Руководство администратора

версия 55 ред. от 22.11.2024

Листов 79

СОДЕРЖАНИЕ

1 Требования к среде функционирования 10
1.1 Требования к аппаратной платформе 10
1.2 Требования к виртуальной платформе 11
1.2.1 Требования к настройке среды виртуализации 12
2 Установка и первоначальная настройка системы 13
2.1 Установка 13
2.1.1 Работа в режиме «live» с USB-накопителя 14
2.1.2 Установка с заданными параметрами 16
2.1.3 Создание программного RAID 21
2.2 Первоначальная настройка 24
2.2.1 Назначение сетевых интерфейсов 24
2.2.2 Настройка IP-адресов 27
2.3 Настройка ARMA FW посредством веб-интерфейса 27
2.3.1 Подключение к веб-интерфейсу 27
2.3.2 Активация лицензии 28
2.3.2.1 Активация лицензии с доступом в Интернет 29
2.3.2.2 Активация лицензии без доступа в Интернет 29
2.3.2.3 Информация о лицензии 31
2.3.2.4 Типы лицензий 32
2.3.3 Мастер первоначальной настройки 33
2.3.3.1 Шаги Мастера первоначальной настройки 33
2.3.4 Включение русского языка 36
2.3.5 Оптимизация веб-сервера 37
2.3.6 Настройки безопасности 38
2.3.6.1 Настройка доступа по SSH 38
2.3.6.2 Настройка доступа к локальному консольному интерфейсу 39
2.3.6.3 Настройка блокирования сеанса пользователя при неактивности .40
2.3.6.4 Настройка блокирования сессии после ввода некорректных учётных данных 41
2.4 Проверка состояния служб ARMA FW 42
3 Варианты развёртывания 44

3.1 Маршрутизация 44
3.2 Прозрачный мост 44
3.3 Sniffing mode 45
3.4 Отказоустойчивый кластер 45
4 Контроль управления доступом 47
4.1 Аутентификация 47
4.1.1 Локальная база данных пользователей 47
4.1.2 Ваучер-сервер 48
4.1.3 LDAP 48
4.1.4 Radius 49
4.1.5 Двухфакторная аутентификация 49
4.2 Пользовательские учетные записи, группы и привилегии 49
4.2.1 Добавление пользовательских учетных записей и их привилегий 50
4.2.2 Создание группы и добавление им привилегий 51
4.3 Сброс пароля учетной записи суперпользователя 52
5 Сервисы 54
5.1 Маршрутизация 54
5.1.1 Статическая маршрутизация 54
5.1.2 Динамическая маршрутизация 54
5.2 Прокси 54
5.3 DHCP 55
5.4 Сервисы мониторинга 55
5.4.1 Syslog 55
5.4.2 SNMP 55
6 Описание локального консольного интерфейса 56
6.1 Выход из консольного интерфейса 56
6.2 Назначение сетевых интерфейсов и настройка VLAN 56
6.3 Настройка IPv4-адреса 58
6.4 Настройка IPv6-адреса 59
6.5 Изменение пароля учетной записи Root 60
6.6 Восстановление настроек по умолчанию 60
6.7 Выключение ARMA FW 60

6.8 Перезагрузка ARMA FW 61
6.9 Проверка доступности хоста 61
6.10 Доступ к командной строке 61
6.11 Просмотр состояния пакетного фильтра 61
6.12 Просмотр журнала МЭ 61
6.13 Перезапуск сервисов 61
6.14 Восстановление из резервной копии 61
6.15 Активация лицензии 62
7 Обслуживание 63
7.1 Резервное копирование и восстановление 63
7.2 История изменений 64
7.2.1 Указание количества хранимых резервных копий 64
7.2.2 Просмотр истории изменений 65
7.2.3 Возврат к предыдущей сохранённой конфигурации 65
7.2.4 Локальное сохранение конфигурации 66
7.3 Восстановление конфигурации 66
7.4 Экспорт конфигурации на удалённый FTP/SMB-сервер 67
7.4.1 Экспорт конфигурации по расписанию 69
7.5 Сброс настроек 69
7.5.1 Сброс настроек через веб-интерфейс 69
7.6 Обновление программного обеспечения 70
7.7 Контроль целостности 71
7.7.1 Запуск проверки контрольных сумм вручную 73
7.7.2 Запуск проверки контрольных сумм по расписанию 73
7.8 Подключение к ARMA MC 74
8 Возможные ошибки и их решения 75
8.1 Ошибка копирования файла во время установки с использованием ISO-образа 75
8.2 Ошибки диска на «VMware» 75
8.3 Ограничение трафика не работает на «VMware» 75
8.4 Отсутствует доступ к веб-интерфейсу 75
8.5 Неверный пароль в консольном интерфейсе 75

8.6 Не работает FTP-прокси 76
8.7 Невозможно авторизоваться в прокси-сервере 76
8.8 Не срабатывает правило межсетевого экрана 76
8.9 Отсутствует доступ к порталу авторизации 76
8.10 Не включается служба snmpd 77
8.11 Ошибка инициализации контрольных сумм проверки целостности 77
8.12 Ошибка конфигурации псевдонимов 77
9 Приложение А 78

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
ЛВС	Локально-вычислительная сеть
Массив	Система дискового хранения, содержащая несколько дисков
МЭ	Межсетевой экран
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
СОВ	Система обнаружения вторжений
ЦП	Центральный процессор
ARMA FW	InfoWatch ARMA Firewall
CA	Certification authority – центр сертификации
CARP	Common Address Redundancy Protocol – протокол дупликации общего адреса
CIDR	Classless Inter-Domain Routing – бесклассовая междоменная маршрутизация
CRC	Cyclic Redundancy Check – циклический избыточный код
DHCP	Dynamic Host Configuration Protocol, протокол динамической настройки узла
DVI	Digital Visual Interface – цифровой видеоинтерфейс
FTP	File Transfer Protocol – протокол передачи файлов по сети
GPT/UEFI	GUID Partition Table – таблица разделов GUID
HTTP	HyperText Transfer Protocol, протокол передачи гипертекста – протокол прикладного уровня передачи данных

Термины и сокращения	Значение
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
LDAP	Lightweight Directory Access Protocol – легковесный протокол доступа к каталогам
MBR	Master Boot Record – главная загрузочная запись
NTP	Network Time Protocol, протокол сетевого времени – сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью
RAID	Redundant Array of Independent Disks, избыточный массив независимых дисков – технология виртуализации данных для объединения нескольких дисковых устройств в логический модуль
RFC	Request for Comments, рабочее предложение – документ из серии пронумерованных информационных документов Интернета
SNMP	Simple Network Management Protocol, простой протокол сетевого управления – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDPB
SPAN	Switch Port Analyzer – анализатор коммутируемых портов
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
SSL	Secure Sockets Layer, уровень защищённых сокетов – криптографический протокол

Термины и сокращения	Значение
TCP	Transmission Control Protocol, протокол управления передачей – один из основных протоколов передачи данных интернета
TLS	Transport layer security – протокол защиты транспортного уровня
USB	Universal Serial Bus – универсальная последовательная шина
VGA	Video Graphics Array – компонентный видеоинтерфейс
VLAN	Virtual Local Area Network – виртуальная локальная компьютерная сеть
VPN	Virtual Private Network, виртуальная частная сеть – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети
WAN	Wide Area Network – глобальная вычислительная сеть

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

Таблица «Смежные документы»

Сокращённое наименование	Полное наименование
Руководство пользователя ARMA FW	Руководство пользователя по эксплуатации InfoWatch ARMA Firewall
Руководство пользователя ARMA MC	Руководство пользователя по эксплуатации InfoWatch ARMA Management Console

АННОТАЦИЯ

Настоящее руководство администратора предназначено для пользователей, производящих установку, запуск и первоначальную настройку конфигурации работы **ARMA Firewall v.3.13**.

К первоначальным настройкам относятся:

- назначение физических интерфейсов;
- настройка IP-адресов;
- подключение к веб-интерфейсу;
- активация лицензии;
- создание пользовательских учётных записей и назначение им привилегий.

Роль пользователя и администратора может выполнять один сотрудник предприятия.

1 ТРЕБОВАНИЯ К СРЕДЕ ФУНКЦИОНИРОВАНИЯ

Инсталляция **ARMA Firewall** производится на аппаратную или виртуальную платформы.

Установка на аппаратную платформу производится с использованием USB-накопителя с записанным образом **ARMA FW** в формате **«img»**.

Установка на виртуальную платформу производится с помощью образа оптического диска в формате **«iso»**.

При любом из вариантов установки, для корректного отображения веб-интерфейса, к веб-браузерам предъявляются следующие требования:

- для ОС семейства Windows – Яндекс Браузер, Chrome, Firefox;
- для ОС семейства Linux – Яндекс Браузер, Chrome для Linux, Firefox для Linux.

Примечание:

Для корректной работы веб-интерфейса **ARMA FW** следует отключать блокировщики рекламы и всплывающих окон.

Примечание:

Во избежание некорректной работы **ARMA FW** не рекомендуется допускать незапланированные отключения питания оборудования. В случае отключения питания во время активации лицензии, изменения конфигурации, создания/удаления правил МЭ и т.п. внесённые изменения сохранены не будут.

1.1 Требования к аппаратной платформе

Технические требования, предъявляемые к аппаратной платформе:

1. Микропроцессорная архитектура x64.
2. Для корректного функционирования **ARMA FW** с общей пропускной способностью 150 Мбит/с при работе функций МЭ и СОВ минимальные требования к оборудованию:
   - **Процессор** – 2,0 ГГц, двухъядерный, x64;
   - **ОЗУ** – 16 ГБ;
   - **Интерфейсы** – Последовательная консоль или видео-выход (VGA или DVI) с USB (или PS/2) интерфейсами для подключения клавиатуры;
   - **Жёсткий диск** – 120 ГБ, SSD;
   - **Сетевой интерфейс** – Не менее 2 x Ethernet 10/100/1000 Мбит/сек.

Примечание:

К сетевым адаптерам **ARMA FW** предъявляются следующие требования:

- модели используемых сетевых адаптеров должны быть идентичными;
- не используемые сетевые адаптеры должны быть отключены на аппаратном уровне.

1.2 Требования к виртуальной платформе

Технические требования, предъявляемые к виртуальной платформе:

1. Виртуализация **ARMA FW** поддерживается для следующих гипервизоров:
   - HyperV Generation 1;
   - VirtualBox версии 6.0.4 и выше;
   - VMware ESXi версии 5.5 обновления 2 и выше;
   - QEMU/KVM.
2. Для корректного функционирования **ARMA FW** с общей пропускной способностью 100 Мбит/с при работе функций МЭ и СОВ минимальные требования к виртуальной среде:
   - Количество процессоров – 1;
   - Количество ядер процессора – 8;
   - Объем оперативной памяти – 16 ГБ;
   - Размер виртуального диска – 25 ГБ;
   - Количество сетевых интерфейсов – 2.

В случае требования обеспечения более высокой производительности и хранения большего количества записей журналов необходимо руководствоваться значениями минимальных требований к аппаратной платформе, представленных в разделе Требования к аппаратной платформе.

Примечание:

Все необходимые сетевые интерфейсы для виртуальной машины должны быть добавлены до начала процесса установки **ARMA FW**.

К сетевым адаптерам **ARMA FW** предъявляются следующие требования:

- модели используемых сетевых адаптеров должны быть идентичными;

- не используемые сетевые адаптеры должны быть отключены на аппаратном уровне.

Примечание:

Кластеризация **ARMA FW** не поддерживается на виртуальных машинах.

1.2.1 Требования к настройке среды виртуализации

Для уточнения возможности включения технологии виртуализации для физической платформы необходимо обратиться к описанию по использованию данной платформы.

Проверка работоспособности технологии виртуализации осуществляется следующим образом:

1. Для ОС семейства Linux необходимо выполнить команду «cat /proc/cpuinfo | grep vmx svm» и убедиться, что вывод команды пуст, в противном случае имеются ошибки в настройках или в системе отсутствуют необходимые расширения.
2. Для ОС семейства Windows – убедиться в поддержке виртуализации руководствуясь документацией на данную ОС, либо успешной попыткой запуска произвольной ВМ.

2 УСТАНОВКА И ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА СИСТЕМЫ

2.1 Установка

Для записи установочного образа **ARMA FW** на USB-накопитель необходимо использовать ПО для записи образа на внешние накопители, например, ПО «Rufus» (https://rufus-usb.ru.uptodown.com/windows). Запись образа производится в соответствии с описанием по использованию данного ПО.

При загрузке с USB-накопителя запустится режим автоустановки. В данном режиме будут выполнены следующие действия:

- установка **ARMA FW** на первый определившийся жёсткий диск;
- добавление в **ARMA FW** всех доступных сетевых интерфейсов – после установки интерфейсы необходимо включить и настроить вручную;
- выключение **ARMA FW** с продолжительным воспроизведением звука.

Возможна работа **ARMA FW** в режиме **«live»** с USB-накопителя. Данный режим позволяет подключаться к веб-интерфейсу в целях ознакомления с функциональными возможностями ПО без непосредственной установки.

До начала процесса установки существует возможность вручную назначить сетевые интерфейсы. Для этого необходимо при появлении надписи **«Press any key to start the manual interface assignment:»** (см. Рисунок – Предложение ручного назначения интерфейсов) нажать любую клавишу в течение 5 секунд, в противном случае будут применены настройки по умолчанию:

- первый определённый сетевой порт, **«em0»** – будет назначен как интерфейс LAN с присвоенным IP-адресом «192.168.1.1/24»;
- второй определённый системой сетевой порт, **«em1»** – будет назначен как интерфейс WAN с присвоенным IP-адресом по DHCP, в случае его наличия.

Назначение физических интерфейсов подробнее описано в разделах Назначение сетевых интерфейсов и Назначение сетевых интерфейсов и настройка VLAN.

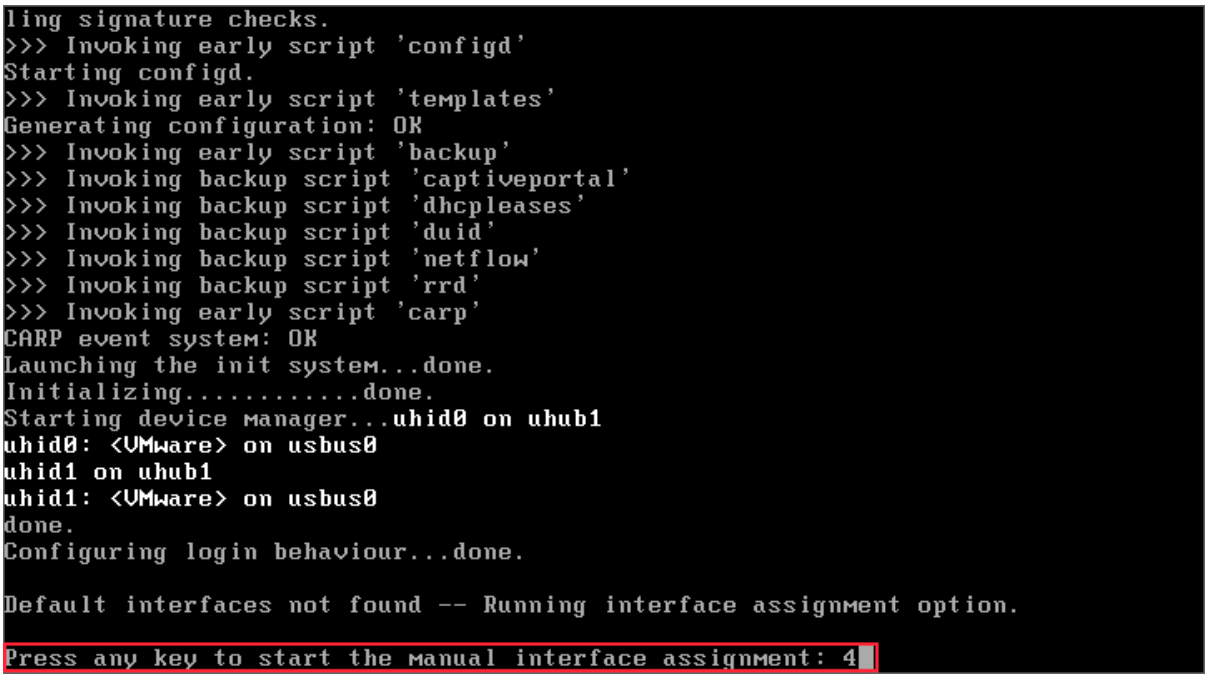

Рисунок – Предложение ручного назначения интерфейсов

Примечание:

В консольном интерфейсе управление происходит только с использованием клавиатуры. Выбор производится с помощью **клавиш со стрелками вверх и вниз**, а подтверждение выбора осуществляется с помощью **клавиши «ENTER»**.

2.1.1 Работа в режиме «live» с USB-накопителя

Для начала работы в режиме **«live»** с USB-накопителя необходимо выполнить следующие действия:

1. При появлении надписи **«Press any key to stop auto installation and run manual installation»** (см. Рисунок – Предложение отмены автоустановки) нажать **любую клавишу**.

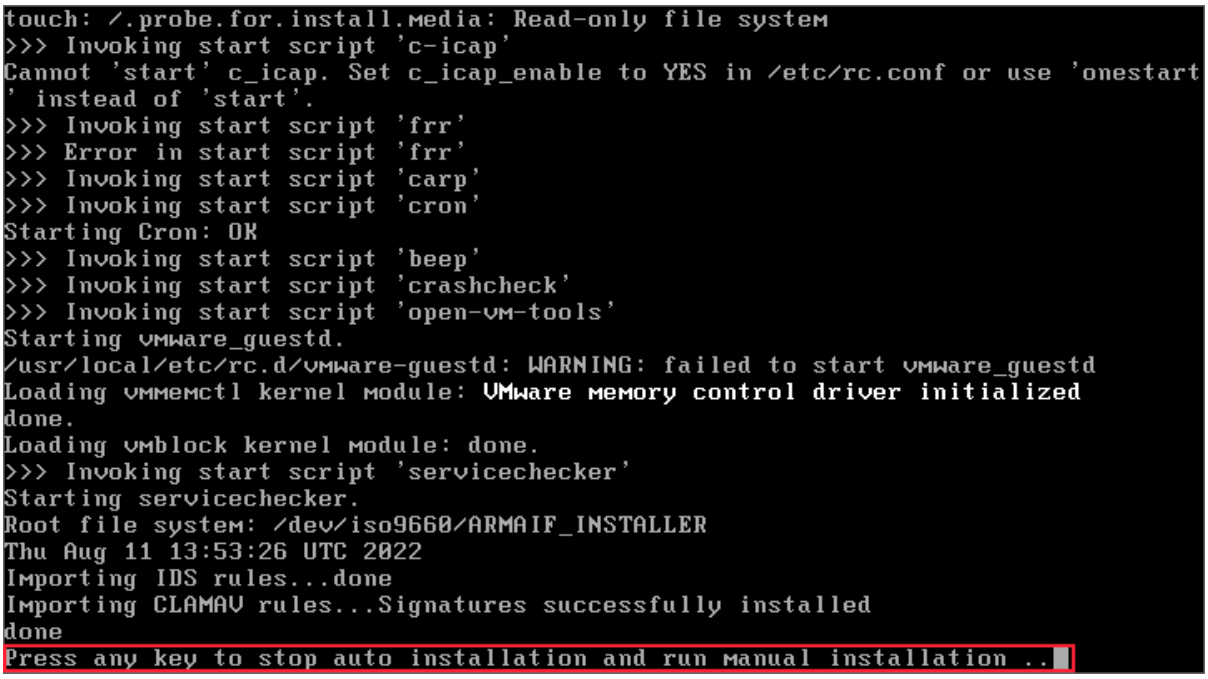

Рисунок – Предложение отмены автоустановки

2. В появившейся форме (см. Рисунок – Приветственное сообщение) нажать сочетание **клавиш «Ctrl»** + **«C»**.

Рисунок – Приветственное сообщение

3. После появления приглашения на вход в консольном интерфейсе указать следующие учётные данные и нажать **клавишу «ENTER»** после каждого ввода:
   - **«login:»** – «root»;
   - **«password:»** – «root».

По умолчанию в режиме работы **«live»** с USB-накопителя веб-интерфейс доступен по адресу «https://192.168.1.1/».

Для входа в веб-интерфейс необходимо выполнить следующие действия:

1. Открыть веб-браузер на ПК, подключённым ethernet-кабелем к сетевому порту **«em0»**. Сетевые настройки ПК должны быть получены автоматически по DHCP.
2. В веб-браузере перейти по адресу «https://192.168.1.1/» и произвести аутентификацию со следующей УЗ:
   - **«Username»** – «root»;
   - **«Password»** – «root».

Все изменения, сделанные в режиме **«live»** с USB-накопителя, будут потеряны после перезагрузки, однако при установке без перезагрузки все изменения, внесённые в конфигурацию, будут сохранены.

2.1.2 Установка с заданными параметрами

Для установки **ARMA FW** с заданными параметрами необходимо выполнить следующие действия:

1. При появлении надписи **«Press any key to stop auto installation and run manual installation»** (см. Рисунок – Предложение отмены автоустановки) нажать **любую клавишу**.
2. В открывшейся форме выбрать **«Ok, let's go»** (см. Рисунок – Приветственное сообщение) для запуска мастера установки **ARMA FW**.

Шаги мастера установки:

1. Шаг мастера – **«Настройка консоли»** (см. Рисунок – Настройка консоли).

   Доступные варианты установки:

   - **«Accept these Setting»** – «Принять настройки по умолчанию»;
   - **«Change Keymap (default)»** – «Изменить раскладку клавиатуры»;
   - **«Change Video Font (default)»** – «Изменить шифры текста», то есть способ начертания символа и его размер.

   В случае, когда нет необходимости изменять раскладку клавиатуры, следует выбрать пункт **«Accept these Settings»**.

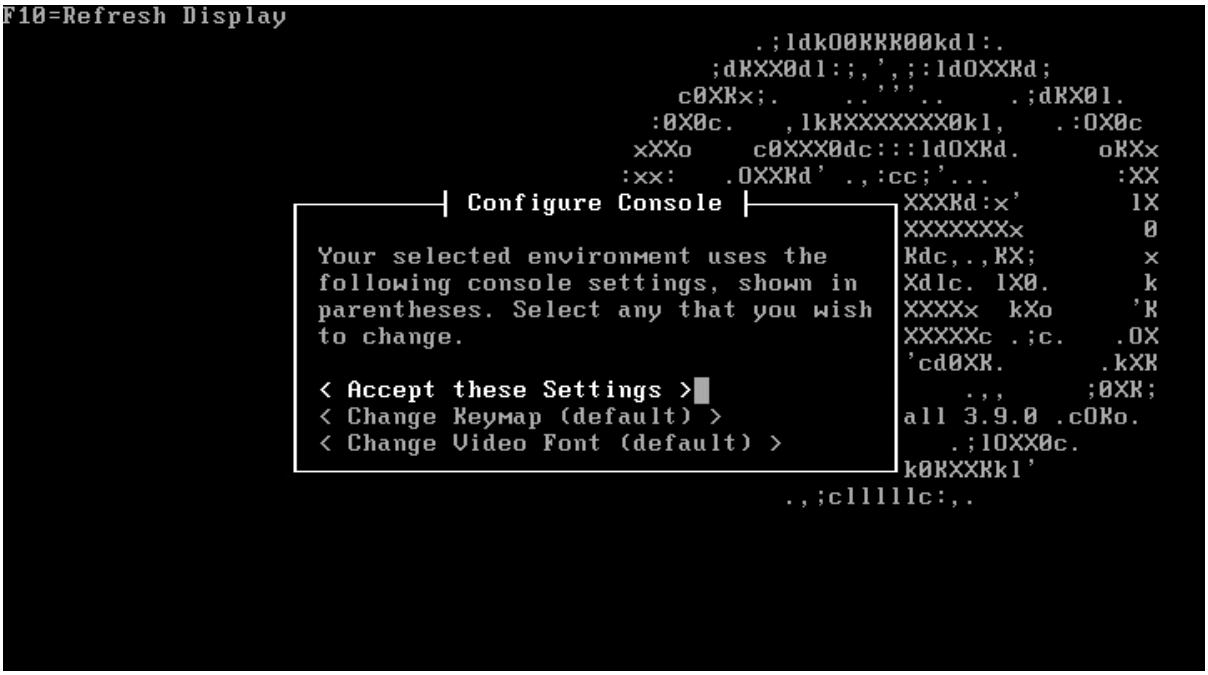

Рисунок – Настройка консоли

2. Шаг мастера – **«Выбор задачи»** (см. Рисунок – Выбор задачи).

   Доступные варианты задач и список возможных действий представлены в таблице (см. Таблица «Варианты задач и возможные действия»). Для продолжения установки **ARMA FW** необходимо выбрать параметр **«Guided installation»**.

Рисунок – Выбор задачи

Таблица «Варианты задач и возможные действия»

Название задачи	Действие
Guided installation	Установить
Manual installation	Установить вручную
Import configuration	Импортировать конфигурацию
Reset password	Сбросить пароль
Setup GEOM mirror	Настроить зеркалирование
Power off	Выключить
Exit	Выйти

3. Шаг мастера – **«Выбор диска»** (см. Рисунок – Выбор диска).

   На данном шаге выбирается диск, на который будет устанавливаться **ARMA FW**. Для возврата назад необходимо выбрать пункт **«Return to Select Task»**, а для продолжения установки необходимо выбрать целевой накопитель. Все данные на выбранном накопителе будут стёрты.

   В случае настроенного программного RAID (см. Создание программного RAID) созданный массив будет отображаться пунктом **«mirror/ARMAFW»**.

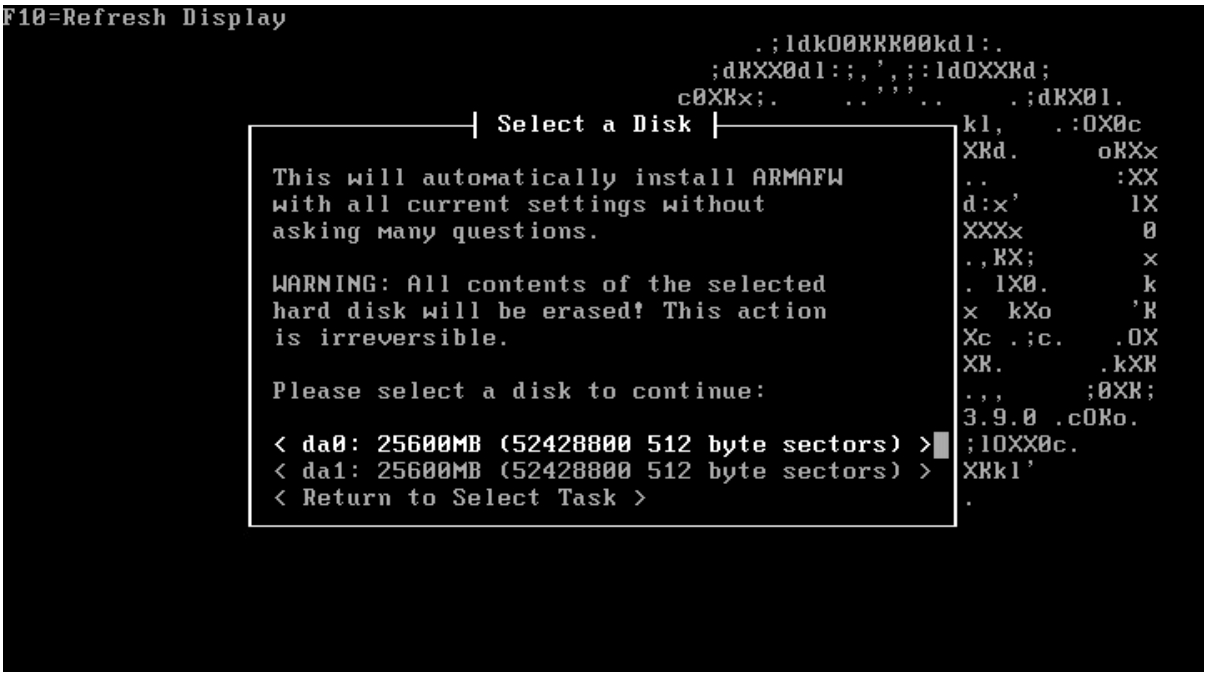

Рисунок – Выбор диска

4. Шаг мастера – **«Выбор режима установки»** (см. Рисунок – Выбор режима установки).

   Доступные варианты режимов записи на диск представлены в таблице (см. Таблица «Варианты режима установки»). Для продолжения установки

рекомендуется выбрать пункт **«GPT/UEFI mode»**. Для возвращения назад необходимо выбрать пункт **«Return to Select Disk»**.

Рисунок – Выбор режима установки

Таблица «Варианты режима установки»

Название режима установки	Описание
GPT/UEFI mode	Запись в раздел GPT/UEFI жёсткого диска
MBR mode	Запись в раздел MBR жёсткого диска

5. Шаг мастера – **«Выполнение установки»** (см. Рисунок – Установка системы).

   На данном шаге отображается процесс установки **ARMA FW**. Для прерывания процесса установки необходимо выбрать **«Cancel»** и нажать **клавишу «ENTER»**.

Рисунок – Установка системы

6. Шаг мастера – **«Установка пароля суперпользователя»** (см. Рисунок – Выбор пароля).

   На данном шаге необходимо указать новый пароль УЗ «Root»:

   - в поле **«Root Password»** и нажать **клавишу «ENTER»**;
   - в поле **«Re-type Root Password»** и нажать **клавишу «ENTER»**.

   После ввода пароля необходимо выбрать пункт **«Accept and Set Password»** и нажать **клавишу «ENTER»**.

Рисунок – Выбор пароля

7. Шаг мастера – **«Выключение»** (см. Рисунок – Выключение).

   На данном шаге возможно:

   - вернуться к шагу 2 **«Выбор задачи»** – для этого выбрать **«Return to Select Task»** и нажать **клавишу «ENTER»**;
   - выполнить выключение **ARMA FW** – для этого выбрать пункт **«Power off»** и нажать **клавишу «ENTER»**.

   Перед последующей загрузкой необходимо извлечь USB-накопитель.

Рисунок – Выключение

2.1.3 Создание программного RAID

Для создания программного RAID 1 при установке **ARMA FW** необходимо выполнить следующие действия:

1. Запустить мастер установки с заданными параметрами (см. Установка с заданными параметрами).
2. Выбрать пункт **«Setup GEOM mirror»** (см. Рисунок – Выбор задачи) на втором шаге мастера.
3. Подтвердить выполнение задачи, выбрав пункт **«Yes, setup a GEOM mirror»** при запросе **«Would you like to setup a GEOM mirror?»**.
4. Выбрать первый диск создаваемого массива (см. Рисунок – Выбор первого диска).

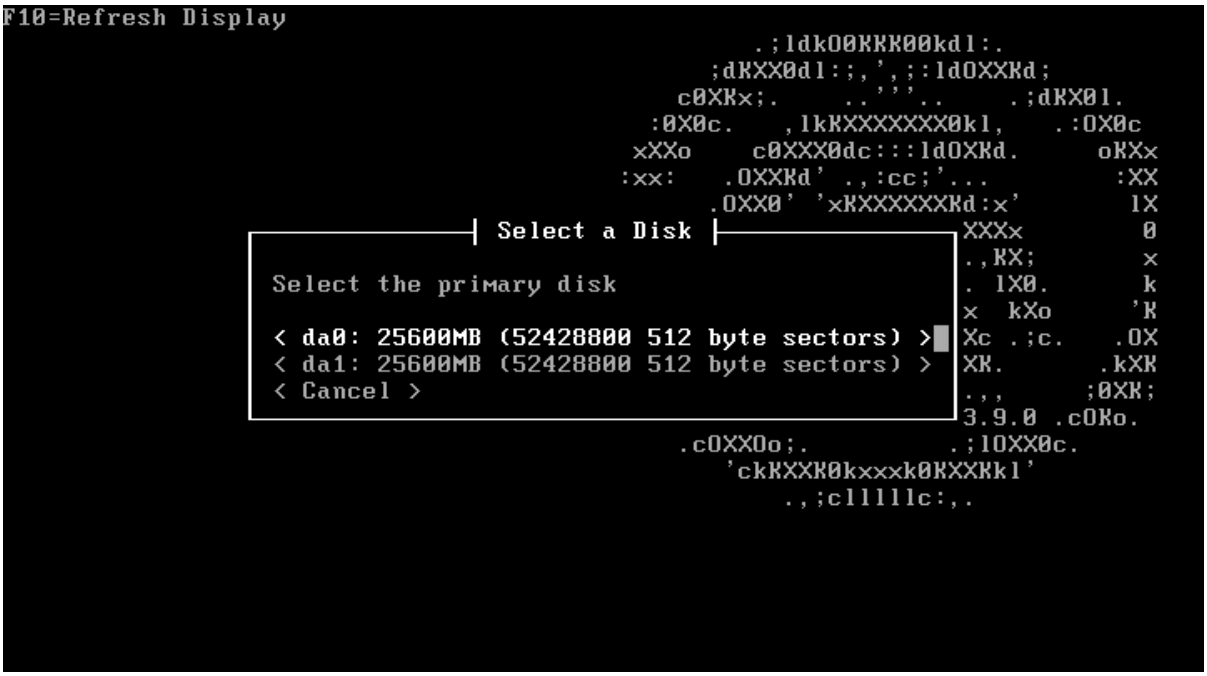

Рисунок – Выбор первого диска

5. Выбрать второй диск создаваемого массива (см. Рисунок – Выбор второго диска).

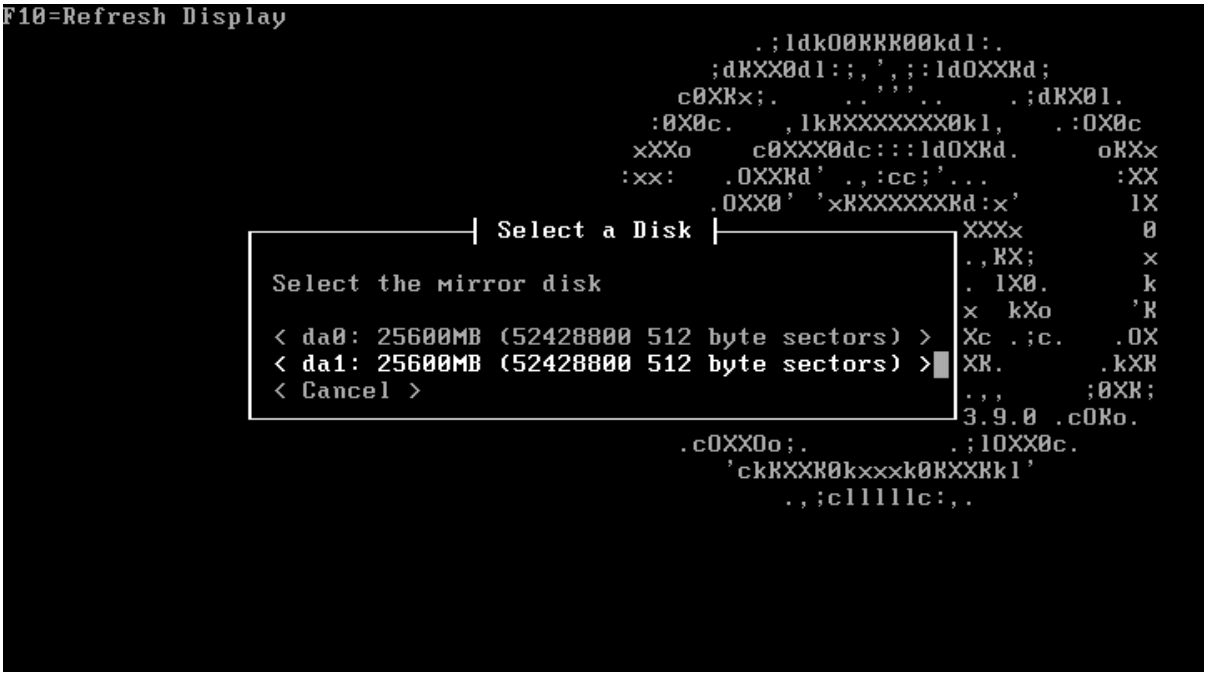

Рисунок – Выбор второго диска

В случае успешного создания массива будет отображена соответствующая информация (см. Рисунок – Успешное создание массива), с которой следует ознакомиться и нажать **клавишу «Enter»**. После чего будет выполнен переход на второй шаг мастера установки с заданными параметрами (см. Установка с заданными параметрами).

Рисунок – Успешное создание массива

Для проверки статуса массива после установки **ARMA FW** необходимо выполнить следующие действия:

1. Авторизоваться в локальном консольном интерфейсе **ARMA FW** (см. Первоначальная настройка).
2. Выбрать пункт меню **«8) Shell»** для перехода в командный интерфейс (см. Описание локального консольного интерфейса).
3. Ввести команду **«gmirror status»** и нажать **клавишу «Enter»**.
4. Убедиться, что статусы массива и дисков в его составе являются **«COMPLETE»** и **«ACTIVE»** соответственно (см. Рисунок – Проверка статуса массива).

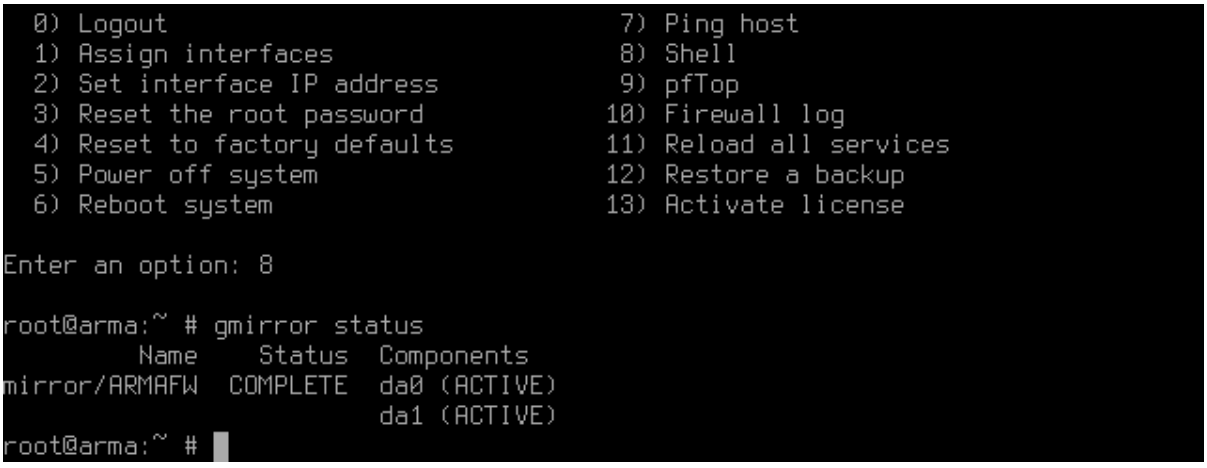

Рисунок – Проверка статуса массива

2.2 Первоначальная настройка

Перед загрузкой **ARMA FW** необходимо убедиться, что установочный носитель извлечён.

Загрузка системы завершается приглашением для входа (см. Рисунок – Приглашение для входа в консольное меню).

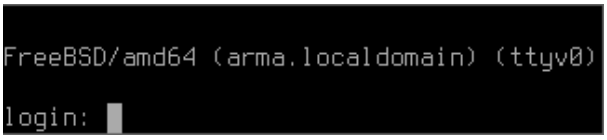

Рисунок – Приглашение для входа в консольное меню

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

- **«login:»** – «root»;
- **«password:»** – пароль, заданный на этапе установки, по умолчанию «root».

После успешной аутентификации будет отображено консольное меню, отображающее действия, представленные в таблице (см. Таблица «Действия консольного меню»).

Таблица «Действия консольного меню»

Действие	Действие
0 Logout	7 Ping host
1 Assign interfaces	8 Shell
2 Set interface IP address	9 pfTop
3 Reset the root password	10 Firewall log
4 Reset to factory defaults	11 Reload all services
5 Power off system	12 Restore a backup
6 Reboot system	13 Activate license

Управление в локальном консольном интерфейсе происходит только с использованием клавиатуры. Выбор пунктов меню осуществляется вводом порядкового номера пункта, а подтверждение выбора нажатием **клавиши «ENTER»**.

2.2.1 Назначение сетевых интерфейсов

Для ручного назначения сетевых интерфейсов необходимо выбрать пункт меню **«1) Assign interfaces»**. В результате выбора будут отображены доступные сетевые интерфейсы и будет выведен запрос на настройку интерфейсов.

Каждое из представленных имён сетевых интерфейсов, кроме «OVPNS1», соответствует физическому интерфейсу. Сопоставление сетевых интерфейсов с именами производится на уровне ОС.

Запросы на назначение интерфейсов выводятся в следующей последовательности (см. Рисунок – Настройка интерфейсов):

1. **VLAN**. Настройка VLAN является необязательной, в случае если VLAN не используется, необходимо ввести **«n»** и нажать **клавишу «ENTER»**. Настройка VLAN описана в разделе Назначение сетевых интерфейсов и настройка VLAN настоящего руководства.
2. **WAN**. В случае отсутствия потребности в настройке WAN, необходимо нажать **клавишу «ENTER»**, в противном случае ввести соответствующее имя физического интерфейса, например, **«em1»** и нажать **клавишу «ENTER»**.
3. **LAN**. В случае отсутствия потребности в настройке LAN, необходимо нажать **клавишу «ENTER»**, в противном случае ввести соответствующее имя физического интерфейса, например, **«em0»** и нажать **клавишу «ENTER»**.
4. **OPTx**, где x – номер дополнительного сетевого интерфейса. В случае отсутствия потребности в настройке OPTx, необходимо нажать **клавишу «ENTER»**, в противном случае ввести соответствующее имя физического интерфейса, например, **«em2»** и нажать **клавишу «ENTER»**. Количество предложенных настроек для дополнительных интерфейсов равно количеству определённых ОС сетевых интерфейсов.

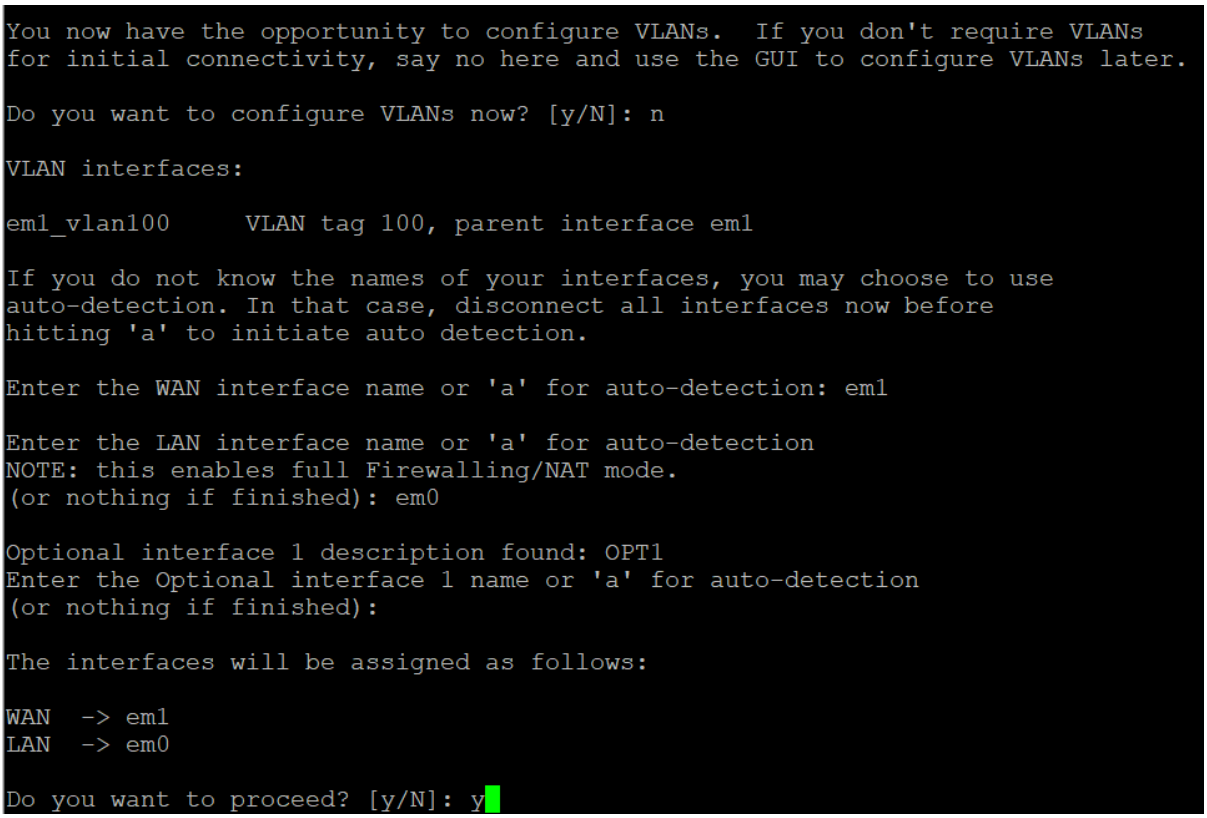

Рисунок – Настройка интерфейсов

Когда все сетевые интерфейсы назначены, необходимо нажать **клавишу «ENTER»** на вопрос о назначении последующего сетевого интерфейса. Далее необходимо удостовериться в правильности назначения интерфейсов и подтвердить настройки, нажав **клавишу «y»**, а затем **клавишу «ENTER»** в ответ на сообщение **«Do you want proceed?»** (см. Рисунок – Настройка интерфейсов). **ARMA FW** настроит сетевые интерфейсы и представит приглашение для входа в систему по завершении.

Примечание:

В случае, когда имена сетевых портов, используемых в качестве LAN, WAN или OPTx, неизвестны, необходимо выполнить следующие действия:

1. Отключить все сетевые кабели от **ARMA FW**.
   - Ввести **«a»** и нажать **клавишу «ENTER»** на запрос **«Enter the [Имя интерфейса] interface name or 'a' for auto-detection:»**, где [Имя интерфейса] – имя настраиваемого интерфейса.
2. Подключить сетевой кабель, используемый для настраиваемого интерфейса, убедиться в наличии линка и нажать **клавишу «ENTER»**.
3. В результате найденный сетевой порт будет назначен настраиваемому интерфейсу.

2.2.2 Настройка IP-адресов

Для настройки IP-адресов на назначенных интерфейсах необходимо выбрать пункт меню **«2) Set interface(s) IP address»**. Подробная настройка описана в разделах Настройка IPv4-адреса и Настройка IPv6-адреса.

Настройка IP-адресов может быть выполнена через веб-интерфейс **ARMA FW**. Подробная настройка через веб-интерфейс описана в разделе **«Настройка сетевых интерфейсов»** Руководства пользователя **ARMA FW**.

2.3 Настройка ARMA FW посредством веб-интерфейса

2.3.1 Подключение к веб-интерфейсу

Для подключения к веб-интерфейсу необходимо открыть веб-браузер и ввести IP-адрес, указанный в консольном интерфейсе, по умолчанию – 192.168.1.1 (см. Рисунок – IP-адрес веб-интерфейса).

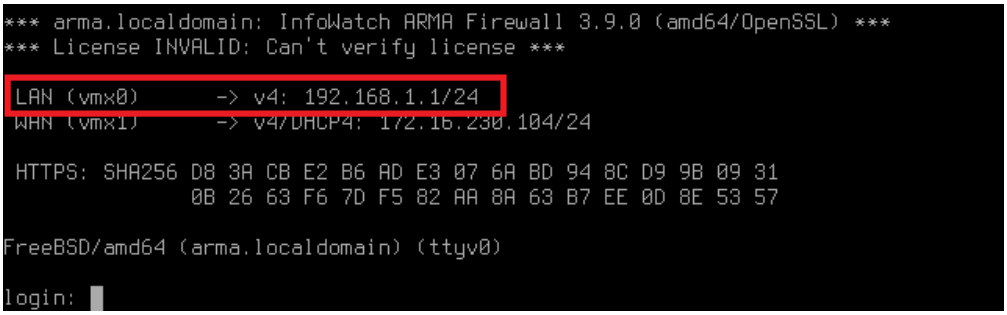

Рисунок – IP-адрес веб-интерфейса

Примечание:

При первом подключении для успешной авторизации в **ARMA FW** необходимо активировать лицензию одним из способов, представленных в разделе Активация лицензии настоящего руководства.

Для начала работы с **ARMA FW** необходимо авторизоваться (см. Рисунок – Вход в систему). Для этого выполнить следующие действия:

1. В поле **«Username:»** ввести «root».
2. В поле **«Password:»** ввести пароль, заданный при установке **ARMA FW** (см. Рисунок – Выбор пароля), по умолчанию – «root».
3. Нажать кнопку **«Login»** для входа в систему.

Рисунок – Вход в систему

При первой успешной авторизации в веб-интерфейсе и активации лицензии будет запущен мастер первоначальной настройки **ARMA FW**. Мастер будет запущен на английском языке.

Подробное описание шагов мастера первоначальной настройки описана в разделе **«Мастер первоначальной настройки»** Руководства пользователя **ARMA FW**.

2.3.2 Активация лицензии

При первом подключении или в случае истечения периода активации запрос на активацию лицензии будет выведен автоматически после авторизации в веб-интерфейсе.

Активация лицензии доступна одним из следующих способов (см. Рисунок – Активация лицензии):

- **«Online activation»** – активация лицензии с доступом в Интернет;
- **«Offline activation»** – активация лицензии без доступа в Интернет.

Рисунок – Активация лицензии

Примечание:

Лицензионный ключ предоставляется согласно условиям в договоре поставки.

2.3.2.1 Активация лицензии с доступом в Интернет

Для активации лицензии с доступом в Интернет необходимо в параметре **«Activation type»** выбрать значение **«Online activation»**, в поле параметра **«License key»** указать лицензионный ключ и нажать **кнопку «Activate»** (см. Рисунок – Активация лицензии с доступом в Интернет).

Рисунок – Активация лицензии с доступом в Интернет

2.3.2.2 Активация лицензии без доступа в Интернет

Для активации лицензии без доступа в Интернет необходимо выполнить следующие действия:

1. В параметре **«Activation type»** выбрать значение **«Offline activation»**, в поле параметра **«License key»** указать лицензионный ключ и нажать **кнопку «Get token»** (см. Рисунок – Активация лицензии без доступа в Интернет, получение токена).

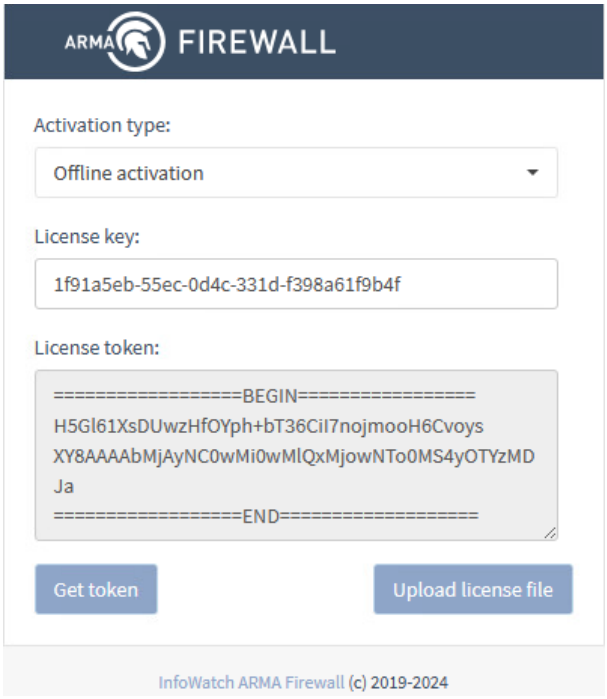

Рисунок – Активация лицензии без доступа в Интернет, получение токена

2. Скопировать значение поля параметра **«License token»** и направить в техподдержку **ООО «ИнфоВотч АРМА»** для получения файла лицензии **«license.bin»**.
3. Нажать **кнопку «Upload license file»**, в открывшемся окне проводника выбрать полученный файл **«license.bin»** и нажать **кнопку «Открыть»**.
4. После успешной активации лицензии (см. Рисунок – Успешная активация лицензии без доступа в Интернет) произойдёт перенаправление на окно мастера первоначальной настройки **ARMA FW** в течение 3 секунд.

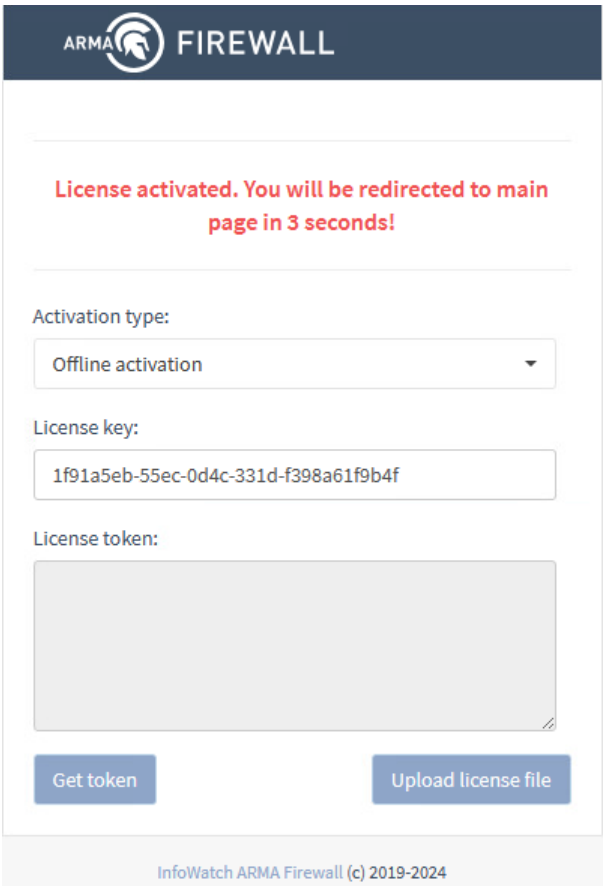

Рисунок – Успешная активация лицензии без доступа в Интернет

2.3.2.3 Информация о лицензии

Информация о действующей лицензии отображается в виджете **«Информация о лицензии»** (см. Рисунок – Виджет «Информация о лицензии»).

Подробная информация о добавлении виджетов описана в разделе **«Мониторинг системы с помощью информационных виджетов»** Руководства пользователя **ARMA FW**.

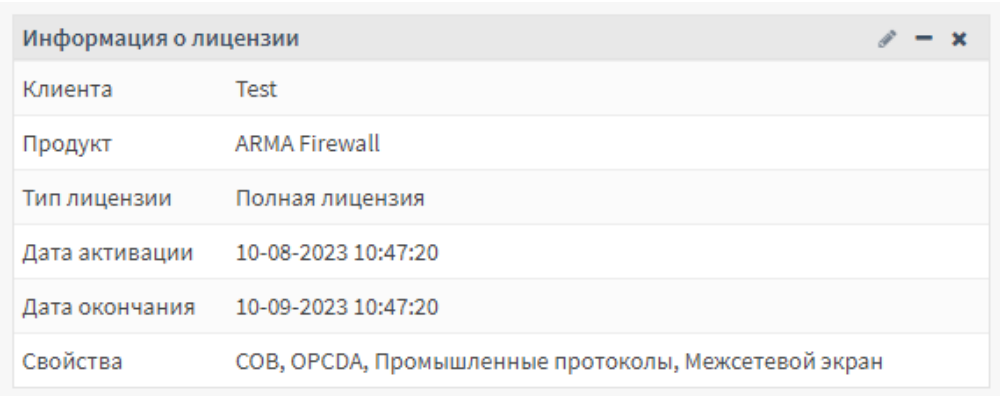

Рисунок – Виджет «Информация о лицензии»

Примечание:

В случае отсутствия ответа локального сервиса лицензирования, например, при остановке сервиса, в веб-интерфейсе будет выведено соответствующее уведомление с указанием количества дней до блокировки **ARMA FW** и рекомендуемыми действиями (см. Рисунок – Уведомление о недоступности службы лицензий).

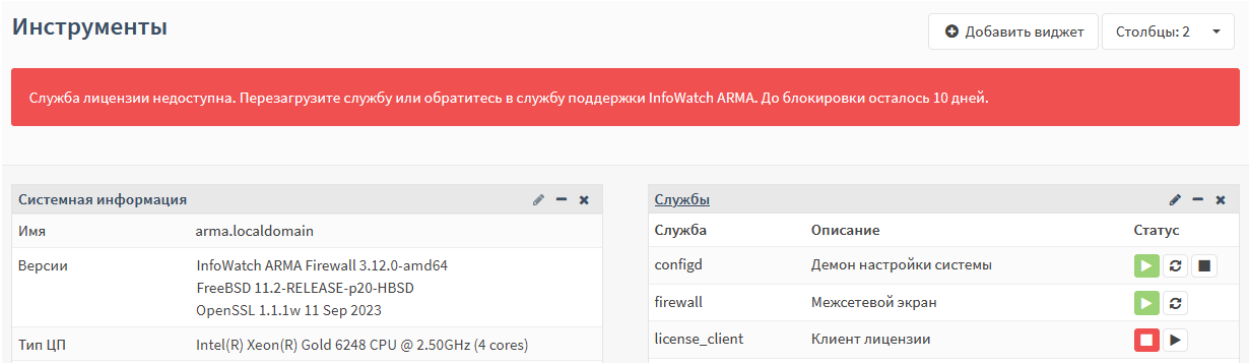

Рисунок – Уведомление о недоступности службы лицензий

По истечении указанного периода доступ к **ARMA FW** будет заблокирован (см. Рисунок – Доступ заблокирован).

Рисунок – Доступ заблокирован

2.3.2.4 Типы лицензий

В **ARMA FW** предусмотрены следующие типы лицензий:

1. **«МЭ»** – предоставляет доступ ко всем функциям **ARMA FW**, кроме раздела **«Обнаружение вторжений»**. Срок лицензии не ограничен.
2. **«МЭ + СОВ»** – предоставляет доступ ко всем функциям **ARMA FW**, кроме раздела **«Контроль промышленных протоколов»**. Срок лицензии не ограничен.
3. **«МЭ + СОВ + Пром. протоколы»** – предоставляет доступ ко всем функциям **ARMA FW**, кроме инструментария по промышленному протоколу **«OPC DA»**. Срок лицензии не ограничен.

4. **«МЭ + СОВ + Пром. протоколы + OPC DA»** – предоставляет доступ ко всем функциям **ARMA FW**. Срок лицензии не ограничен.

2.3.3 Мастер первоначальной настройки

При первом входе пользователя в веб-интерфейс **ARMA FW** автоматически совершает запуск мастера первоначальной настройки системы (см. Рисунок – Мастер первоначальной настройки). Мастер будет запущен на английском языке.

Для перехода на следующий шаг необходимо нажать **кнопку «Next»**.

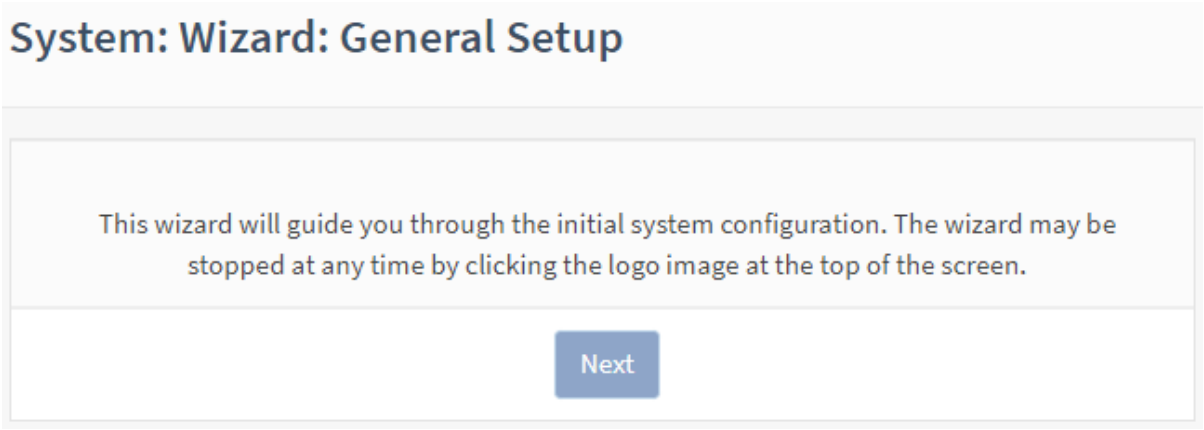

Рисунок – Мастер первоначальной настройки

Примечание:

Использование мастера первоначальной установки необязательно. Для выхода из мастера необходимо нажать на логотип FIREWALL в верхнем левом углу страницы на любом этапе настройки.

2.3.3.1 Шаги Мастера первоначальной настройки

2.3.3.1.1 Мастер: шаг 1

На данном шаге предлагается настроить имя хоста, необходимое для идентификации межсетевого экрана, указать домен, в котором находится **ARMA FW**, и сменить язык интерфейса (см. Рисунок – Мастер первоначальной настройки. Шаг 1).

Имя хоста должно начинаться с буквы и может содержать только буквы, цифры или дефис. Доменное имя также можно задать любое.

В параметре **«Language»** предполагается выбор значения **«Russian»** для смены языка интерфейса на русский. Выбранный язык будет применён на третьем шаге.

Для перехода к следующему шагу необходимо нажать **кнопку «Next»**.

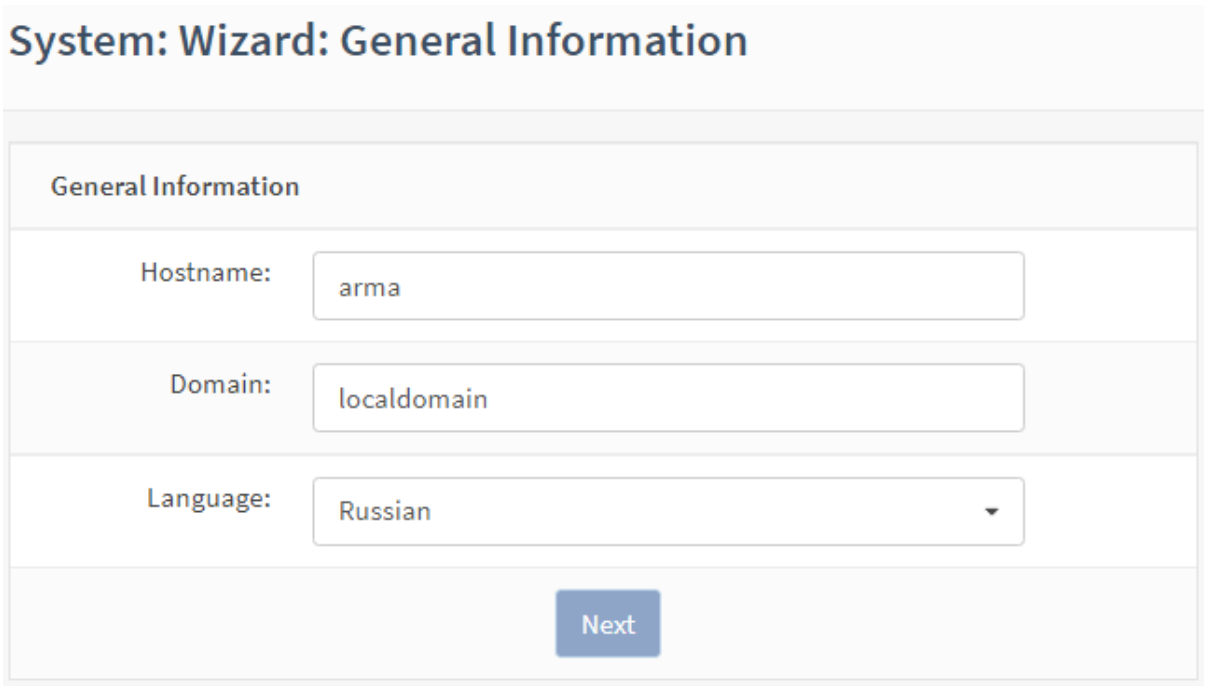

Рисунок – Мастер первоначальной настройки. Шаг 1

2.3.3.1.2 Мастер: шаг 2

На данном шаге предлагается задать параметры NTP-сервера и часового пояса (см. Рисунок – Мастер первоначальной настройки. Шаг 2). Для NTP-сервера указывается полное доменное имя или IP-адрес хоста. Если не требуется конкретный NTP-сервер, рекомендуется оставить имя сервера времени по умолчанию. Чтобы использовать несколько серверов времени необходимо добавлять их в одно поле, разделяя каждый сервер пробелом. Часовой пояс рекомендуется выбирать в соответствии с физическим расположением МЭ.

Для перехода к следующему шагу необходимо нажать **кнопку «Next»**.

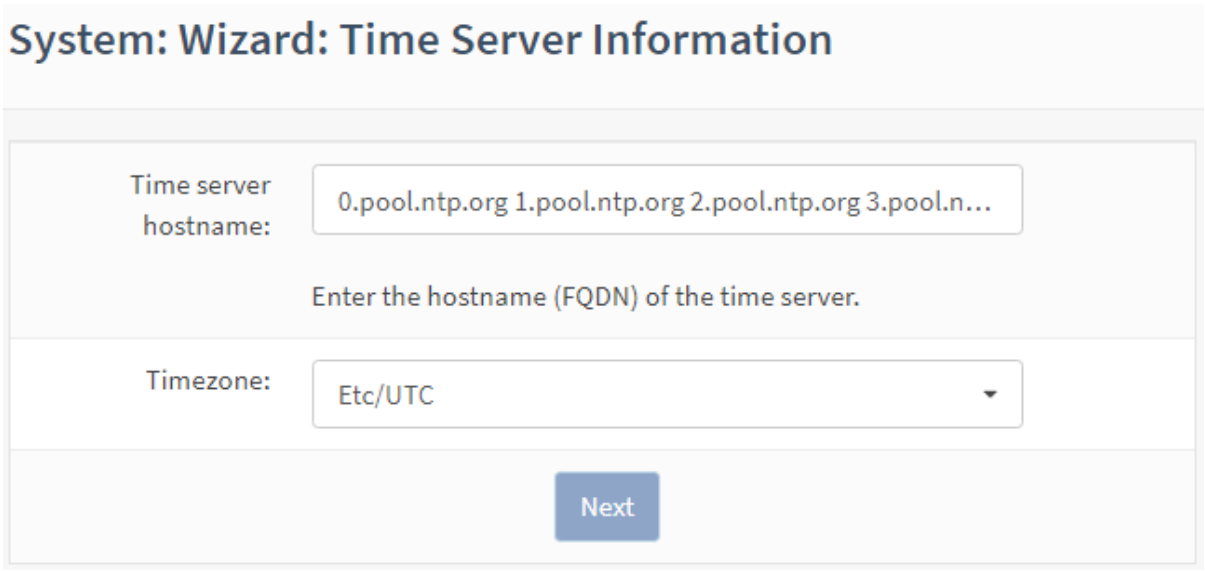

Рисунок – Мастер первоначальной настройки. Шаг 2

Примечание:

ARMA FW может иметь более двух NTP-серверов, добавить которые возможно в подразделе сетевого времени (**«Службы» - «Сетевое время» - «Общие настройки»**) после завершения работы мастера.

2.3.3.1.3 Мастер: шаг 3

На данном шаге предлагается указать пароль к системной УЗ **«root»** (см. Рисунок – Мастер первоначальной настройки. Шаг 3). Автоматически никакие ограничения к паролю не применяются, рекомендуется использовать надёжный пароль.

Для продолжения необходимо нажать **кнопку «Далее»**.

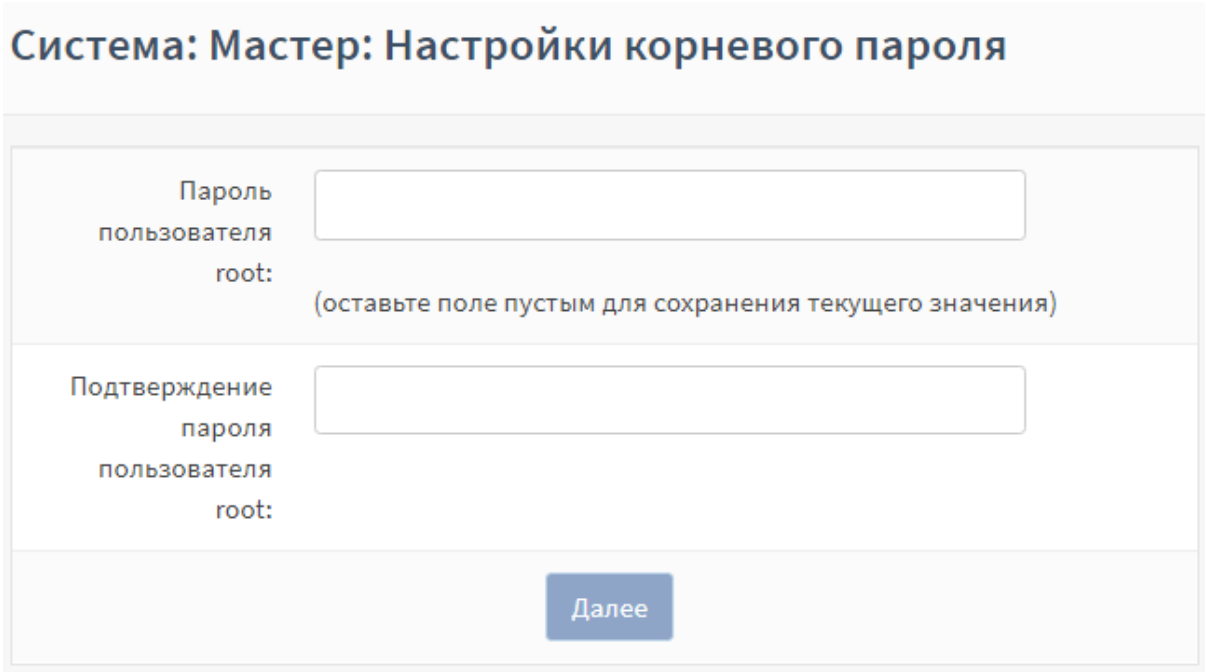

Рисунок – Мастер первоначальной настройки. Шаг 3

2.3.3.1.4 Мастер: шаг 4

На данном шаге предлагается выполнить перезагрузку для применения настроек (см. Рисунок – Мастер первоначальной настройки. Шаг 4). Необходимо нажать **кнопку «Перезагрузить»**.

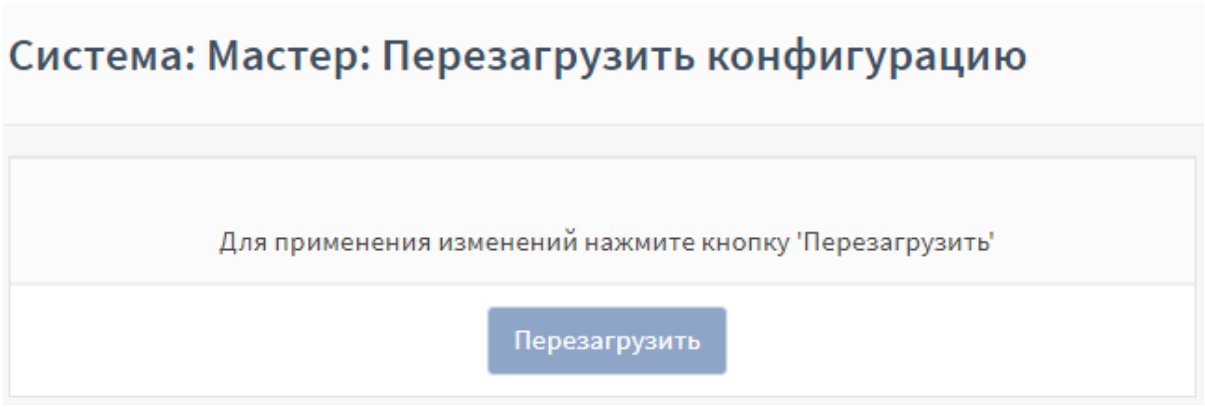

Рисунок – Мастер первоначальной настройки. Шаг 4

В случае, когда необходимо, будет выполнена перезагрузка **ARMA FW**, в остальных случаях будет выведена страница с информацией об окончании настройки и предложением перейти на страницу **«Инструменты»** с виджетами.

2.3.4 Включение русского языка

По умолчанию веб-интерфейс представлен на английском языке. Для переключения на русский язык необходимо выполнить следующие действия:

1. Перейти в подраздел общих настроек **ARMA FW** (**«System» - «Setting» - «General»**).
2. В параметре **«Language»** выбрать значение **«Russian»** (см. Рисунок – Включение русского языка) и нажать **кнопку «Save»** в нижней части формы.

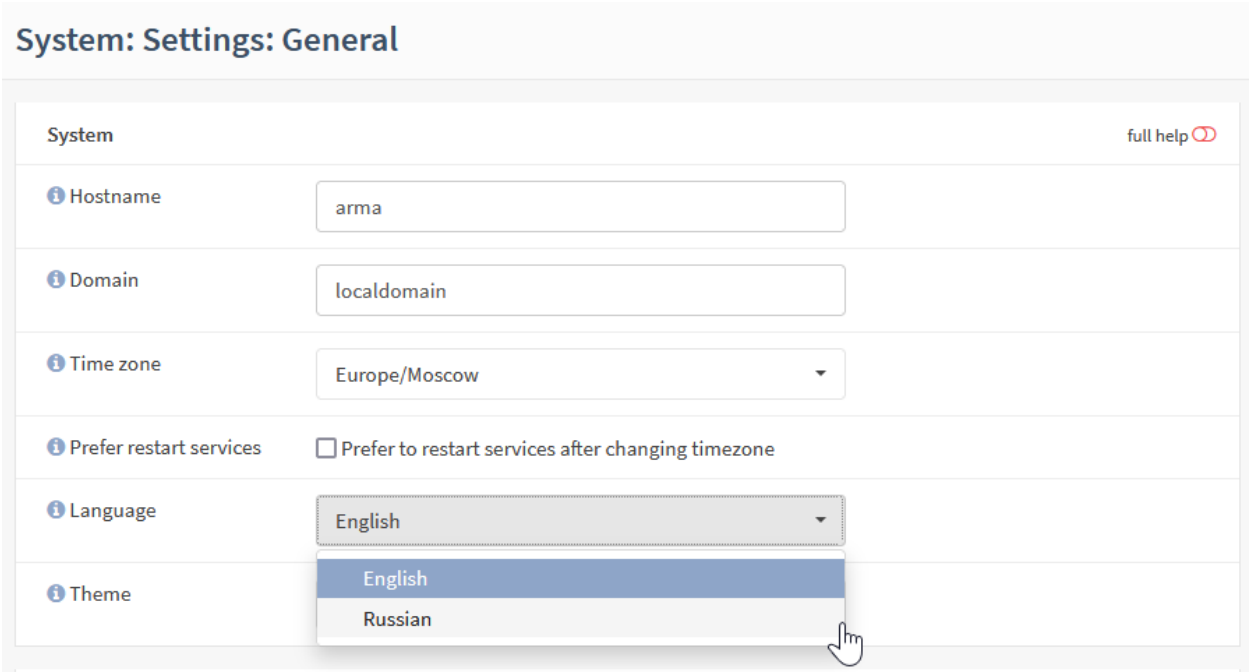

Рисунок – Включение русского языка

В настоящем руководстве все последующие действия в веб-интерфейсе приведены на русском языке.

2.3.5 Оптимизация веб-сервера

В целях оптимизации веб-сервера в разделе дополнительных настроек сетевых интерфейсов (**«Интерфейсы» - «Настройки»**) отключены следующие параметры (см. Рисунок – Обеспечение оптимальной производительности):

- **«CRC»** – расчёт контрольной суммы Ethernet-кадра средствами сетевой карты без участия ЦП;
- **«TSO»** – сегментирование TCP-пакета без участия ЦП с помощью аппаратных возможностей сетевой карты;
- **«LRO»** – буферизация входящих пакетов и их передача сетевому стеку в агрегированном виде с целью избежания неэффективной передачи каждого пакета в отдельности.

Данные параметры включать не рекомендуется.

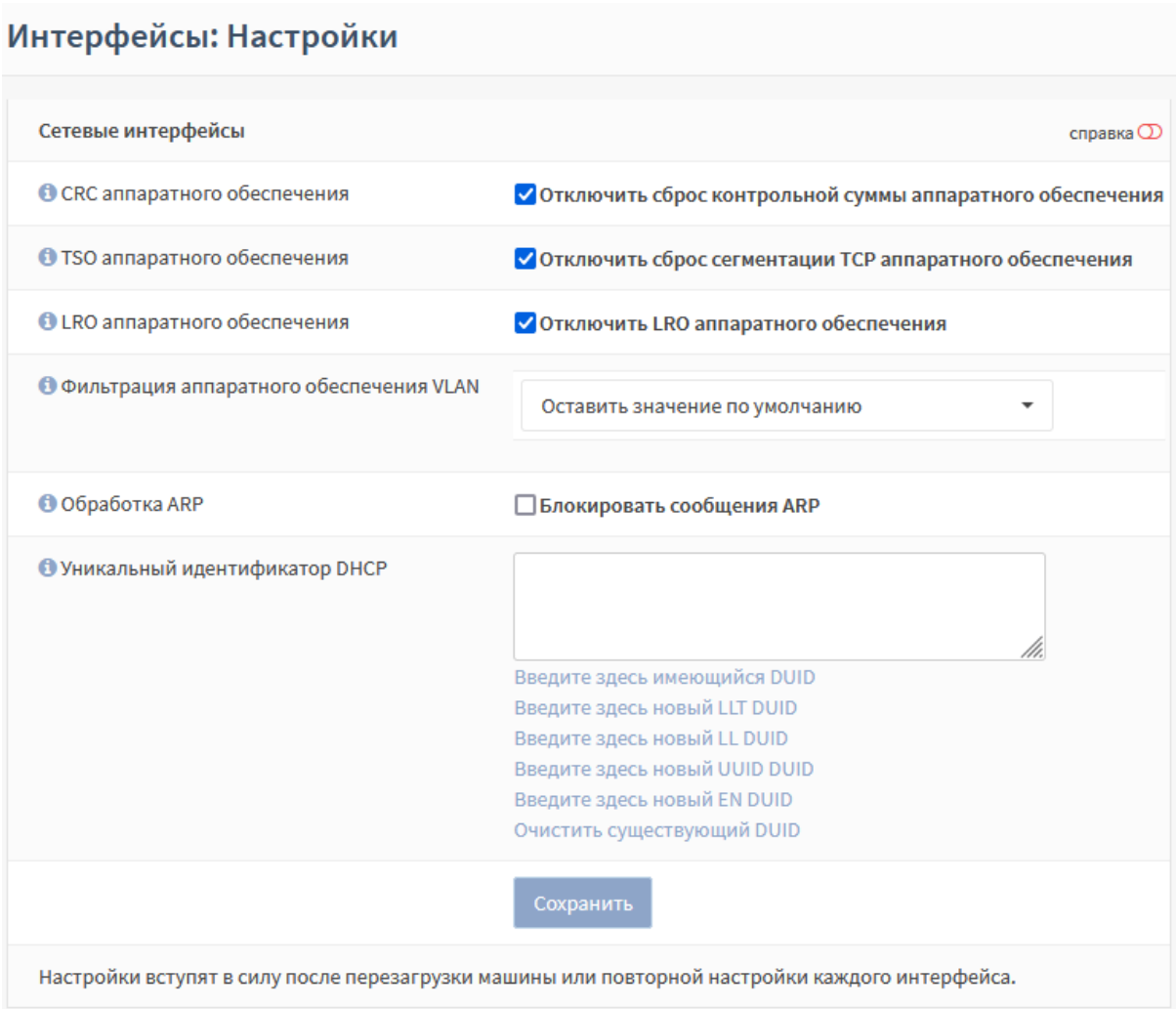

Рисунок – Обеспечение оптимальной производительности

2.3.6 Настройки безопасности

Настройки безопасности необходимы для ограничения доступа по различным интерфейсам управления.

2.3.6.1 Настройка доступа по SSH

По умолчанию доступ по SSH отключён. Настройка доступа по SSH производится в подразделе настроек администрирования системы (**«Система» - «Настройки» - «Администрирование»**) (см. Рисунок – Настройка доступа по SSH).

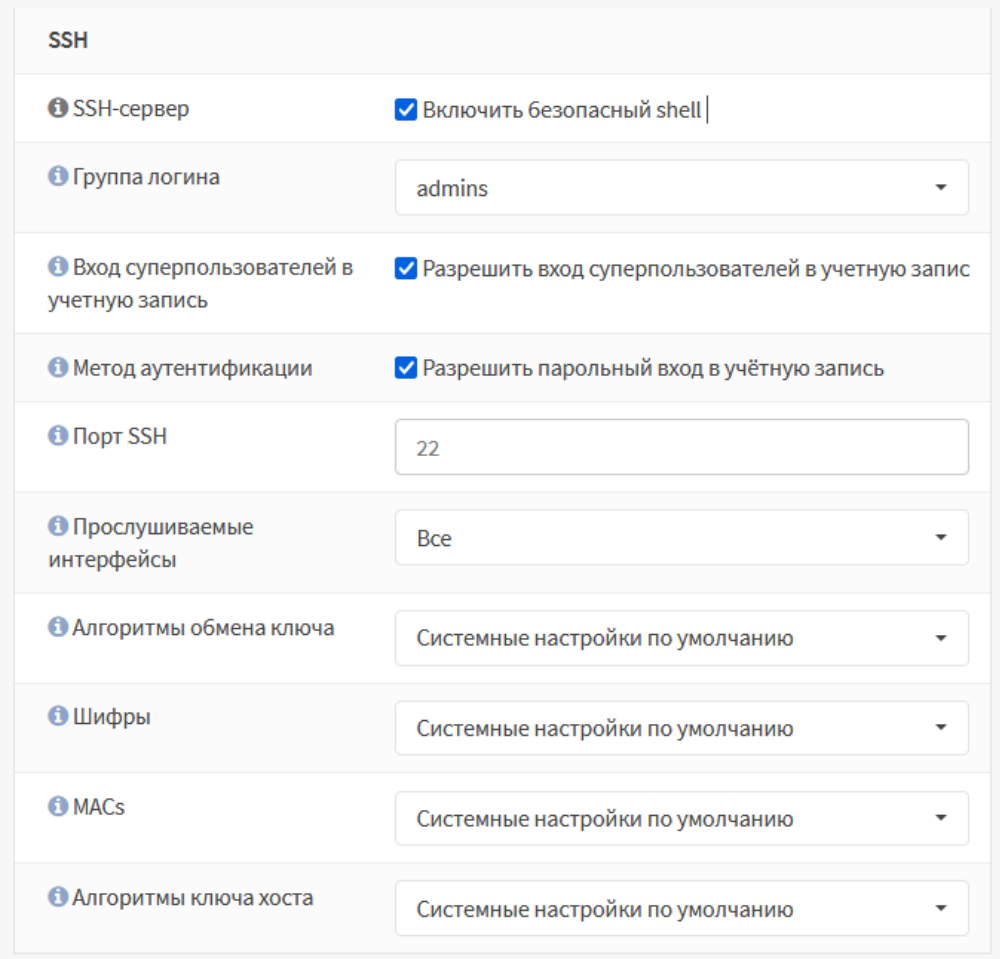

Рисунок – Настройка доступа по SSH

Для включения доступа по SSH необходимо выполнить следующие действия:

1. В блоке настроек **«SSH»** установить флажок для значения **«Включить безопасный shell»** параметра **«SSH-сервер»**.
2. В параметре **«Группа логина»** выбрать разрешённые группы пользователей для удалённого подключения по SSH.
3. Установить флажок для значения **«Разрешить вход суперпользователя в учетную запись»** параметра **«Вход суперпользователей (root) в учетную запись»** для снятия запрета входа пользователя «root» через SSH.

4. Установить флажок для значения **«Разрешить парольный вход в учетную запись»** параметра **«Метод аутентификации»** для разрешения аутентификации при подключении по SSH с помощью логина и пароля.
5. Указать новое значение параметра **«Порт SSH»** при необходимости смены используемого по умолчанию 22 порта.
6. Выбрать значения в параметре **«Прослушиваемые интерфейсы»** при необходимости ограничения интерфейсов для подключения по SSH. Рекомендуется оставить только внутренний интерфейс.
7. Нажать **кнопку «Сохранить»** в нижней части формы.

   Дополнительные параметры шифрования:

   - **«Алгоритмы обмена ключа»**;
   - **«Шифры»**;
   - **«MACs»**;
   - **«Алгоритмы ключа хоста»**;

   рекомендуется изменять только при необходимости, так как некорректные значения указанных параметров могут привести к уменьшению уровня безопасности SSH-соединения или потере доступности SSH-сервиса для легитимных пользователей.

2.3.6.2 Настройка доступа к локальному консольному интерфейсу

Настройки доступа к локальному консольному интерфейсу в подразделе настроек администрирования системы (**«Система» - «Настройки» - «Администрирование»**) (см. Рисунок – Настройка доступа к локальному консольному интерфейсу).

Доступ к локальному консольному интерфейсу **ARMA FW** включён по умолчанию.

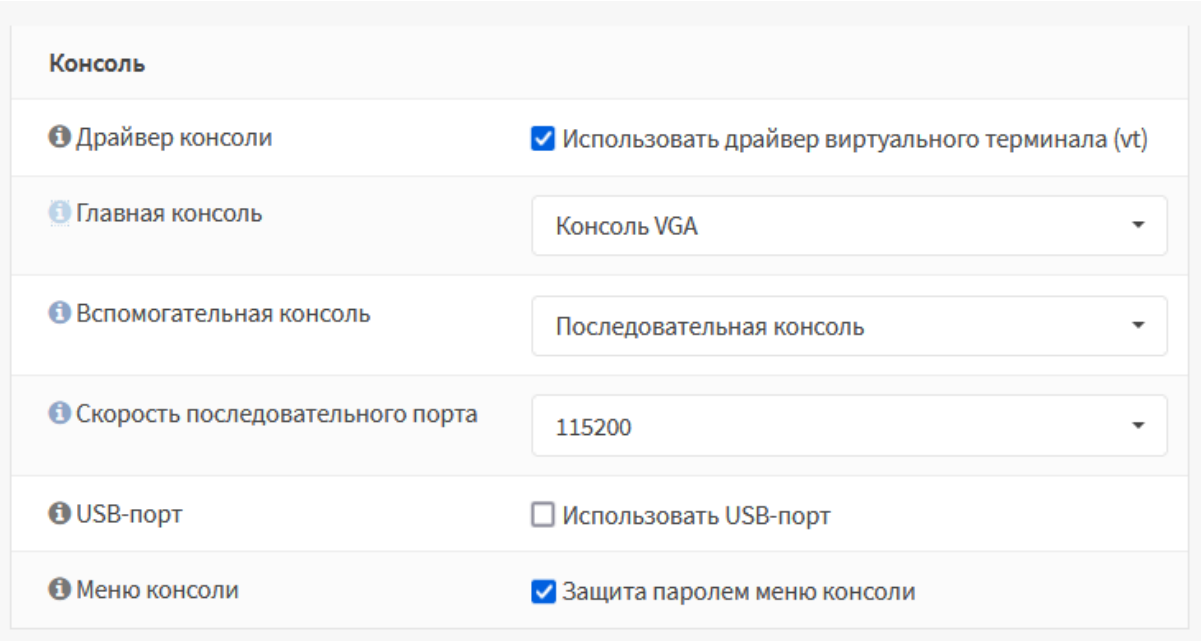

Рисунок – Настройка доступа к локальному консольному интерфейсу

В блоке настроек **«Консоль»** доступны следующие параметры:

- **«Драйвер консоли»** – флажок для значения **«Использовать драйвер виртуального терминала (vt)»** устанавливается для использования драйвера виртуального терминала;
- **«Главная консоль»** – выбирается основная консоль, показывающая вывод сценариев загрузки;
- **«Вспомогательная консоль»** – выбирается вспомогательная консоль, отображающая сообщения загрузчика ОС, сообщения консоли и меню консоли;
- **«Скорость последовательного порта»** – указывается значение пропускной способности последовательного порта консоли;
- **«USB-порт»** – флажок для значения **«Использовать USB-порт»** устанавливается для использования USB-порта;
- **«Меню консоли»** – флажок для значения **«Защита паролем меню консоли»** устанавливается для защиты паролем консольного меню.

После внесения необходимых изменений в конфигурацию для сохранения настроек необходимо нажать **кнопку «Сохранить»** в нижней части формы.

2.3.6.3 Настройка блокирования сеанса пользователя при неактивности

Для настройки блокирования сеанса доступа пользователя при неактивности необходимо выполнить следующие действия:

1. Перейти в подраздел настроек администрирования системы (**«Система» - «Настройки» - «Администрирование»**).

2. В параметре **«Тайм-аут сессии»** блока настроек **«Web-интерфейс»** указать количество минут, через которое сеанс доступа будет заблокирован при неактивности пользователя.
3. Нажать **кнопку «Сохранить»** в нижней части формы.

Примечание:

Не рекомендуется указывать в поле параметра **«Тайм-аут сессии»** значение более «15».

2.3.6.4 Настройка блокирования сессии после ввода некорректных учётных данных

В случае достижения определённого количества выполняемых подряд попыток авторизации с указанием некорректных учётных данных, **ARMA FW** автоматически выполняет временное блокирование сессии по IP-адресу пользователя или сервера SSH.

По умолчанию установлены следующие значения параметров временного блокирования сессии после ввода некорректных учётных данных:

- **«Максимальное количество попыток авторизации»** – «5»;
- **«Время блокировки сессии»** – «10», значение принимается в минутах;
- **«Максимальное количество попыток авторизации по SSH»** – «5».

Для настройки параметров временного блокирования сессии необходимо выполнить следующие действия:

1. Перейти в подраздел настроек администрирования системы (**«Система» - «Настройки» - «Администрирование»**).
2. В параметре **«Максимальное количество попыток авторизации»** блока настроек **«Web-интерфейс»** ввести количество возможных подряд попыток авторизации в веб-интерфейсе с указанием некорректных учётных данных, при достижении которого сессия будет автоматически заблокирована.
3. В параметре **«Время блокировки сессии»** блока настроек **«Web-интерфейс»** ввести длительность блокирования сессии в минутах. Допустимо указание значения не менее «5».
4. В параметре **«Максимальное количество попыток авторизации по SSH»** блока настроек **«SSH»** ввести количество возможных подряд попыток авторизации по SSH с указанием некорректных учётных данных, при достижении которого сессия будет автоматически заблокирована.
5. Нажать **кнопку «Сохранить»** в нижней части формы.

2.4 Проверка состояния служб ARMA FW

Для проверки состояния системных служб **ARMA FW** необходимо перейти в подраздел настроенных служб (**«Система» - «Диагностика» - Службы»**) (см. Рисунок – Проверка работоспособности служб ARMA FW).

Список системных служб может меняться в зависимости от настроек **ARMA FW**, список системных служб по умолчанию представлен в таблице (см. Таблица «Системные службы по умолчанию»).

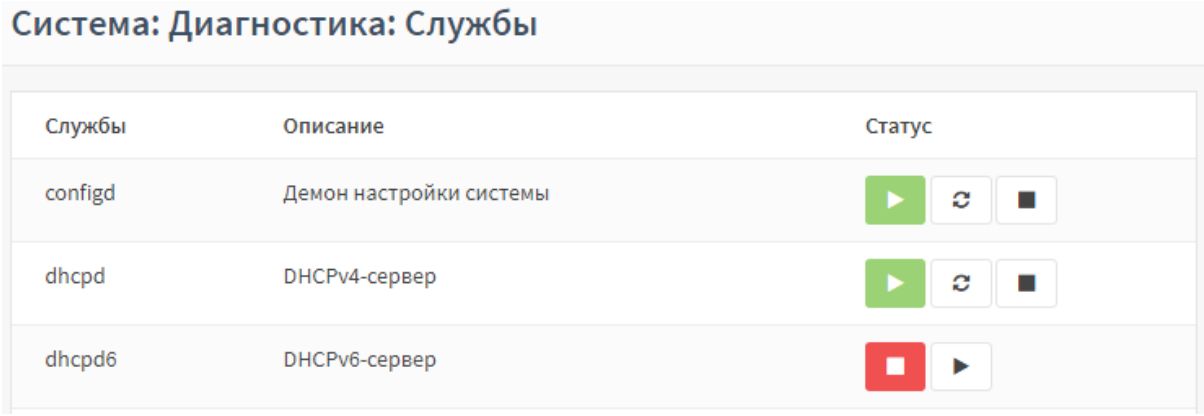

Рисунок – Проверка работоспособности служб ARMA FW

В столбце **«Статус»** для каждой службы возможны два состояния:

- **«Запущена»** – отображается значком « »;
- **«Остановлена»** – отображается значком « ».

Таблица «Системные службы по умолчанию»

Служба	Описание
configd	Демон настройки системы
dhcpd	DHCPv4-сервер
dhcpd6	DHCPv6-сервер
firewall	Межсетевой экран
license_client	Клиент лицензии
login	Пользователи и группы
ntpd	Демон сетевого времени
openvpn	OpenVPN server
pf	Фильтр пакетов
radvd	Демон объявления маршрутизатора
syslog-ng	Удаленный Syslog

Служба	Описание
syslogd	Системный журнал
unbound	Кэширующий DNS-сервер
webgui	Веб-интерфейс

3 ВАРИАНТЫ РАЗВЁРТЫВАНИЯ

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

- режим маршрутизации;
- режим прозрачного моста;
- режим «sniffing mode»;
- режим отказоустойчивого кластера.

Каждый вариант отличается настройкой сетевых интерфейсов.

3.1 Маршрутизация

В режиме маршрутизации **ARMA FW** работает как МЭ с функцией обнаружения и предотвращения вторжений, обеспечивая защиту передачи информации на уровне L3 с возможностью маршрутизации. Режим маршрутизации может использоваться при объединении сетей, имеющих разное адресное пространство.

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

Типы поддерживаемой маршрутизации описаны в разделе Маршрутизация.

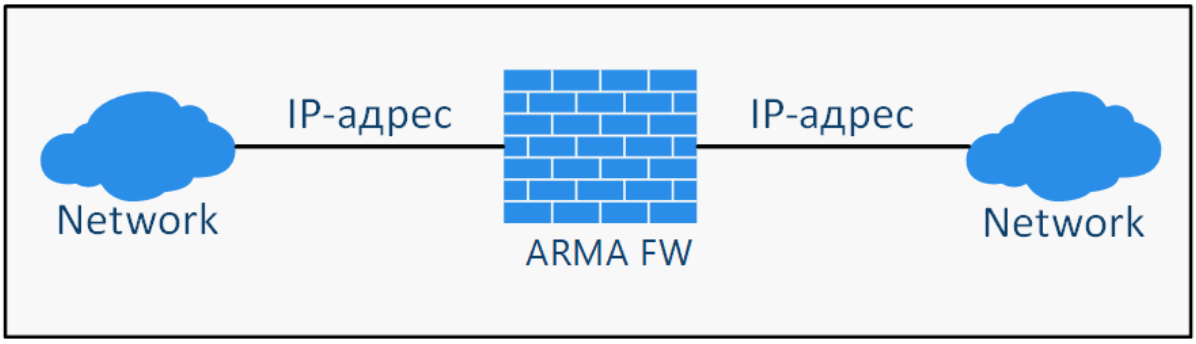

Рисунок – Режим маршрутизации

3.2 Прозрачный мост

В режиме прозрачного моста **ARMA FW** работает как система обнаружения и предотвращения вторжений в прозрачном режиме с возможностью блокировки вредоносных пакетов. Интерфейсы при этом соединены в сетевой мост.

Данный режим предназначен для фильтрации трафика между сетями одного адресного пространства. При обнаружении подозрительного или вредоносного трафика информация отправляется в веб-интерфейс для последующего оповещения пользователя и, при необходимости, блокируется.

Общая схема подключения **ARMA FW** в режиме прозрачного моста представлена на рисунке (см. Рисунок – Режим прозрачного моста).

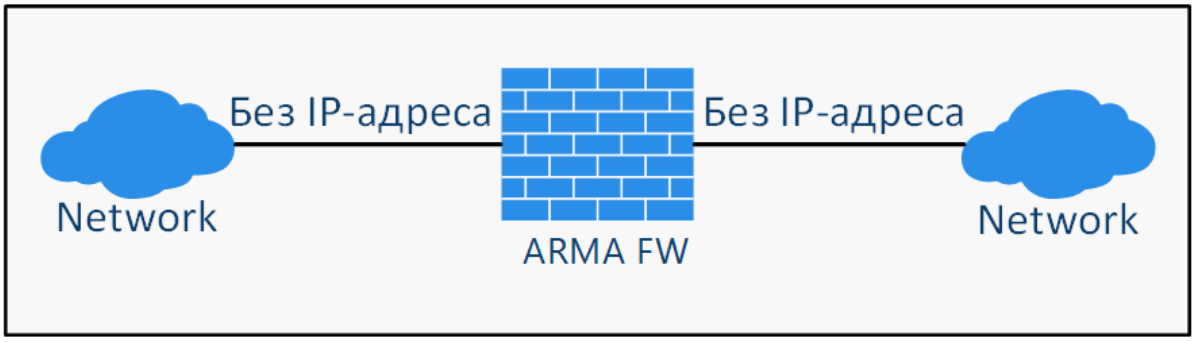

Рисунок – Режим прозрачного моста

Подробная информация о настройке сетевых мостов описана в разделе **«Сетевой мост»** Руководства пользователя **ARMA FW**.

3.3 Sniffing mode

В режиме «sniffing mode» **ARMA FW** работает в качестве системы обнаружения вторжений, анализирующей копию сетевого трафика, снятого со SPAN порта. В режиме возможен только мониторинг трафика.

В режиме «sniffing mode» необходимо настроить на коммутаторе перенаправление на **ARMA FW** всего сетевого трафика с помощью технологии SPAN или аналогичной. **ARMA FW** проводит глубокий анализ пакетов – «DPI» и, в случае необходимости, уведомляет пользователя о событиях ИБ.

Общая схема подключения **ARMA FW** в режиме «sniffing mode» представлена на рисунке (см. Рисунок – Режим «sniffing mode»).

Подробная информация о настройке SPAN описана в разделе **«Настройка SPAN»** Руководства пользователя **ARMA FW**.

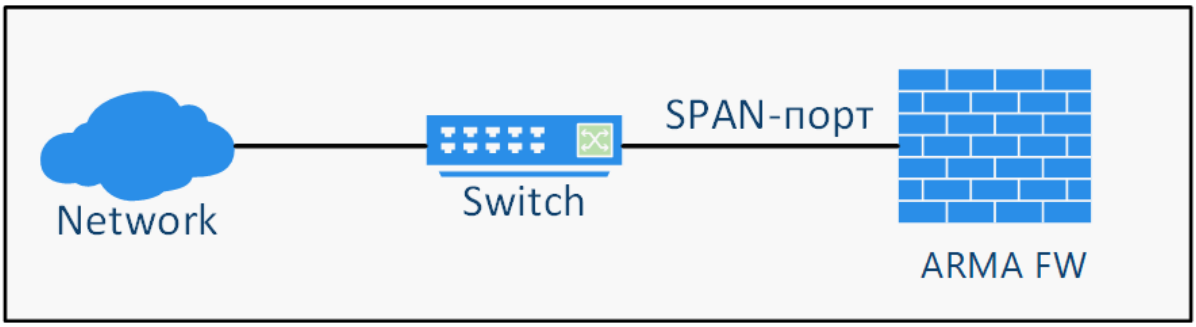

Рисунок – Режим «sniffing mode»

3.4 Отказоустойчивый кластер

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

В случае объединения нескольких **ARMA FW** в каждый момент времени только одно устройство **ARMA FW** в кластере обрабатывает весь трафик, такое устройство считается ведущим. Подчинённые, резервные устройства постоянно

синхронизируют своё состояние с ведущим устройством. В случае выхода из строя ведущего устройства его подменяет одно из резервных устройств, которое само становится ведущим и начинает обрабатывать трафик. В случае если «старое» ведущее устройство вновь переходит в рабочее состояние, то текущее ведущее устройство возвращается в статус подчинённого резервного устройства.

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

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

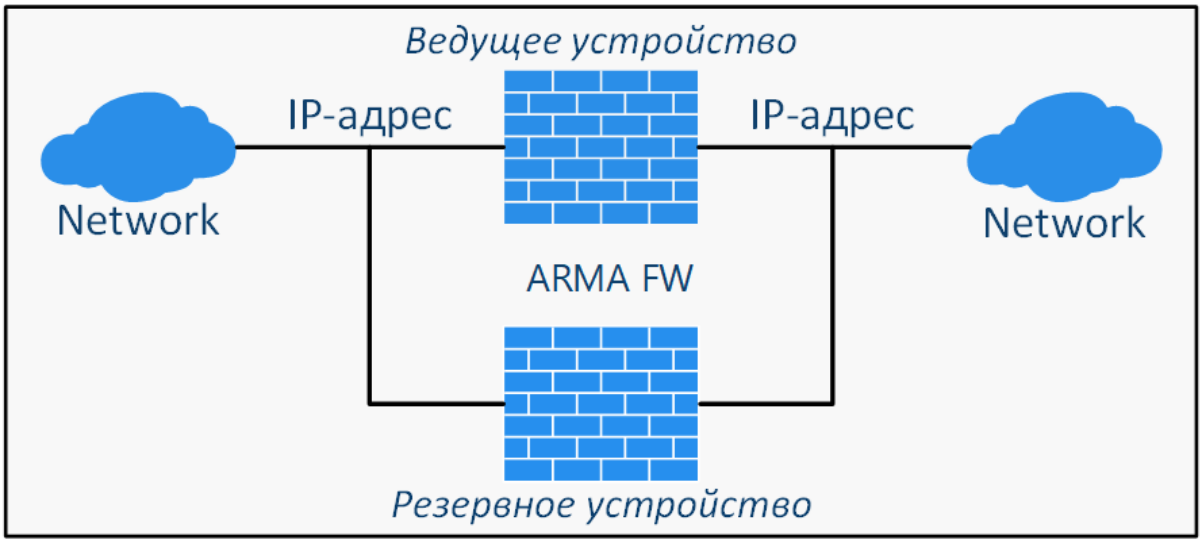

Рисунок – Режим отказоустойчивого кластера

4 КОНТРОЛЬ УПРАВЛЕНИЯ ДОСТУПОМ

4.1 Аутентификация

Аутентификация – это процесс проверки подлинности введённых пользователем имени и пароля. В **ARMA FW** возможна аутентификация с использованием локальной или внешней БД пользователей. В качестве внешней БД служат различные внешние серверы авторизации. **ARMA FW** поддерживает работу со следующими внешними серверами:

- **«LDAP»** – OpenLDAP, MS Active Directory, Novell eDirectory;
- **«Radius»**.

По умолчанию в **ARMA FW** аутентификация осуществляется с использованием локальной БД пользователей. К дополнительным мерам защиты при аутентификации с использованием внутреннего сервера относится ваучер-сервер. К дополнительным мерам защиты при аутентификации с использованием внешних серверов относится сервис двухфакторной аутентификации.

Для авторизации и предоставления соответствующих привилегий пользовательской УЗ, настроенной с помощью внешнего сервера, необходимо импортировать пользовательскую УЗ в локальную БД пользователей **ARMA FW**.

4.1.1 Локальная база данных пользователей

Для хранения УЗ пользователей по умолчанию используется локальная БД, например, запись суперпользователя по умолчанию – «root».

Для настройки параметров локальной БД необходимо перейти в раздел настроек серверов аутентификации (**«Система» - «Доступ» - «Серверы»**) и в строке **«Локальная база данных»** нажать **кнопку** «  » для перехода в режим редактирования.

В режиме редактирования возможно задать настройки пароля для всех пользователей локальной базы пользователей, а именно – в поле **«Длина»** задать необходимую длину пароля, в графе **«Сложность»** установить флажок, если необходимо включить дополнительные обязательные требования к сложности пароля: пароль должен содержать цифры, прописные буквы, строчные буквы, специальные символы.

Для сохранения настроек необходимо нажать **кнопку «Сохранить»** внизу страницы (см. Рисунок – Локальная БД пользователей, редактирование).

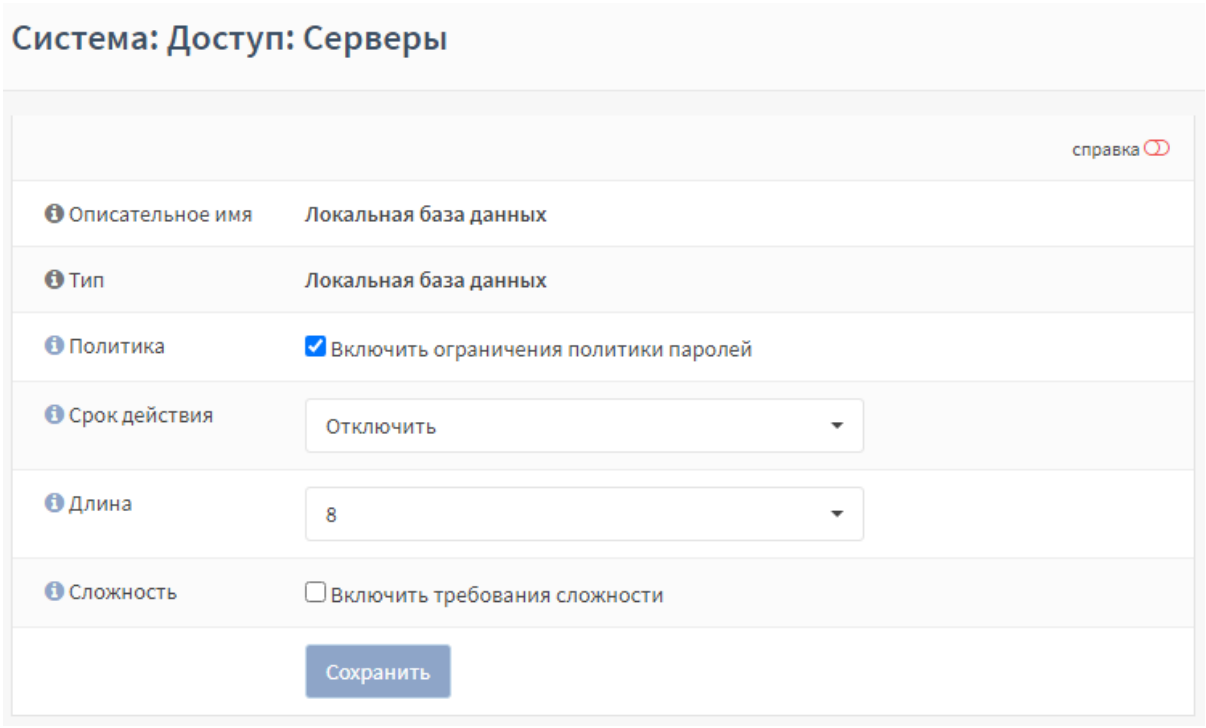

Рисунок – Локальная БД пользователей, редактирование

4.1.2 Ваучер-сервер

Ваучер-сервер используется для обеспечения аутентификации на портале авторизации в **ARMA FW**.

Ваучер – это запись с логином и паролем, которую **ARMA FW** генерирует по запросу. Ваучеры имеют настраиваемый срок действия, по истечении которого пользователю необходимо получить новый ваучер.

Конфигурация ваучер-сервера производится в подразделе настроек серверов аутентификации (**«Система» - «Доступ» - «Серверы»**).

Подробная настройка ваучер-сервера описана в разделе **«Ваучер-сервер»** Руководства пользователя **ARMA FW**.

4.1.3 LDAP

LDAP – протокол прикладного уровня для доступа к службе каталогов, использующий TCP/IP и позволяющий производить операции аутентификации, поиска и сравнения, а также операции добавления, изменения или удаления записей. При использовании учётных записей LDAP-сервера для доступа к веб-интерфейсу **ARMA FW** необходимо определить привилегии УЗ, путем импорта пользовательских УЗ из LDAP-сервера.

Конфигурация внешнего LDAP-сервера производится в подразделе настроек серверов аутентификации (**«Система» - «Доступ» - «Серверы»**).

Подробная настройка внешнего LDAP-сервера описана в разделе **«LDAP»** Руководства пользователя **ARMA FW**.

4.1.4 Radius

Radius – сетевой протокол, предназначенный для обеспечения централизованной аутентификации, авторизации и учёта пользователей, подключающихся к различным сетевым службам.

ARMA FW поддерживает использование внешнего Radius-сервера для аутентификации пользователей в сервисах VPN и портал авторизации.

Конфигурация внешнего Radius-сервера производится в подразделе настроек серверов аутентификации (**«Система» - «Доступ» - «Серверы»**).

Подробная настройка внешнего Radius-сервера описана в разделе **«Radius»** Руководства пользователя **ARMA FW**.

4.1.5 Двухфакторная аутентификация

Двухфакторная аутентификация в **ARMA FW** – это аутентификация, в процессе которой помимо постоянного пароля от локальной УЗ, необходимо указать временный одноразовый пароль – **«Time-based One-Time Password»**.

ARMA FW поддерживает RFC 6238. Для поддержки двухфакторной аутентификации используются мобильные приложения, совместимые с RFC 6238.

Подробная настройка двухфакторной аутентификации описана в разделе **«Двухфакторная аутентификация»** Руководства пользователя **ARMA FW**.

4.2 Пользовательские учетные записи, группы и привилегии

Для пользовательской УЗ или определённой группы пользователей возможно определить набор привилегий, используя локальную базу пользователей, в том числе в сочетании с внешним сервером проверки подлинности.

Назначить привилегии пользовательской УЗ возможно при создании или редактировании пользовательской УЗ (см. Добавление пользовательских учетных записей и их привилегий).

Назначить привилегии группе пользователей возможно при создании или редактировании группы пользователей (см. Создание группы и добавление им привилегий).

Системные УЗ, используемые в различных целях на уровне ОС, создаются по умолчанию при установке **ARMA FW**. Системные УЗ не отображаются в настройках **ARMA FW** и используются только для обеспечения системных требований, их права не могут быть присвоены пользовательским УЗ, часть прав доступа является системной, часть присвоена администратору.

Список всех системных УЗ приведён в разделе Приложение А настоящего руководства.

4.2.1 Добавление пользовательских учетных записей и их привилегий

Для создания пользовательской УЗ необходимо выполнить следующие действия:

1. Перейти в подраздел управления пользователями (**«Система» - «Доступ» - «Пользователи»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме заполнить обязательные параметры **«Имя пользователя»** и **«Пароль»** (см. Рисунок – Создание пользовательской УЗ) и нажать **кнопку «Сохранить»**.

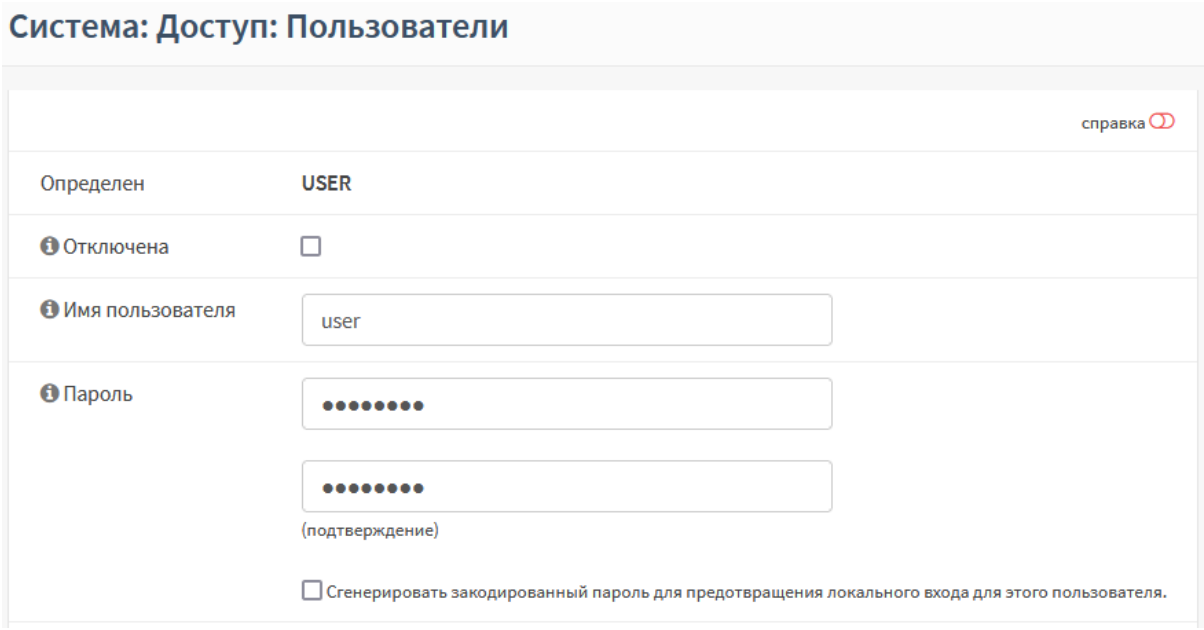

Рисунок – Создание пользовательской УЗ

Описание дополнительных настроек при создании пользовательской УЗ описаны в разделе **«Дополнительные параметры УЗ»** Руководства пользователя **ARMA FW**.

Назначение привилегий пользовательской УЗ возможно двумя способами:

- добавление пользователя в определённую группу с уже заданными привилегиями;
- выбор привилегий из списка – установив флажок напротив соответствующей привилегии в блоке настроек **«Системные привилегии»** (см. Рисунок – Установка системных привилегий).

Для удобства в блоке настроек **«Системные привилегии»** существует поле фильтра и функции множественного выбора:

- **«Веб-интерфейс: Все страницы»**;
- **«Функция: Очистить все журналы»**;
- **«Выбрать все (видимые)»**;
- **«Отменить выбор (видимые)»**.

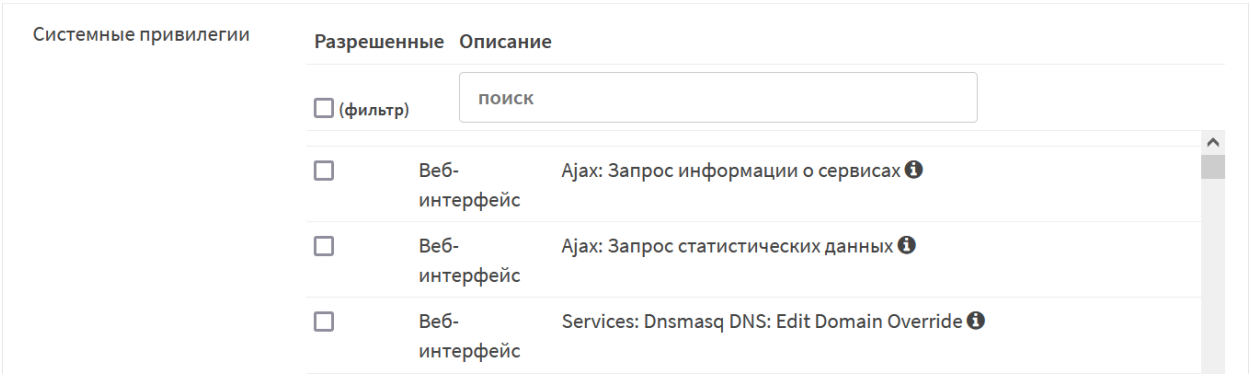

Рисунок – Установка системных привилегий

В случае необходимости назначения УЗ пользователя возможности добавления или редактирования других УЗ, требуется в блоке **«Системные привилегии»** формы редактирования УЗ пользователя установить флажок для параметра **«Система Система: Изменить настройки»**.

4.2.2 Создание группы и добавление им привилегий

Для удобства и простоты управления правами доступа существует возможность создания и редактирования групп. Каждую УЗ возможно включить в состав нескольких групп, в таком случае УЗ будет обладать совокупностью привилегий каждой из групп.

Для создания группы пользователей необходимо выполнить следующие действия:

1. Перейти в подраздел управления группами пользователей (**«Система» - «Доступ» - «Группы»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме заполнить обязательный параметр **«Имя группы»** (см. Рисунок – Создание группы пользователей) и нажать **кнопку «Сохранить»**.

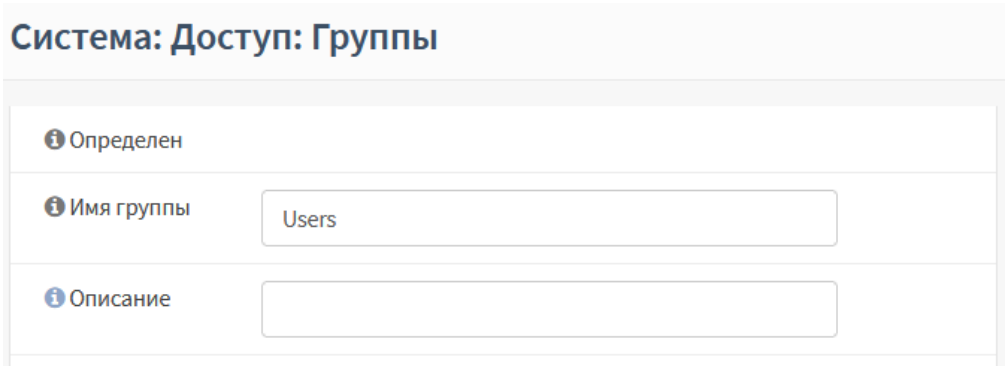

Рисунок – Создание группы пользователей

Для добавления пользователей в создаваемую группу необходимо в блоке настроек **«Участники группы»** перенести имена пользователей из левой части в правую, нажав **кнопку** « → » (см. Рисунок – Добавление участников в группу).

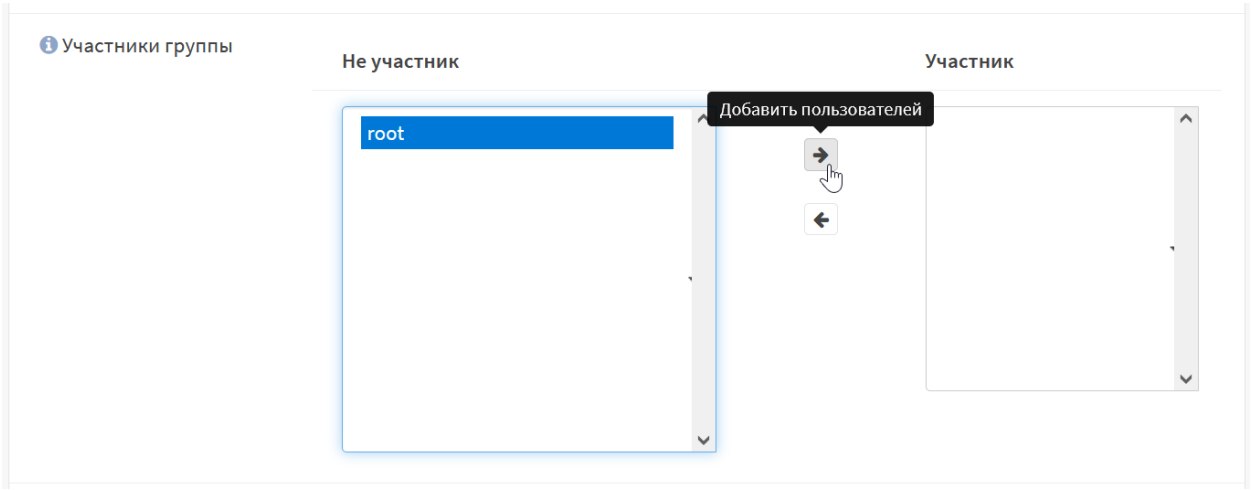

Рисунок – Добавление участников в группу

Для назначения привилегий группе пользователей необходимо выбрать привилегии из списка, установив флажок напротив соответствующей привилегии в блоке настроек **«Системные привилегии»** аналогично назначению привилегий пользовательской УЗ (см. Добавление пользовательских учетных записей и их привилегий).

4.3 Сброс пароля учетной записи суперпользователя

Для сброса пароля УЗ суперпользователя необходимо выполнить следующие действия:

1. Выполнить вход в однопользовательском режиме – при загрузке **ARMA FW** выбрать вариант **«2) Boot Single User»**, нажав **клавишу «2»** (см. Рисунок – Загрузка ARMA FW).

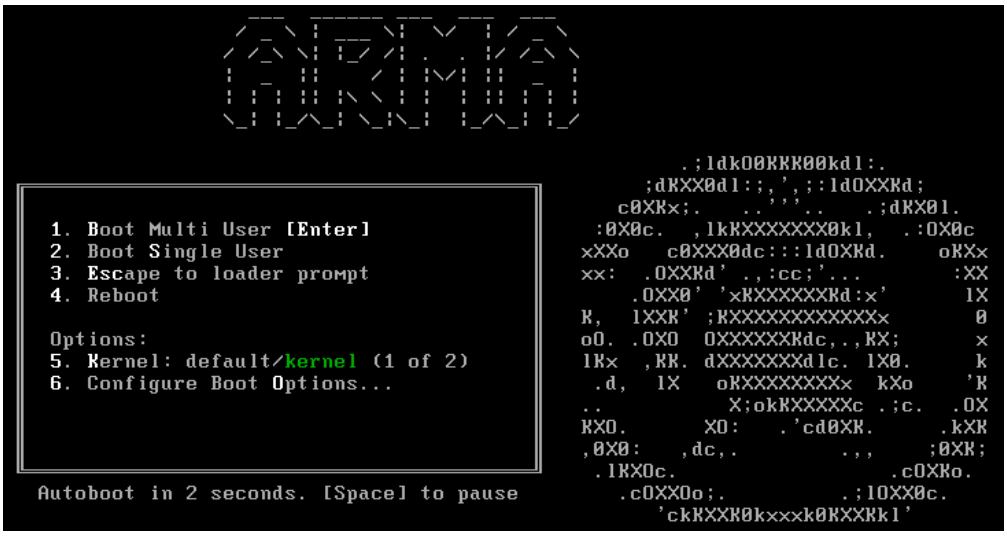

Рисунок – Загрузка ARMA FW

2. Ввести **«/bin/sh»** и нажать **клавишу «ENTER»** для указания пути расположения исполняемого файла командной оболочки, которую необходимо запустить.

3. В запущенной командной оболочке, выполнить команду на перемонтирование корневой файловой системы:
    - ввести **«mount -uw /»** и нажать **клавишу «ENTER»**;
    - ввести **«mount -a»** нажать **клавишу «ENTER»**.

    Файловая система будет перемонтирована с возможностью чтения/записи.
4. Ввести **«opnsense-shell»** и нажать **клавишу «ENTER»** для запуска консольного меню.
5. Выбрать пункт меню **«3) Reset the root password»**, нажав **клавишу «3»**, а затем **клавишу «ENTER»**.
6. Ввести **«y»** и нажать **клавишу «ENTER»** на запрос **«Do you want to proceed? [y/n]»**.
7. Ввести новый пароль на запрос **«Type a new password»** и нажать **клавишу «ENTER»**.
8. Повторить ввод нового пароля на запрос **«Confirm new password»** и нажать **клавишу «ENTER»**.
9. Выбрать пункт меню **«6) Reboot system»**, нажав **клавишу «6»**, а затем **клавишу «ENTER»** для перезагрузки **ARMA FW**.

5 СЕРВИСЫ

5.1 Маршрутизация

ARMA FW поддерживает статическую и динамическую маршрутизацию.

5.1.1 Статическая маршрутизация

Статическая маршрутизация – это запись маршрутизации, настроенная вручную, без применения протоколов маршрутизации. Статические маршруты используются в случае, когда узлы или сети доступны через маршрутизатор, отличный от шлюза по умолчанию.

Подробная настройка статической маршрутизации описана в разделе **«Статическая маршрутизация»** Руководства пользователя **ARMA FW**.

5.1.2 Динамическая маршрутизация

Динамическая маршрутизация – это вид маршрутизации, в котором отличительной особенностью является автоматический выбор оптимального маршрута при прохождении трафика между поддерживающими динамическую маршрутизацию сетевыми устройствами.

ARMA FW поддерживает динамическую маршрутизацию по протоколам RIP v.1, 2, BGP и OSPF.

Подробная настройка динамической маршрутизации описана в разделе **«Динамическая маршрутизация»** Руководства пользователя **ARMA FW**.

5.2 Прокси

Прокси-сервер обеспечивает контролируемый доступ хостов локальной сети в сеть Интернет, а также защиту локальной сети от внешнего доступа.

Прокси-сервер поддерживает ряд методов аутентификации:

- без аутентификации;
- аутентификация по локальной базе пользователей;
- аутентификация по LDAP;
- аутентификация по RADIUS;
- двухфакторная аутентификация.

Подробная настройка прокси-сервера описана в разделе **«Прокси»** Руководства пользователя **ARMA FW**.

5.3 DHCP

DHCP-сервер используется для автоматического предоставления клиентам IP-адреса и других параметров, необходимых для работы в сети TCP/IP. Настройки DHCP-сервера доступны для протоколов IPv4 и IPv6.

Подробная настройка DHCP-сервера описана в разделе **«DHCP-сервер»** Руководства пользователя **ARMA FW**.

5.4 Сервисы мониторинга

5.4.1 Syslog

Syslog – это стандарт отправки и регистрации сообщений о происходящих в системе событиях, используемый для удобства администрирования и обеспечения ИБ. **ARMA FW** формирует текстовые сообщения о происходящих в нём событиях, инцидентах безопасности с точной меткой времени и идентификационными данными и передаёт их на обработку серверу Syslog. Формат событий МЭ – IPFW, формат событий СОВ – Suricata.

Подробная настройка Syslog описана в разделе **«Сервис syslog»** Руководства пользователя **ARMA FW**.

5.4.2 SNMP

SNMP – простой протокол сетевого управления, позволяющий осуществлять удалённый мониторинг некоторых системных параметров **ARMA FW** с помощью различных систем мониторинга.

В зависимости от выбранных опций мониторинг может выполняться для:

- общей системной информации – использование ЦП, памяти и диска;
- сведений об устройстве, сетевого трафика;
- сведений об интерфейсах, активных процессов и установленного ПО.

За реализацию SNMP в **ARMA FW** отвечает сервис «snmpd». **ARMA FW** поддерживает следующие версии SNMP:

- SNMP v.1, 2;
- SNMP v.3.

Подробная настройка мониторинга по SNMP описана в разделе **«SNMP»** Руководства пользователя **ARMA FW**.

6 ОПИСАНИЕ ЛОКАЛЬНОГО КОНСОЛЬНОГО ИНТЕРФЕЙСА

Меню локального консольного интерфейса отображает варианты действия, представленные в таблице (см. Таблица «Действия консольного меню»). Данное меню доступно после успешной аутентификации.

Примечание:

При бездействии пользователя в течение 5 минут в локальном консольном интерфейсе **ARMA FW**, автоматически будет произведён выход из меню и возврат к форме входа. При бездействии пользователя в течение 10 минут в интерфейсе командной строки **ARMA FW**, автоматически будет произведён переход в меню локального консольного интерфейса.

Таблица «Действия консольного меню»

Действие	Действие
0 Logout	7 Ping host
1 Assign interfaces	8 Shell
2 Set interface(s) IP address	9 pfTop
3 Reset the root password	10 Firewall log
4 Reset to factory defaults	11 Reload all services
5 Power off system	12 Restore a backup
6 Reboot system	13 Activate license

Управление в локальном консольном интерфейсе происходит только с использованием клавиатуры. Выбор пунктов меню осуществляется вводом порядкового номера пункта, а подтверждение выбора нажатием **клавиши «ENTER»**.

6.1 Выход из консольного интерфейса

Для выхода из меню и возвращения к форме входа необходимо выбрать пункт меню **«0) Logout»**.

6.2 Назначение сетевых интерфейсов и настройка VLAN

Для ручного назначения соответствия интерфейсов необходимо выбрать пункт меню **«1) Assign interfaces»**. В результате выбора будут отображены доступные сетевые порты и будет выведен запрос на настройку интерфейсов.

Порядок назначения интерфейсов описан в разделе Назначение сетевых интерфейсов настоящего руководства.

В случае необходимости указания параметров VLAN для какого-либо сетевого интерфейса необходимо выполнить следующие действия:

1. Ввести **«y»** и нажать **клавишу «ENTER»** на запрос **«Do you want to Configure VLANs now?»**. В результате будут отображены доступные сетевые интерфейсы и будет выведен запрос на выбор интерфейса для настройки.
2. Ввести номер интерфейса, на котором требуется настроить VLAN, и нажать **клавишу «ENTER»** на запрос **«Enter the parent interface name for the new VLAN (or nothing if finished):»**.
3. Указать тег VLAN, при наличии идентификатора принадлежности трафика к VLAN интерфейсу, и нажать **клавишу «ENTER»** на запрос **«Enter the VLAN tag (1-4094):»**.
4. В результате указанному сетевому интерфейсу будет присвоен указанный идентификатор VLAN (см. Рисунок – Настройка VLAN) и повторно будет выведен запрос на выбор интерфейса для настройки. Настройка параметров VLAN для других интерфейсов производится аналогично пунктам 2 и 3.
5. После завершения настройки параметров VLAN для всех необходимых сетевых интерфейсов нажать **клавишу «ENTER»** без ввода имени интерфейса. В результате произойдёт переход к назначению сетевых интерфейсов.

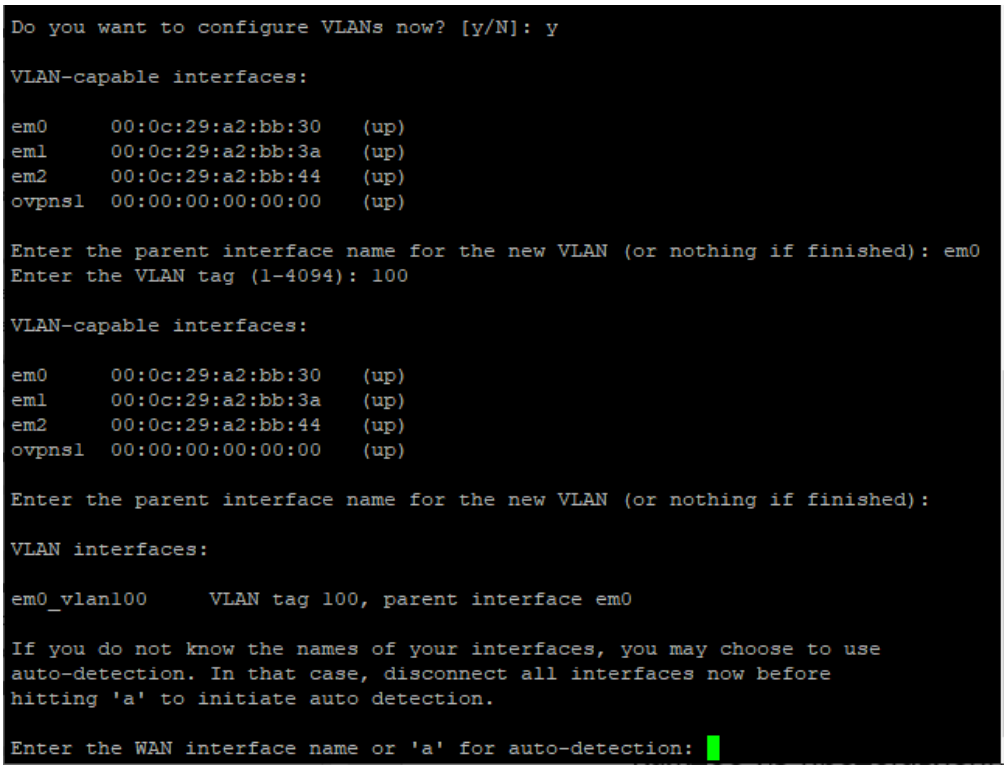

Рисунок – Настройка VLAN

6.3 Настройка IPv4-адреса

Для настройки IPv4-адресов на назначенных интерфейсах необходимо выбрать пункт меню **«2) Set interface(s) IP address»**. В результате выбора будут отображены доступные интерфейсы и будет выведен запрос на настройку интерфейсов.

Необходимо ввести номер интерфейса и нажать **клавишу «ENTER»** для настройки IPv4. Настройка IPv4-адреса возможна двумя способами:

- автоматическая настройка посредством DHCP-сервера;
- ручная настройка.

Примечание:

Сетевые интерфейсы, настроенные посредством DHCP-сервера, будут отображены не во всех функциях **ARMA FW**, например, будут отсутствовать в списке доступных интерфейсов при настройке функции прокси-сервер.

Для автоматической настройки посредством DHCP-сервера необходимо ввести **«y»** и нажать **клавишу «ENTER»** на запрос **«Configure IPv4 address [Имя интерфейса] via DHCP? [y/N]»**. Здесь и далее [Имя интерфейса] – имя выбранного интерфейса.

Для ручной настройки IPv4-адреса необходимо выполнить следующие действия:

1. Ввести **«n»** и нажать **клавишу «ENTER»** на запрос **«Configure IPv4 address [Имя интерфейса] via DHCP? [y/N]»**.
2. Ввести IPv4-адрес интерфейса и нажать **клавишу «ENTER»** на запрос **«Enter the new [Имя интерфейса] IPv4 address. Press «ENTER» for none:»**.
3. Ввести маску подсети в формате CIDR и нажать **клавишу «ENTER»** на запрос **«Enter the new [Имя интерфейса] IPv4 subnet bit count (1 to 32):»**.
4. Ввести IPv4-адрес шлюза и нажать **клавишу «ENTER»** на запрос **«For a WAN, enter the new [Имя интерфейса] IPv4 upsteream gateway address»** в случае настройки WAN-интерфейса, в противном случае пропустить настройку шлюза, нажав **клавишу «ENTER»**.

После окончания настройки IPv4 будет предложено настроить IPv6 (см. Настройка IPv6-адреса), в случае отсутствия необходимости настройки IPv6 выполнить следующие действия:

1. Ввести **«n»** и нажать **клавишу «ENTER»** на запросы:
   - **«Configure IPv6 address [Имя интерфейса] interface via WAN tracking? [Y/n]»**;
   - **«Configure IPv6 address [Имя интерфейса] interface via DHCP6? [y/N]»**;

2. Нажать **клавишу «ENTER»** на запрос **«Enter the new [Имя интерфейса] IPv6 address. Press <ENTER> for none:»**.

Далее будет предложена настройка DHCP-сервера на выбранном интерфейсе. При отсутствии необходимости настройки ввести **«n»** и нажать **клавишу «ENTER»** на запрос **«Do you want to enable the DHCP server on [Имя интерфейса]? [y/N]»**, в противном случае ввести **«y»** и нажать **клавишу «ENTER»** и выполнить настройку DHCP-сервера.

Для настройки DHCP-сервера на выбранном интерфейсе необходимо выполнить следующие действия:

1. Ввести начальный IPv4-адрес диапазона выдаваемых адресов DHCP-сервером и нажать **клавишу «ENTER»** на запрос **«Enter the start address of the IPv4 client address range:»**.
2. Ввести конечный IPv4-адрес диапазона выдаваемых адресов DHCP-сервером и нажать **клавишу «ENTER»** на запрос **«Enter the and address of the IPv4 client address range:»**.

6.4 Настройка IPv6-адреса

Для настройки IPv6-адресов на назначенных интерфейсах необходимо выбрать пункт меню **«2) Set interface(s) IP address»** и либо произвести настройку IPv4 (см. Настройка IPv4-адреса), либо пропустить настройку IPv4, нажав **клавишу «ENTER»** на запрос **«Enter the new [Имя интерфейса] IPv4 address. Press «ENTER» for none:»**.

Настройка IPv6-адреса возможна тремя способами:

- автоматическая настройка посредством отслеживания состояния WAN;
- автоматическая настройка посредством DHCP-сервера;
- ручная настройка.

Для автоматической настройки посредством отслеживания состояния WAN необходимо ввести **«y»** и нажать **клавишу «ENTER»** на запрос **«Configure IPv6 address OPT1 [Имя интерфейса] interface via WAN tracking? [Y/n]»**.

Для автоматической настройки посредством DHCP-сервера необходимо выполнить следующие действия:

1. Ввести **«n»** и нажать **клавишу «ENTER»** на запрос **«Configure IPv6 address OPT1 [Имя интерфейса] interface via WAN tracking? [Y/n]»**.
2. Ввести **«y»** и нажать **клавишу «ENTER»** на запрос **Configure IPv6 address [Имя интерфейса] interface via DHCP6? [y/N]»**.

Для ручной настройки IPv6-адреса необходимо выполнить следующие действия:

1. Ввести **«n»** и нажать **клавишу «ENTER»** на запрос **«Configure IPv6 address OPT1 [Имя интерфейса] interface via WAN tracking? [Y/n]»**.
2. Ввести **«n»** и нажать **клавишу «ENTER»** на запрос **Configure IPv6 address [Имя интерфейса] interface via DHCP6? [y/N]»**.
3. Ввести IPv6-адрес интерфейса и нажать **клавишу «ENTER»** на запрос **«Configure IPv6 address [Имя интерфейса] via DHCPv6? [y/N]»**.
4. Ввести маску подсети в формате CIDR и нажать **клавишу «ENTER»** на запрос **«Enter the new OPT1 [Имя интерфейса] IPv6 subnet bit count (1 to 128):»**.
5. Ввести IPv6-адрес шлюза и нажать **клавишу «ENTER»** на запрос **«For a WAN, enter the new [Имя интерфейса] IPv6 upsteream gateway address»** в случае настройки WAN-интерфейса, в противном случае пропустить настройку шлюза, нажав **клавишу «ENTER»**.

После настройки рекомендуется перезагрузить **ARMA FW** (см. Перезагрузка ARMA FW).

6.5 Изменение пароля учетной записи Root

Для изменения пароля необходимо выбрать пункт меню **«3) Reset the root password»** и выполнить следующие действия:

1. Ввести **«y»** на запрос **«Do you want to proceed? [y/N]»** и нажать **клавишу «ENTER»**.
2. Ввести новый пароль на запрос **«Type a new password»** и нажать **клавишу «ENTER»**.
3. Повторить ввод нового пароля на запрос **«Confirm new password»** и нажать **клавишу «ENTER»**.

6.6 Восстановление настроек по умолчанию

Для восстановления настроек **ARMA FW** по умолчанию необходимо выбрать пункт меню **«4) Reset to factory defaults»**, ввести **«y»** после запроса **«Do you want to proceed? [y/N]»** и нажать **клавишу «ENTER»**.

6.7 Выключение ARMA FW

Для выключения **ARMA FW** необходимо выбрать пункт меню **«5) Power off system»**, ввести **«y»** после запроса **«The system will halt and power off. Do you want to proceed? [y/N]»** и нажать **клавишу «ENTER»**.

6.8 Перезагрузка ARMA FW

Для перезагрузки **ARMA FW** необходимо выбрать пункт меню **«6) Reboot system»**, ввести **«y»** после вопроса **«The system will reboot. Do you want to proceed? [y/N]»** и нажать **клавишу «ENTER»**.

6.9 Проверка доступности хоста

Для выполнения проверки доступности хоста с помощью команды «ping» необходимо выбрать пункт меню **«7) Ping host»**, ввести IP-адрес хоста или доменное имя хоста на запрос **«Enter a host name or IP address:»** и нажать **клавишу «ENTER»**.

6.10 Доступ к командной строке

Для перехода в интерфейс командной строки «command line interface – CLI» необходимо выбрать пункт меню **«8) Shell»**. Для выхода необходимо нажать комбинацию **клавиш «Ctrl»** + **«D»**.

6.11 Просмотр состояния пакетного фильтра

Для просмотра активного состояния пакетного фильтра «PF» и его правил в режиме реального времени в виде подробной таблицы необходимо выбрать пункт меню **«9) pfTop»**. Для выхода необходимо нажать **клавишу «q»**.

6.12 Просмотр журнала МЭ

Для просмотра журнала МЭ необходимо выбрать пункт меню **«10) Firewall log»**. Для выхода необходимо нажать комбинацию **клавиш «Ctrl»** + **«C»**.

6.13 Перезапуск сервисов

Для перезапуска всех настроенных сервисов необходимо выбрать пункт меню **«11) Reload all services»**.

6.14 Восстановление из резервной копии

Для восстановления **ARMA FW** необходимо выбрать пункт меню **«12) Restore a backup»** (см. Рисунок – Восстановление из резервной копии), ввести номер выбранной резервной копии на запрос **«Select backup to restore or leave blank to exit:»** и нажать **клавишу «ENTER»**. **ARMA FW** будет восстановлен и перезагружен после подтверждения на запрос **«Do you want to reboot to apply the backup cleanly? [y/N]»** вводом **«y»** и нажатием **клавиши «ENTER»**.

Для выхода без восстановления необходимо оставить поле ввода пустым и нажать **клавишу «ENTER»** на запрос **«Select backup to restore or leave blank to exit:»**.

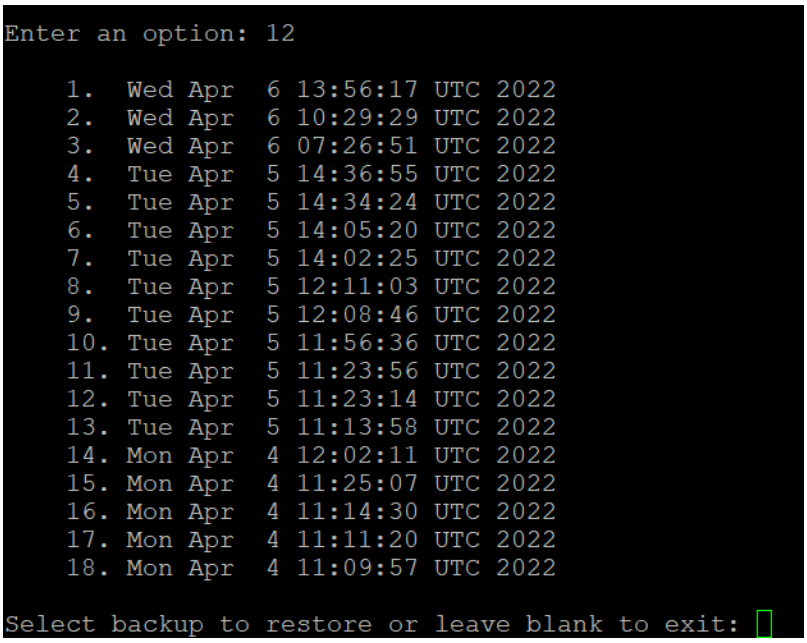

Рисунок – Восстановление из резервной копии

6.15 Активация лицензии

Для активации лицензии необходимо выбрать пункт меню **«13) Activate license»**, ввести лицензионный ключ и нажать **клавишу «ENTER»** (см. Рисунок – Активация лицензии).

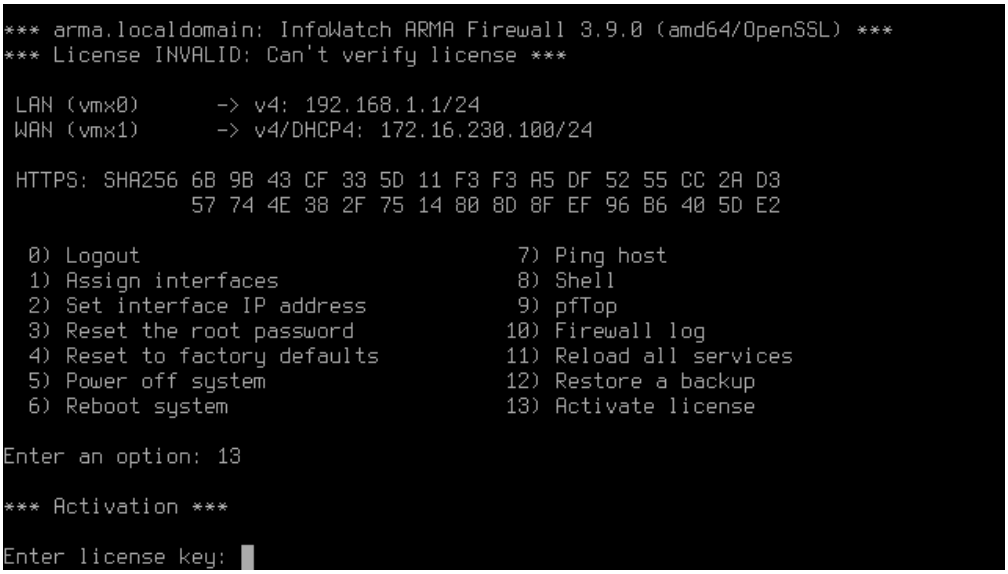

Рисунок – Активация лицензии

7 ОБСЛУЖИВАНИЕ

В разделе **«Конфигурация»** реализована возможность выполнять следующие действия:

- создавать локальные резервные копии конфигурации;
- экспортировать по расписанию текущую конфигурацию системы на удалённый FTP/SMB-сервер;
- восстанавливать конфигурацию;
- сбрасывать настройки системы до начальных;
- просматривать историю изменений с возможностью отмены действий.

7.1 Резервное копирование и восстановление

Резервное копирование конфигурации выполняется в виде сохранения файла с расширением **«xml»**. В дальнейшем данный файл возможно использовать для восстановления конфигурации при её повреждении, отката изменений конфигурации или переноса конфигурации на новое устройство.

Для создания локальной резервной копии конфигурации необходимо выполнить следующие действия:

1. Перейти в подраздел резервного копирования (**«Система» - «Конфигурация» - «Резервные копии»**) (см. Рисунок – Сохранение текущей конфигурации).
2. Для отключения создания резервной копии БД установить флажок для параметра **«Не делать резервную копию базу данных RRD»**.
3. Задать пароль для резервной копии в полях параметров **«Пароль»** и **«Подтверждение»**, а затем нажать **кнопку «Сохранить конфигурацию»**.

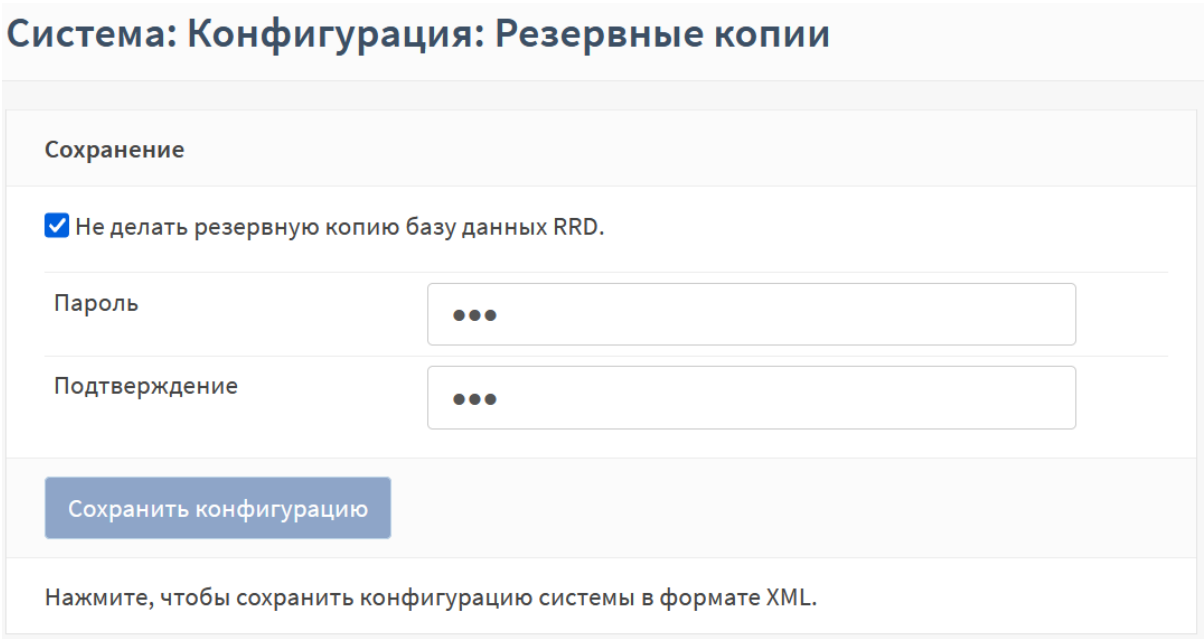

Рисунок – Сохранение текущей конфигурации

4. Следовать указаниям веб-браузера для сохранения конфигурационного файла.

7.2 История изменений

ARMA FW хранит историю вносимых изменений в конфигурацию для возможности просмотра изменений и отката к предыдущей версии.

Управление историей изменений осуществляется в одноимённом подразделе конфигурации (**«Система» - «Конфигурация» - «История изменений»**).

7.2.1 Указание количества хранимых резервных копий

Для указания количества хранимых резервных копий конфигурации необходимо в блоке настроек **«Количество резервных копий»** задать требуемое значение (см. Рисунок – Настройка количества резервных копий) и нажать **кнопку «Сохранить»**. На каждое изменение конфигурации создается отдельная резервная копия. По истечении заданного количества резервных копий последняя копия будет удалена и создана новая.

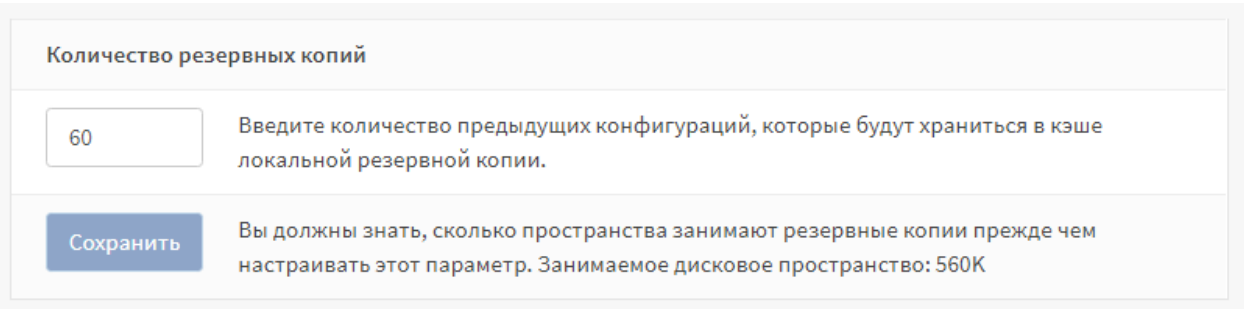

Рисунок – Настройка количества резервных копий

7.2.2 Просмотр истории изменений

Для просмотра истории изменений необходимо выполнить следующие действия:

1. В блоке настроек **«История изменений»**, в списке сохранённых конфигураций выбрать более раннюю версию в левом столбце, а более позднюю в правом столбце и нажать **кнопку «Просмотреть отличия»**.
2. Отличия между выбранными версиями будут отображены в блоке **«Отличия конфигурации»** в универсальном формате diff-файла:
   - строки, начинающиеся со знака **«-»** показывают, что было удалено из конфигурации;
   - строки, начинающиеся со знака **«+»** показывают, что было добавлено в конфигурацию;
   - строки без знаков показывают, что осталось без изменений (см. Рисунок – Просмотр изменений между конфигурациями).

Рисунок – Просмотр изменений между конфигурациями

7.2.3 Возврат к предыдущей сохранённой конфигурации

Для возврата к предыдущей сохранённой конфигурации выполнить следующие действия:

1. В строке выбранной конфигурации нажать **кнопку** « » и, в открывшейся форме (см. Рисунок – Всплывающее окно о подтверждении действия), подтвердить действие, нажав **кнопку «Да»**.

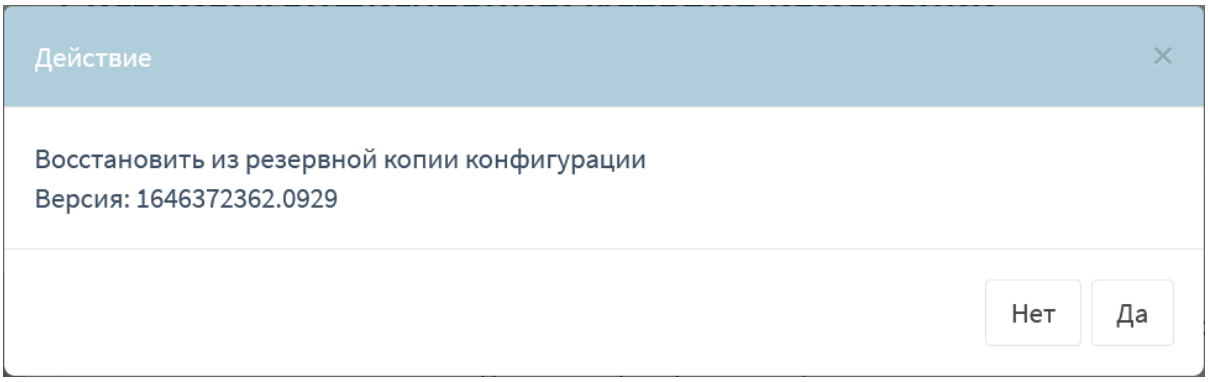

Рисунок – Всплывающее окно о подтверждении действия

2. В случае успешного возврата к предыдущей версии конфигурации появится соответствующее сообщение (см. Рисунок – Сообщение об успешном возврате к предыдущей версии конфигурации).

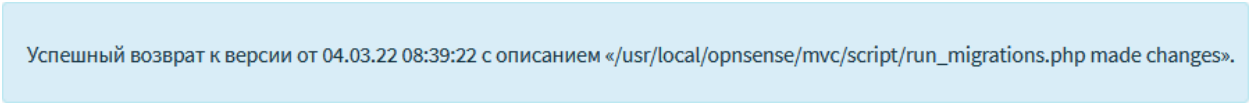

Рисунок – Сообщение об успешном возврате к предыдущей версии конфигурации

7.2.4 Локальное сохранение конфигурации

Для локального сохранения конфигурации необходимо в строке выбранной конфигурации нажать **кнопку** « » и следовать указаниям веб-браузера для скачивания файла.

7.3 Восстановление конфигурации

Восстановление конфигурации применяется для:

- восстановления конфигурации при её повреждении;
- отката изменений конфигурации;
- переноса конфигурации на новое устройство, в том числе при настройке большого количества устройств с однотипными параметрами.

Восстановление возможно, как всей конфигурации **ARMA FW**, так и отдельных групп настроек – зон.

Для восстановления конфигурации необходимо выполнить следующие действия:

1. Перейти в подраздел резервного копирования (**«Система» - «Конфигурация» - «Резервные копии»**).
2. В выпадающем списке **«Восстановить зону»** (см. Рисунок – Восстановление конфигурации) выбрать:
   - одну зону для восстановления отдельной зоны конфигурации;
   - несколько зон для восстановления нескольких зон конфигурации;

- значение **«ВСЕ»** для восстановления конфигурации в полном объёме.

и нажать **кнопку «Выберите файл»**.

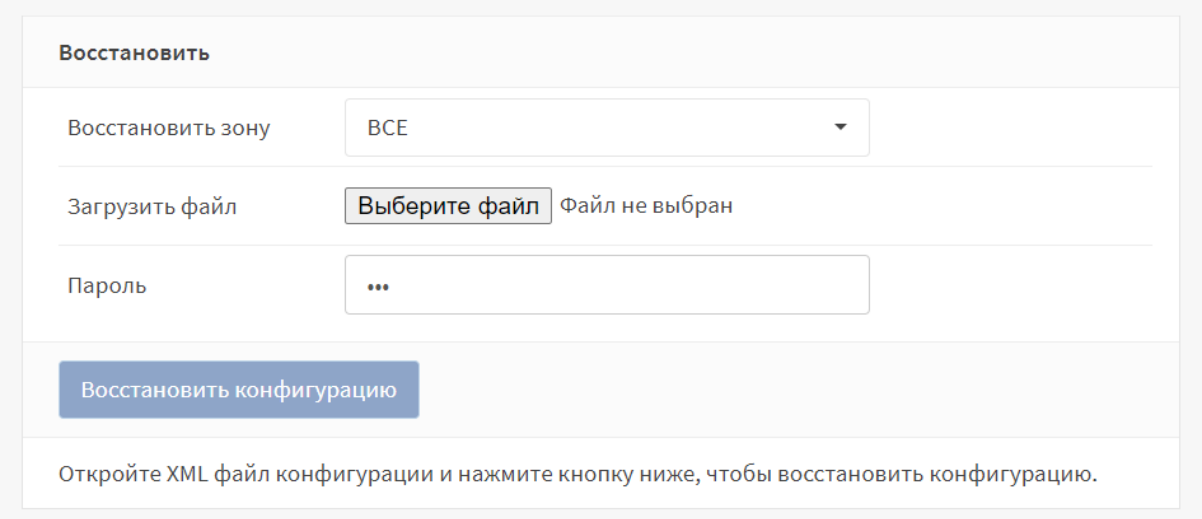

Рисунок – Восстановление конфигурации

3. В открывшемся окне проводника выбрать файл резервной копии конфигурации и нажать **кнопку «Открыть»**.
4. Указать пароль в поле параметра **«Пароль»** и нажать **кнопку «Восстановить конфигурацию»**.
5. Ознакомиться с предупреждением в открывшейся форме и нажать **кнопку «Восстановить»**.

Примечание:

При выборе значения «ВСЕ» в выпадающем списке **«Восстановить зону»** возможна потеря управления **ARMA FW** вследствие восстановления настроек УЗ, сетевых интерфейсов, правил МЭ и т.п.

В случае, когда требуется развернуть большое количество устройств с однотипными параметрами, необходимо повторить описанные действия на всех устройствах. Для автоматизированного применения конфигураций на большом количестве устройств целесообразно использовать **ARMA MC**.

Процесс подключения **ARMA FW** к **ARMA MC** описан в разделе Подключение к ARMA MC.

7.4 Экспорт конфигурации на удалённый FTP/SMB-сервер

Экспорт конфигурации на удалённые FTP/SMB-серверы необходим для автоматического выполнения резервного копирования настроек **ARMA FW**.

ARMA FW поддерживает передачу данных по протоколу SMB 3.1.1.

Примечание:

Для корректной передачи данных на принимающем сервере должно быть настроено шифрование.

Экспорт конфигурации осуществляется в формате архива с расширением **«tar.gz»**, в следующем формате:

- «config_armaif_[версия ARMA FW]_[дата экспорта]_[время экспорта]_[локация].tar.gz»

например,

config_armaif_3.6_20200831_170642_MSK.tar.gz

Для настройки экспорта на удалённый FTP/SMB-сервер необходимо выполнить следующие действия:

1. Перейти в подраздел настройки экспорта конфигурации (**«Система» - «Конфигурация» - «Настройки экспорта»**).
2. Установить флажок в параметре **«Включен»** и указать настройки импорта для требуемого протокола:
   - FTP:
     - **«Адрес»** – Адрес сервера: IP-адрес, хост, доменное имя;
     - **«Имя пользователя»** – Учётные данные;
     - **«Пароль»** – Учётные данные;
     - **«Путь к корневой папке»** – Абсолютный путь к корневой папке. Путь должен начинаться с символа **«/»**. Если экспорт производится в корневую директорию, то необходимо оставить только символ **«/»**;
     - **«Интервал»** – Интервал ожидания в случае неудачной попытки, задаётся в секундах;
   - SMB:
     - **«Адрес»** – Адрес сервера: IP-адрес, хост, доменное имя;
     - **«Общедоступный ресурс Samba»** – Имя общедоступного ресурса Samba;
     - **«Имя пользователя»** – Учётные данные;
     - **«Пароль»** – Учётные данные;

- **«Путь к корневой папке»** – Относительный путь к корневой папке. Путь должен начинаться с символа **«/»**. Если экспорт производится в корневую директорию, то необходимо оставить только символ **«/»**;
- **«Интервал»** – Интервал ожидания в случае неудачной попытки, задаётся в секундах.

3. Для сохранения настроек необходимо нажать **кнопку «Сохранить»**, а для сохранения настроек и последующего экспорта нажать **кнопку «Сохранить и импортировать»**.

После настройки рекомендуется убедиться в наличии файла конфигурации на удалённом сервере для проверки корректности работы экспорта.

Для сохранения и проверки корректности настроек экспорта конфигурации необходимо нажать **кнопку «Сохранить и экспортировать»**. Перейти на удалённый сервер и убедиться в наличии файла конфигурации, если его нет, то убедиться в корректности настроек сервера и его доступа по сети. При необходимости только сохранения настроек необходимо нажать **кнопку «Сохранить»**.

7.4.1 Экспорт конфигурации по расписанию

После успешной настройки экспорта конфигурации на удалённый сервер возможно настроить расписание выполнения экспорта с помощью планировщика задач Cron. Подробная настройка расписания описана в разделе **«Cron»** Руководства пользователя **ARMA FW**. При создании задачи необходимо выбрать «Экспорт конфигурации» в параметре **«Команда»**.

7.5 Сброс настроек

Сброс настроек до заводских значений используется, например, в случае некорректной настройки устройства и невозможности его дальнейшего использования.

Сброс настроек возможен двумя способами:

- **через веб-интерфейс**;
- **через локальный консольный интерфейс** (см. Восстановление настроек по умолчанию).

7.5.1 Сброс настроек через веб-интерфейс

Для сброса настроек системы необходимо перейти в подраздел настроек конфигурации (**«Система» - «Конфигурация» - «Значения по умолчанию»**) и нажать **кнопку «Да»** (см. Рисунок – Первоначальные настройки системы). **ARMA FW** будет сброшен к первоначальным настройкам и выполнена перезагрузка.

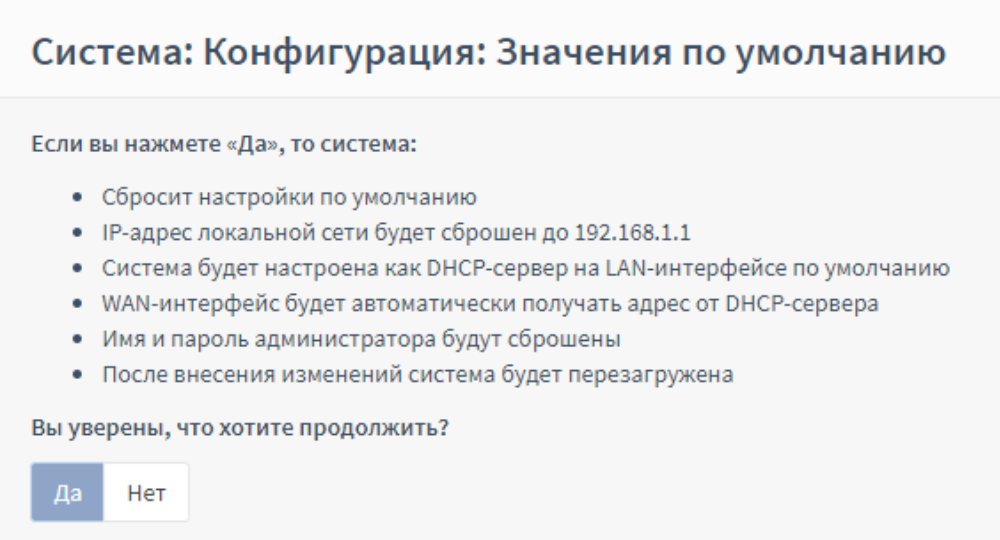

Рисунок – Первоначальные настройки системы

7.6 Обновление программного обеспечения

Обновления ПО представляются разработчиком или технической поддержкой.

Обновление **ARMA FW** производится через веб-интерфейс и доступно для версий 3.7.2 или выше.

Перед обновлением рекомендуется выполнить создание резервной копии конфигурации **ARMA FW**. Процесс создания резервной копии конфигурации **ARMA FW** описан в разделе Резервное копирование и восстановление.

Примечание:

Если текущая версия **ARMA FW** является более ранней, чем предыдущая от устанавливаемой, то обновление до новейшей версии возможно проводить только последовательно, не пропуская промежуточные версии.

Примечание:

Для корректного обновления ПО **ARMA FW**, работающих в режиме отказоустойчивого кластера, необходимо выполнить следующие действия:

- отключить синхронизацию состояния всех **ARMA FW**, входящих в состав кластера;
- обновить ПО каждого **ARMA FW**;
- включить синхронизацию.

В зависимости от производительности платформы функционирования и применённой конфигурации процесс обновления ПО **ARMA FW** может выполняться в течение продолжительного времени.

Для обновления **ARMA FW** необходимо выполнить следующие действия:

1. Перейти в подраздел настройки обновлений (**«Система» - «Прошивка» - «Обновления»**) (см. Рисунок – Обновление системы) и нажать **кнопку «Выберите файл»**.

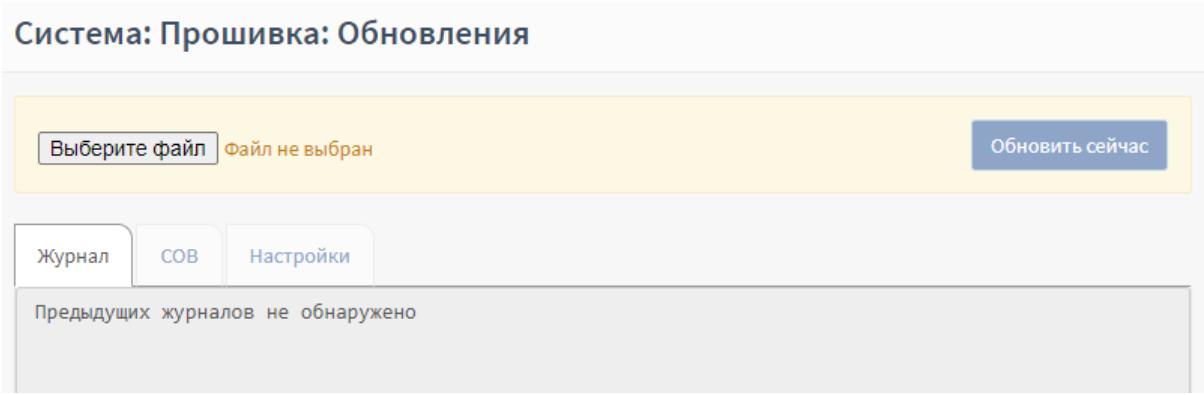

Рисунок – Обновление системы

2. В открывшемся окне проводника выбрать файл обновления, нажать **кнопку «Открыть»**, а затем **кнопку «Обновить сейчас»**.

   Индикатор выполнения процесса обновления отобразится на **кнопке «Обновить сейчас»**.

   Примечание:

   В течение выполнения процесса обновления ПО **ARMA FW** не рекомендуется переходить на другие вкладки подраздела настройки обновлений или иные разделы настройки **ARMA FW**.

3. Дождаться окончания обновления и перезагрузить страницу веб-браузера.

Обновление базы решающих правил СОВ описано в разделе **«Загрузка и включение наборов правил»** Руководства пользователя **ARMA FW**.

7.7 Контроль целостности

Контроль целостности необходим для отслеживания неизменности следующих программных частей **ARMA FW** (см. Рисунок – Контроль целостности программных частей системы):

- **«configuration»** – конфигурация системы;
- **«scripts»** – вспомогательные скрипты для различных задач;
- **«site-python»** – вспомогательные модули языка программирования Python, подключаемые в серверный код;
- **«contrib»** – сторонние вспомогательные библиотеки;
- **«version»** – версионность продукта;

- **«firmware-product»** – прошивка продукта;
- **«legacy-includes, www, mvc»** – программный код, связанный с веб-сервером;
- **«service»** – программный код, связанный с серверным кодом и не связанный с веб-интерфейсом.

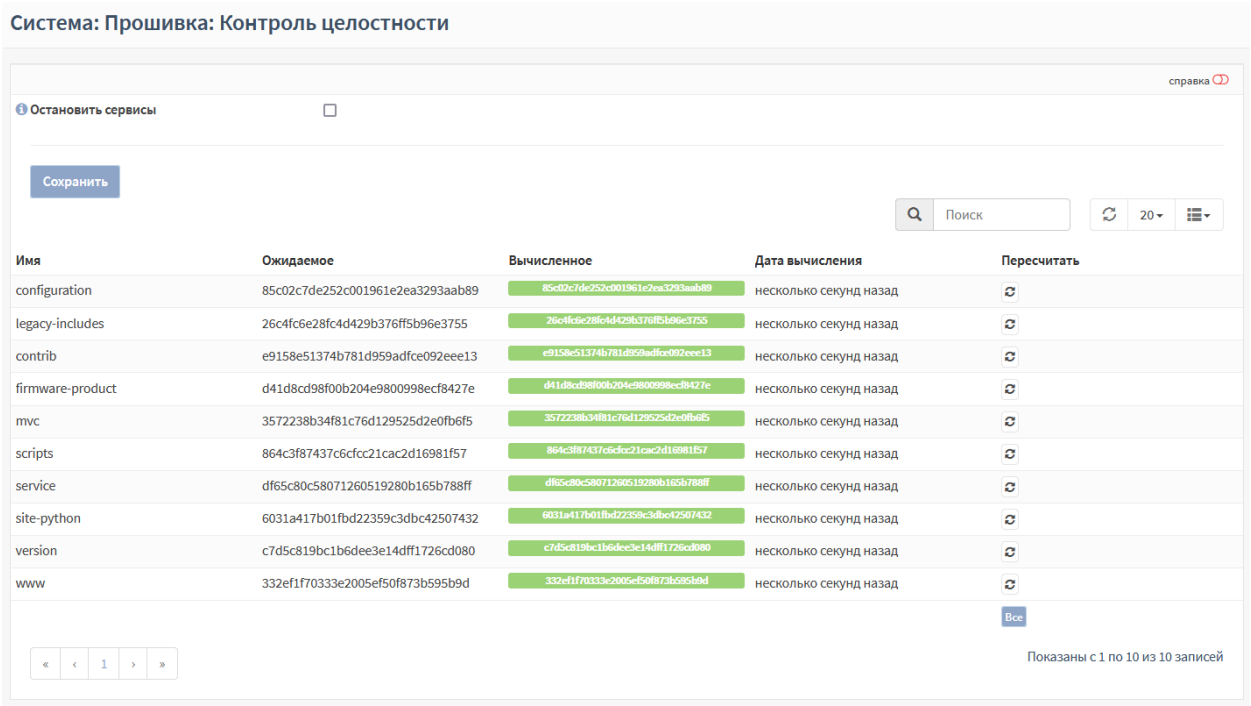

Рисунок – Контроль целостности программных частей системы

Контрольные суммы автоматически пересчитываются при старте системы, но существуют дополнительные средства запуска проверки контрольных сумм:

- вручную;
- по расписанию.

При совпадении значений столбца **«Ожидание»** и **«Вычисленное»** значение столбца **«Вычисленное»** вычисленного значения контрольной суммы с эталонным столбец **«Вычисленное»** будет выделен зелёным цветом.

В случае, если какая-то из частей вышла из строя или была внештатно изменена, то значение столбца **«Вычисленное»** будет выделено красным цветом и появится уведомление о неуспешной проверке целостности вверху страницы (см. Рисунок – Неуспешная проверка целостности). Уведомление сохраняется при переходе в любой раздел веб-интерфейса.

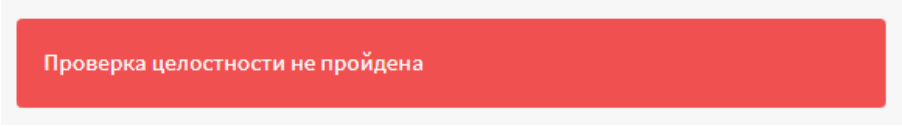

Рисунок – Неуспешная проверка целостности

Дополнительно существует возможность останавливать сервисы в случае нарушения целостности. Для этого необходимо установить флажок напротив поля **«Остановить сервисы»** и нажать **кнопку «Сохранить»**. В случае нарушения целостности любой части **ARMA FW**, блокируется работа всех сервисов **ARMA FW** – дальнейшая эксплуатация невозможна, при этом появится соответствующее уведомление (см. Рисунок – Автоматическая блокировка межсетевого экрана).

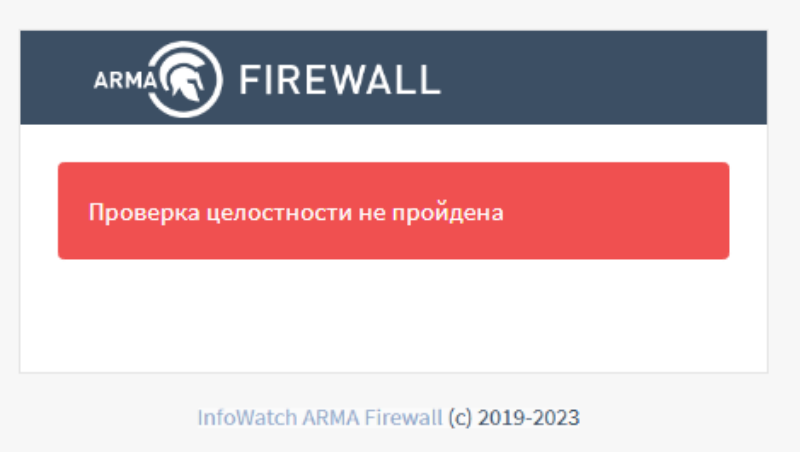

Рисунок – Автоматическая блокировка межсетевого экрана

Для продолжения эксплуатации **ARMA FW** необходимо произвести восстановление из установочного дистрибутива. Процесс восстановления идентичен повторной установке, но с последующим импортом конфигурации.

7.7.1 Запуск проверки контрольных сумм вручную

Для запуска проверки контрольных сумм вручную необходимо выполнить следующие действия:

1. Перейти в подраздел контроля целостности системы (**«Система» - «Прошивка» - «Контроль целостности»**) (см. Рисунок – Контроль целостности программных частей системы).
2. Нажать **кнопку** « » напротив строки программной части, нуждающейся в проверке или нажать **кнопку «Все»** для запуска проверки всех программных частей **ARMA FW**.

7.7.2 Запуск проверки контрольных сумм по расписанию

Возможна настройка расписания выполнения проверки контрольных сумм **ARMA FW** с помощью планировщика задач Cron. Подробная настройка расписания описана в разделе **«Cron»** Руководства пользователя **ARMA FW**. При создании задачи необходимо выбрать «Пересчитать все чек-суммы» в параметре **«Команда»**.

7.8 Подключение к ARMA MC

ARMA FW позволяет отправлять системные события и события безопасности в единый центр управления **ARMA MC**.

Взаимодействие **ARMA MC** и **ARMA FW** осуществляется по протоколу HTTPS.

Для успешной обработки событий от **ARMA FW** в **ARMA MC** необходима точная синхронизация времени между устройствами. Перед началом настройки следует убедиться в доступности устройств и при необходимости добавить разрешающее правило МЭ.

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

1. В **ARMA FW** создать УЗ с правами администратора и с ключом API. Процесс создания УЗ в **ARMA FW** описан в разделе **«Учетные записи и права доступа»** Руководства пользователя **ARMA FW**.
2. В **ARMA MC** добавить источник событий. Процесс добавления источника событий описан в разделе **«Управление источниками событий ARMA FW»** Руководства пользователя **ARMA MC**.
3. В **ARMA FW** настроить экспорт событий по syslog со следующими параметрами:
   - **«Транспортный протокол»** – «UDP(4)»;
   - **«Формат»** – «CEF»;
   - **«Имя хоста»** – IP-адрес или доменное имя **ARMA MC**;
   - **«Порт»** – порт, указанный при добавлении источника событий.

Подробная настройка syslog описана в разделе **«Сервис syslog»** Руководства пользователя **ARMA FW**.

8 ВОЗМОЖНЫЕ ОШИБКИ И ИХ РЕШЕНИЯ

8.1 Ошибка копирования файла во время установки с использованием ISO-образа

Ошибка копирования файла во время установки с использованием ISO-образа чаще всего вызвана нехваткой ОЗУ. Для предотвращения ошибки необходимо убедиться, что среда виртуализации соответствует минимальным требованиям, представленным в разделе Требования к виртуальной платформе настоящего руководства.

8.2 Ошибки диска на «VMware»

Ошибка диска на «VMware» чаще всего вызвана неисправным приводом – носителем. Для предотвращения ошибки необходимо изменить режим работы привода на «IDE».

8.3 Ограничение трафика не работает на «VMware»

В случае, когда в «VMware» используются драйверы «vmxnet3» возможна некорректная работа ограничения трафика. Для исключения ошибок необходимо переключить драйверы на «E1000».

8.4 Отсутствует доступ к веб-интерфейсу

Основные возможные причины отсутствия доступа к веб-интерфейсу:

1. Веб-интерфейс открылся через протокол HTTP. Подключение через HTTP невозможно. Для подключения к веб-интерфейсу по протоколу HTTPS необходимо очистить историю в веб-браузере или открыть страницу веб-браузера в режиме «Инкогнито».
2. При использовании среды виртуализации порядок сетевых адаптеров, представленный в операционной системе, может отличаться от порядка отображения в **ARMA FW**. Для решения данной ошибки необходимо дополнительно сопоставить MAC-адрес и названия физических и сетевых интерфейсов.

8.5 Неверный пароль в консольном интерфейсе

Возможной причиной ошибки авторизации в консольном интерфейсе является использование русских символов в пароле, заданном посредством веб-интерфейса.

В консольном интерфейсе поддерживается только английская раскладка. Необходимо изменить пароль в веб-интерфейсе на содержащий только английские символы или воспользоваться сбросом пароля через локальный консольный интерфейс (см. раздел Сброс пароля учетной записи суперпользователя).

8.6 Не работает FTP-прокси

FTP-прокси обрабатывает только незашифрованный FTP-трафик и работает только при включённом прокси-сервере.

Включение прокси-сервера осуществляется в подразделе настроек прокси-сервера (**«Службы» - «Прокси» - «Основные настройки»**). Необходимо установить флажок для параметра **«Включен»** и нажать **кнопку «Применить»**.

8.7 Невозможно авторизоваться в прокси-сервере

Основные возможные причины невозможности авторизоваться в прокси-сервере:

1. Ни один из методов аутентификации недоступен, если настраивается режим прозрачного HTTP-прокси и/или режим перехвата SSL. Для решения данной ошибки необходимо завершить настройку прозрачного HTTP-прокси и/или режима перехвата SSL.
2. Прокси-сервер преднастроен таким образом, что разрешает проксирование запросов только к некоторому множеству портов, считающихся безопасными, например: 80, 21, 443, 70, 210, 1025-65535, 280, 488, 591, 777. Проксирование SSL/TLS-соединений методом CONNECT разрешено только для порта TCP/443. Для решения данной ошибки необходимо задать поля в соответствии с требованиями к ним.

8.8 Не срабатывает правило межсетевого экрана

Основные возможные причины несрабатывания правила МЭ:

1. Все правила обрабатываются по порядку. При первом совпадении обработка правил прекращается. Для решения данной ошибки необходимо переместить нужное правило в начало списка.

   Подробный алгоритм работы правил МЭ описан в разделе **«Настройка правил МЭ»** Руководства пользователя **ARMA FW**.
2. При работе с Microsoft AD существует проблема поиска пользователя в первичной группе, как правило, это группа Users. В результате это приводит к тому, что если правило создано для некоторой группы, то оно не будет срабатывать для тех пользователей, для которых данная группа является первичной. Для решения данной ошибки необходимо создать дополнительную группу пользователей, для пользователей у которых группа является первичной.

8.9 Отсутствует доступ к порталу авторизации

Основные возможные причины отсутствия доступа к порталу авторизации:

1. Отсутствие разрешающих правил МЭ для портала авторизации. Необходимо создать разрешающие правила МЭ. Параметры правил МЭ описаны в разделе **«Настройка портала авторизации»** Руководства пользователя **ARMA FW**.
2. Неправильно настроенный DHCP-сервер. Необходимо при настройке DHCP-сервера в параметре **«DNS-серверы»** указать IP-адрес интерфейса, на котором развёрнут портал авторизации.

8.10 Не включается служба snmpd

Ошибка включения службы snmpd чаще всего вызвана тем, что не указан IP-адрес для прослушивания. Для решения данной ошибки необходимо перейти в раздел настройки SNMP (**«Система» - «Настройки» - «SNMP» - «Общие настройки»**), указать IP-адрес для мониторинга в **параметре «IP для прослушивания»** и нажать **кнопку «Сохранить»**.

8.11 Ошибка инициализации контрольных сумм проверки целостности

Для устранения ошибки инициализации контрольных сумм проверки целостности с помощью перезапуска исполняемого файла проверки целостности необходимо выполнить следующие действия:

1. Произвести аутентификацию в локальном консольном интерфейсе.
2. Нажать **клавишу «8»**, а затем **клавишу «Enter»** на клавиатуре для выбора пункта меню **«Shell»**.
3. В запущенной командной строке ввести команду:

   ```
   /usr/local/opnsense/scripts/integritycontrol/integritycontrol.py generate-initial -c
   ```

   и нажать **клавишу «Enter»**.

8.12 Ошибка конфигурации псевдонимов

Ошибка возникает в случае нехватки памяти для записей в таблице МЭ. Для увеличения выделенной памяти для записей в таблице МЭ необходимо перейти в раздел дополнительных настроек МЭ (**«Межсетевой экран» - «Настройки» - «Дополнительно»**) и ввести в поле параметра **«Максимальное количество записей в таблице»** значение в диапазоне от «0» до «2147483647». По умолчанию используется значение «1000000».

9 ПРИЛОЖЕНИЕ А

Системные учётные записи представлены в списке:

1. **«root»** – УЗ суперпользователя, System Administrator.
2. **«toor»** – УЗ резервного пользователя с ID = 0, имеющего ровно те же возможности, что и root.
3. **«installer»** – УЗ для установки **ARMA FW**.
4. **«daemon»** – От имени УЗ запускаются сервисы, которым необходима возможность записи файлов на диск.
5. **«operator»** – УЗ предназначена для выполнения административных задач с низкими привилегиями.
6. **«bin»** – УЗ, осуществляющая запуск бинарных команд операционной системы.
7. **«tty»** – Все устройства «/dev/vca» разрешают доступ на чтение и запись УЗ из этой группы.
8. **«kmem»** – УЗ, с предоставленным доступом к виртуальной памяти ядра для управления распределения оперативной памяти.
9. **«games»** – УЗ Games pseudo-user, не используется.
10. **«news»** – УЗ News Subsystem, не используется.
11. **«man»** – УЗ, позволяющая добавлять страницы в директорию «/var/cache/man».
12. **«sshd»** – УЗ для настройки доступа через SSH.
13. **«smmsp»** – УЗ, использующая Sendmail по умолчанию.
14. **«mailnull»** – УЗ для Sendmail, от имени которой по умолчанию отправляются почтовые сообщения.
15. **«bind»** – УЗ по умолчанию сервиса Bind.
16. **«unbound»** – УЗ для настройки и подключения кэширующего DNS.
17. **«proxy»** – УЗ используется прокси-сервером, доступ для записи файлов на диск отсутствует.
18. **«_pflogd»** – УЗ, от имени которой сохраняются события pf.
19. **«_dhcp»** – УЗ для подключения DHCP-сервера.
20. **«uucp»** – УЗ для подключения по протоколу UUCP.
21. **«pop»** – УЗ получения электронной почты.
22. **«auditdistd»** – Демон распределения файлов журнала аудита.
23. **«www»** – УЗ, обеспечивающая подключение в веб-интерфейсу.

24. **«ntpd»** – Демон NTP.
25. **«_ypldap»** – УЗ обеспечивает подключение к LDAP-серверу.
26. **«hast»** – УЗ обеспечивает работу HAST.
27. **«nobody»** – УЗ без привилегий доступа.
28. **«avahi»** – Ahavi демон.
29. **«messagebus»** – D-BUS демон.
30. **«_flowd»** – УЗ, разделяющая привилегии.
31. **«frr»** – УЗ, обеспечивающая подключение пакета протоколов FFRouting.
32. **«dhcpd»** – Демон DHCP.
33. **«_lldpd»** – LLDP демон.
34. **«squid»** – УЗ, обеспечивающая работу кэширующего прокси.
35. **«_tss»** – УЗ TCG Software Stack, TSS.
36. **«drweb»** – УЗ, обеспечивающая работу Dr.Web.