерфейса **ARMA Стена** в **MC** будет предоставлен в соответствии с уровнем прав, назначенных данной учётной записи. В случаях, когда доступ к определённому разделу отсутствует, в нижнем левом углу экрана будет отображаться сообщение об ошибке: **«Request failed with status code 500»**.

Примечание:

Рекомендуется создать API-ключ для учётной записи, относящейся к классу **«NGFW_Administrators»**, либо использовать встроенную учётную запись **«admin»**. В случае если при инсталляции системы **ARMA Стена** для учётной записи **«admin»** был создан API-ключ, и данная учётная запись будет использоваться для подключения к **MC**, выполнять команду «set service https api keys …» не требуется. В этом случае будет использоваться ключ, указанный в процессе инсталляции.

Применить настройки командой **commit**:

```
admin@ngfwos# commit

WARNING: No certificate specified, using build-in self-signed
certificates. Do not use them in a production environment!

[ service https ]

WARNING: No certificate specified, using build-in self-signed
certificates. Do not use them in a production environment!
```

Сохранить конфигурацию командой **save**:

```
admin@ngfwos# save
```

Для подключения **ARMA Стена** к **MC** необходимо выполнить следующие шаги:

1. Авторизоваться в веб-интерфейсе **MC**.
2. Выбрать раздел меню **«Администрирование»**, затем – подраздел **«Источники»** (см. Рисунок – Источники).

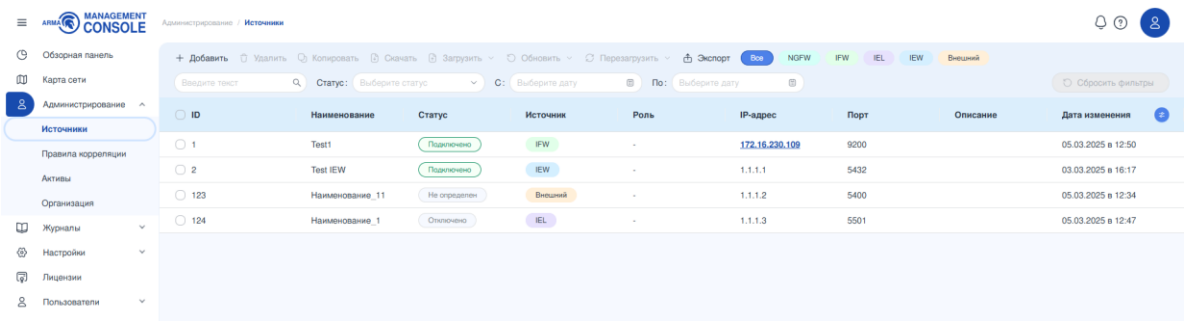


Рисунок – Источники

3. В панели инструментов нажать **кнопку «+ Добавить»**.
4. В открывшейся карточке **«Добавление источника»** выбрать тип источника **«NGFW»** и указать значения следующих параметров (см. Рисунок – Добавление нового источника событий «NGFW»):
   - **«Наименование»** – отображаемое в **MC** имя устройства. Параметр может содержать только латинские и кириллические буквы, пробел, спецсимволы («.», «_», «-») и не может превышать 128 символов;
   - **«IP-адрес»** – IP-адрес подключаемой **ARMA Стена**;
   - **«Логин пользователя»** – ввести имя учётной записи (**<УЗ>**), используемой для создания API-ключа в системе **ARMA Стена**;
   - **«API-Ключ»** – ввести пароль (**<key>**), указанный при создании API-ключа для учётной записи (**<УЗ>**) в **ARMA Стена**;
   - **«Порт»** – значение порта входящих логов. Указываются порты в диапазоне от **«1500»** до **«65535»**. Значение должно быть уникальным, не заданным ранее в источниках **MC**.

   При необходимости заполнить поле **«Описание»** дополнительной информацией об устройстве. Поле может содержать не более 250 символов.

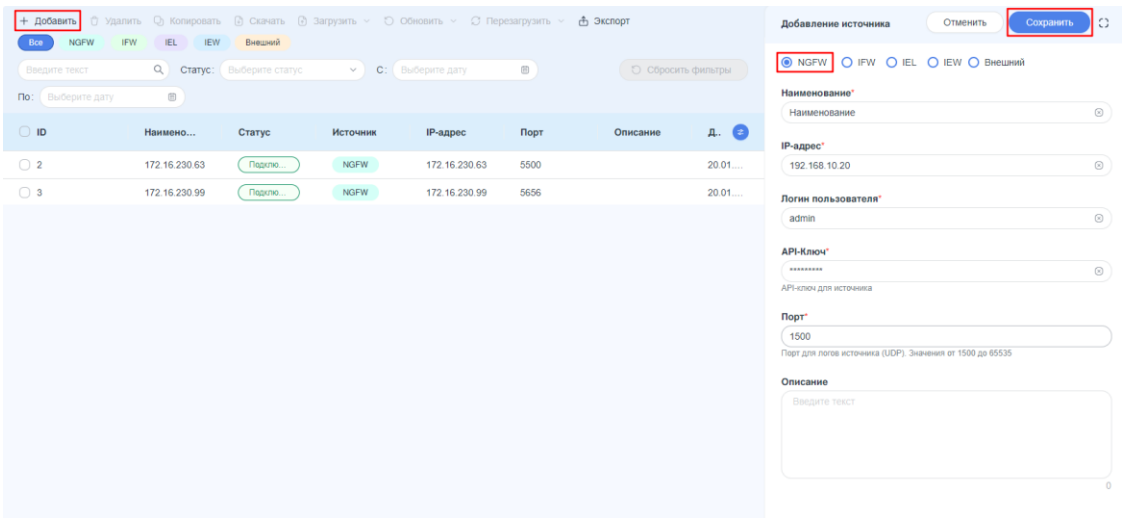


Рисунок – Добавление нового источника событий «NGFW»

После сохранения настроек в столбе **«Статус»** таблицы **«Источники»** отобразится значение **«Подключено»**. При указании неверных учётных данных **МС** отобразит статус **«Не авторизован»**. Статус **«Ошибка»** отображается, если произошла ошибка, которая может быть связана с аппаратным или программным обеспечением источника «NGFW», а также при использовании данных несуществующей локальной учётной записи в **ARMA Стена**.

Порядок работы в веб-интерфейсе системы **ARMA Стена** описан в Приложение А «Веб-интерфейс» руководства пользователя **ARMA Стена**.

2 УПРАВЛЕНИЕ ЛИЦЕНЗИЕЙ

В настоящем разделе представлено описание лицензирования продукта, предусматривающего механизм управления лицензией, который позволяет:

- активировать новую лицензию:
  - автоматическим способом;
  - ручным способом.
- просматривать информацию о действующей лицензии.

2.1 Активация системы ARMA Стена

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии системы **ARMA Стена** в течение срока действия лицензии.

При первоначальной загрузке системы **ARMA Стена** необходимо произвести активацию лицензии. Активация лицензии осуществляется двумя сценариями:

- автоматическая активация через интернет;
- ручная активация без подключения к сети Интернет.

Примечание:

Лицензионный ключ предоставляется согласно условиям в договоре поставки.

В системе **ARMA Стена** в неактивированном состоянии пользователю доступны только следующие действия: настроить сеть, настроить сервис SSH, настроить системный DNS, создать ключи HTTP API и активировать лицензию. Все выполненные настройки в этом состоянии не сохраняются и будут утеряны при перезагрузке системы.

Перечень команд, доступных в системе с неактивированной лицензией (см. Таблица «Команды, разрешённые при неактивированной лицензии»):

Таблица «Команды, разрешённые при неактивированной лицензии»

Режим работы	Команда	Краткое описание
Эксплуатационный	**configure**	Войти в конфигурационный режим
Эксплуатационный	**license**	Лицензирование продукта NGFW
Эксплуатационный	**install**	Установить новую систему
Эксплуатационный	**show**	Показать системную информацию

Режим работы	Команда	Краткое описание
Эксплуатационный	**ping**	Отправить запрос эха ICMP
Эксплуатационный	**emergency exit**	Выход из аварийного режима работы
Эксплуатационный	**reboot**	Перезагрузить систему
Эксплуатационный	**poweroff**	Выключить систему
Эксплуатационный	**traceroute**	Отслеживание сетевого пути к узлу
Эксплуатационный	**telnet**	Telnet к узлу
Эксплуатационный	**exit**	Выход из системы
Конфигурационный	**show**	Показать конфигурацию
Конфигурационный	**comment**	Добавьте комментарий к этому элементу конфигурации
Конфигурационный	**commit**	Зафиксировать текущий набор изменений
Конфигурационный	**commit-confirm**	Зафиксировать текущий набор изменений с обязательным «подтверждением»
Конфигурационный	**save**	Сохранить активную конфигурацию в файл config.boot
Конфигурационный	**confirm**	Подтвердить набор изменений
Конфигурационный	**compare**	Сравнение изменений конфигурации
Конфигурационный	**copy**	Копирование элемента конфигурации
Конфигурационный	**discard**	Отменить незафиксированные изменения
Конфигурационный	**edit**	Редактирование вложенного элемента
Конфигурационный	**run**	Выполнение команд эксплуатационного режима
Конфигурационный	**set service https api keys user**	Команда установки ключа для http-запросов

Режим работы	Команда	Краткое описание
Конфигурационный	**delete service https api keys user**	Команда удаления ключа для http-запросов
Конфигурационный	**set interfaces ethernet**	Команда настройки сетевых интерфейсов
Конфигурационный	**delete interfaces ethernet**	Команда удаления настроек сетевых интерфейсов
Конфигурационный	**set service ssh**	Команда настройки сервиса ssh
Конфигурационный	**delete service ssh**	Команда удаления настроек сервиса ssh
Конфигурационный	**set system name-server**	Команда настройки системного DNS
Конфигурационный	**delete system name-server**	Команда удаления настроек системного DNS
Конфигурационный	**set protocols static route**	Команда настройки шлюза по умолчанию для IPv4
Конфигурационный	**delete protocols static route**	Команда удаления настроек шлюза по умолчанию для IPv4
Конфигурационный	**set protocols static route6**	Команда настройки шлюза по умолчанию для IPv6
Конфигурационный	**delete protocols static route6**	Команда удаления настроек шлюза по умолчанию для IPv6

В случае удаления файла лицензии из активированной системы, **ARMA Стена** заблокирует выполнение команд, которые не входят в перечень разрешённых при неактивированном состоянии (см. Таблица «Команды разрешённые при неактивированной лицензии»). При этом настройки системы останутся неизменными, и она продолжит функционировать, однако возможность внесения изменений будет недоступна. При попытке выполнить неразрешённую команду, будет выведено сообщение об ошибке следующего содержания: **«Invalid command: [введенная команда]»**.

Для возобновления доступа пользователю потребуется повторно активировать систему или восстановить файл лицензии в каталоге **/config/** из сохранённой копии, если таковая имеется.

2.1.1 Автоматическая активация лицензии

Для автоматической активации лицензии необходимо выполнить следующие действия:

1. Настроить сетевой интерфейс для подключения к сети Интернет (см. Настройка интерфейсов).
2. В эксплуатационном режиме ввести команду:

```
admin@ngfwos:~$ license activate <serial>
```

где **<serial>** - лицензионный ключ.

Примечание:

В случае наличия действующей лицензии, в системе будет выведено соответствующее уведомление, и будет предложено подтвердить замену текущей лицензии на новую: **«Successful activation of a new license will overwrite your current license, are you sure you want to proceed ? [Y/n]»**. Для продолжения активации необходимо ввести **«y»** и нажать **клавишу «Enter»**. Если необходимо отменить процедуру, введите **«n»**.

3. В случае успешного применения лицензионного ключа система выведет соответствующие уведомления и предложит перезагрузить устройство для завершения процесса активации.

```
Activation response: license activated, Status: ok
After successful activation of license reboot is required. All unsaved configuration will be lost!
Are you sure you want to reboot this system now ? [Y/n]
```

При вводе некорректного лицензионного ключа отобразится соответствующее сообщение:

```
activation response: bad serial number format , status: error
```

4. Для подтверждения перезагрузки необходимо ввести **«y»** и нажать **клавишу «Enter»**:

```
Are you sure you want to reboot this system now ? [Y/n] y
The system is going to reboot!
admin@ngfwos:~$
Broadcast message from root@ngfwos on pts/1 (Wed 2025-01-22 15:27:36 MSK):

The system will reboot now!
```

5. Активация лицензии выполнена.

2.1.2 Ручная активация лицензии

Для ручной активации лицензии необходимо выполнить следующие действия (см. Рисунок – Ручная активация лицензии):

1. В эксплуатационном режиме ввести команду:

```
admin@ngfwos:~$ license get-token <serial>
```

   где **<serial>** - лицензионный ключ.

2. Система сгенерирует токен и выведет его в консоль:

```
==================BEGIN=================
rXoj/XXXXksAqF6KOKsQ7tt9Rgv9LTjzlliGZ6wc
slQAAAAbMjAyNS0wMS0yMlXXXXo0NjowMy44NDY0NTha
==================END===================

Please be sure to reboot the system, after received 'license.bin' file is placed in /config/license.bin
admin@ngfwos:~$
```

3. Полученный токен необходимо передать в техподдержку ООО **«ИнфоВотч АРМА»**.

4. Специалист **InfoWatch** предоставит файл лицензии в формате **bin**, который необходимо загрузить в систему **ARMA Стена** в каталог **/config/**.

   Для выполнения данной операции возможно использовать программное обеспечение, поддерживающее передачу файлов по протоколам SFTP или SCP (например, WinSCP для операционной системы Windows), либо воспользоваться командой «scp» через интерфейс командной строки. Возможны также альтернативные способы передачи данных.

   Пример использования команды «scp»:

   «C:\Users\test>scp c:\Users\test\Desktop\license.bin admin@172.16.20.76:/config»

   Команда выполнит копирование файл лицензии «license.bin» в каталог «/config/» на системе **ARMA Стена**, доступной по IP-адресу 172.16.20.76.

5. После перемещения файла лицензии **«license.bin»** в каталог **/config/**, необходимо перезагрузить систему. Для этого следует ввести команду **«reboot»** в эксплуатационном режиме, после чего подтвердить перезагрузку, введя **«y»**, и нажать **клавишу «Enter»**:

```
admin@ngfwos:~$ reboot
Are you sure you want to reboot this system? [y/N] y
```

6. Активация лицензии выполнена.

Рисунок – Ручная активация лицензии

2.2 Информация о текущей лицензии

Для просмотра статуса лицензии необходимо в эксплуатационном режиме ввести команду **«show version»**:

```
admin@ngfwos:~$ show version

Version:              NGFWOS 4.5

Built by:             IW ARMA CICD
Built on:             Mon 24 Jan 2025 08:30 UTC
Build UUID:           xx64xx7e-0a33-xxxx-axxd-f2ea8fcxxx8b
Build commit ID:      xxc33ed1xxxxxx-dirty

Architecture:         x86_64
Boot via:             installed image
System type:          KVM guest

Hardware vendor:      QEMU
Hardware model:       Standard PC (Q35 + ICH9, 2009)
Hardware S/N:
Hardware UUID:        xxx30bcb-xxxx-xxxx-xxxx-xxxx1d5d3dcf

license start:        2025-01-24T16:09:02.858887Z
license end:          2025-02-24T16:09:02.861340Z
```

Для ознакомления с пользовательским лицензионным соглашением необходимо ввести команду **«show license»** в эксплуатационном режиме.

3 ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

Доступ к интерфейсу командной строки системы **ARMA Стена** возможно получить при подключении к устройству:

- через HDMI или VGA разъём;
- через консольный порт;
- удалённо при помощи сеанса SSH.

При подключении через консольный порт (RS-232) используются следующие параметры:

- скорость: 9600 бит/с;
- без контроля чётности (No parity);
- 8 бит данных (8 data bits);
- 1 стоповый бит (1 stop bits).

Интерфейс командной строки (CLI) предоставляет возможность получения справочной информации по всем поддерживаемым командам путём ввода символа «?».

Клавиша **TAB** может использоваться для автоматического заполнения строки командами, а также для проверки правильности введённой команды в случае наличия конфликтующих или неизвестных значений. При вводе в командной строке значения «sh» и последующем нажатии клавиши TAB система предложит вариант команды «show». Повторное нажатие клавиши **TAB** приведёт к выводу на экран всех возможных дополнительных команд и параметров, связанных с командой «show»:

```
admin@ngfwos:~$ s[pressTAB]
set       show       suricata

admin@ngfwos:~$ show [tab]
Possible completions:
      arp                 Show Address Resolution Protocol (ARP) information
      bridge              Show bridging information
      cluster             Show clustering information
      configuration       Show running configuration
      conntrack           Show conntrack entries in the conntrack table
      conntrack-sync      Show connection syncing information
      date                Show system date and time
      dhcp                      Show Dynamic Host Configuration Protocol (DHCP)
information
      dhcpv6              Show status related to DHCPv6
```

```
    disk                Show status of disk device
    dns                 Show Domain Name Server (DNS) information
    file                Show files for a particular image
    firewall            Show firewall information
    flow-accounting Show flow accounting statistics
    hardware            Show system hardware details
    history             show command history
    host                Show host information
    incoming            Show ethernet input-policy information
: q
```

Допускается перемещать информацию на экране вверх с помощью сочетания клавиш **Shift+PageUp** и вниз с помощью сочетания клавиш **Shift+PageDown**.

Если вывод данных в командной строке в ответ на заданную команду содержит количество строк, превышающее размер буфера отображаемой информации, то данные будут разделены на части, что будет обозначено символом **«:»**.

При просмотре вывода данных с разделённой информацией доступны следующие действия:

- Для прекращения вывода данных используется клавиша **«q»**.
- Для перехода к следующей странице используется клавиша **«SPACE»**.
- Для перехода к предыдущей странице используется клавиша **«b»**.
- Для перемещения выводимой на экран информации на одну строчку вниз используется клавиша **«ENTER»**.
- Для перемещения выводимой информации на одну строчку вверх и на одну строчку вниз используются клавиши **«⇧»** и **«⇩»** соответственно.
- Для перемещения выводимой информации влево и вправо используются клавиши **«⇦»** и **«⇨»** соответственно, если вывод данных в строке содержит количество символов, превышающее буфер отображаемой на экране информации по горизонтали.

В **ARMA Стена** используются следующие режимы работы:

- **«эксплуатационный режим»** – позволяет осуществлять мониторинг состояния системы и служб, а также выполнять операции с файлами;
- **«конфигурационный режим»** – позволяет вносить изменения в конфигурацию **ARMA Стена**.

После авторизации в системе **ARMA Стена** пользователь автоматически попадает в эксплуатационный режим. Для доступа к настройкам системы необходимо выполнить переход в конфигурационный режим с помощью команды **«configure»**.

Для возврата из конфигурационного режима в эксплуатационный режим используется команда **«exit»**. Если были внесены изменения в конфигурацию, их необходимо зафиксировать с помощью команды **«commit»** или отменить с помощью команды **«discard»** (или **«exit discard»**), прежде чем выйти в эксплуатационный режим.

Выполнение команды **«exit»** в эксплуатационном режиме приводит к выходу текущей УЗ из системы **ARMA Стена**.

Действующую в данный момент конфигурацию возможно сохранить в файл при помощи команды **«save»** в конфигурационном режиме. По умолчанию, конфигурация сохраняется в файл **«config.boot»** расположенном в каталоге **«/config/»**. При инициализации системы происходит автоматическая загрузка конфигурации из файла **«/config/config.boot»**. В связи с этим, после завершения настройки всех требуемых сервисов, необходимо выполнить сохранение текущей конфигурации в указанный файл для обеспечения корректной загрузки параметров при следующем запуске устройства. Рекомендуется выполнять регулярное сохранение конфигурации после внесения любых изменений в настройки системы.

Запрос для ввода команд предоставляет пользователю следующую информацию:

- имя учётной записи пользователя под которой выполнен вход в систему;
- имя узла системы, на который выполнен вход;
- текущий режим интерфейса командной строки;
- текущий уровень в иерархии конфигурации (только для режима настройки).

В таблице «Запрос на ввод команд» приведены некоторые примеры запросов на ввод команд и их значения.

Таблица «Запрос на ввод команд»

Вид запроса	Описание запроса
admin@ngfwos:~$	Пользователь: *admin* Имя узла: *ngfwos* Режим работы: *эксплуатационный режим*
[edit] **admin@ngfwos#**	Пользователь: *admin* Имя узла: *ngfwos* Режим работы: *конфигурационный режим* Уровень в иерархии конфигурации: *[edit] (верхний уровень)*

3.1 Эксплуатационный режим

Эксплуатационный режим предоставляет возможность управлять питанием устройства, получать информацию о текущем состоянии операционной системы и её сервисов, а также выполнять диагностические команды, такие как traceroute или ping.

Основные команды эксплуатационного режима представлены в таблице «Команды эксплуатационного режима»

Таблица «Команды эксплуатационного режима»

Команда	Краткое описание
add	Добавить объект в службу
clear	Очистить информацию о системе
clone	Клонировать объект
configure	Войти в конфигурационный режим
connect	Установить соединение
copy	Копировать объект
delete	Удалить объект
disconnect	Разорвать соединение
exit	Выход из системы
force	Принудительное выполнение операции
format	Форматировать устройство
generate	Сгенерировать объект/ключ
import	Импортировать объект
install	Установить новую систему
monitor	Мониторинг системной информации
mtr	Проследить путь Traceroute и ping к цели
ping	Отправка эхо-запроса ICMP
poweroff	Выключить систему
reboot	Перезагрузить систему
release	Освободить указанную переменную
rename	Переименовать объект
renew	Обновить указанную переменную

Команда	Краткое описание
reset	Сброс службы
restart	Перезапустить отдельную службу
set	Установить новую систему
show	Показать информацию о системе
suricata	Работает с правилами suricata
telnet	Telnet к узлу
traceroute	Трассировка сетевого пути к узлу
update	Обновление данных для службы
wake-on-lan	Отправка пакета Wake-On-LAN (WOL)

3.2 Конфигурационный режим

Конфигурационный режим предназначен для внесения и фиксации изменений конфигурации, а также сохранения конфигурационных файлов.

Для перехода из эксплуатационного режима в конфигурационный режим необходимо ввести команду **«configure»**.

```
admin@ngfwos:~$ configure
[edit]
admin@ngfwos#
```

Подтверждением входа в конфигурационный режим является отображение символа **«#»** в командной строке.

Примечание:

Наличие символов **«admin@ngfwos:~$»** в примерах кода указывает на то, что команду следует вводить в эксплуатационном режиме.

Для работы в конфигурационном режиме используются следующие команды:

1. **«set»** – добавить значение параметра конфигурации, например, назначить IP-адрес для интерфейса «eth1».

```
[edit]
admin@ngfwos# set interfaces ethernet eth1 address 192.168.22.1/24
```

2. **«delete»** – удалить значение параметра конфигурации. При этом также удаляются все подуровни ниже текущего уровня, указанного в команде. При

удалении записи элемент также примет значение по умолчанию, если таковое существует. Например, удалить IP-адрес для интерфейса «eth1».

```
[edit]
admin@ngfwos# delete interfaces ethernet eth1 address
```

3. **«edit»** – перейти к другому уровню редактирования конфигурации. Все команды, выполняемые в режиме конфигурации, связаны с определённым уровнем иерархической структуры, который задаётся администратором при вводе команд. В режиме конфигурации можно вносить изменения в настройки операционной системы с самого верхнего уровня иерархической структуры, однако в таком случае цепочка команд при ручном вводе будет достаточно длинной. Изменение уровня иерархической структуры позволяет сократить длину используемых команд и упростить настройку конфигурации операционной системы.

   Например:

```
[edit]
admin@ngfwos# edit interfaces ethernet eth1
[edit interfaces ethernet eth1]
admin@ngfwos# set address 192.168.22.1/24
admin@ngfwos# set description "LAN"
```

   Пример выше демонстрирует работу команды **«edit»**. После ввода команды «edit interfaces ethernet eth1» система переходит на уровень иерархической структуры конфигурации, связанный с цепочкой команд «interfaces ethernet eth1». Все команды, будут выполняться в отношение данного уровня.

   Для возвращения на самый верхний уровень иерархической структуры используются команды: **«top»** или **«exit»**.

   Для перемещения на один уровень иерархической структуры вверх используется команда **«up»**.

4. **«commit»** – зафиксировать изменения, внесённые в конфигурацию.

   После фиксации изменений «рабочая» конфигурация становится «активной».

   Возможно добавить сообщении о фиксации с помощью команды:

```
commit comment <message>.
```

Примечание:

При выходе из конфигурационного режима без предварительного выполнения команды **«commit»** настройки не будут применены.

5. **«commit-confirm»** – зафиксировать изменения конфигурации и по истечении 10 минут автоматически перезагрузить систему с использованием предыдущей сохранённой конфигурации.

   Для подтверждения выполнения команды следует ввести **«y»** на запрос:

   ```
   commit-confirm will automatically reboot in 10 minutes unless changes are confirmed.
   Proceed ? [Y/n]
   ```

   Примечание:

   Возможно дополнить команду указанием исчисляемого в минутах промежутка времени до перезагрузки системы, например **«commit-confirm 25»**.

6. **«save»** – сохранить активную конфигурацию в файл config.boot:

   ```
   [edit]
   save
   ```

   Примечание:

   В случае попытки перезагрузки или выключения системы **ARMA Стена** без предварительного сохранения изменённых настроек конфигурации, будет выведено следующее предупреждение:

   ```
   Warning: there are unsaved configuration changes!
   Run 'save' command if you do not want to lose those changes after reboot/shutdown.
   ```

7. **«exit»** – выйти из конфигурационного режима в эксплуатационный режим. Также команда может использоваться для перехода из какого-либо уровня редактирования конфигурации.

   ```
   [edit interfaces ethernet eth1]
   admin@ngfwos# exit
   [edit]
   admin@ngfwos# exit
   exit
   admin@ngfwos:~$
   ```

   Примечание:

   Команда **«exit»** не применится для выхода из конфигурационного режима в случае наличия в конфигурации незафиксированных изменений.

```
[edit]
admin@ngfwos# exit
Cannot exit: configuration modified.
Use 'exit discard' to discard the changes and exit.
```

В случае выхода из конфигурационного режима без сохранения внесенных настроек системы выведет предупреждение и перейдёт в эксплуатационный режим:

```
[edit]
admin@ngfwos# exit
Warning: configuration changes have not been saved.
exit
admin@ngfwos:~$
```

8. **«exit discard»** – выйти из конфигурационного режима без сохранения изменений.
9. **«run»** – выполнить команду эксплуатационного режима без предварительного выхода из конфигурационного режима.

```
[edit]
admin@ngfwos# run show system commit
```

10. Команда **«show»**, используемая в режиме конфигурации, позволяет отобразить рабочую конфигурацию с указанием **«+»** добавленных, **«>»** изменённых и **«–»** удалённых строк.

```
[edit]
admin@ngfwos# show
```

Для команды возможно указать дополнительные параметры вывода информации о конфигурации системы **ARMA Стена**:

- **show | commands** - вывести конфигурацию системы в виде команд set.

Примечание:

Для вывода информации обо всех выполненных командах **«set»** используется команда **«run show configuration commands»** в конфигурационном режиме или **«show configuration commands»** в эксплуатационном режиме.

- **show | json** - вывести конфигурацию системы в формате json.

- **show | strip-private** - скрытия конфиденциальных данных при выводе конфигурацию системы. При использовании данной команды происходит фильтрация выходных данных команды show, в результате чего удаляются или скрываются конфиденциальные данные, такие как пароли, ключи шифрования и другая чувствительная информация. Это может быть полезно, например, при необходимости предоставить техническую поддержку или сообществу доступ к логам или конфигурации устройства для устранения неполадок, при этом сохраняя конфиденциальность данных.
- **show | count** - вывести количество строк в конфигурационном файле системы.
- **show | match <pattern>** - выводить только строки, которые соответствуют указанному шаблону <pattern>.
- **show | no-match <pattern>** - выводить только строки, которые не соответствуют заданному шаблону <pattern>.
- **show | more** - разбить вывод на страницы.
- **show | no-more** - не разбивать вывод на страницы.

4 УПРАВЛЕНИЕ

4.1 Управление питанием

4.1.1 Перезагрузка

Для перезагрузки **ARMA Стена** необходимо в эксплуатационном режиме ввести команду **«reboot»**, а затем ввести **«y»** и нажать **клавишу «ENTER»** на запрос **«Are you sure you want to reboot this system? [y/N]»**.

```
admin@ngfwos:~$ reboot
Are you sure you want to reboot this system? [y/N] y
```

4.1.2 Выключение

Для выключения **ARMA Стена** необходимо в эксплуатационном режиме ввести команду **«poweroff»**, а затем ввести **«y»** и нажать **клавишу «ENTER»** на запрос **«Are you sure you want to poweroff this system? [y/N]»**.

```
admin@ngfwos:~$ poweroff
Are you sure you want to poweroff this system? [y/N] y
```

4.2 Конфигурации

ARMA Стена использует единый конфигурационный файл для всей системы — **/config/config.boot**. Это позволяет легко создавать шаблоны, делать резервные копии и тиражировать конфигурацию системы. Также есть возможность сохранения конфигурации на удалённый сервер для архивации или резервного копирования.

В системе **ARMA Стена** предусмотрены три основных типа конфигурации:

1. **Активная конфигурация** – это конфигурация системы, которая в данный момент загружена и используется. Любое изменение конфигурации должно быть зафиксировано, чтобы оно стало принадлежать активной конфигурации.
2. **Рабочая конфигурация** – это конфигурация, которая в данный момент изменяется в конфигурационном режиме. Изменения, внесённые в рабочую конфигурацию, не вступают в силу до тех пор, пока они не будут зафиксированы командой **«commit»**. В этот момент рабочая конфигурация становится активной конфигурацией.
3. **Сохранённая конфигурация** – это конфигурация, которая была сохранена в файл с помощью команды **«save»**. Это позволяет сохранить конфигурацию для последующего использования. Файлов конфигурации может быть несколько. Конфигурация по умолчанию или «загрузочная» сохраняется и загружается из файла **/config/config.boot**.

Для просмотра параметров активной конфигурации необходимо ввести команду **«show configuration»**.

```
admin@ngfwos:~$ show configuration
```

Навигация при просмотре выведенной информации, осуществляется с помощью **клавиш клавиатуры со стрелками вверх и вниз**. Для завершения просмотра параметров конфигурации следует нажать **клавишу «q»**.

Для просмотра нумерованного списка всех существующих локальных версий конфигурации (см. Рисунок – Список резервных версий конфигурации) необходимо в эксплуатационном режиме ввести следующую команду:

```
admin@ngfwos:~$ show system commit
```

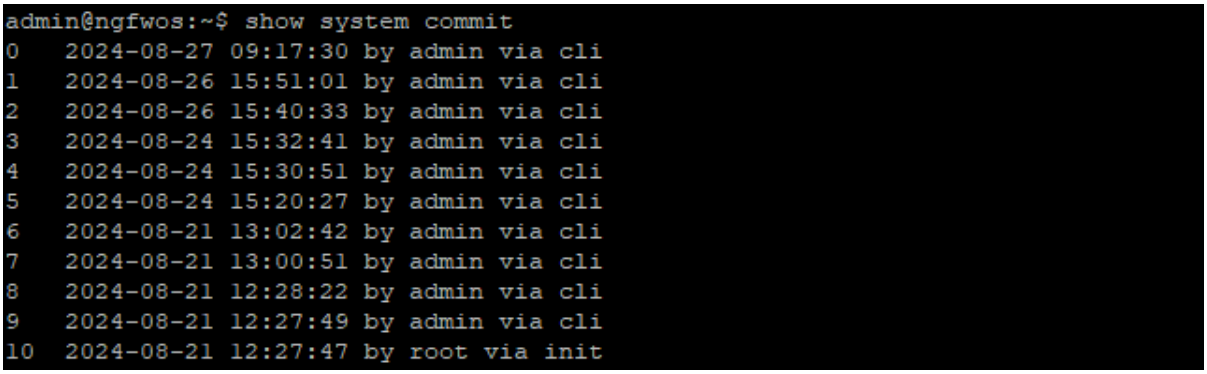


Рисунок – Список резервных версий конфигурации

Для указания максимально возможного количества локально хранящихся версий конфигурации необходимо ввести следующую команду:

```
set system config-management commit-revisions <N>
```

где **<N>** – максимально возможное количество хранящихся активных конфигураций. Возможно указание значения в диапазоне от **«1»** до **«65535»**. По умолчанию используется значение **«100»**.

В случае достижения установленного количества хранящихся версий, будет перезаписываться самая ранняя сохранённая версия.

Примечание:

При увеличении размера конфигурационного файла процесс применения новых настроек может замедлиться, а также может увеличиться время загрузки системы, поскольку для обработки объёмного конфигурационного файла при загрузке может потребоваться больше времени.

4.2.1 Сравнение конфигураций

Для выполнения сравнения различных версий конфигурации следует использовать команду **«compare»**.

Возможны следующие варианты сравнения конфигураций:

1. Для сравнения версии активной конфигурации **<N>** с версией **<M>** необходимо ввести следующую команду:

   ```
   compare <N> <M> [commands]
   ```

   где **<N>** и **<M>** – номера версий активной конфигурации.

   Выведенный список будет содержать информацию о добавленных и удалённых параметрах версии активной конфигурации **<N>** относительно версии **<M>** в виде строк, отмеченных знаками **«+»** и **«-»** соответственно.

   Дополнительный параметр **«commands»** выводит различие конфигураций в виде команд.

2. Для сравнения рабочей и активной конфигурации необходимо ввести следующую команду:

   ```
   compare
   ```

3. Для сравнения рабочей и активной конфигурации и вывода списка команд «set», выполненных в рабочей конфигурации, необходимо ввести следующую команду:

   ```
   compare commands
   ```

4. Для сравнения рабочей конфигурации с сохранённой необходимо ввести следующую команду:

   ```
   compare saved
   ```

5. Для сравнения рабочей конфигурации с выбранной версией **<N>** активной конфигурации необходимо ввести следующую команду:

   ```
   compare <N> [commands]
   ```

   где **<N>** – номер версии активной конфигурации.

6. В эксплуатационном режиме для сравнения рабочей и активной конфигурации необходимо ввести следующую команду:

   ```
   ~$ show system commit diff <N>
   ```

Примечание:

Для текущего пользователя команда **compare** позволяет просматривать изменения только в тех разделах конфигурации, которые были указаны в его пользовательском классе в параметре **«configure-command show [раздел_конфигурации]»**. Если изменения, внесённые с помощью команд **set** или **delete**, не затрагивают разрешённые для отображения разделы, то на экране появится сообщение **«No changes between working and active configurations»** или, в случае использования команды **compare commands**, пустая строка.

Если у пользовательского класса указана общая команда **«configure-command show»**, то будут показаны все изменения во всех разделах конфигурации без каких-либо ограничений.

Если команда **show** не задана ни для конкретных разделов, ни в общем виде, то также появится сообщение **«No changes between working and active configurations»** (или пустая строка для команды **compare commands**), даже если были внесены изменения в конфигурацию.

4.2.2 Восстановление конфигурации

Для выполнения восстановления конфигурации к какой-либо версии активной конфигурации необходимо использовать команду **«rollback»**.

В процессе восстановления автоматически будет создана сохранённая конфигурация, аналогичная выбранной версии активной конфигурации, и выполнена перезагрузка **ARMA Стена**, для подтверждения которой необходимо ввести **«y»** и нажать **клавишу «ENTER»**:

```
rollback <N>
Proceed with reboot? [Y/n] y
```

Примечание:

Не рекомендуется восстанавливать конфигурацию с пометкой **«init»**, так как это может привести к некорректной работе системы (см. Рисунок – Список резервных версий конфигурации).

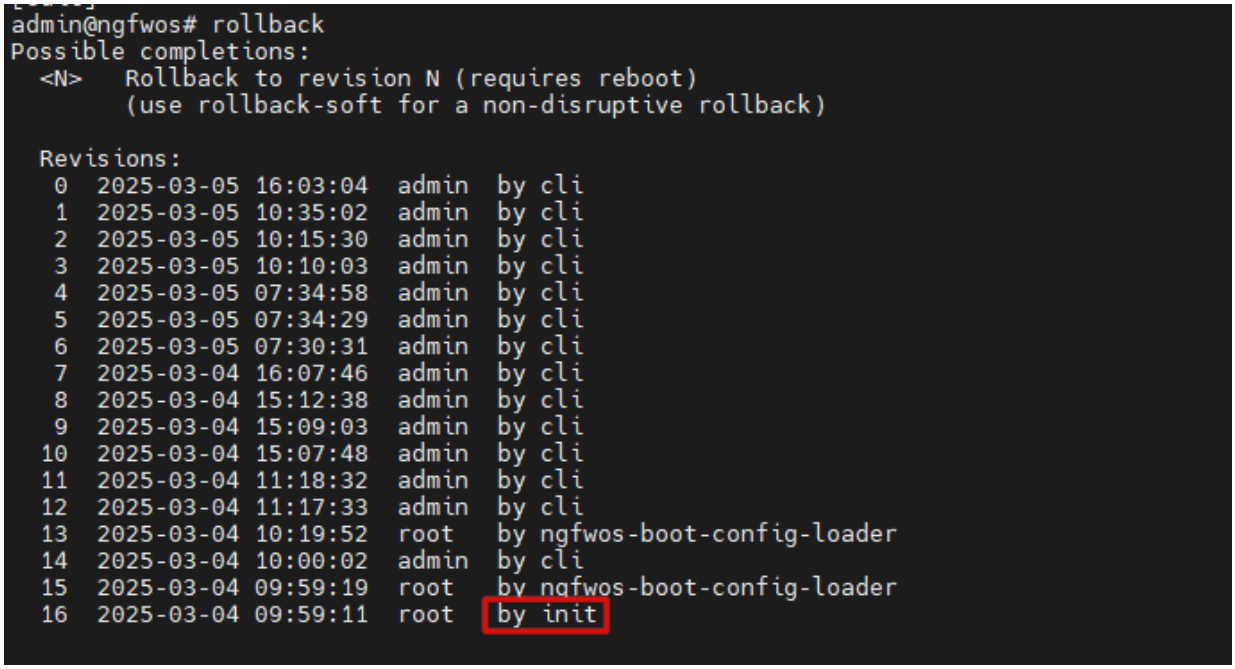


Рисунок – Список резервных версий конфигурации

4.2.3 Удаление конфигурации

Для удаления локального архива конфигурации необходимо ввести следующую команду в эксплуатационном режиме:

```
admin@ngfwos:~$ delete commit <N>
```

где **<N>** - номер архива конфигурации в локальном хранилище.

После успешного удаления система выведет соответствующее уведомление:

```
Successfully deleted revision <N>.
admin@ngfwos:~$
```

4.2.4 Экспорт конфигурации

Для экспорта конфигурационного файла в указанную директорию необходимо ввести следующую команду:

```
save <track>/<file>
```

где:

- **<track>** – директория для сохранения;
- **<file>** – имя файла конфигурации.

Возможны следующие варианты экспорта файла конфигурации:

- **<file>** – экспорт файла конфигурации на локальный диск в файл с указанным изменён:

```
[edit]
admin@ngfwos# save /config/test.boot
```

  Если указано только имя файла, без каталога для сохранения, то файл будет сохранён в каталоге пользователя, от имени которого была выполнена команда. Например, для пользователя с именем admin это будет каталог /home/admin/.

- **scp://<user>:<passwd>@<host>:/<file>** – экспорт файла на удалённый сервер SCP.
- **sftp://<user>:<passwd>@<host>/<file>** – экспорт файла на удалённый сервер SFTP.
- **ftp://<user>:<passwd>@<host>/<file>** – экспорт файла на удалённый сервер FTP.
- **tftp://<host>/<file>** – экспорт файла на удалённый компьютер.

где:

- **<user>** – имя УЗ;
- **<passwd>** – пароль УЗ;
- **<host>** – адрес компьютера.

В качестве примера приведены команды для выполнения:

- экспорта конфигурационного файла под именем «ngfw1.config.boot» на удалённый компьютер «tftp://192.168.0.100»:

```
save tftp://192.168.0.100/ngfw1.config.boot
```

- экспорта конфигурационного файла под именем «ngfw1.config.boot» в локальную директорию по умолчанию «/config/»:

```
save ngfw1.config.boot
```

4.2.4.1 Экспорт конфигурации на удалённый сервер

ARMA Стена позволяет экспортировать конфигурацию на удалённый сервер после каждого выполнения команды **«commit»**.

Поддерживается экспорт на удалённые серверы по следующим протоколам: **TFTP**, **FTP**, **SCP**, **SFTP**. В случае успешного выполнения команды **«commit»** копия файла «config.boot» экспортируется на указанный удалённый сервер. Файл будет сохранён с именем следующего вида:

- **«config.boot-hostname.ГГГГММДД_ЧЧММСС»**.

Для назначения ресурса для удалённого хранения копий конфигурационного файла:

```
set system config-management commit-archive location <URI>
```

где **<URI>** – идентификатор ресурса.

Для удалённого расположения архива конфигурации возможно использование следующих шаблонов **<URI>**:

- http://<user>:<passwd>@<host>:/<dir>
- https://<user>:<passwd>@<host>:/<dir>
- ftp://<user>:<passwd>@<host>/<dir>
- sftp://<user>:<passwd>@<host>/<dir>
- scp://<user>:<passwd>@<host>/<dir>
- tftp://<host>/<dir>
- git+https://<user>:<passwd>@<host>/<path>

где:

- **<user>** – имя УЗ;
- **<passwd>** – пароль УЗ;
- **<host>** – адрес компьютера;
- **<dir>** – директория для сохранения файла конфигурации.

4.2.5 Импорт конфигурации

Для импорта новой конфигурации с заменой текущей необходимо ввести следующую команду:

```
load <track>/<file>
```

где:

- **<track>** – источник расположения нового файла конфигурации;
- **<file>** – имя загружаемого файла конфигурации.

Возможно использование следующих шаблонов источников для загрузки файла конфигурации:

- **<file>**
- **scp://<user>:<passwd>@<host>:/<file>**
- **sftp://<user>:<passwd>@<host>/<file>**

- **ftp://<user>:<passwd>@<host>/<file>**
- **http://<host>/<file>**
- **https://<host>/<file>**
- **tftp://<host>/<file>**

где:

- **<user>** – имя УЗ;
- **<passwd>** – пароль УЗ;
- **<host>** – адрес компьютера.

В качестве примера приведены команды для выполнения:

- импорта конфигурационного файла «ngfw1.config.boot» из локальной директории «/config/»:

```
load ngfw1.config.boot
```

- импорта конфигурационного файла «050424.config.boot» с FTP-сервера «ftp://46.24.16.27»:

```
load ftp://ngfw:Fgw43!dweP@46.24.16.27/050424.config.boot
```

4.3 Обновление образа ARMA Стена

Обновление системы **ARMA Стена** поставляется в виде файла в формате **«ISO»**.

Возможны следующие способы получения файла обновления **ARMA Стена**:

- Загрузка файла с удалённого сервера **InfoWatch ARMA**;
- USB-накопитель, предоставляемый **InfoWatch ARMA**.

Примечание:

После обновления системы лицензия становится недействительной. Требуется повторная активация **ARMA Стена** с использованием нового лицензионного ключа.

Рекомендуется заранее обратиться в службу технической поддержки ООО **«ИнфоВотч АРМА»** для получения нового ключа активации.

Примечание:

После обновления системы будет создан новый экземпляр глобального журнала событий. Все предыдущие записи событий останутся доступны в старой версии системы.

Примечание:

Перед обновлением рекомендуется выполнить резервное копирование конфигурации **ARMA Стена**. Процесс создания резервной копии конфигурации описан в разделе «Экспорт конфигурации» настоящего руководства.

Примечание:

Перед обновлением необходимо выполнить резервное копирование пользовательских правил СОВ. По умолчанию все правила СОВ хранятся в каталоге «/var/lib/suricata/rules/».

Для выполнения данной операции возможно использовать программное обеспечение, поддерживающее передачу файлов по протоколам SFTP или SCP (например, WinSCP для операционной системы Windows), либо воспользоваться командой «scp» через интерфейс командной строки. Возможны также альтернативные способы передачи данных.

Пример использования команды «scp»:

«C:\Users\test>scp
admin@172.16.230.105:/var/lib/suricata/rules/user.rules
admin@172.16.230.105:/config»

Команда выполнит копирование файла пользовательских правил СОВ «user.rules» из каталога «/var/lib/suricata/rules/» в каталог «/config/» на системе **ARMA Стена**, доступной по IP-адресу 172.16.20.105.

После обновления системы требуется восстановить файл пользовательских правил СОВ в исходный каталог либо указать новое расположение файла в конфигурации Suricata. Для этого необходимо выполнить команду в конфигурационном режиме: «set suricata rule-files file-name /config/user.rules».

Примечание:

Если в системе настроена аутентификация по протоколу **Kerberos**, перед выполнением обновления необходимо скопировать файл **«*.keytab»** из каталога **«/home/admin/»** (каталог указан по умолчанию и может отличаться от фактически используемого пользователем) в каталог **«/config/»**.

В случае необходимости сохранения критически важных данных, таких как внешние сертификаты или пользовательские скрипты, которые расположены за пределами директории **«/config/»**, требуется осуществить их предварительное копирование в указанную директорию перед выполнением обновления.

После завершения обновления системы следует вернуть перенесённые файлы обратно в их первоначальные директории.

Примечание:

Для корректного выполнения обновления системы **ARMA Стена** в режиме отказоустойчивого кластера с настроенной синхронизацией конфигурации следует придерживаться следующего порядка действий:

1. Выполнить обновление программного обеспечения на резервной системе **ARMA Стена**.
2. После успешного завершения обновления резервной системы произвести обновление основной (мастер) системы **ARMA Стена**.

Во время обновления одного из узлов кластера **ARMA Стена** отключать второе устройство, которое не участвует в обновлении, не требуется.

В процессе обновления устройств не рекомендуется вносить изменения в конфигурационный файл на обоих устройствах **ARMA Стена**, чтобы избежать возможных конфликтов или некорректного применения настроек.

Примечание:

В версии **ARMA Стена 4.5** по умолчанию применяется блокировка всего транзитного трафика. При обновлении с версии **4.4** до **4.5** блокировка транзитного трафика не активируется, так как в версии **4.4** данное ограничение отсутствовало. Для активации блокировки транзитного трафика после обновления необходимо выполнить в конфигурационном режиме команду: **«set firewall <ipv4 | ipv6 | bridge> forward filter default-action accept»**.

Примечание:

Начиная с версии **ARMA Стена 4.5**, в систему по умолчанию интегрированы стандартные классы пользователей, а также специальный класс для встроенной учётной записи **«admin»** - **«NGFW_Super_Administrators»**.

При обновлении системы с версии **4.4** до **4.5** или **выше**, в случае, если для встроенной учётной записи **«admin»** был назначен пользовательский класс, после завершения обновления данной учётной записи будет автоматически присвоен предопределённый системный класс **«NGFW_Super_Administrators»**.

Для установки обновления необходимо выполнить следующие действия:

1. Авторизоваться в системе **ARMA Стена** посредством встроенной учётной записи **«admin»** либо учётной записи, принадлежащей к классу с назначенными полномочиями на выполнение команды установки обновлений системы в эксплуатационном режиме - **«add»** (см. раздел «Назначение прав доступа пользовательским учётным записям»).
2. Скопировать полученный ISO-образ обновления в локальную директорию файловой системы **ARMA Стена**.

   Для выполнения данной операции возможно использовать программное обеспечение, поддерживающее передачу файлов по протоколам SFTP или SCP (например, WinSCP для операционной системы Windows), либо воспользоваться командой «scp» через интерфейс командной строки. Возможны также альтернативные способы передачи данных.
3. В эксплуатационном режиме ввести следующую команду:

```
admin@ngfwos:~$ add system image </config/ngfw-4.5.iso>
```

   где:

   - **</config/ngfw-4.5.iso>** – путь к файлу обновления, приведён в качестве примера;
4. В случае успешной проверки установщиком контрольной суммы ISO-образа, указать имя сборки и нажать **клавишу «ENTER»**:

```
Validating image checksums
What would you like to name this image? (Default: номер_релизной_версии_ПО)
```

5. Ввести **«y»** и нажать **клавишу «ENTER»** для назначения новой конфигурации в качестве используемой для загрузки по умолчанию:

```
Would you like to set the new image as the default one for boot? [Y/n]
```

6. Для сохранения текущей конфигурации ввести **«y»** и нажать **клавишу «ENTER»**:

```
An active configuration was found. Would you like to copy it to the new image? [Y/n]
```

7. Для сохранения SSH-ключей текущей конфигурации ввести **«y»** и нажать **клавишу «ENTER»** :

```
Copying configuration directory
Would you like to copy SSH host keys? [Y/n]
```

Примечание:

В случае отсутствия свободного места на диске установка будет отменена.

8. При успешном завершении обновления перезагрузить **ARMA Стена**:

```
Copying SSH host keys
Copying system image files
Cleaning up
Unmounting target filesystems
Removing temporary files

# Команда перезагрузки системы:
admin@ngfwos:~$ reboot

# Ввести «y» для подтвержения перезагрузки системы:
Are you sure you want to reboot this system? [y/N] y
```

Примечание:

В случае недоступности системы **ARMA Стена** по сети после выполнения процедуры перезагрузки, требуется инициировать повторную перезагрузку устройства через локальный интерфейс CLI. Данное действие обеспечит восстановление сетевого доступа к системе.

Переназначить используемый для загрузки по умолчанию образ **ARMA Стена** возможно следующими способами:

- с помощью ввода команды **«set system image default-boot»** в эксплуатационном режиме;
- с помощью меню **GRUB**.

Для переназначения используемого для загрузки по умолчанию образа **ARMA Стена** необходимо в командной строке выполнить следующие действия:

1. В эксплуатационном режиме ввести команду **«set system image default-boot»**:

```
admin@ngfwos:~$ set system image default-boot
```

2. Определить в выведенном списке образ для загрузки по умолчанию, ввести номер соответствующей строки и нажать **клавишу «ENTER»**:

```
The following images are available:
      1: 4.5 (running) (default boot)
      2: 4.4
Select an image to set as default:
```

3. Перезагрузить **ARMA Стена**:

```
Select the default boot image: 2
The image "4.4" is now default boot image

admin@ngfwos:~$ reboot
```

Для установки образа **ARMA Стена**, используемого для загрузки, через меню **GRUB**, необходимо выполнить перезагрузку системы. В течение 5 секунд после старта процесса загрузки следует выбрать требуемый образ из списка, представленного в меню **GRUB** (см. Рисунок – Выбор образа для загрузки).

Рисунок – Выбор образа для загрузки

Для удаления архивного образа **ARMA Стена** с целью освобождения места на диске следует выполнить следующие действия:

1. В эксплуатационном режиме ввести команду **«delete system image»**:

```
admin@ngfwos:~$ delete system image
```

2. Определить в выведенном списке образ, подлежащий удалению, ввести номер соответствующей строки, например **«2»**, и нажать **клавишу «ENTER»**:

```
The following image(s) can be deleted:

    1: 4.5 (running) (default boot)
    2: 4.4

Select an image to delete: 2
```

Примечание:

Если образ системы, предназначенный для удаления, назначен в качестве загрузочного по умолчанию, система выведет предупреждение о невозможности его удаления. Для выполнения операции необходимо сначала переназначить загрузочный образ по умолчанию на другой, а затем повторно выполнить команду удаления.

3. Ввести **«y»** и нажать **клавишу «ENTER»** для подтверждения удаления:

```
Do you really want to delete the image 4.4? [y/N] y
```

4. По завершении процесса будет выведено сообщение об успешном удалении образа: **«The image "4.4" was successfully deleted»**.

Для просмотра информации о текущей версии конфигурации необходимо в эксплуатационном режиме ввести команду **«show version»**.

Для просмотра информации о сохранённых образах необходимо в эксплуатационном режиме ввести команду **«show system image»**.

4.4 Сброс настроек

В **ARMA Стена** реализована возможность сброса конфигурации к заводским настройкам.

Для сброса конфигурации к заводским настройкам необходимо выполнить следующие действия:

1. В режиме конфигурирования ввести следующую команду:

```
load /opt/ngfwos/etc/config.boot.default
```

2. При появлении сообщения о завершении загрузки конфигурации **«Load complete. Use 'commit' to make changes effective.»** ввести команду **«commit»**:

```
Load complete. Use 'commit' to make changes effective.
[edit]
commit
```

Примечание:

Для отмены сброса конфигурации следует ввести команду **«discard»**.

3. Ввести команду **«save»** для сохранения новой конфигурации.
4. Выполнить перезагрузку **ARMA Стена**.

4.5 Служба NTP

Служба NTP позволяет устанавливать и поддерживать системное время, синхронизированное с серверами точного времени.

В **ARMA Стена** используется протокол NTPv4, соответствующий международному стандарту «RFC-5905». Обмен с серверами информацией о временных метках выполняется по протоколу UDP через порт «123».

ARMA Стена использует следующие адреса NTP-серверов первого уровня:

- **«ntp1.vniiftri.ru»**;
- **«ntp2.vniiftri.ru»**;
- **«ntp3.vniiftri.ru»**;
- **«ntp4.vniiftri.ru»**;
- **«ntp1.niiftri.irkutsk.ru»**;
- **«ntp2.niiftri.irkutsk.ru»**;
- **«vniiftri.khv.ru»**;
- **«vniiftri2.khv.ru»**;
- **«ntp.sstf.nsk.ru»**.

Для добавления NTP-сервера необходимо ввести следующую команду:

```
set service ntp server <address>
```

где **<address>** – адрес NTP-сервера, указываемый в формате **IPv4/IPv6-адреса** или **FQDN**.

Для удаления NTP-сервера необходимо ввести следующую команду:

```
delete service ntp server <address>
```

Для просмотра списка используемых NTP-серверов необходимо в режиме конфигурирования ввести следующую команду:

```
show service ntp
```

4.5.1 Дополнительные настройки NTP

Для включения или отключения какого-либо дополнительного параметра сервера NTP, следует ввести соответствующую команду:

```
set service ntp server <address> <attribute>
delete service ntp server <address> <attribute>
```

где **<attribute>** – дополнительный параметр NTP.

Возможна настройка следующих дополнительных параметров сервера NTP:

- **«noselect»** – назначение сервера NTP как неиспользуемого;
- **«nts»** – включение защиты сетевого времени NTS для сервера NTP;
- **«pool»** – указание адреса, являющегося пулом серверов NTP;
- **«prefer»** – назначение сервера NTP как предпочтительного.

4.6 Планировщик задач Cron

Планировщик задач **Cron** позволяет выполнять различные задачи согласно заданному расписанию.

Для установки времени запуска задачи необходимо ввести следующую команду:

```
set system task-scheduler task <task> crontab-spec <spec>
```

где:

- **<task>** – имя задачи;
- **<spec>** – время запуска задачи.

Для настройки параметра **<spec>** используется стандартный синтаксис сервиса **Cron** в виде пяти атрибутов **«* * * * *»**, воспринимаемых как:

- **«минуты»** – возможно использование значений в диапазоне от **«0»** до **«59»**;
- **«часы»** – возможно использование значений в диапазоне от **«0»** до **«23»**;
- **«число»** – возможно использование значений в диапазоне от **«1»** до **«31»**;
- **«месяц»** – возможно использование значений в диапазоне от **«1»** до **«12»**;
- **«дни недели»** – возможно использование значений в диапазоне от **«0»** до **«7»**. Значения от **«1»** до **«6»** принимаются как дни недели с «понедельника» до «субботы» соответственно. Значения **«0»** или **«7»** принимаются как «воскресенье».

Поля могут содержать одно или несколько значений, разделённых запятыми, или диапазон значений, разделённых дефисом. Существует возможность указать шаг, используя символ **«/»**. Например, при указании атрибутов следующим образом: **«* */2 * * *»** – задача будет выполняться каждые два часа.

В качестве примера приведена команда для настройки выполнения задачи «Task1» ежедневно в 07:00 и 18:00:

```
set system task-scheduler task Task1 crontab-spec 00 07,18 * * *
```

Для настройки интервала запуска задачи возможно применение параметра **«interval»**:

```
set system task-scheduler task <task> interval <interval>
```

где **<interval>** – интервал времени, в течение которого задача должна быть выполнена. Задается в виде числа с одним из следующих суффиксов: **«m»** – минуты, **«h»** – часы, **«d»** – дни. В случае ввода значения без суффикса, интервал воспринимается в минутах.

Для указания скрипта, запускаемого по расписанию, необходимо ввести следующую команду с параметром **«executable path»**:

```
set system task-scheduler task <task> executable path <path>
```

где **<path>** – путь к скрипту.

Для установки параметров скрипта необходимо ввести следующую команду:

```
set system task-scheduler task <task> executable arguments <args>
```

где **<args>** – параметр скрипта.

Создание и редактирование скриптов возможно выполнять с помощью какого-либо текстового редактора, например **«nano»**.

4.7 Zabbix

Zabbix предназначен для мониторинга состояния IT-инфраструктуры, включая серверы, сетевые устройства и приложения. Система позволяет собирать метрики, анализировать данные и оповещать об инцидентах. В системе **ARMA Стена** интегрирован zabbix-агент версии **7.0.10** для обеспечения взаимодействия и передачи данных о состоянии системы.

Команды настройки zabbix-агента:

1. Установить имя хоста, используемое Zabbix-агентом для идентификации устройства в интерфейсе Zabbix-сервера:

   ```
   set service monitoring zabbix-agent host-name <name>
   ```

   где **<name>** – имя хоста Zabbix-агента.

2. Установить IP-адрес или DNS-имя Zabbix-сервера, который будет подключаться к Zabbix-агенту в пассивном режиме работы:

   ```
   set service monitoring zabbix-agent server <server>
   ```

где **<server>** – адрес Zabbix-сервера в формате <x.x.x.x>, <h:h:h:h:h:h:h:h> или <hostname>.

3. Установить порт подключения к Zabbix-агенту в пассивном режиме, через который Zabbix-сервер опрашивает клиентов:

```
set service monitoring zabbix-agent port <1-65535>
```

где **<1-65535>** – номер порта. Возможно указать значение в диапазоне от «1» до «65535». По умолчанию используется порт «10050».

4. Установить IP-адрес или DNS-имя Zabbix-сервера, который будет подключаться к Zabbix-агенту в активном режиме работы:

```
set service monitoring zabbix-agent server-active <server> port <1-65535>
```

где:

- **<server>** – адрес Zabbix-сервера в формате <x.x.x.x>, <h:h:h:h:h:h:h:h> или <hostname>;
- **<1-65535>** – номер порта, который будет использоваться для подключения к Zabbix-серверу в активном режиме. Возможно указать значение в диапазоне от «1» до «65535».

5. Определить на каких IP-адресах агент должен прослушивать входящие соединения:

```
set service monitoring zabbix-agent listen-address <address>
```

где **<address>** – IP-адрес в формате <x.x.x.x> и/или <h:h:h:h:h:h:h:h>. Возможно указать как один, так и несколько IP-адресов. По умолчанию используется значение «0.0.0.0» - агент прослушивает все интерфейсы.

6. Установить максимальное время ожидания ответа при обмене информацией с Zabbix-сервером:

```
set service monitoring zabbix-agent timeout <1-30>
```

где **<1-30>** – целочисленное значение времени ожидания в секундах. Возможно указать значение в диапазоне от «1» до «30». По умолчанию используется значение «3».

7. Определить максимальный размер данных в буфере памяти:

```
set service monitoring zabbix-agent limits buffer-size <2-65535>
```

где **<2-65535>** – размер буфера. Возможно указать значение в диапазоне от «2» до «65535». По умолчанию используется значение «1000». Агент

отправит все собранные данные на Zabbix-сервер, если буфер будет заполнен.

8. Определить частоту отправки значений из буфера на Zabbix-сервер:

```
set service monitoring zabbix-agent limits buffer-flush-interval <1-3600>
```

где **<1-3600>** – значение частоты отправки данных из буфера. Возможно указать значение в диапазоне от «1» до «3600». По умолчанию используется значение «5». Агент отправит все собранные данные на Zabbix-сервер раньше установленного времени, если буфер будет заполнен.

9. Определить путь к директории, содержащей отдельные конфигурационные файлы для Zabbix-agent:

```
set service monitoring zabbix-agent directory <text>
```

где **<text>** – путь к директории.

10. Включить логирование выполняемых команд через Zabbix-agent:

```
set service monitoring zabbix-agent log remote-commands
```

11. Настройки уровня логирования Zabbix-agent:

```
set service monitoring zabbix-agent log debug-level <level>
```

где **<level>** – уровень детализации журнала. Возможно указать следующие значения:

- **basic** - базовый уровень логирования. Включает только самую важную информацию о работе Zabbix-agent.
- **critical** - логируются только критически важные события, которые могут привести к сбою работы Zabbix-agent.
- **error** - логируются ошибки, возникающие в процессе работы Zabbix-agent. Это более детальный уровень по сравнению с «critical».
- **warning** - логируются предупреждения, которые указывают на потенциальные проблемы, но не являются критическими. Используется по умолчанию.
- **debug** - логируется отладочная информация, включая технические детали работы Zabbix-agent.
- **extended-debug** - расширенный уровень отладочной информации. Включает максимально подробные данные о работе Zabbix-agent.

12. Установить максимальный размер файла журнала:

```
set service monitoring zabbix-agent log size <0-1024>
```

где **<0-1024>** – максимальный размер файла журнала в мегабайтах. Возможно указать значение в диапазоне от «1» до «1024». По умолчанию используется значение «0» - ротация файла отключена. Если предельный размер файла журнала достигнут и ротация файлов по какой-либо причине не удалась, существующий файл журнала затирается и начинается заново.

5 ВАРИАНТЫ РАЗВЁРТЫВАНИЯ

Предусмотрены следующие варианты развёртывания **ARMA Стена** в ЛВС:

- режим маршрутизации;
- режим отказоустойчивого кластера.

Каждый вариант отличается настройкой сетевых интерфейсов.

5.1 Маршрутизация

В режиме маршрутизации **ARMA Стена** работает как МЭ с функцией обнаружения и предотвращения вторжений, обеспечивая защиту передачи информации с возможностью маршрутизации. Режим маршрутизации может использоваться при объединении сетей, имеющих разное адресное пространство.

Общая схема подключения **ARMA Стена** в режиме маршрутизации представлена на рисунке (см. Рисунок – Режим маршрутизации).

Рисунок – Режим маршрутизации

5.2 Отказоустойчивый кластер

В режиме отказоустойчивого кластера несколько **ARMA Стена** объединяются в единый кластер в режиме «active-backup».

В случае объединения нескольких **ARMA Стена** в каждый момент времени только одно устройство **ARMA Стена** в кластере обрабатывает весь трафик, такое устройство считается ведущим. При выходе из строя ведущего устройства его подменяет одно из резервных устройств, которое само становится ведущим и начинает обрабатывать трафик. В случае если изначально ведущее устройство вновь переходит в рабочее состояние, то текущее ведущее устройство возвращается в статус подчинённого резервного устройства.

Общая схема подключения **ARMA Стена** в режиме отказоустойчивого кластера представлена на рисунке (см. Рисунок – Режим отказоустойчивого кластера).

Подробная информация о настройке отказоустойчивого кластера описана в разделе **«Отказоустойчивость»** Руководства пользователя **ARMA Стена**.

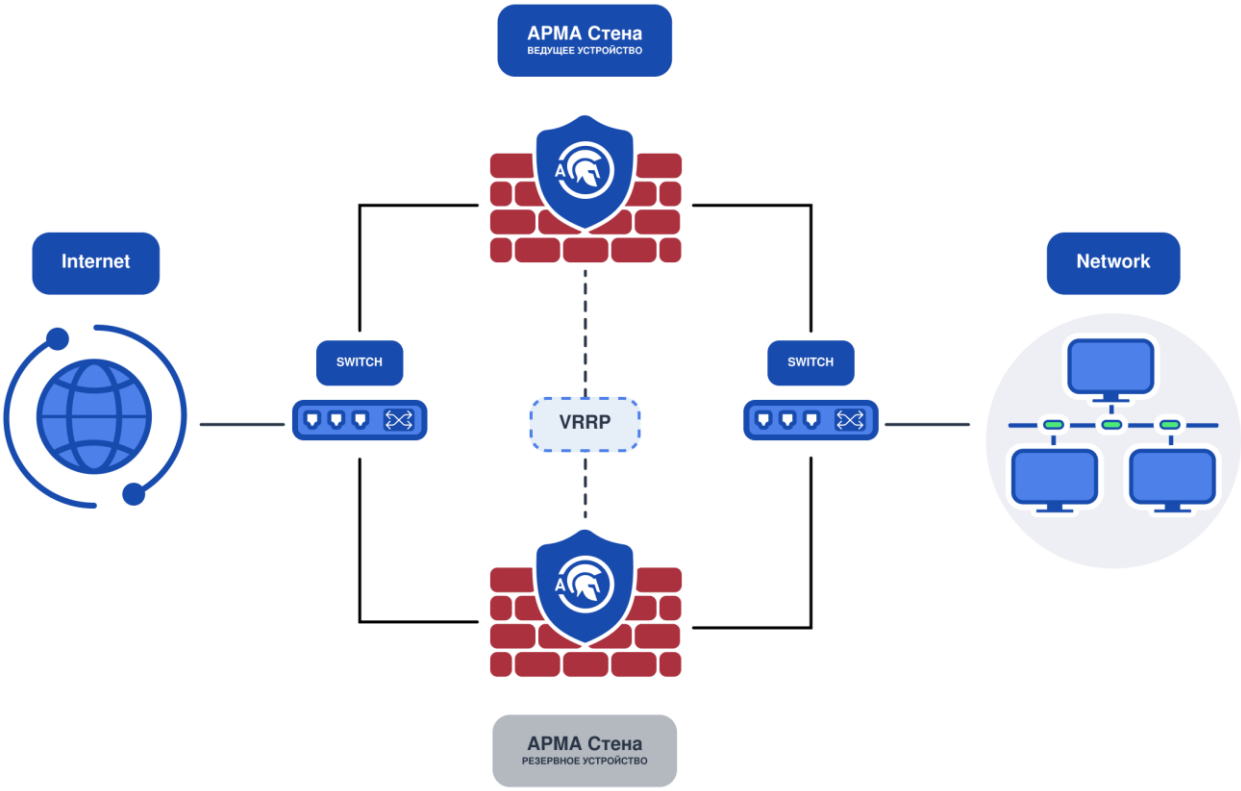


Рисунок – Режим отказоустойчивого кластера

6 КОНТРОЛЬ УПРАВЛЕНИЯ ДОСТУПОМ

6.1 Аутентификация

Аутентификация – это процесс проверки подлинности введённых пользователем имени и пароля. В **ARMA Стена** возможна аутентификация с использованием локальной или внешней БД пользователей. Для хранения УЗ пользователей по умолчанию применяется локальная БД. В качестве внешней БД служат различные внешние серверы авторизации.

В системе **ARMA Стена** предусмотрена учётная запись **«admin»**, обладающая правами суперпользователя.

6.2 Локальные учётные записи

6.2.1 Добавление пользовательских учётных записей

Для создания пользовательской УЗ необходимо в режиме конфигурирования ввести следующие команды с указанием учётных данных:

```
set system login user User1 full-name "Fedor Volov"
set system login user User1 authentication plaintext-password PasswordUser1
```

где:

- **«User1»** – логин;
- **«Fedor Volov»** – имя пользователя;
- **«PasswordUser1»** – пароль.

Учётные данные приведены в качестве примера.

Для просмотра списка УЗ необходимо ввести следующую команду:

- в эксплуатационном режиме:

```
admin@ngfwos:~$ show system login users

#Пример просмотра списка УЗ:
Username        Type        Locked        Tty        From              Last login
----------    ------    --------    -----    -----------    ------------------------
admin              ngfwos    False          pts/0    10.20.21.11    Wed Mar 19 09:34:37 2025
test               ngfwos    False          pts/1    10.20.21.11    Wed Mar 19 13:47:46 2025
admin@ngfwos:~$
```

- в конфигурационном режиме:

```
show system login user

#Пример просмотра списка УЗ:
 user admin {
        authentication {
            encrypted-password $6$rounds=6560...30
        }
        class NGFW_Super_Administrators
 }
 user test {
        authentication {
            encrypted-password $6$rounds=6560...j1
        }
 }
[edit]
admin@ngfwos#
```

6.2.2 Политика паролей учётных записей

Команды конфигурации политики паролей УЗ:

1. Указать максимальную длину пароля:

```
set system login password maximum-length <max>
```

где **<max>** - значение максимальной длины пароля. Возможно указать значение в диапазоне от «1» до «128». По умолчанию используется значение «128».

2. Указать минимальную длину пароля:

```
set system login password minimum-length <min>
```

где **<min>** - значение минимальной длины пароля. Возможно указать значение в диапазоне от «1» до «64». По умолчанию используется значение «1».

3. Указать минимальное количество цифр в пароле:

```
set system login password minimum-numerics <number>
```

где **<number>** - количество цифр в пароле. Возможно указать значение в диапазоне от «1» до «32». По умолчанию используется значение «0».

4. Указать минимальное количество специальных символов в пароле:

```
set system login password minimum-special <number>
```

где **<number>** - количество специальных символов. Возможно указать значение в диапазоне от «1» до «32». По умолчанию используется значение «0».

В пароле допускается использовать следующие специальные символы: **«!», «#», «%», «&», «(», «)», «*», «+», «,», «.», «/», «:», «;», «<», «=», «>», «@», «[», «]», «^», «_», «{», «|», «}», «~», «`», «$»**.

5. Указать минимальное количество букв в нижнем регистре в пароле:

```
set system login password minimum-lower-case <number
```

где **<number>** - количество букв в нижнем регистре. Возможно указать значение в диапазоне от «1» до «32». По умолчанию используется значение «0».

6. Указать минимальное количество букв в верхнем регистре в пароле:

```
set system login password minimum-upper-case <number>
```

где **<number>** - количество букв в верхнем регистре. Возможно указать значение в диапазоне от «1» до «32». По умолчанию используется значение «0».

6.2.3 Настройка временной блокировки УЗ

1. Указать количество попыток ввода пароля, после которых УЗ будет заблокирована:

```
set system login retry-options attemps-before-block <number>
```

где **<number>** - количество попыток. Возможно указать значение в диапазоне от «1» до «100».

Примечание:

Для повышения безопасности и снижения эффективности брутфорс-атак рекомендуется ограничить количество попыток ввода пароля для учётных записей пользователей.

2. Указать время блокировки УЗ после превышения количества попыток ввода пароля:

```
set system login retry-options lockout-period seconds <sec>
set system login retry-options lockout-period minutes <min>
set system login retry-options lockout-period hours <hour>
```

где:

- **<sec>** - количество секунд. Возможно указать значение в диапазоне от «0» до «60»;

- **<min>** - количество минут. Возможно указать значение в диапазоне от «0» до «60»;
- **<hour>** - количество часов. Возможно указать значение в диапазоне от «0» до «168».

Общее время блокировки будет равняться сумме настроенных секунд, минут и часов. По умолчанию УЗ блокируется на 10 минут.

Примечание:

Настройки временной блокировки учётной записи в системе **ARMA Стена** действуют независимо от используемого метода аутентификации.

Примечание:

Для досрочной разблокировки УЗ необходимо ввести команду **«sudo pam_tally2 -u <user> –reset»** под УЗ **«admin»**.

6.2.4 Назначение прав доступа пользовательским учётным записям

Для ограничения прав пользовательских учётных записей используются классы.

Класс представляет собой перечень разрешённых команд для использования в **ARMA Стена**.

В системе **ARMA Стена** по умолчанию предусмотрено четыре класса (см. Таблица «Список классов по умолчанию»).

Таблица «Список классов по умолчанию»

Класс	Описание	Список разрешённых команд
NGFW_Super_Administrators	Специальный класс для встроенной УЗ admin	ЭКСПЛУАТАЦИОННЫЙ РЕЖИМ: ● полный доступ. КОНФИГУРАЦИОННЫЙ РЕЖИМ: ● полный доступ.
NGFW_Administrators	Группа администраторов с полными правами	ЭКСПЛУАТАЦИОННЫЙ РЕЖИМ: ● полный доступ, за исключением команды пересчёта контрольной суммы (integrity-control). КОНФИГУРАЦИОННЫЙ РЕЖИМ: ● полный доступ, за исключением

Класс	Описание	Список разрешённых команд
		команды редактирования - *edit* и выключения блокировки сетевых интерфейсов в аварийном режиме - *emergency remove-nics*.
Network_Administrators	Группа администраторов сети	ЭКСПЛУАТАЦИОННЫЙ РЕЖИМ: ● clear ● force • arp • ipv6-nd • ipv6-rd • mtu • ntp • openconnect-server • owping • twping • vrf ● generate • interfaces • ipsec • macsec • openconnect • openvpn • pki • public-key-command • ssh • system

Класс	Описание	Список разрешённых команд
		• tech-support • wireguard • import • monitor • mtr • ping • poweroff • reboot • release • renew • reset • restart • set • pppoe-server • show • arp • babel • bfd • bgp • bridge • conntrack • conntrack-sync • date • dhcp • dhcpv6 • dns • evpn • host • interfaces

Класс	Описание	Список разрешённых команд

		• ip
		• ipoe-server
		• ipv6
		• isis
		• l2tp-server
		• lldp
		• logging
		  ○ conntrack-sync
		  ○ dhcp
		  ○ dhcpv6
		  ○ dns
		  ○ https
		  ○ ipoe-server
		  ○ lldp
		  ○ nat
		  ○ ntp
		  ○ pppoe
		  ○ pppoe-server
		  ○ snmp
		  ○ ssh
		  ○ vpn
		  ○ vrrp
		  ○ webproxy
		• monitoring
		• mpls
		• nat

Класс	Описание	Список разрешённых команд
		• nat66 • nhrp • ntp • openconnect-server • openvpn • pki • policy • poweroff • pppoe-server • pptp-server • protocols • reboot • reverse-proxy • route-map • rpki • segment-routing • sflow • snmp • ssh • sstp-server • table • tech-support • version • vpn • vrf • vrrp • wan-load-balabce • webproxy • zebra

Класс	Описание	Список разрешённых команд

		• telnet
		• traceroute
		• update
		• wake-on-lan
		КОНФИГУРАЦИОННЫЙ РЕЖИМ:
		• comment
		• copy/delete/rename/set/show
		  • high-availability
		  • interfaces
		  • load-balancing
		  • nat
		  • nat64
		  • nat66
		  • policy
		  • protocols
		  • pki
		  • qos
		  • service
		  ○ active-sync-proxy
		  ○ broadcast-relay
		  ○ dhcp-relay
		  ○ dhcp-server
		  ○ dhcpv6-relay
		  ○ dhcpv6-server

Класс	Описание	Список разрешённых команд
		○ dns ○ event-handler ○ https ○ ipoe-server ○ lldp ○ mdns ○ ndp-proxy ○ ntp ○ pppoe-server ○ router-advert ○ snmp ○ ssh ○ stunnel ○ tftp-server ○ webproxy • system ○ conntrack ○ flow-accounting ○ frr ○ ip ○ ipv6

Класс	Описание	Список разрешённых команд
		○ logging ○ name-server ○ proxy ○ sflow ○ static-host-mapping • vpn • vrf
Security_Engineers	Группа инженеров безопасности	ЭКСПЛУАТАЦИОННЫЙ РЕЖИМ: ● generate • firewall ● monitor ● ping ● poweroff ● reboot ● show • date • conntrack • firewall • flow-accounting • host • interfaces • logging ○ firewall ○ idps ○ nat • nat • nat66

Класс	Описание	Список разрешённых команд
		• pki • poweroff • reboot • tech-support • version ● suricata ● telnet ● traceroute ● update КОНФИГУРАЦИОННЫЙ РЕЖИМ: ● comment ● copy/delete/rename/set/show • nat • nat64 • nat66 • pki • service ○ event-handler ○ ids • suricata • system ○ conntrack ○ logging

Примечание:

Класс пользователя **«NGFW_Super_Administrators»** предназначен исключительно для встроенной учётной записи **«admin»**. Добавление других учётных записей в этот класс не допускается.

Класс пользователя **«NGFW_Super_Administrators»** не может быть изменён или удалён.

Для настройки классов необходимо ввести следующую команду в конфигурационном режиме:

```
set system login class <name_class> <operational-command | configure-command> <team>
```

где:

- **<name_class>** - уникальное имя класса;
- **<operational-command>** - установка прав на использование команд в эксплуатационном режиме;
- **<configure-command>** - установка прав на использование команд в конфигурационном режиме;
- **<team>** - разрешённая команда.

Для добавления описания класса следует ввести команду:

```
set system login class <name_class> description <text>
```

где **<text>** - текстовое описание класса. Описание не должно превышать «255» символов. Если описание содержит пробелы или символ «#», то его необходимо заключить в двойные кавычки.

Для добавления класса к учётной записи пользователя необходимо ввести команду:

```
set system login user <name_user> class <name_class>
```

где **<name_user>** - имя учётной записи пользователя.

Для каждой учётной записи пользователя возможно назначить только один класс.

Для просмотра списка разрешённых команд для класса необходимо в режиме конфигурации ввести команду:

```
show system login class [name_class] [operational-command | configure-command]
```

Примечание:

Встроенной учётной записи **«admin»** запрещено изменять класс, удалять или отключать её.

Примечание:

При отсутствии назначенного класса доступа или наличии класса с пустым набором разрешённых команд, пользователь получает доступ к минимальному набору команд. Данный механизм обеспечивает необходимый минимум функционала для взаимодействия с системой в условиях отсутствия явных прав доступа.

Список разрешённых команд в **эксплуатационном режиме**:

- **configure** - войти в режим настройки;
- **exit** - выйти из системы.

Список разрешённых команд в **конфигурационном режиме**:

- **commit** - зафиксировать текущий набор изменений;
- **commit-confirm** - зафиксировать текущий набор изменений с обязательным «подтверждением»;
- **confirm** - подтвердить предыдущую фиксацию - подтвердить;
- **discard** - отменить незафиксированные изменения;
- **exit** - выход с этого уровня конфигурации;
- **run** - выполнить команду эксплуатационного режима;
- **save** - сохранить конфигурацию в файл.

6.2.4.1 Пример настройки прав учётной записи пользователя

В качестве примера приведён список команд для создания учётной записи **«test»** с паролем **«Password»** и разрешением прав на использование команд: ping, set service dns, delete service dns, show service dns.

```
set system login user test authentication plaintext-password Password
set system login class c_dns
set system login class c_dns operational-command ping
set system login class c_dns operational-command configure
set system login class c_dns configure-command "set service dns"
set system login class c_dns configure-command "delete service dns"
set system login class c_dns configure-command "show service dns"
set system login user test class c_dns
commit
save
```

6.2.5 Блокирование доступа пользователя

При необходимости блокирования доступа пользователя следует ввести следующую команду:

```
set system login user User1 disable
```

6.2.6 Завершение сессии пользователя

Для завершения сессии пользователя необходимо в эксплуатационном режиме ввести команду **«exit»**:

```
admin@ngfwos:~$ exit
```

6.3 Аутентификация RADIUS

RADIUS (Remote Authentication Dial-In User Service) — это сетевой протокол, который обеспечивает централизованную аутентификацию, авторизацию и учёт пользователей.

Система **ARMA Стена** поддерживает RADIUS-серверы в качестве серверной части для пользовательской аутентификации.

Атрибут **«cisco-avpair = shell:priv-lvl»** в **Radius**-сервере предназначен для определения уровня привилегий учётных записей. В системе **ARMA Стена** реализованы два уровня доступа для учётных записей **Radius**-сервера:

- **Полный доступ (priv-lvl=15)** - предоставляет разрешение на выполнение всех команд системы, за исключением команды «sudo».
- **Ограниченный доступ (priv-lvl=0-14)** - предоставляет разрешение на выполнение ограниченного набора команд, представленных таблице «Список разрешённых команд для УЗ RADIUS-сервера с ограниченным доступом»).

Таблица «Список разрешённых команд для УЗ RADIUS-сервера с ограниченным доступом»

Режим работы	Команда	Краткое описание
Эксплуатационный	**exit**	Выход из системы
Эксплуатационный	**monitor**	Мониторинг системной информации
Эксплуатационный	**ping**	Отправить запрос эха ICMP
Эксплуатационный	**show**	Просмотр настроек и журнала событий системы
Эксплуатационный	**telnet**	Telnet к узлу
Эксплуатационный	**traceroute**	Трассировка сетевого пути к узлу

Перед началом настройки внешнего **Radius**-сервера необходимо убедиться в наличии сетевого доступа к данному серверу.

Примечание:

При обнаружении идентичных учётных записей в локальной базе данных пользователей и в **Radius**-сервере, система **ARMA Стена** осуществляет аутентификацию посредством локальной учётной записи. Данный механизм приоритезации не применяется в случае установки режима безопасности **«mandatory»**, который принудительно использует аутентификацию через **Radius**-сервер, игнорируя наличие дублирующих учётных записей в локальной базе данных.

6.3.1 Добавление внешнего Radius-сервера

Для добавления внешнего **Radius**-сервера необходимо выполнить следующие настройки:

1. Указать IP-адрес **Radius**-сервера и общий ключ, который используется для шифрования обмена данными между **ARMA Стена** и **Radius**-сервером:

```
set system login radius server <address> key <secret>
```

где:

- **<address>** - IP-адрес Radius-сервера в формате <x.x.x.x> для IPv4 или <h:h:h:h:h:h:h:h> для IPv6;
- **<secret>** - значение ключа, который используется для шифрования.

2. Указать порт, через который будет осуществляться доступ к **Radius**-серверу:

```
set system login radius server <address> port <port>
```

где **<port>** - номер порта. Возможно указать значение в диапазоне от «1» до «65535». По умолчанию используется порт «1812».

6.3.2 Дополнительные команды настройки Radius-сервера

- Указать приоритет **Radius**-серверу:

```
set system login radius server <address> priority <1-255>
```

где **<1-255>** - номер приоритета для указанного Radius-сервера. Возможно указать значение в диапазоне от «1» до «255». По умолчанию используется значение «255». Чем ниже число, тем выше приоритет сервера.

Используется для определения порядка обращения к Radius-серверам при аутентификации.

- Установить время ожидания для получения ответа от **Radius**-сервера:

```
set system login radius server <address> timeout <timeout>
```

где **<timeout>** - время ожидания в секундах. Возможно указать значение в диапазоне от «1» до «240». По умолчанию используется значение «2».

Определяет, как долго **ARMA Стена** будет ожидать ответа от Radius-сервера. Помогает предотвратить зависание системы при недоступности сервера. При отсутствии ответа в течение заданного времени система перейдёт к локальной аутентификации или к другим настроенным Radius-серверам.

При настройке тайм-аута необходимо определить значение, которое обеспечит оптимальное соотношение между скоростью проверки подлинности и безопасностью. Слишком малое значение тайм-аута может привести к ложным отказам при нормальной работе сети, а слишком большое — к замедлению процесса аутентификации.

- Временно отключить указанный **Radius**-сервера:

```
set system login radius server <address> disable
```

Команда временно отключает указанный Radius-сервер, в результате чего система перестаёт обращаться к нему при попытке аутентификации пользователей. Для отмены отключения сервера необходимо удалить данную настройку через команду «delete».

- Установить IP-адрес источника, с которого будут отправляться запросы к **Radius**-серверам:

```
set system login radius source-address <address>
```

где **<address>** - IP-адрес источника в формате <x.x.x.x> для IPv4 или <h:h:h:h:h:h:h:h> для IPv6.

Команда задает фиксированный IP-адрес, с которого **ARMA Стена** будет отправлять запросы ко всем настроенным Radius-серверам. Это особенно важно в случаях, когда Radius-серверы ограничивают доступ только с определенных IP-адресов.

- Определить режим безопасности для аутентификации Radius:

```
set system login radius security-mode <mandatory | optional>
```

- **mandatory** - вся аутентификация осуществляется исключительно через Radius-сервер. Локальная база пользователей отключается. При недоступности Radius-сервера доступ к устройству блокируется.
- **optional** - осуществляется первичная попытка аутентификации через Radius-сервер, при неудаче производится попытка локальной аутентификации. Доступ к устройству сохраняется при недоступности Radius-сервера. По умолчанию установлен режим «optional».

Команда определяет порядок аутентификации пользователей на устройстве **ARMA Стена**. Режим **«mandatory»** обеспечивает максимальную безопасность, но несет риски потери доступа. Режим **«optional»** предоставляет баланс между безопасностью и доступностью, но требует дополнительного администрирования.

- Указать виртуальную сеть (VRF), через которую будет осуществляться подключение к **Radius**-серверу:

```
set system login radius vrf <vrf>
```

где **<vrf>** - имя виртуальной сети vrf.

Команда используется для указания, что все подключения к Radius-серверам должны исходить из указанной виртуальной сети (vrf). Это позволяет изолировать трафик аутентификации RADIUS в определённой виртуальной сети, что может быть полезно в сложных сетевых конфигурациях, где требуется сегментация трафика.

6.4 Multifactor Radius Adapter

ARMA Стена предоставляет возможность проводить аутентификацию пользователей на удалённом **Radius**-сервере. В данном примере в качестве **Radius**-сервера будет использоваться **Multifactor Radius Adapter**, который доступен в двух версиях: для Windows и для Linux.

6.4.1 Multifactor Radius Adapter - Windows

В качестве примера настройки Multifactor Radius Adapter для Windows будет использоваться стенд представленный на рисунке (см. Рисунок – Схема стенда для настройки Multifactor Radius Adapter - Windows).

Рисунок – Схема стенда для настройки Multifactor Radius Adapter - Windows

Для получения доступа необходимо выполнить следующие шаги:

1. Настроить **ARMA Стена**.
2. Настроить Windows Server.
3. Проверка работы службы.

6.4.1.1 Настройка ARMA Стена

6.4.1.1.1 Настройка интерфейсов

На первом шаге необходимо предоставить **ARMA Стена** доступ к интернету. Для этого требуется подключить интерфейс «eth0» к корпоративной сети, назначить ему IP-адрес вручную или через DHCP-сервер и присвоить описание «WAN»:

```
set interfaces ethernet eth0 address <x.x.x.x/x | dhcp>
set interfaces ethernet eth0 description "WAN"
commit
save
```

Далее необходимо назначить интерфейсу «eth1», направленному в локальную подсеть, IP-адрес и присвоить ему описание «LAN»:

```
set interfaces ethernet eth1 address 192.168.1.1/24
set interfaces ethernet eth1 description "LAN"
commit
save
```

Для просмотра информации о настройках интерфейсов необходимо ввести следующую команду в эксплуатационном режиме (см. Рисунок – Назначенные IP-адреса интерфейсам LAN и WAN):

```
admin@ngfwos:~$ show interfaces
```

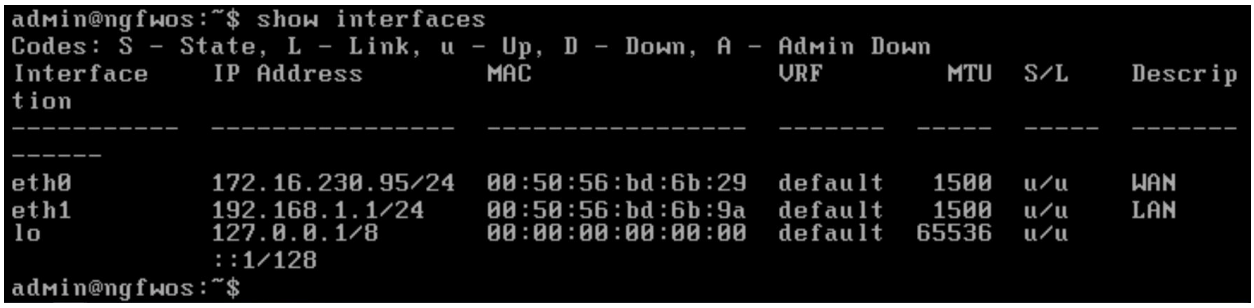


Рисунок – Назначенные IP-адреса интерфейсам LAN и WAN

6.4.1.1.2 Настройка DHCP-сервера

Необходимо настроить DHCP-сервер на интерфейсе «eth1» для автоматической выдачи адресов устройствам в локальной сети:

```
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 default-router 192.168.1.1
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 name-server 192.168.1.1
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 lease 86400
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 range 0 start 192.168.1.100
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 range 0 stop 192.168.1.150
commit
save
```

где:

- **LAN** - имя пула;
- **192.168.1.1** - IP-адрес шлюза по умолчанию;
- **86400** - время аренды IP-адресов в секундах;
- **192.168.1.100** - начальный IP-адрес пула адресов;
- **192.168.1.150** - конечный IP-адрес пула адресов.

6.4.1.1.3 Настройка DNS-ретрансляции

Команды настройки DNS-ретрансляции:

```
set service dns forwarding cache-size 0
set service dns forwarding listen-address 192.168.1.1
set service dns forwarding allow-from 192.168.1.0/24
commit
save
```

где:

- **cache-size 0** - запись в кэш DNS-ретрансляции отключена;
- **192.168.1.1** - IP-адрес интерфейса, на котором прослушиваются запросы DNS;
- **192.168.1.0/24** - подсеть, на которой разрешён доступ к DNS-ретрансляции.

6.4.1.1.4 Настройка NAT

Для настройки правил NAT необходимо ввести следующие команды:

```
set nat source rule 11 outbound-interface name eth1
set nat source rule 11 source address 192.168.1.0/24
set nat source rule 11 translation address masquerade
commit
save
```

6.4.1.1.5 Добавление DNS-сервера

Для настройки DNS-сервера необходимо ввести следующие команды:

```
set system name-server 8.8.8.8
set system name-server 172.16.230.11
commit
save
```

где:

- **8.8.8.8** - публичный DNS-сервер google;
- **172.16.230.11** - DNS-сервер корпоративной сети.

6.4.1.1.6 Настройка маршрутизации

Для настройки шлюза по умолчанию необходимо ввести следующую команду:

```
set protocols static route 0.0.0.0/0 next-hop 172.16.230.1
commit
save
```

6.4.1.1.7 Добавление Radius-server

Для добавления Radius-server необходимо ввести следующие команды:

```
set system login radius server <192.168.1.x> key <secretRadius>
set system login radius server <192.168.1.x> port 1812
commit
save
```

где:

- **<192.168.1.x>** - IP-адрес, который был выдан Windows Server;
- **<secretRadius>** - секретный ключ, который был указан при конфигурировании Radius адаптера.

6.4.1.2 Настройка Windows Server

6.4.1.2.1 Первичная настройка

Перед началом работы необходимо, чтобы был настроен контроллер домена с установленными доменными службами Active Directory.

6.4.1.2.1.1 Настройка контроллера домена под Windows Server

1. Открыть окно «Сетевые подключения». Для этого необходимо нажать сочетание клавиш «Win+R» и в открывшемся окне «Выполнить» ввести команду «ncpa.cpl».
2. Нажать ПКМ по сетевому адаптеру, выбрать пункт меню «Свойства» и в открывшемся окне «Свойства» перейти в параметры «IP версии 4 (TCP/IPv4)» двойным нажатием ЛКМ (см. Рисунок – Окно свойств сетевого адаптера). Изменить динамические параметры IP и DNS на статические и ввести необходимые значения.

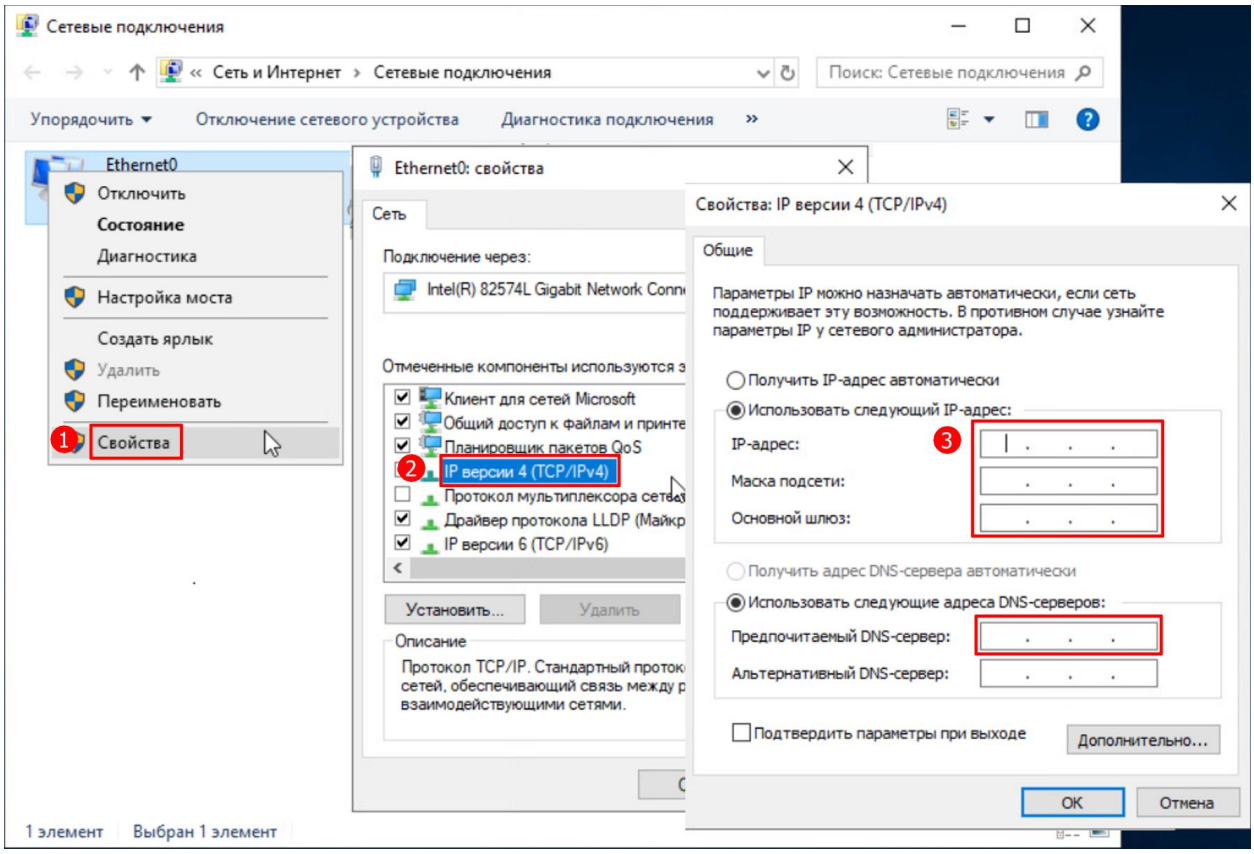


Рисунок – Окно свойств сетевого адаптера

3. Открыть окно «Свойство системы». Для этого необходимо нажать сочетание клавиш «Win+R» и в открывшемся окне «Выполнить» ввести команду «sysdm.cpl». Нажать кнопку «Изменить» и в окне «Изменение имени компьютера или домена» переименовать компьютер в «DC1» (см. Рисунок – Изменение имени хоста).

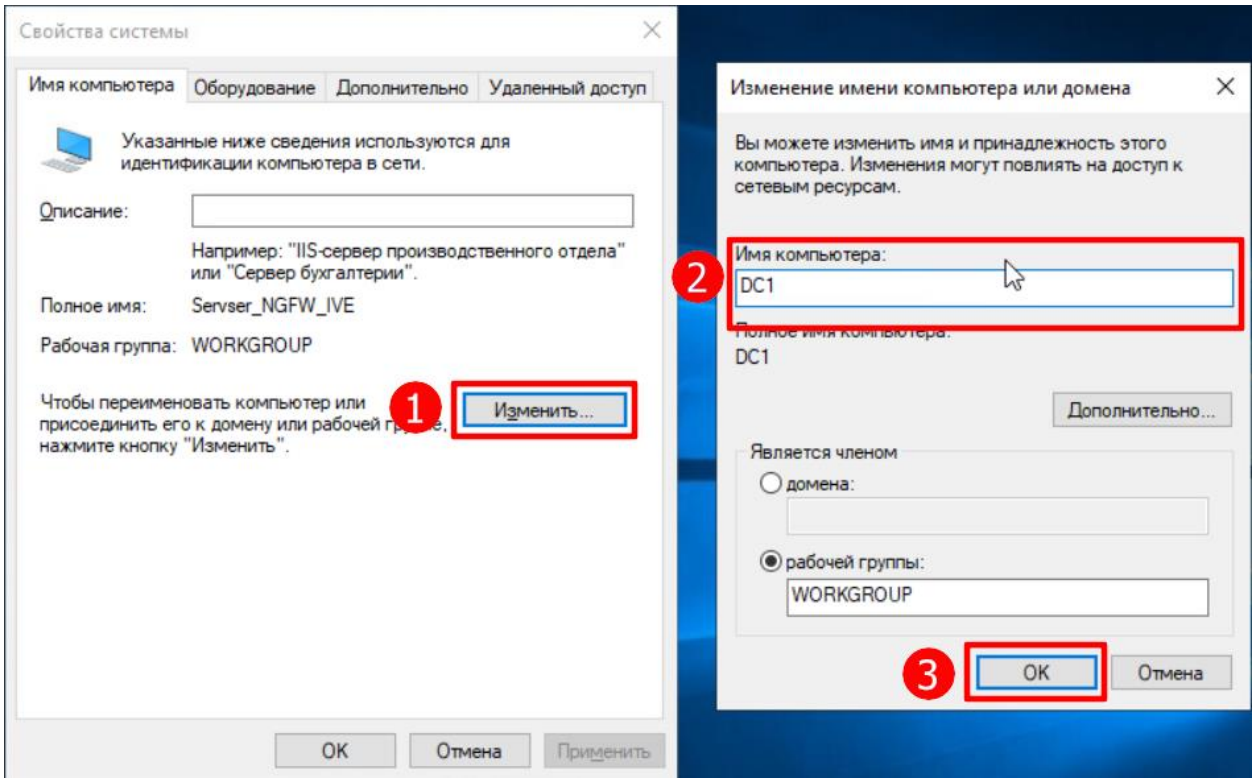


Рисунок – Изменение имени хоста

После применения настроек необходимо перезагрузить компьютер.

4. После перезагрузки компьютера необходимо открыть «Диспетчер серверов», выбрать опцию «Добавить роли и компоненты», указать сервер DC1 и нажать кнопку «Далее» (см. Рисунок – Выбор целевого сервера).

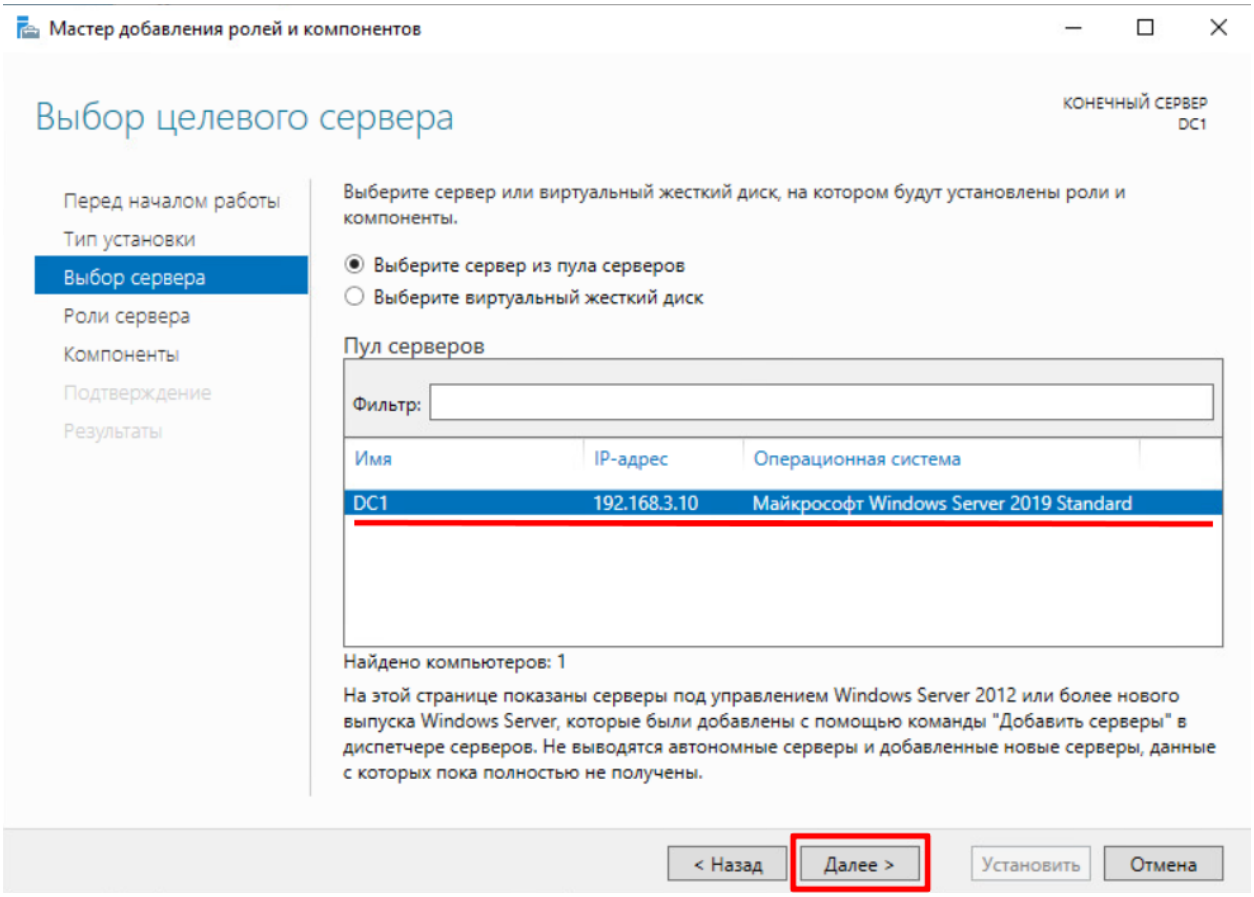


Рисунок – Выбор целевого сервера

5. В ролях выбрать «DNS-сервер» и «Доменные службы Active Directory», в компонентах оставить всё как есть и следовать мастеру установки (см. Рисунок – Роли сервера).

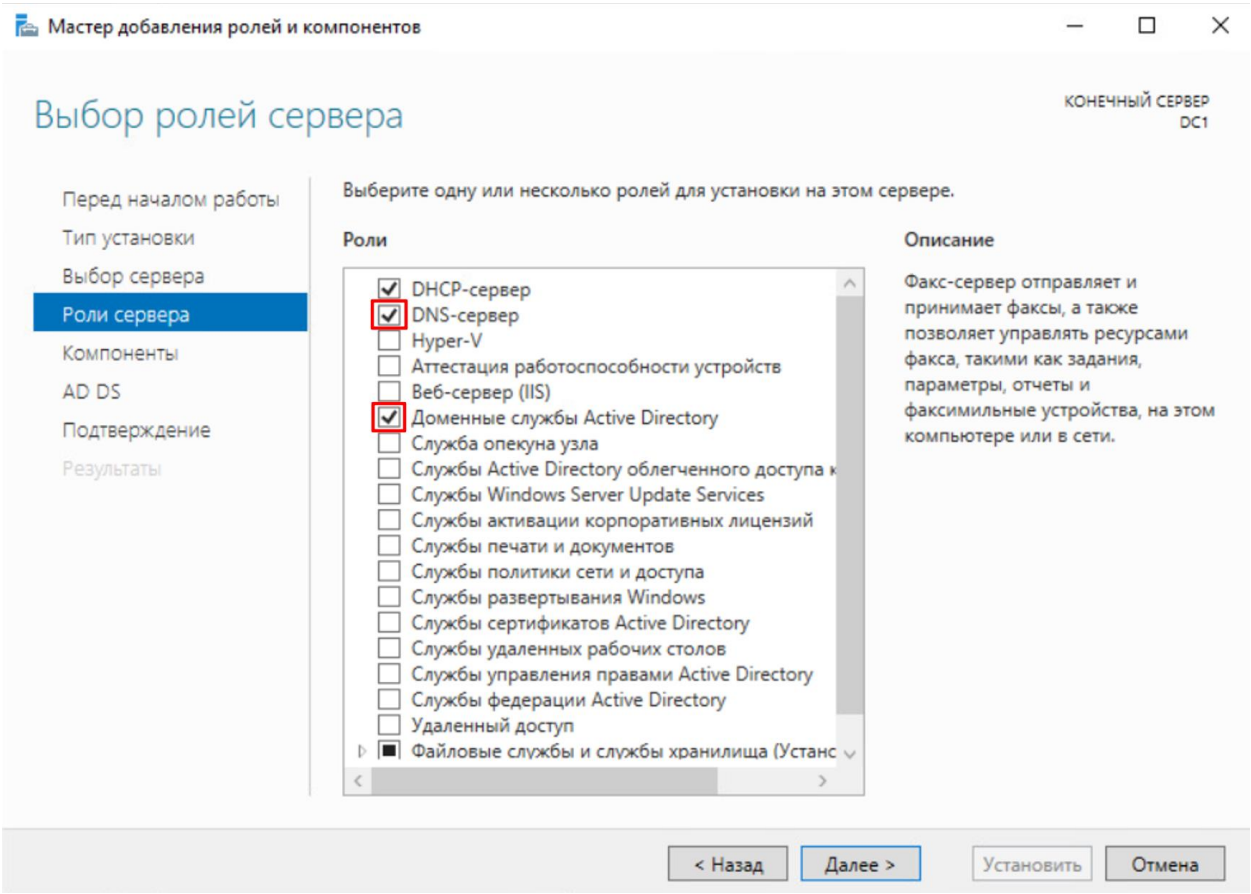


Рисунок – Роли сервера

6. Далее необходимо настроить Active Directory. Для этого требуется нажать на иконку флага с восклицательным знаком в Диспетчере устройств и выбрать «Повысить роль этого сервера до уровня контроллера домена» (см. Рисунок – Настройка Active Directory).

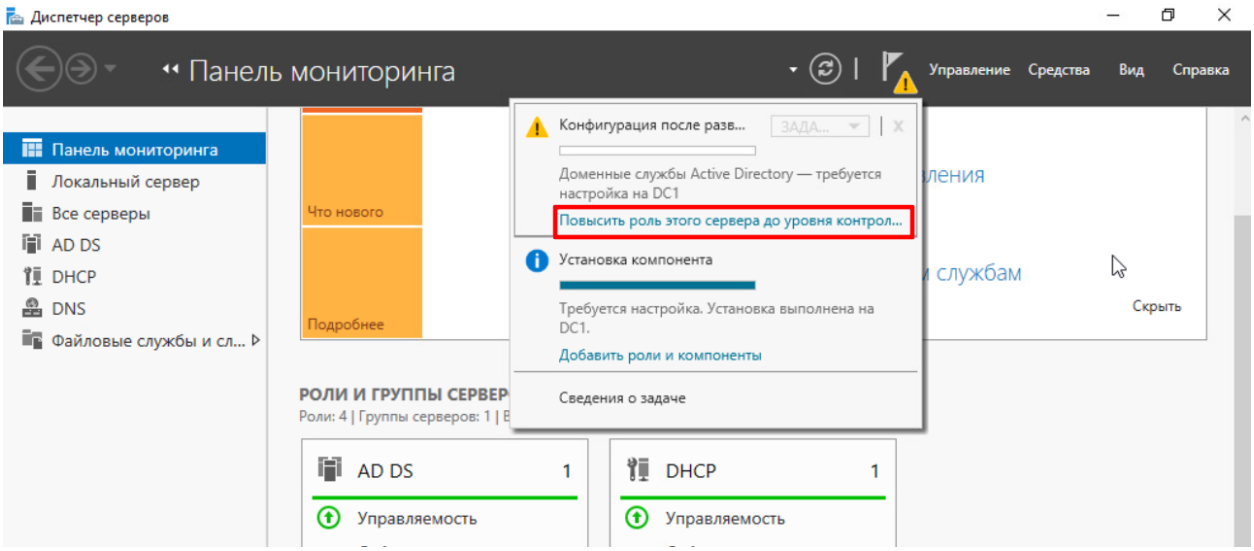


Рисунок – Настройка Active Directory

7. В открывшемся окне «Мастер настройки доменных служб Active Directory» выбрать «Добавить новый лес» и указать имя корневого домена. Имя

«IW2FA.ru» указано в качестве примера (см. Рисунок – Конфигурация Active Directory).

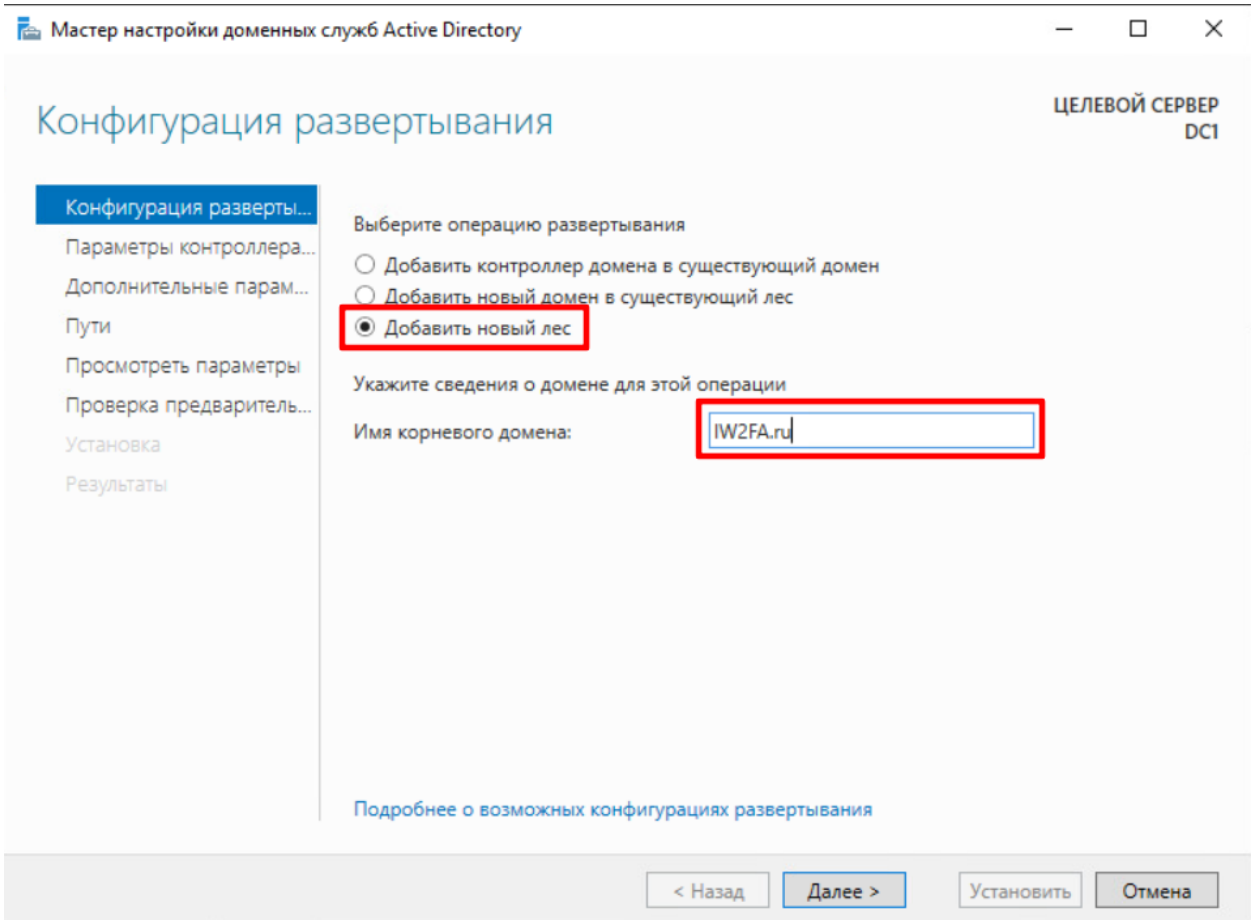


Рисунок – Конфигурация Active Directory

8. На следующем шаге необходимо придумать пароль для службы восстановления каталогов (см. Рисунок – Пароль для службы восстановления каталогов).

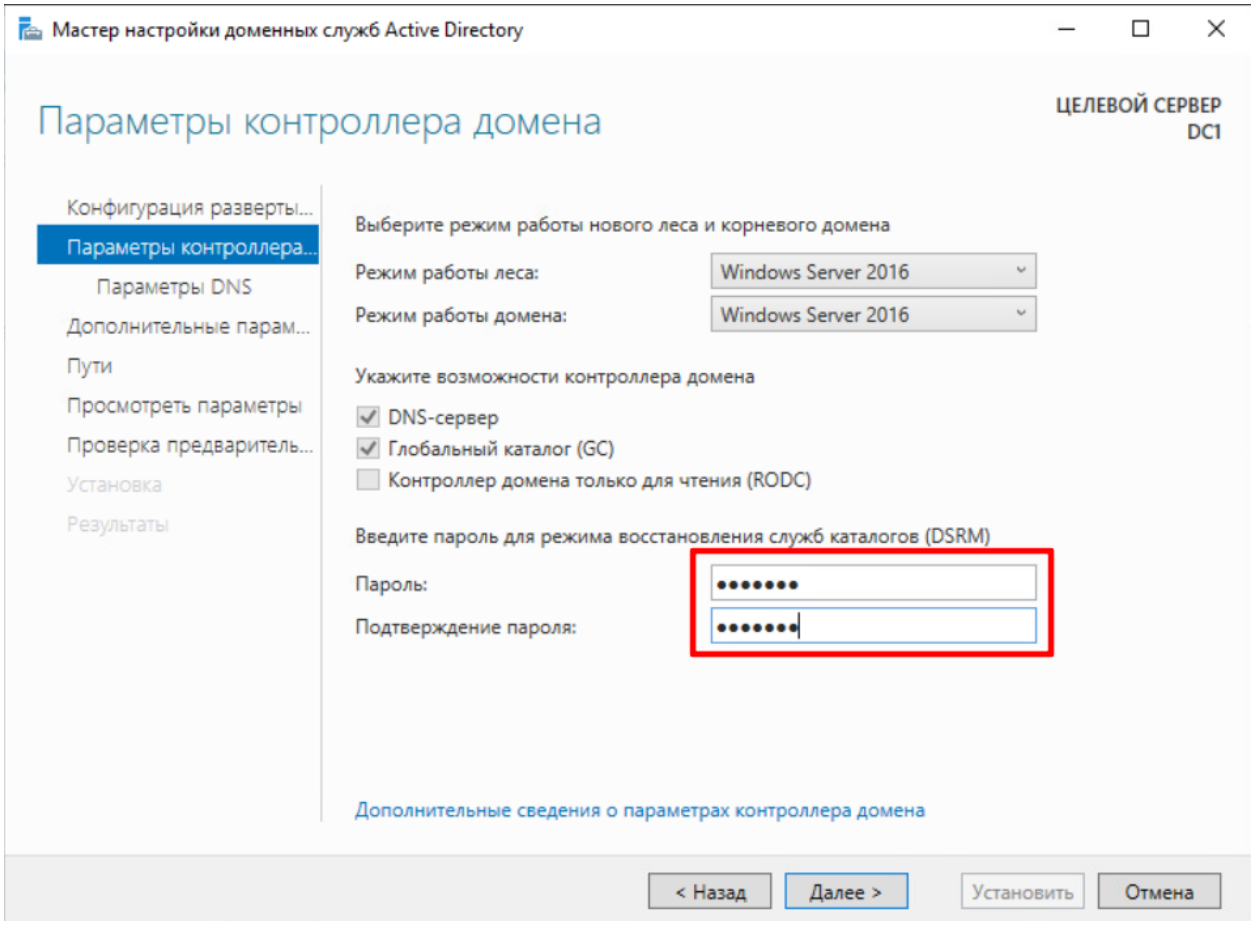


Рисунок – Пароль для службы восстановления каталогов

9. Мастер настройки предложит создать делегирование DNS. Однако в данном случае это не требуется, поэтому можно пропустить этот этап.
10. На следующем этапе мастер настройки автоматически пропишет имя домена NetBIOS. При необходимости возможно изменить его (см. Рисунок – Имя домена NetBIOS).

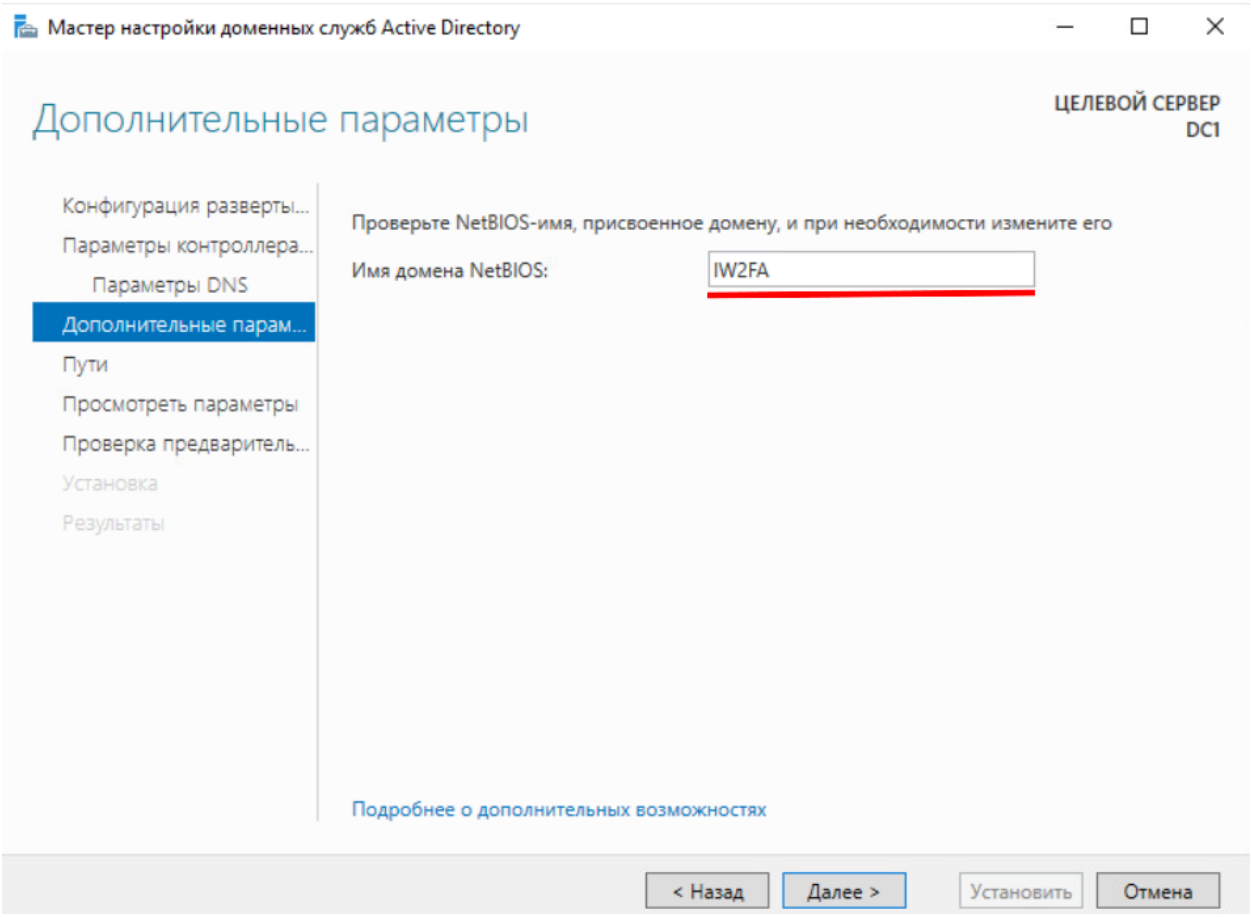


Рисунок – Имя домена NetBIOS

11. Выполнить настройку доменных служб Active Directory в соответствии с инструкциями мастера, не изменяя параметры по умолчанию. По завершении настройки перезагрузить компьютер.

6.4.1.2.1.2 Создание пользователей и групп Active Directory

1. Перейти в диспетчер серверов, открыть вкладку «Средства» и выбрать «Пользователи и компьютеры Active Directory» (см. Рисунок – Настройка пользователей Active Directory).

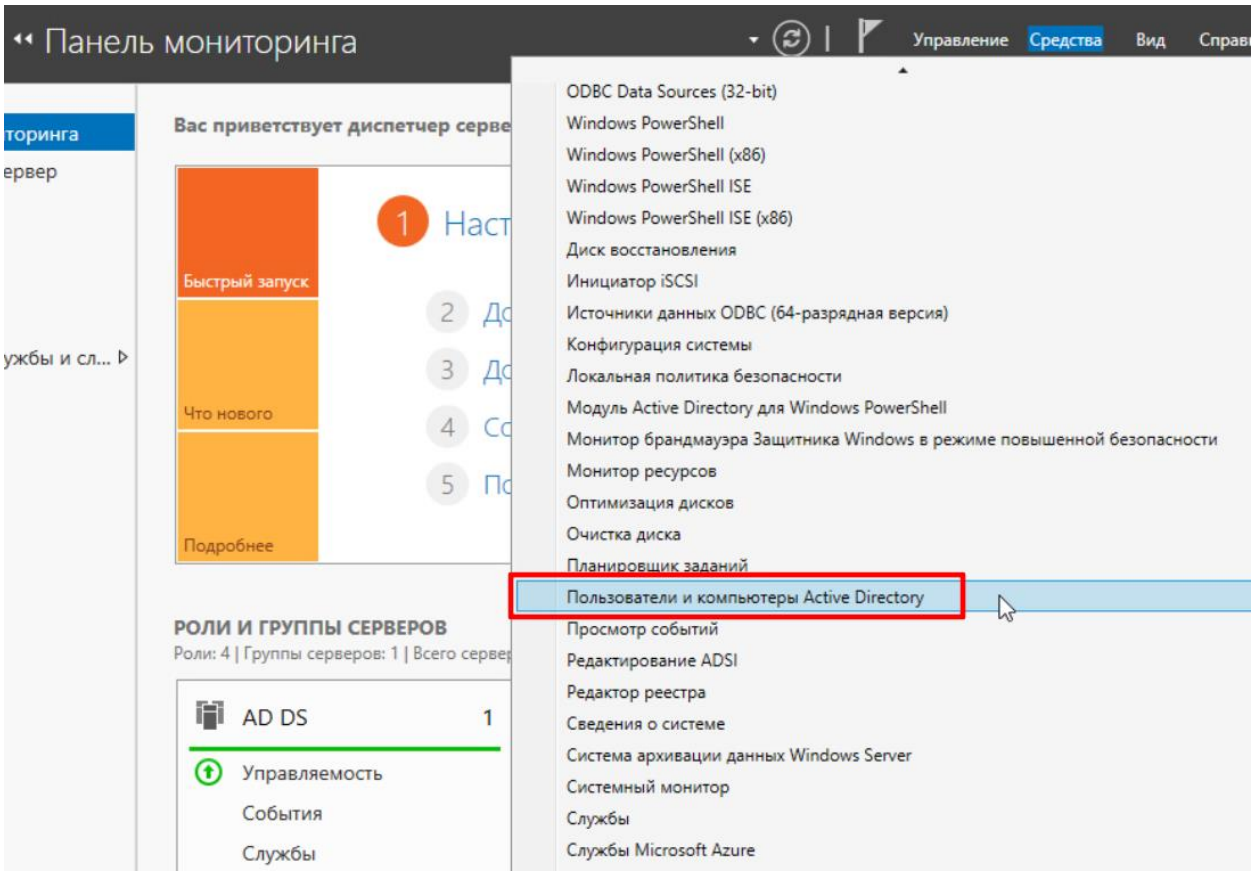


Рисунок – Настройка пользователей Active Directory

2. В открывшемся окне «Active Directory - пользователи и компьютеры» перейти в лес «IW2FA.ru», нажать ПКМ по директории «Users» и выбрать «Создать». В меню «Создать» выбрать «Пользователь» (см. Рисунок – Добавление пользователя).

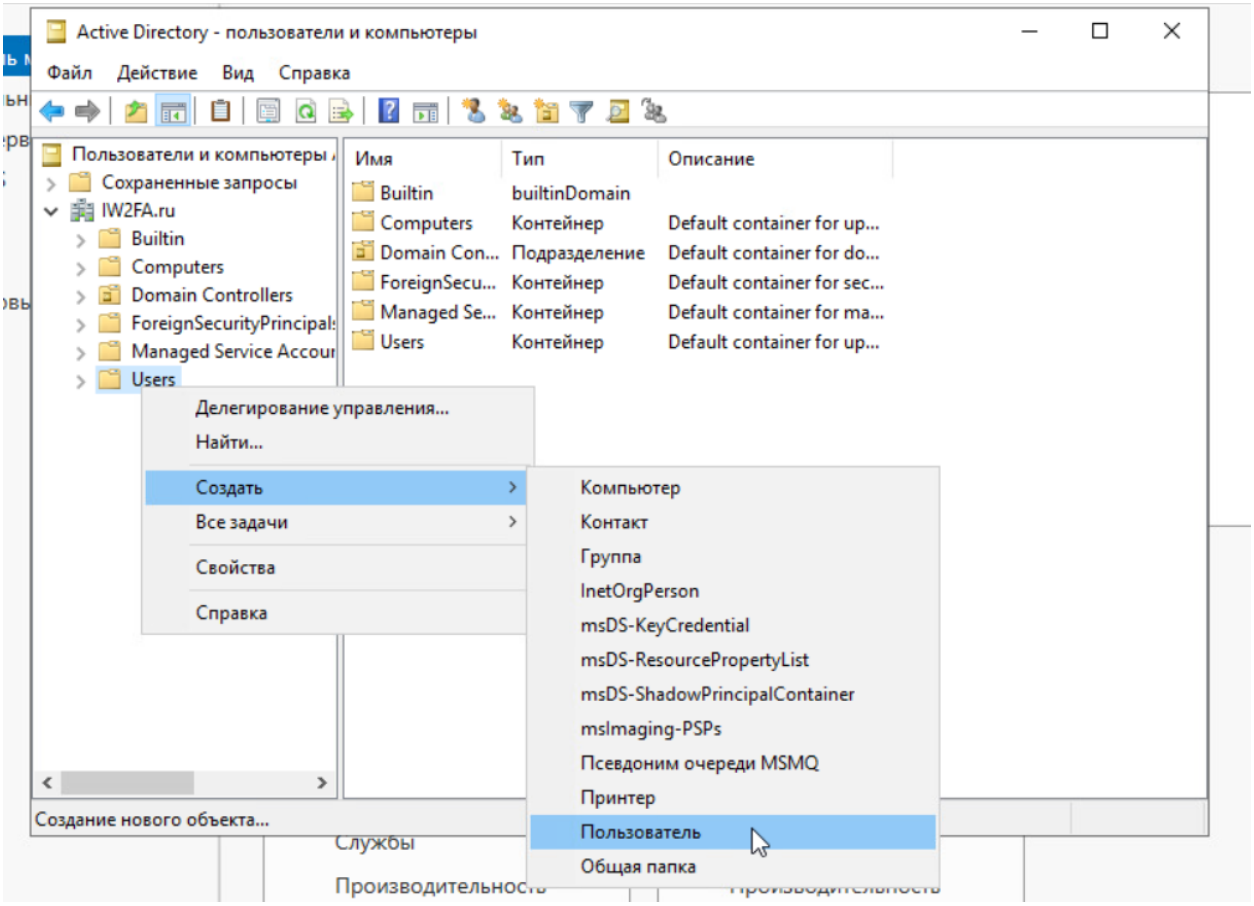


Рисунок – Добавление пользователя

3. Откроется окно «Новый объект - Пользователь». Заполнить поля: «Имя», в примере используется имя «User(6)01»; «Имя входа пользователя», в примере используется - «user01». По завершению ввода параметров, нажать кнопку «Далее». Ввести пароль для создаваемого пользователя и установить флажок в чекбокс «Срок действия пароля не ограничен».
4. По аналогии с созданием пользователей, для создания группы пользователей необходимо нажать ПКМ по директории «Users», выбрать «Создать», после чего выбрать «Группа».
5. В открывшемся окне «Новый объект - Группа» ввести название группы.
6. Для добавления пользователей в созданную группу необходимо нажать ПКМ по необходимой группе. В контекстном меню выберите пункт «Добавить в группу...» и в открывшемся окне найти и добавить требуемых пользователей.

6.4.1.2.2 Подготовка Radius адаптера

1. Необходимо скачать актуальную версию утилиты Radius адаптер с официального сайта https://multifactor.ru. Для этого в пункте «Теория» перейти во вкладку «RADIUS адаптер» и затем во вкладку «Windows версия», далее перейти по ссылке «сборка» (см. Рисунок – Документация Radius адаптера).

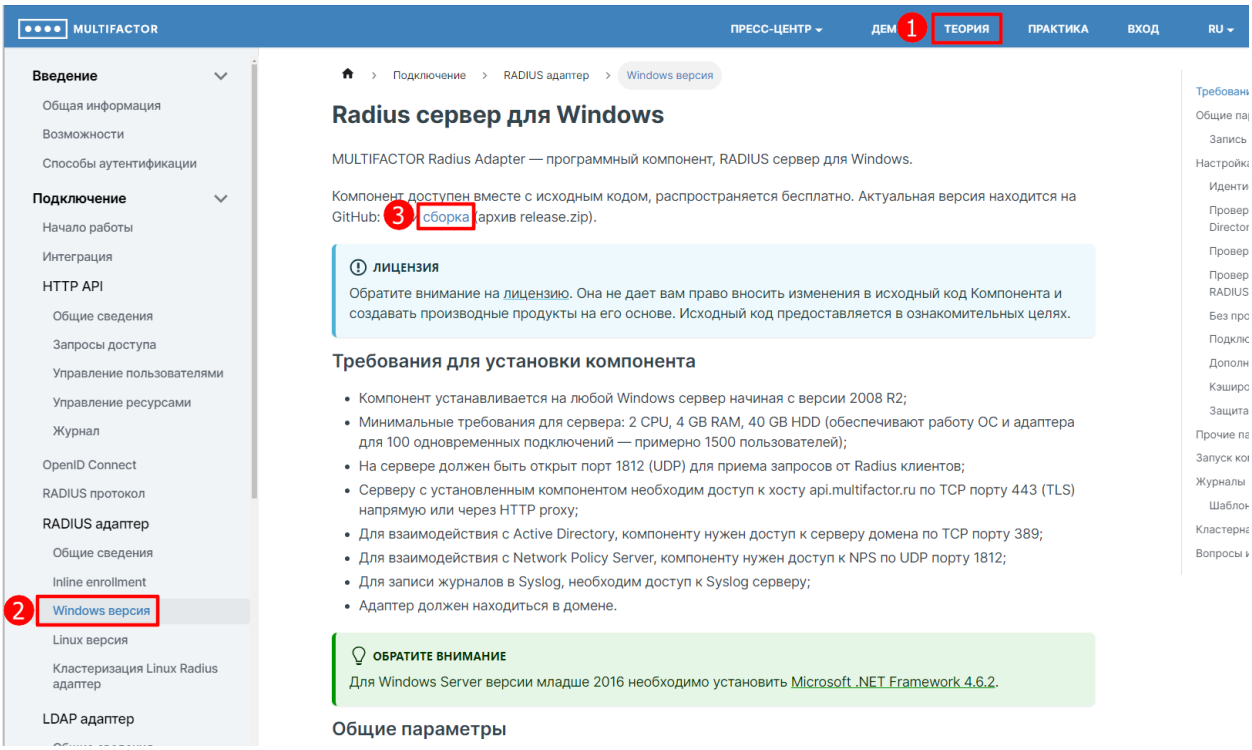


Рисунок – Документация Radius адаптера

2. После загрузки, распаковать скачанный архив и поместить его в корневую папку диска C в Windows Server.

6.4.1.2.3 Добавление Multifactor Radius Adapter

1. Перейти на сайт https://admin.multifactor.ru/account/login и зарегистрироваться (см. Рисунок – Регистрация на сайте Multifactor).

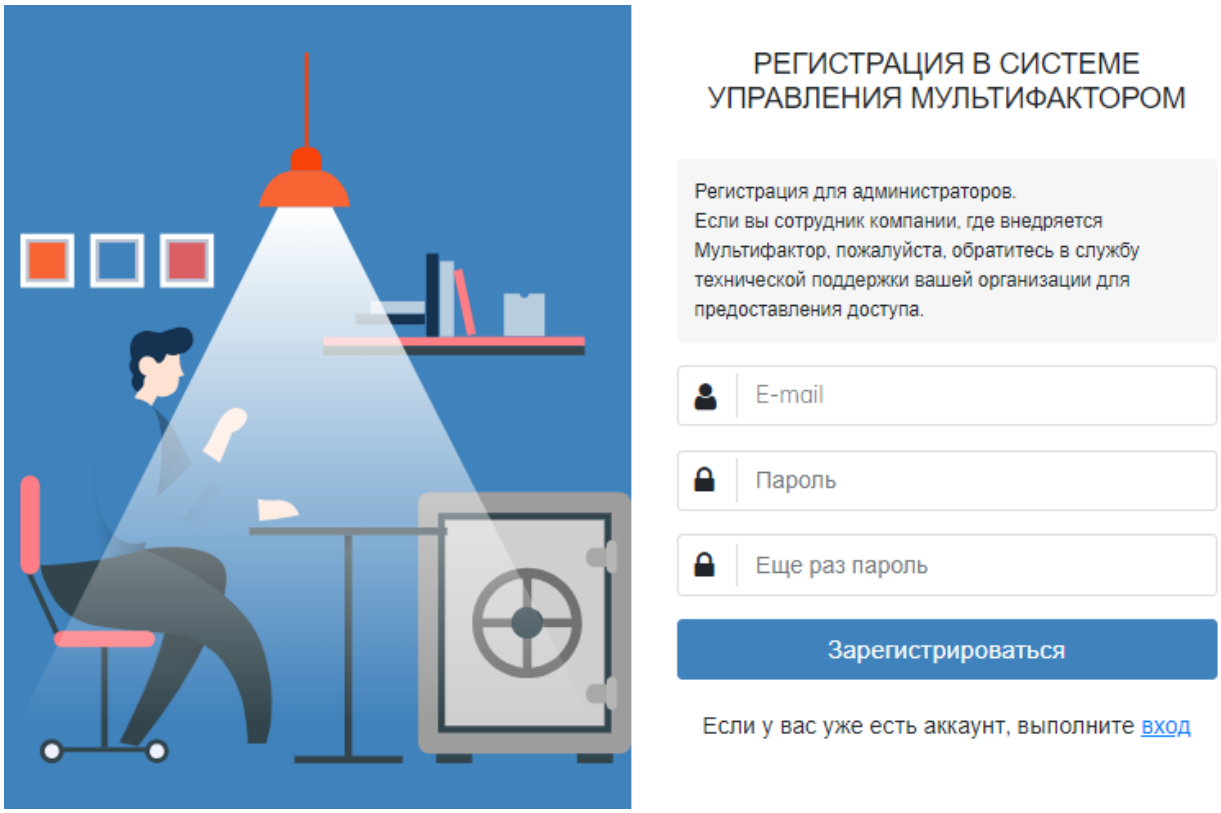


Рисунок – Регистрация на сайте Multifactor

2. После завершения регистрации будет запущен мастер настройки многофакторной аутентификации для административной панели. Будет предложено установить приложение Multifactor на смартфон для входа на сайт (см. Рисунок – Установка приложения Multifactor). Если необходимо выбрать другой способ аутентификации, требуется нажать на значок в виде шестерёнки в правом верхнем углу окна настройки, перейти в раздел «Расширенные настройки» и выбрать подходящий способ аутентификации (см. Рисунок – Расширенные настройки).

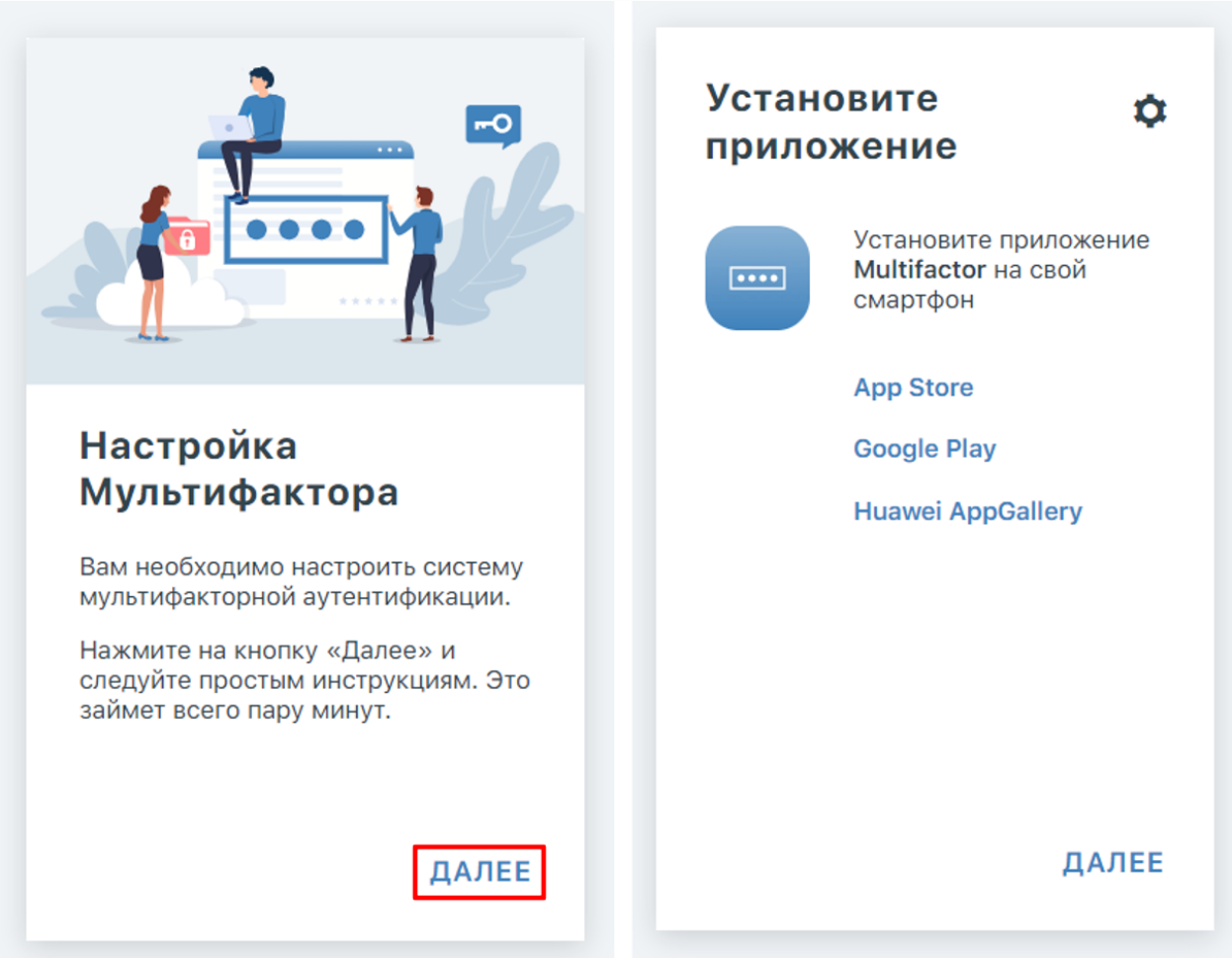


Рисунок – Установка приложения Multifactor

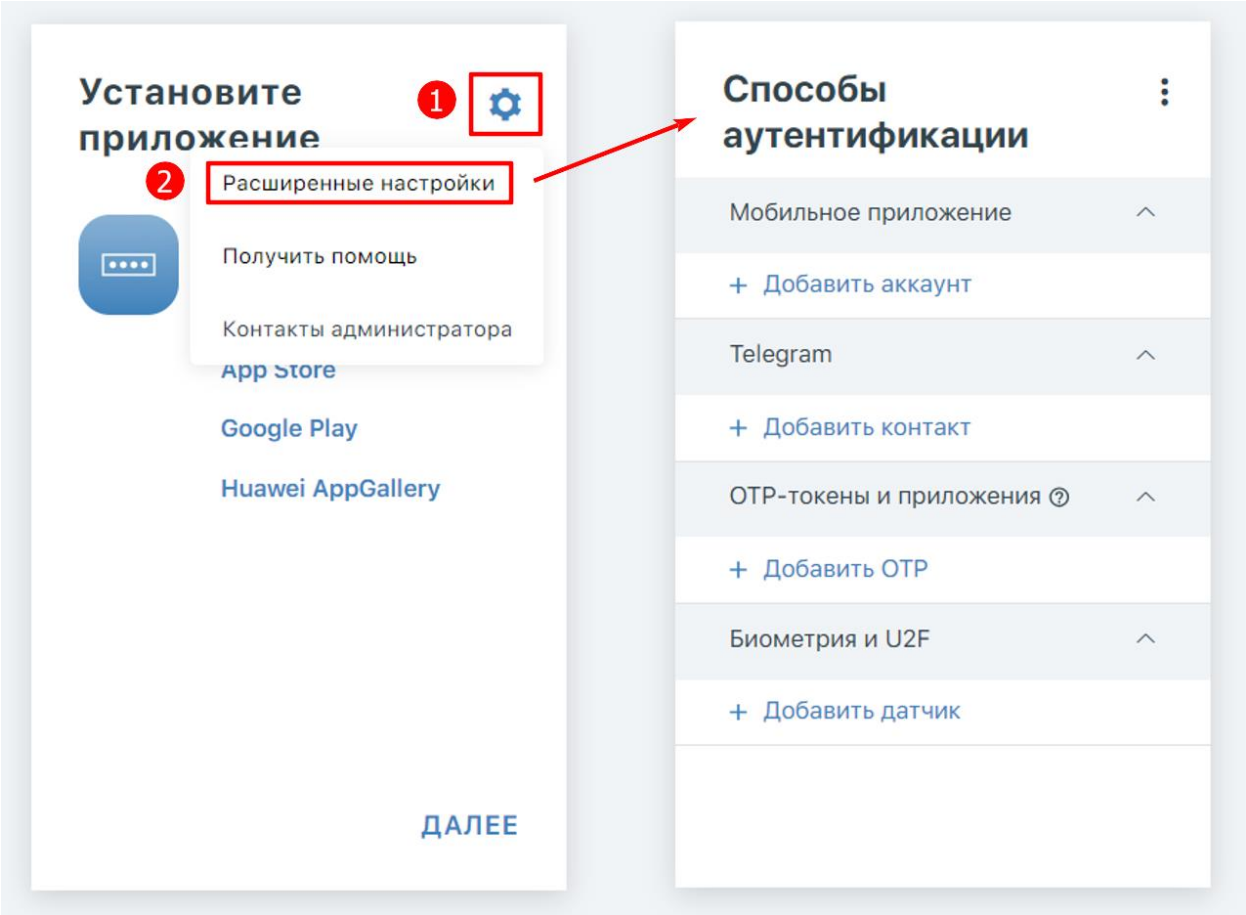


Рисунок – Расширенные настройки

3. После добавления способа аутентификации необходимо подтвердить вход в панель администратора с помощью выбранного ранее способа.
4. В панели администратора перейти в раздел «Ресурсы» и нажать кнопку «Добавить ресурсы» (см. Рисунок – Добавление ресурсов).

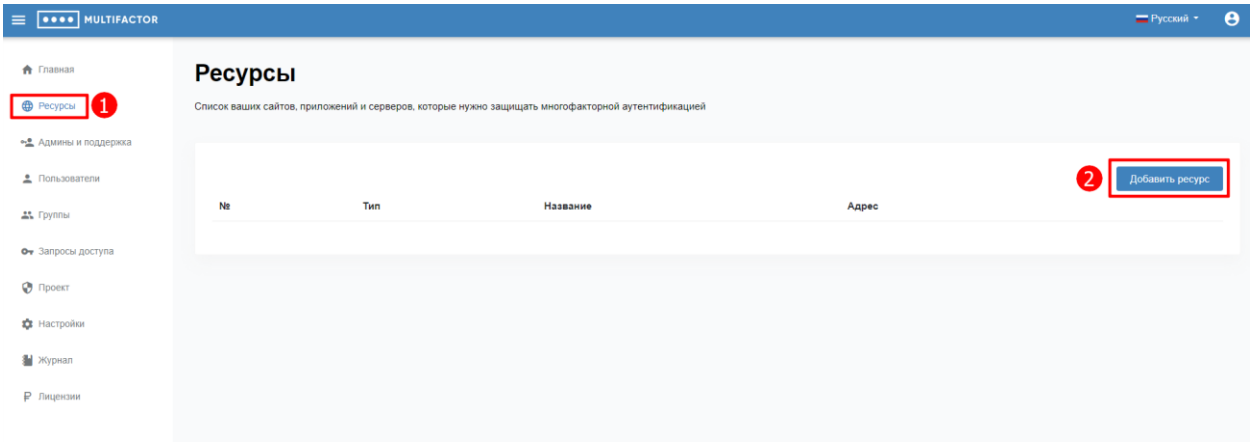


Рисунок – Добавление ресурсов

5. Выбрать добавление ресурса «Другое» и в открывшемся окне заполнить необходимые настройки (см. Рисунок – Настройка ресурса).

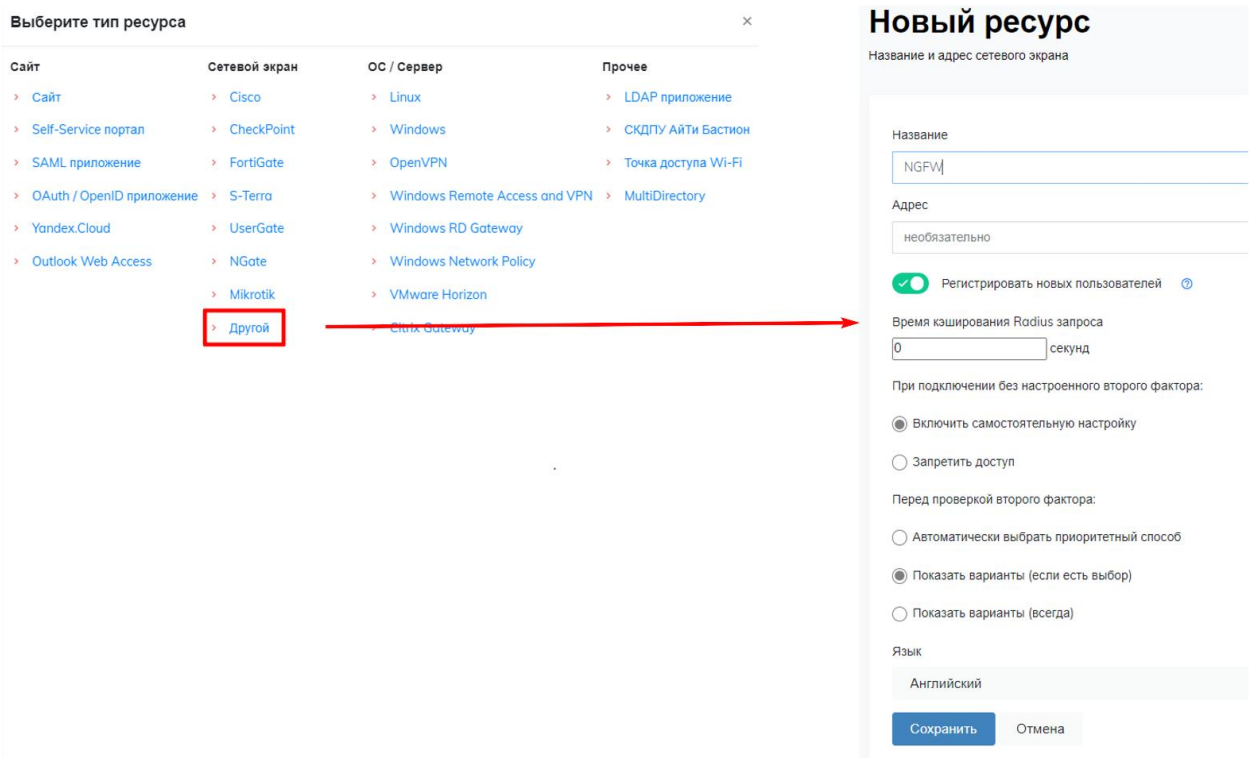


Рисунок – Настройка ресурса

6. После добавления ресурса откроется окно с его параметрами. Необходимо скопировать параметры «NAS Identifier» и «Shared Secret» (см. Рисунок – Параметры добавленного ресурса). Они необходимы для конфигурирования Radius адаптер на Windows Server и для добавления Radius-server в **ARMA Стена**.

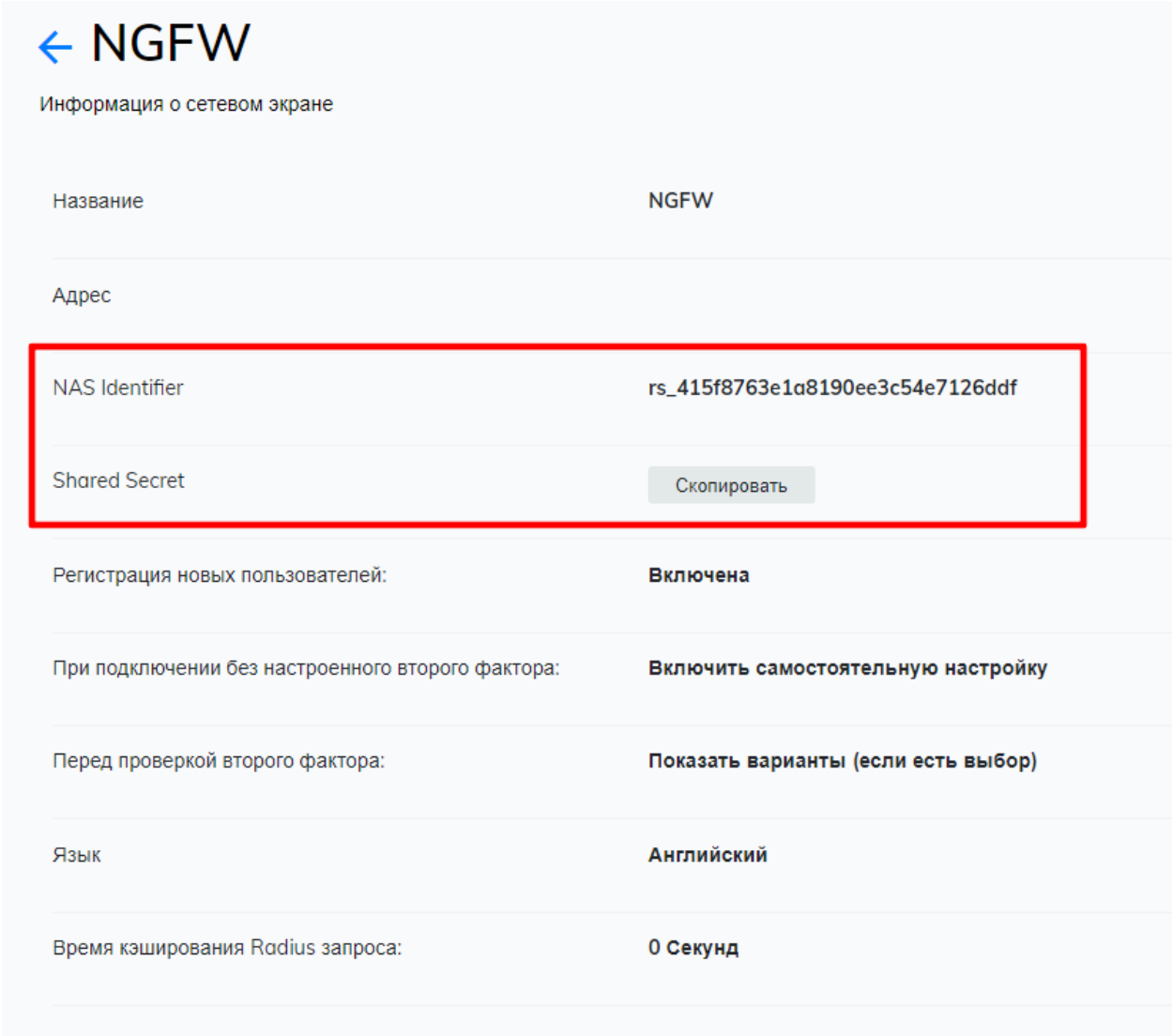


Рисунок – Параметры добавленного ресурса

6.4.1.2.4 Конфигурирование Radius адаптера

1. Открыть директорию с ранее извлечёнными из архива файлами Radius адаптера. Скопировать файл «cisco with ad.config.template», расположенный в папке «Clients» и переименовать его в «arma with ad.config.template». Удалить расширение «.template», чтобы получилось «arma with ad.config». Таким образом, из предустановленного шаблона получится файл для конфигурации подключения адаптера к **ARMA Стена**.
2. Открыть полученный файл «arma with ad.config» для редактирования с помощью программы «Блокнот» и внести следующие изменения в файле (см. Рисунок – Исходный шаблон конфигурации):
    1. установить IP-адрес **ARMA Стена**;
    2. ввести придуманный секретный ключ, который будет использоваться при настройке Radius-сервера в **ARMA Стена**;

3. внести имя домена Active Directory, по которому будет проводиться аутентификация;
4. указать группу, которой предоставляется доступ без второго фактора аутентификации;
5. указать группу, у которой будет запрашиваться второй фактор аутентификации;
6. ввести NAS Identifier, полученный на сайте Multifactor;
7. ввести Shared Secret, полученный на сайте Multifactor.

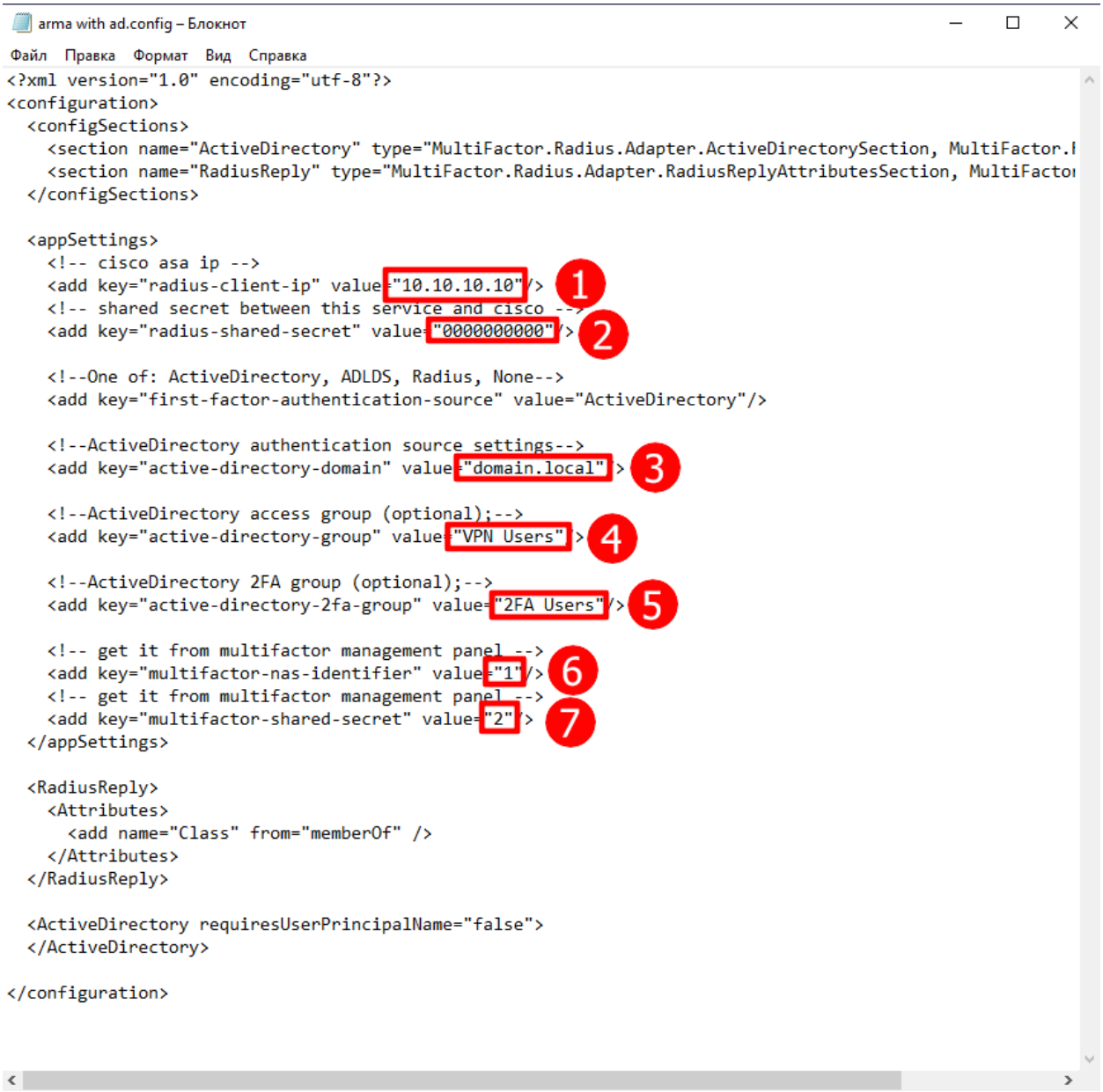


Рисунок – Исходный шаблон конфигурации

Пример конфигурационного файла, в котором не предусмотрена поддержка группы без второго фактора аутентификации (см. Рисунок – Пример конфигурационного файла):

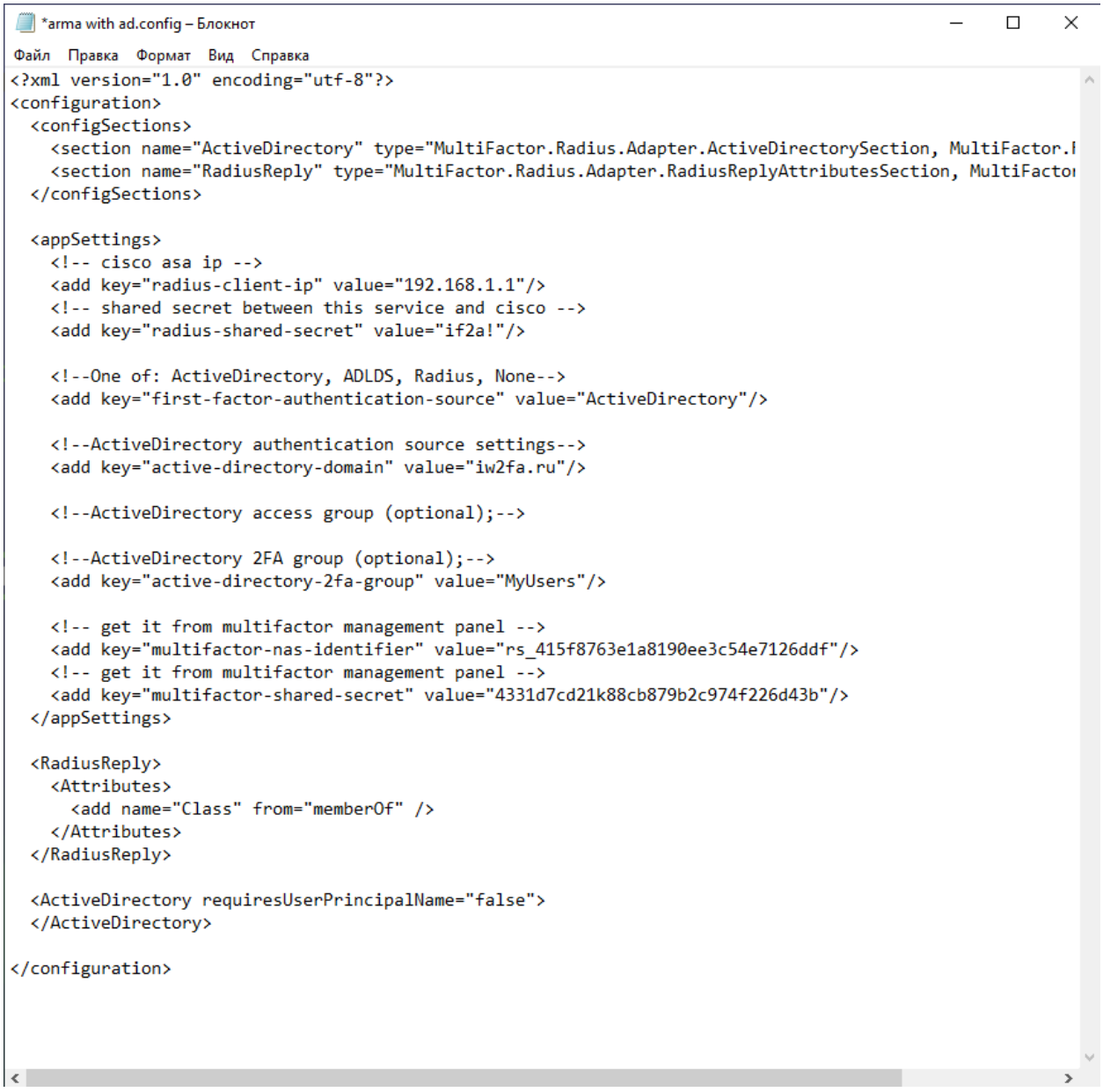


Рисунок – Пример конфигурационного файла

6.4.1.2.5 Запуск Radius адаптера

Компонент может работать как в режиме консоли, так и в качестве службы операционной системы Windows. Для запуска компонента в режиме консоли достаточно запустить приложение.

Для установки Radius адаптера в качестве службы Windows необходимо перейти в папку с файлами адаптера и выполнить команду с ключом «/i» от имени администратора: «MultiFactor.Radius.Adapter.exe /i».

Для удаления Radius адаптера необходимо выполнить команду от имени администратора: «sc delete MFRadiusAdapter».

6.4.1.3 Проверка работы службы

Примечание:

Перед началом работы необходимо отключить брандмауэр Windows!

При входе в NGFW и аутентификации с использованием учётных данных из группы, указанной в поле «active_directory_2fa_group» при настройке адаптера, система предложит зарегистрировать второй фактор аутентификации для пользователя (если он ещё не был зарегистрирован). В случае, если второй фактор уже зарегистрирован, система проверит его (см. Рисунок – Аутентификация):

```
ngfwos login: Pyatnitsa
Password:
To continue, configure second authentication factor. Enter number: 1 - Mobile ap
p; 2 - Telegram1
Install MultiFactor App on your phone. Then press + and enter the code: 71178327
0125
Welcome to NGFWOS!
Pyatnitsa@ngfwos:~$
```

Рисунок – Аутентификация

6.4.2 Multifactor Radius Adapter - Linux

В качестве примера настройки Multifactor Radius Adapter для CentOS будет использоваться стенд представленный на рисунке (см. Рисунок – Схема стенда для настройки Multifactor Radius Adapter - Linux).

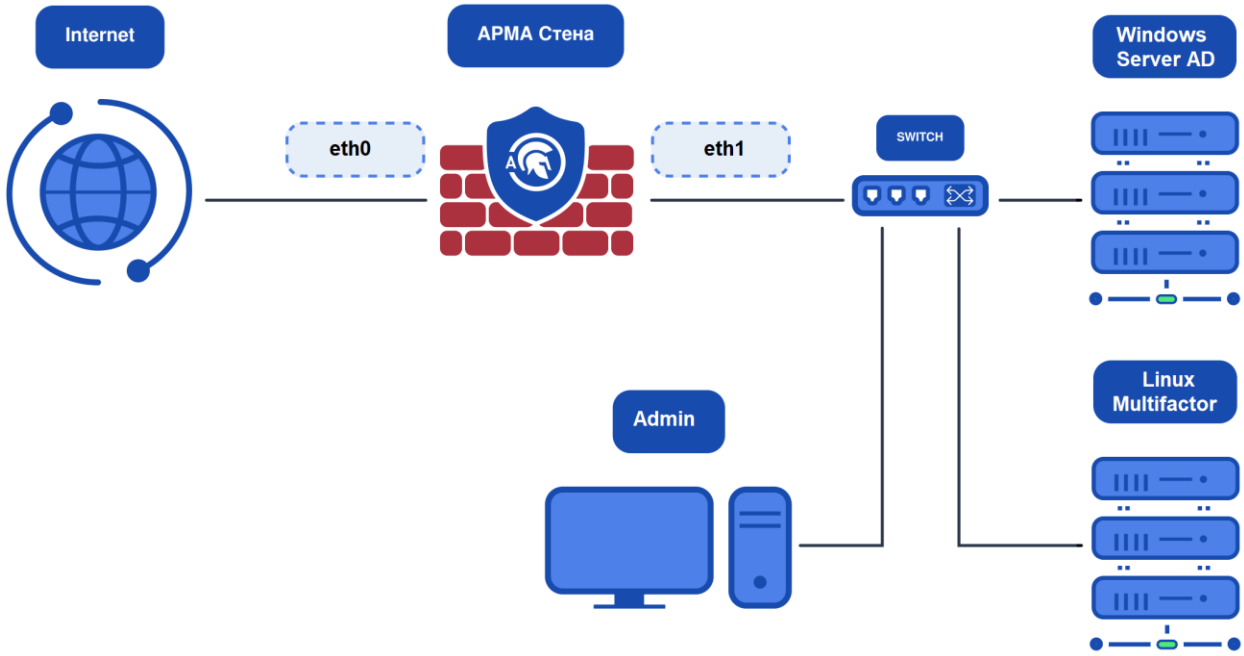


Рисунок – Схема стенда для настройки Multifactor Radius Adapter - Linux

Инструкции по настройке **ARMA Стена** и **Multifactor Radius Adapter** представлены в соответствующих разделах: «Настройка ARMA Стена» и «Добавление Multifactor Radius Adapter».

6.4.2.1 Настройка CentOS 7

Необходимо внести изменения в конфигурацию сетевого интерфейса CentOS. Для этого следует изменить параметр «ONBOOT» в файле **«/etc/sysconfig/network-scripts/ifcfg-eth0»** с **«ONBOOT=no»** на **«ONBOOT=yes»**. После этого необходимо перезагрузить сетевую службу с помощью команды **«systemctl restart network»**. Это позволит интерфейсу автоматически включаться при загрузке системы.

Для начала установки компонента **Multifactor Radius Adapter** необходимо обновить имеющиеся пакеты и проверить наличие доступа к репозиториям. Это осуществляется с помощью команды **«yum -y update && yum -y upgrade»**. Однако при выполнении этой команды может возникнуть ошибка (см. Рисунок – Возможная ошибка).

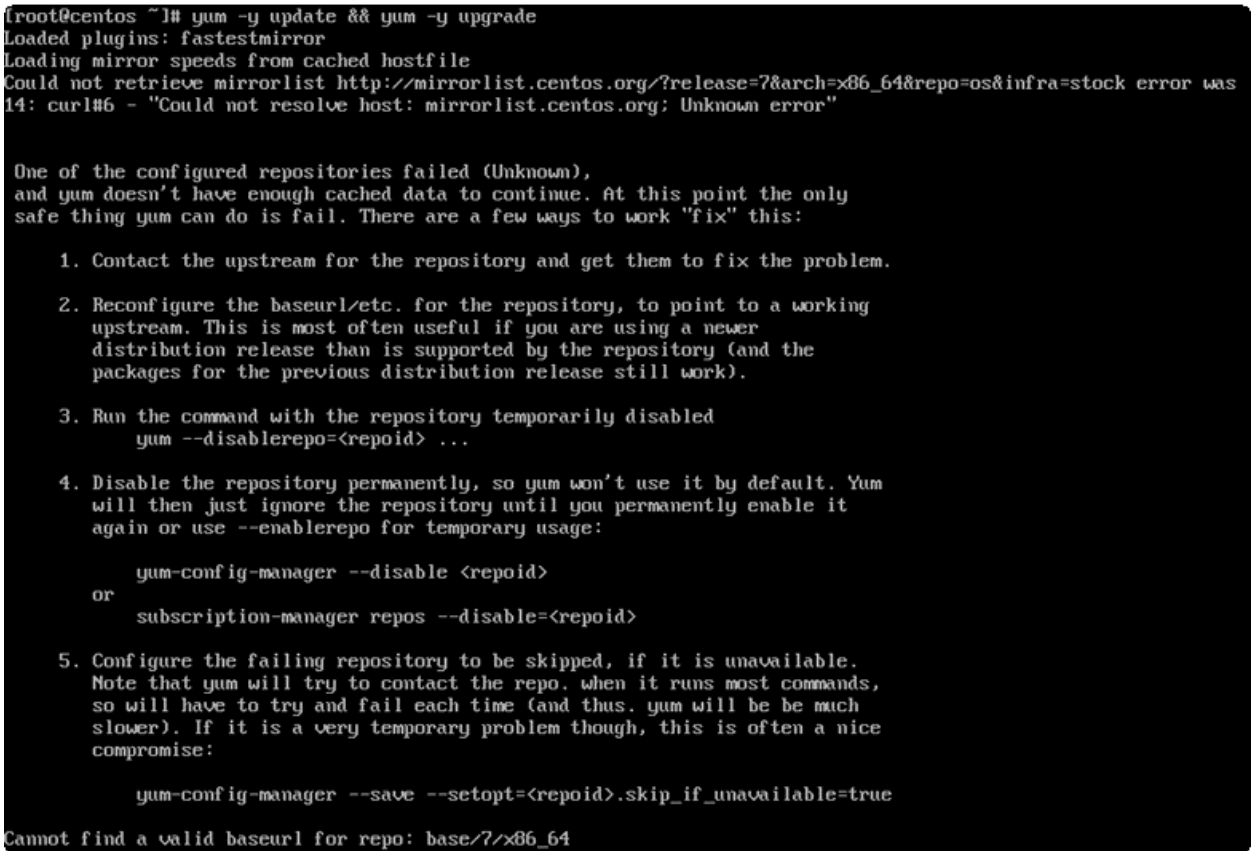
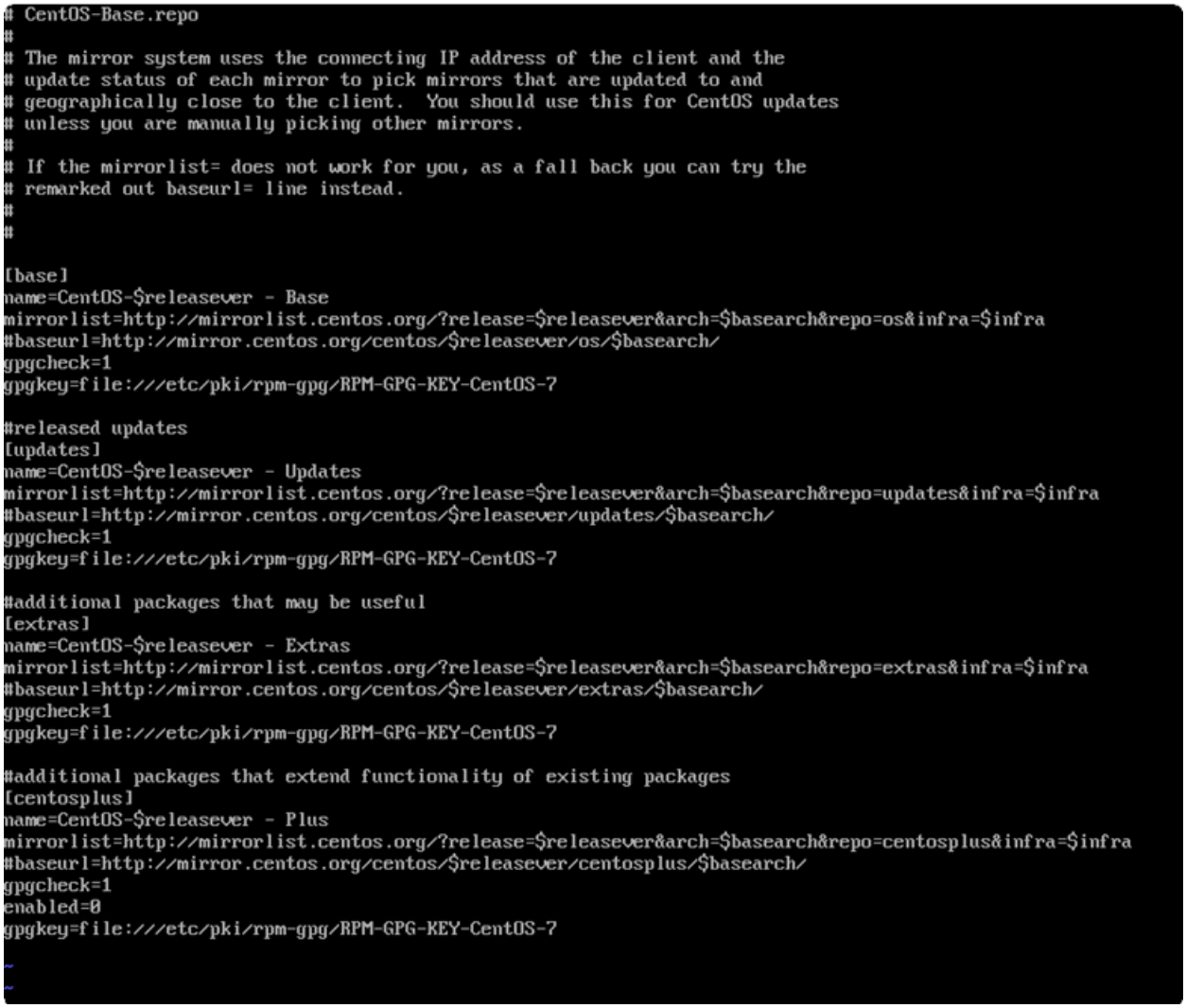


Рисунок – Возможная ошибка

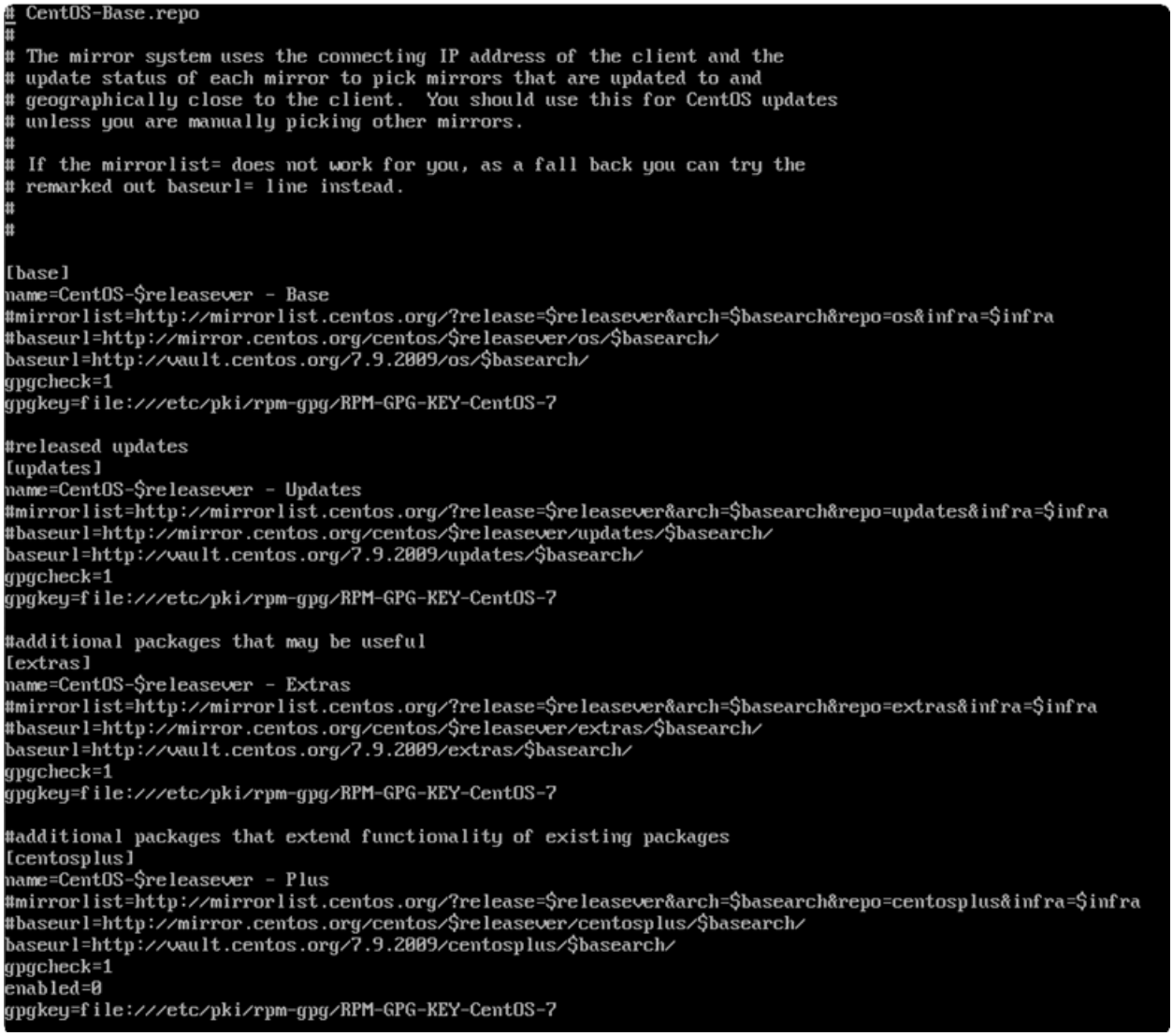
Это свидетельствует о том, что доменное имя зеркал репозиториев не разрешается по неизвестной причине. Данная проблема может быть решена путём настройки других репозиториев, которые находятся в каталоге **«/etc/yum.repos.d/CentOS-Base.repo»**. Вот так выглядят репозитории по умолчанию (см. Рисунок – Репозитории по умолчанию):



```
# CentOS-Base.repo
#
# The mirror system uses the connecting IP address of the client and the
# update status of each mirror to pick mirrors that are updated to and
# geographically close to the client.  You should use this for CentOS updates
# unless you are manually picking other mirrors.
#
# If the mirrorlist= does not work for you, as a fall back you can try the
# remarked out baseurl= line instead.
#
#

[base]
name=CentOS-$releasever - Base
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#released updates
[updates]
name=CentOS-$releasever - Updates
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extras&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/extras/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=centosplus&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

~
~
```

Рисунок – Репозитории по умолчанию

Необходимо закомментировать имеющиеся зеркала и указать другие значения **«baseurl»** в каждом блоке. В данном примере используются архивы snapshot 2021 г. (см. Рисунок – Комментирование имеющихся зеркал):



```
# CentOS-Base.repo
#
# The mirror system uses the connecting IP address of the client and the
# update status of each mirror to pick mirrors that are updated to and
# geographically close to the client.  You should use this for CentOS updates
# unless you are manually picking other mirrors.
#
# If the mirrorlist= does not work for you, as a fall back you can try the
# remarked out baseurl= line instead.
#
#

[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/
baseurl=http://vault.centos.org/7.9.2009/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/updates/$basearch/
baseurl=http://vault.centos.org/7.9.2009/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extras&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/extras/$basearch/
baseurl=http://vault.centos.org/7.9.2009/extras/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=centosplus&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/centosplus/$basearch/
baseurl=http://vault.centos.org/7.9.2009/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
```

Рисунок – Комментирование имеющихся зеркал

После этих действий команда **«yum -y update && yum -y upgrade»** выполнится без ошибок.

Далее необходимо установить среду выполнения APS.NET Core runtime версии 6:

```
sudo rpm -Uvh https: packages.microsoft.com/config/centos/7/packages-microsoft-prod.rpm
sudo yum install aspnetcore-runtime-6.0
```

После этого необходимо сформировать каталог для файлов инструмента, скопировать сборку в созданную папку и создать учётную запись, под которой будет работать служба:

```
sudo mkdir /opt/multifactor /opt/multifactor/radius/opt/multifactor/radius/logs # создание папок для файлов адаптера
sudo wget https: github.com/MultifactorLab/multifactor-radius-adapter/releases/latest/download/release_linux_x64.zip # клонирование сборки
sudo unzip release_linux_x64.zip -d /opt/multifactor/radius # распаковка архива
sudo useradd -r mfa # создание пользователя
sudo chown -R mfa:mfa /opt/multifactor/radius/ # присвоение директорий пользователю
sudo chown -R mfa:mfa /opt/multifactor/radius/clients
sudo chmod -R 700 /opt/multifactor/radius/ # изменять директории может только пользователь
sudo chmod -R 700 /opt/multifactor/radius/clients
```

Необходимо создать службу systemd для адаптера. Для этого сначала требуется создать файл службы с помощью команды **«sudo vi /etc/systemd/system/multifactor-radius.service»**, а затем изменить его содержимое:

```
[Unit]
Description=Multifactor Radius Adapter

[Service]
WorkingDirectory=/opt/multifactor/radius/
ExecStart=/usr/bin/dotnet /opt/multifactor/radius/multifactor-radius- adapter.dll
Restart=always
# Restart service after 10 seconds if the service crashes:
RestartSec=10
KillSignal=SIGINT
SyslogIdentifier=multifactor-radius
User=mfa
Environment=ASPNETCORE_ENVIRONMENT=Production
Environment=DOTNET_PRINT_TELEMETRY_MESSAGE=false

# How many seconds to wait for the app to shut down after it receives the initial interrupt signal.
# If the app doesn't shut down in this period, SIGKILL is issued to terminate the app.
# The default timeout for most distributions is 90 seconds.
TimeoutStopSec=30

[Install]
WantedBy=multi-user.target
```

После этого необходимо выполнить команду для запуска службы: **«sudo systemctl enable multifactor-radius»**.

Затем приступить к редактированию конфигурации серверов Radius. Общие параметры работы компонента хранятся в файле **«/opt/multifactor/radius/multifactor-radius-adapter.dll.config»** в формате «xml»:

```
<!-- Адрес и порт (UDP), по которому адаптер будет принимать запросы на аутентификацию от клиентов -->
<add key="adapter-server-endpoint" value="0.0.0.0:1812"/>

<!-- Адрес API MULTIFACTOR -->
<add key="multifactor-api-url" value="https: api.multifactor.ru"/>

<!-- Доступ к API MULTIFACTOR через HTTP прокси (опционально) -->
<!-- <add key="multifactor-api-proxy" value="http: login:password@proxy:3128"/> -->
<!-- Уровень логирования: 'Debug', 'Info', 'Warn', 'Error' -->
<add key="logging-level" value="Debug"/>
```

Шаблоны для настройки отдельных подключений находятся в каталоге **«/opt/multifactor/radius/clients»**. Для создания необходимой конфигурации, требуется скопировать имеющийся шаблон **«cisco with ad.config.template»** с помощью команды **«cp cisco/with/ad.config.template [указать имя].config»**. Таким образом, будет скопирован шаблон конфигурации для связи с Active Directory, содержащий следующие данные:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="RadiusReply" type="MultiFactor.Radius.Adapter.RadiusReplyAttributesSection, multifactor-radius-adapter"/>
  </configSections>
  <appSettings>
    <!-- cisco asa ip -->
    <add key="radius-client-ip" value="10.10.10.10"/>
    <!-- shared secret between this service and cisco -->
    <add key="radius-shared-secret" value="0000000000"/>
    <!-- One of: ActiveDirectory, ADLDS, Radius, None -->
    <add key="first-factor-authentication-source" value="ActiveDirectory"/>
    <!-- ActiveDirectory authentication settings: for example domain local on host
```

```
10.0.0.4 -->
      <add                                                    key="active-directory-domain"
value="ldaps:10.0.0.4/DC=domain,DC=local"/>
      <!-- ActiveDirectory access group (optiona): -->
      <add key="active-directory-group" value="UPN Users"/>
      <!-- ActiveDirectory 2FA group (optional) -->
      <add key="active-directory-2fa-group" value="2FA Users"/>
      <!-- get it from multifactor management panel -->
      <add key="multifactor-nas-identifier" value="1"/>
      <!-- get it from multifactor management panel -->
      <add key="multifactor-shared-secret" value="2"/>
    </appSettings>
  <RadiusReply>
      <Attributes>
        <add name="Class" from="memberOf"/>
      </Attributes>
  </RadiusReply>
</configuration>
```

Необходимо внести следующие изменения в файл шаблона конфигурации:

- поле **«radius-client-ip»** должно быть изменено на 192.168.1.1, так как Radius-сервер находится в локальной сети, а клиентом является **ARMA Стена**;
- поле **«radius-shared-secret»** должно содержать значение, которое было придумано при настройке аутентификации Radius на **ARMA Стена**;
- поле **«active-directory-domain»** должно быть изменено в соответствии с доменом Active Directory, который присутствует в подсети;
- поле **«active-directory-group»** должно быть удалено, чтобы всегда использовался второй фактор аутентификации, указанный в поле **«active-directory-2fa-group»**;
- поля **«multifactor-nas-identifier»** и **«multifactor-shared-secret»** должны быть взяты из панели администратора при создании ресурса для аутентификации.

Необходимо перезагрузить подсистемы служб и созданную службу для применения изменений:

```
sudo systemctl daemon-reload
sudo systemctl restart multifactor-radius
```

6.4.2.2 Возможные ошибки

1. В случае возникновения ошибки **«Unable to load shared library „ldap.so.2“ or one of its dependencies»**, необходимо внести коррективы в цепочку таким образом, чтобы симлинк **«libldap.so.2»** в конечном итоге указывал на конкретную библиотеку **«libldap-2.X.so.2.Y.Z»**.

   Пример: libldap.so.2 * libldap-2.4.so.2 это симлинк libldap-2.4.so.2 * libldap_r-2.4.so.2 это симлинк libldap_r-2.4.so.2 * libldap_r-2.4.so.2.11.5 это симлинк libldap_r-2.4.so.2.11.5 это сама библиотека.

   Проверка и исправление символических ссылок: для проверки символических ссылок необходимо определить местоположение библиотеки **«libldap»**. Обычно она находится в каталоге **«/usr/lib/x86_64-linux-gnu»**.

   Далее необходимо выполнить команду **«ls -la»**, чтобы просмотреть список всех файлов и символических ссылок. Необходимо найти информацию о том, как и кто ссылается на библиотеку **«libldap»**, а также определить, каких ссылок не хватает.

   Чаще всего отсутствует одна ссылка — с **«libldap.so.2»** на основную версию библиотеки. Команды создания недостающего симлинка:

   ```
   Для Debian и Ubuntu:
   ln -s/usr/lib/x86_64-linux-gnu/libldap-2.4.so.2 /usr/lib/x86_64-linux-gnu/libldap.so.2

   Для CentOS и REDOS:
   ln -s /usr/lib64/libldap_r-2.4.so.2.10.9 /usr/lib64/libldap.so.2 #Версии библиотек могут отличаться
   ```

   Аналогичные действия выполняются с библиотекой **«liblber»**.

2. В случае возникновения ошибки **«Unable to start: Address already in use»**, существует два способа её устранения:

   - Если используете запуск адаптера через **«/opt/multifactor/radius/multifactor-radius-adapter»**, то необходимо отключить адаптер как службу:

     ```
     sudo systemctl stop multifactor-radius
     sudo systemctl disable multifactor-radius
     sudo rm /etc/systemd/system/multifactor-radius.service
     sudo systemctl daemon-reload
     ```

   - Перейти в **«/opt/multifactor/radius/multifactor-radius-adapter.dll.config»** используя команду **«sudo nano /opt/multifactor/radius/multifactor-**

radius-adapter.dll.config» и изменить порт в поле **«adapter-server-endpoint»**.

7 АВАРИЙНЫЙ РЕЖИМ

В системе **ARMA Стена** предусмотрено два механизма активации аварийного режима:

1. автоматический переход в аварийный режим;
2. переход в аварийный режим по команде оператора.

Примечание:

В случае перехода системы **ARMA Стена** в аварийный режим, весь трафик, проходящий через неё, будет заблокирован до устранения причин, вызвавших сбой. В этот период управление системой будет осуществляться исключительно через локальную консоль.

Примечание:

В случае возникновения критических ошибок в ядре системы **ARMA Стена** *(kernel panic)*, система выведет уведомление **«Rebooting in 60 seconds»** и автоматически перезагрузится через 60 секунд для восстановления работоспособности.

Если после запуска системы **ARMA Стена** не удалось восстановить работоспособность, рекомендуется обратиться в службу технической поддержки **ООО «ИнфоВотч АРМА»**.

7.1 Автоматический переход в аварийный режим

Автоматический переход в аварийный режим работы системы происходит по следующим причинам:

1. Нарушение целостности конфигурационного файла системы.

Функция контроля целостности обеспечивает мониторинг состояния конфигурационных файлов, и в случае обнаружения нарушения целостности система автоматически переходит в аварийный режим работы.

Для восстановления конфигурационного файла рекомендуется использовать процедуру восстановления конфигурации из архивных локальных копий (см. раздел «Восстановление конфигурации»).

В случае невозможности восстановления файла конфигурации, существует возможность выполнить сброс настроек системы до заводских параметров (см. раздел «Сброс настроек»).

Загрузка системы в аварийном режиме при неисправном физическом интерфейсе

В случае отказа физического интерфейса, система **ARMA Стена** после перезагрузки автоматически переходит в аварийный режим работы (см. Рисунок – Загрузка системы в аварийном режиме при неисправном физическом интерфейсе). Возврат к штатному режиму функционирования посредством команды «emergency exit» невозможен, так как в конфигурационном файле сохраняются данные о неисправном интерфейсе. При последующих загрузках система выполняет проверку конфигурации, и при отсутствии вышедшего из строя физического интерфейса повторно активирует аварийный режим.

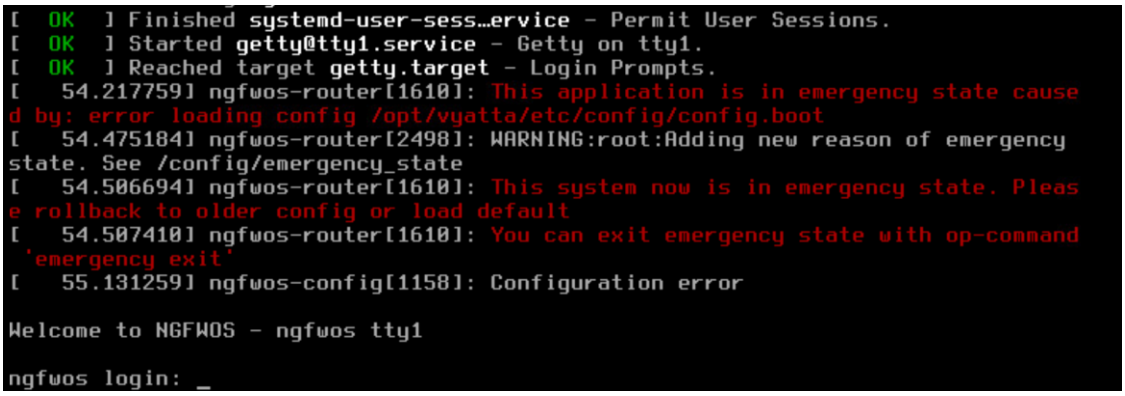


Рисунок – Загрузка системы в аварийном режиме при неисправном физическом интерфейсе

Для восстановления штатного режима работы системы необходимо выполнить следующую последовательность действий:

1. сохранить текущую конфигурацию с помощью команды **«save»** в конфигурационном режиме;
2. деактивировать аварийный режим с использованием команды **«emergency exit»**.

```
# Перейди в конфигурационный режим:
admin@ngfwos:~$ configure

WARNING: There was a config error on boot: saving the configuration now could overwrite data.
You may want to check and reload the boot config

# Сохранить конфигурацию:
admin@ngfwos# save

# Выйди из конфигурационного режима:
admin@ngfwos# exit

# Выйти из аварийного режима работы системы:
admin@ngfwos:~$ emergency exit

# Подтвердить выход из аварийного режима работы системы, ввести «y» и нажать клавишу «Enter»:
WARNING!!! ALL SYSTEM INTEGRITY WILL RECALCULATED!!!
To exit from emergency mode you will need to reboot. Reboot now? [y/N]
y
```

После выполнения указанных действий система перезагрузится и возобновит работу в штатном режиме. Информация о вышедшем из строя физическом интерфейсе будет удалена из конфигурационного файла, что исключит повторный переход в аварийный режим.

2. Наличие менее 5% свободного места на диске.

В случае возникновения ситуации, когда система не сможет вести журнал событий из-за недостатка свободного места на диске, она автоматически перейдёт в аварийный режим для обеспечения безопасности и контроля сетевого трафика.

Если на диске остаётся менее **10%** свободного места, система будет выводить предупреждение каждые 60 секунд о необходимости освободить место: *«Free space on disk is low, please clear logs»*.

Для освобождения места на диске рекомендуется очистить глобальный журнал событий (см. раздел «Настройки глобального журнала» руководства пользователя ARMA Стена).

7.2 Переход в аварийный режим по команде оператора

Для включения аварийного режима необходимо выполнить следующие действия:

1. Ввести в эксплуатационном режиме команду:

```
admin@ngfwos:~$ emergency enter
```

2. Ввести **«y»** для подтверждения перехода в аварийный режим:

```
Emergency mode will block all network traffic and you will need to manually exit it.
Continue? [y/N]
```

Примечание:

В случае выполнения команды перехода в аварийный режим через удалённое подключение по протоколу SSH, связь с системой **ARMA Стена** будет прервана после подтверждения. Дальнейшее управление системой будет осуществляться только через локальную консоль.

3. Система выведет уведомление о временной блокировке всего сетевого трафика:

```
Entering emergency state

All network traffic was stopped

admin@ngfwos:~$
```

После перезагрузки системы выведет предупреждение о работе в аварийном режиме (см. Рисунок – Аварийный режим работы).

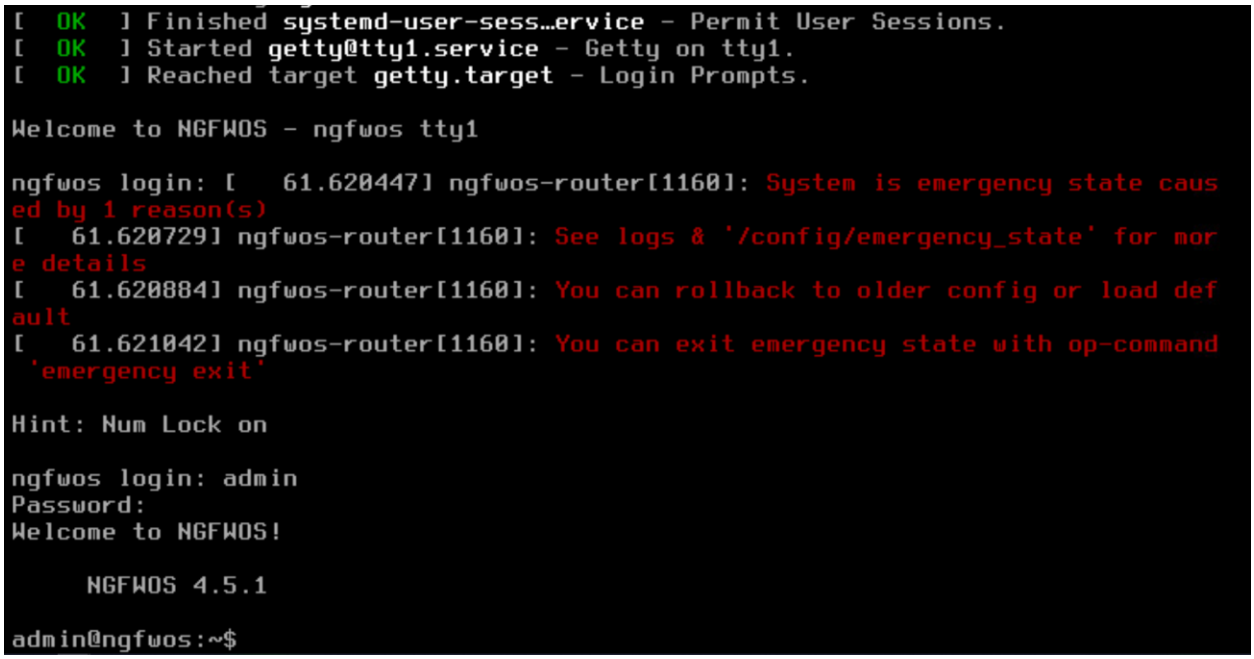


Рисунок – Аварийный режим работы

Примечание:

При выполнении команды **«emergency enter»** в активированном аварийном режиме, система выведет сообщение **«Already in emergency state»**, информирующее о том, что она уже находится в этом режиме.

При функционировании системы в режиме аварийной работы возникновение сообщения **«System is emergency state»** указывает на повторное нарушение целостности контролируемых объектов.

7.3 Отключение аварийного режима

Независимо от способа перехода в аварийный режим (автоматический или ручной), для выхода из него необходимо выполнить команду отключения аварийного режима. Для этого необходимо выполнить следующие действия:

1. Устранить причину активации аварийного режима.
2. Ввести команду для выхода из аварийного режима:

```
admin@ngfwos:~$ emergency exit
```

3. Подтвердить перезагрузку системы, введя «y»:

```
WARNING!!! ALL SYSTEM INTEGRITY WILL RECALCULATED!!!
To exit from emergency mode you will need to reboot. Reboot now? [y/N]
```

Примечание:

В случае подтверждения перезагрузки и отключения аварийного режима система произведёт пересчёт контрольных сумм для всех отслеживаемых файлов.

4. Если причина неполадки устранена, система будет загружаться в штатном режиме.

7.4 Дополнительные параметры

В системе **ARMA Стена** предусмотрена возможность деактивации механизма блокировки сетевых интерфейсов при переходе в режим аварийной работы. Данная функциональность необходима в случаях ограниченной физической доступности управляющего оборудования или при критичных требованиях к обеспечению непрерывности сетевого трафика.

Примечание:

В целях обеспечения безопасности и соответствия требованиям ФСТЭК России рекомендуется не отключать механизм блокировки сетевых интерфейсов при переходе системы в аварийный режим работы.

Примечание:

Право на деактивацию функции блокировки сетевых интерфейсов в случае перевода системы в аварийный режим предоставлено исключительно встроенной учётной записи **«admin»**.

Для выключения блокировки сетевых интерфейсов в аварийном режиме необходимо ввести следующие команды в конфигурационном режиме:

```
admin@ngfwos# set system option emergency remove-nics no

# Применить настройку:
admin@ngfwos# commit

WARNING! You are disabling the automated removal of nics after entering emergency state.
FSTEC of Russia strongly recommends to have this option enabled. You are acting at your own risk!

# Сохранить изменения:
admin@ngfwos# save
```

При установленном параметре **«remove-nics»** в значение **«yes»** будут блокироваться все сетевые интерфейсы устройста при переходе в аварийный режим работы. В данном режиме управление системой осуществляется исключительно посредством локальной консоли. **Значение используется по умолчанию**.

В случае установки параметра **«remove-nics»** в значение **«no»**, система продолжит функционировать без блокировки сетевых интерфейсов, при этом будут выводиться предупреждающие сообщения о работе в аварийном режиме.

8 КОНТРОЛЬ ЦЕЛОСТНОСТИ

Контроль целостности (**КЦ**) представляет собой процесс, направленный на обнаружение и предотвращение несанкционированных изменений или повреждений файлов, которые могут привести к нарушению безопасности и работоспособности системы **ARMA Стена**.

Контроль целостности осуществляется автоматически при запуске системы и затем каждый час (xx:00:00), а также при выполнении команд «reboot» и «poweroff».

Существует возможность инициировать проверку целостности вручную с помощью команды:

```
admin@ngfwos:~$ integrity-check run <path/to/file | all>
```

где:

- **<path/to/file>** - путь к контролируемому файлу;
- **<all>** - проверить целостность всех контролируемых объектов.

8.1 Регистрация событий КЦ

Целостность объекта верифицируется посредством сопоставления его хэша с эталонным значением в базе данных механизма **КЦ**.

В случае обнаружения несоответствия текущего хэш-значения объекта наблюдения эталонному значению в процессе функционирования системы **ARMA Стена**, система выведет предупреждающее сообщение и выполнит предусмотренные действия в отношении данного объекта: перейдёт в режим аварийной работы (см. Рисунок – Переход в аварийный режим при нарушении КЦ) или выведет уведомление о нарушении целостности объекта (см. Рисунок – Предупреждение о нарушении КЦ)).

Рисунок – Переход в аварийный режим при нарушении КЦ

Рисунок – Предупреждение о нарушении КЦ

В случае если при загрузке системы контрольные объекты не пройдут проверку на целостность, то в зависимости от заданного параметра **«action»**, после завершения

загрузки будет выведено предупреждение (см. Рисунок – Не удалось выполнить проверку КЦ) или произойдёт переход в аварийный режим (см. Рисунок – Аварийный режим. Не удалось выполнить проверку КЦ).

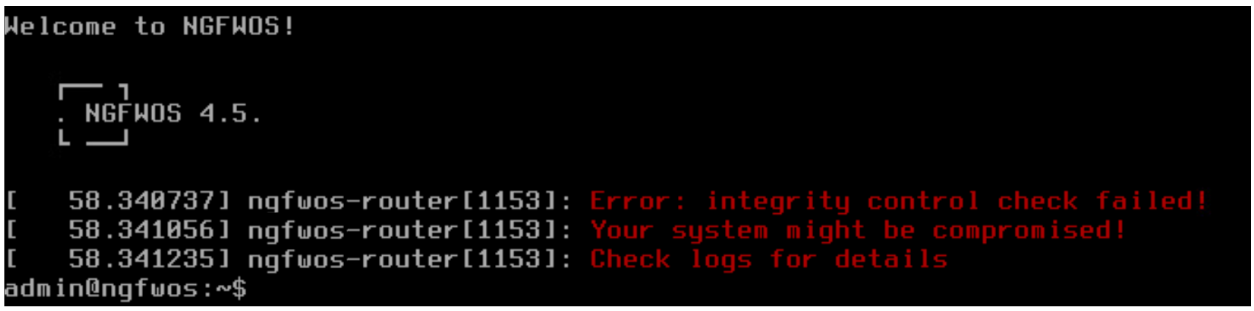


Рисунок – Не удалось выполнить проверку КЦ

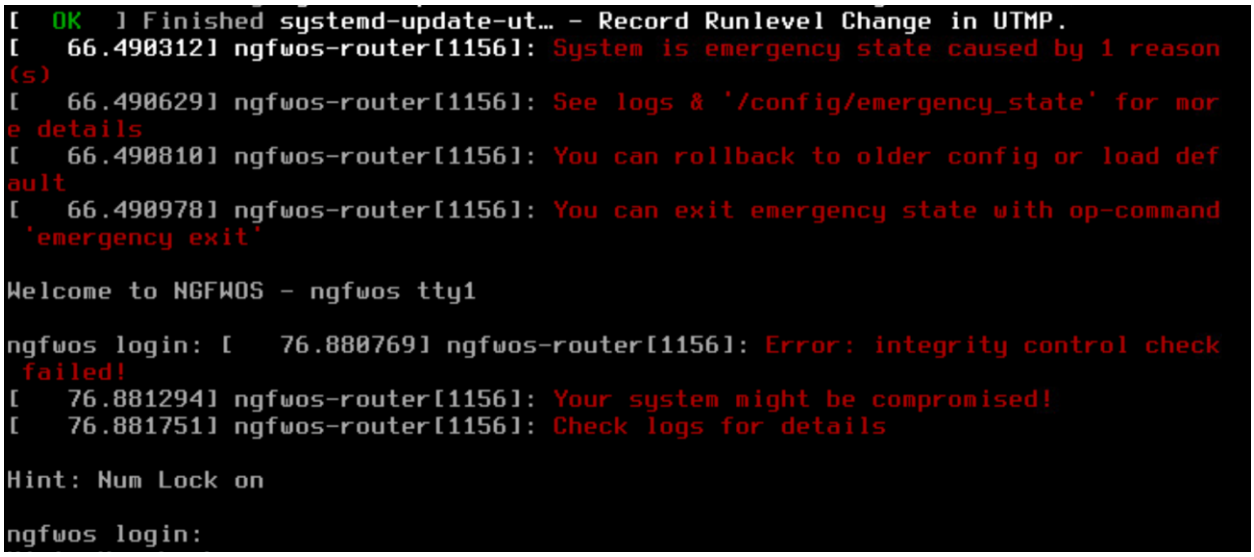


Рисунок – Аварийный режим. Не удалось выполнить проверку КЦ

Для выявления объекта, который не прошёл проверку **КЦ**, необходимо ввести в эксплуатационном режиме команду **«integrity-check run all»**. Система выдаст предупреждение и укажет на объект, который не прошёл проверку:

```
admin@ngfwos:~$ integrity-check run all

Violation checking integrity of file ['/usr/bin/apt']
```

Файл «apt» не прошёл проверку **КЦ**. Это событие приведено в качестве примера.

Все события, связанные с функционированием механизма контроля целостности, включая действия администратора, регистрируются в глобальном журнале. Для просмотра этих событий возможно использовать фильтр **«arma-endpoint»** для глобального журнала:

```
admin@ngfwos:~$ show logging arma-endpoint
```

8.2 Пересчёт эталонных значений КЦ

Предусмотрено два механизма пересчёта эталонных значений **КЦ**: *автоматический* и *ручной*.

Автоматический пересчёт эталонных значений КЦ

Автоматический пересчёт эталонных значений **КЦ** выполняется после каждой команды **«save»**.

Примечание:

В аварийном режиме работы системы автоматический пересчёт эталонных значений **КЦ** не производится.

Ручной пересчёт эталонных значений КЦ

Для пересчёта эталонных значений контроля целостности необходимо ввести команду:

```
admin@ngfwos:~$ integrity-control update <path/to/file | all>
```

где:

- **<path/to/file>** - путь к объекту, для которого необходимо пересчитать эталонное значение;
- **<all>** - пересчёт эталонных значений для всех контролируемых объектов.

Примечание:

Право на выполнение команды пересчёта эталонных значений для контроля целостности предоставлено исключительно встроенной учётной записи **«admin»**.

8.3 Настройка списка объектов КЦ

Для вывода списка контролируемых объектов необходимо ввести следующую команду:

```
admin@ngfwos:~$ integrity-check list
```

Список контролируемых объектов по умолчанию (см. Таблица «Список контролируемых объектов по умолчанию»):

Таблица «Список контролируемых объектов по умолчанию»

Действие	Объект
emergency	/config/config.boot

Действие	Объект
emergency	/opt/ngfwos/etc/config.boot.default
emergency	/opt/ngfwos/etc/config.boot.ssh_dhcp
emergency	/opt/ngfwos/etc/config.boot.ssh_dhcp_static_ips
notify	/boot/initrd.img
notify	/boot/initrd.img-6.6.54-amd64-vyos
notify	/boot/vmlinuz
notify	/boot/vmlinuz-6.6.54-amd64-vyos
notify	/etc/containers/containers.conf
notify	/etc/containers/registries.conf
notify	/etc/containers/storage.conf
notify	/etc/curlrc
notify	/etc/hosts
notify	/etc/logrotate.d/vyos-rsyslog
notify	/etc/modprobe.d/vyatta_nf_conntrack.conf
notify	/etc/motd
notify	/etc/nginx/sites-enabled/default
notify	/etc/nginx/sites-enabled/ngfw-web.conf
notify	/etc/nsswitch.conf
notify	/etc/resolv.conf
notify	/etc/rsyslog.d/00-vyos.conf
notify	/etc/ssh/ssh_config.d/91-ngfwos-ssh-client-options.conf
notify	/etc/systemd/journald.conf
notify	/home/admin/.ssh/authorized_keys
notify	/usr/bin/
notify	/usr/bin/*все файлы каталога*
notify	/usr/lib/live/mount/persistence//boot/grub/grub.cfg.d/vyos-versions/4.5._имя_сборки.cfg
notify	/usr/sbin/
notify	/usr/sbin/*все файлы каталога*
notify	/usr/share/pam-configs/ngfwos_auth

Для добавления файла, подлежащего контролю, необходимо ввести команду:

```
admin@ngfwos:~$ integrity-control add <path/to/file> [action <emergency|notify>]
```

где:

- **<path/to/file>** - путь к объекту;
- **<emergency|notify>** - действие в случае нарушения целостности объекта. Возможно указать следующие значения:
  - **emergency** - в случае нарушения целостности контролируемого объекта система перейдёт в аварийный режим работы (см. Рисунок – Переход в аварийный режим при нарушении КЦ);
  - **notify** - в случае нарушения целостности контролируемого объекта система выведет предупреждение (см. Рисунок – Предупреждение о нарушении КЦ)».

В случае отсутствия параметра **«action»**, система автоматически применит к объекту действие **«notify»**.

Для удаления объекта наблюдения из списка КЦ необходимо ввести следующую команду:

```
admin@ngfwos:~$ integrity-control delete <path/to/file>
```

где **<path/to/file>** - путь к объекту.

Примечание:

Удаление объекта КЦ из списка мониторинга, при установленном параметре «action» со значением **«emergency»**, не допускается. В случае попытки удаления такого объекта из списка, система выведет предупреждающее сообщение о невозможности выполнить операцию: *«</.../имя_файла> in emergency action mode. If you wish to delete, please change it's action to `notify`»*.

Для удаления необходимо предварительно изменить значение параметра «action» на **«notify»**, после чего произвести операцию удаления.

Примечание:

Запрещено удалять из списка объекты по умолчанию (см. Таблица «Список контролируемых объектов по умолчанию»).