INFOWATCH ARMA

Программный комплекс

InfoWatch ARMA Industrial Firewall

Межсетевой экран с функцией обнаружения вторжений

**Руководство администратора**

Листов 87

2020

Содержание

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

| | | |
|---|---|---|
| ГБ | — | гигабайт |
| ГГц | — | гигагерц |
| МЭ | — | межсетевой экран |
| ОЗУ | — | оперативное запоминающее устройство |
| ОС | — | операционная система |
| ПК | — | программный комплекс |
| ПО | — | программное обеспечение |
| СОВ | — | система обнаружения вторжений |
| ЦП | — | центральный процессор |
| CRC | — | циклический избыточный код (Cyclic Redundancy Check) |
| DHCP | — | протокол динамической настройки узла (Dynamic Host Configuration Protocol) |
| DVI | — | цифровой видеоинтерфейс (Digital Visual Interface) |
| FTP | — | протокол передачи файлов по сети (File Transfer Protocol) |
| GPT/UEFI | — | таблица разделов GUID (GUID Partition Table) |
| GUI | — | графический интерфейс пользователя (Graphical User Interface) |
| HTTP | — | протокол передачи гипертекста (HyperText Transfer Protocol) |
| HTTPS | — | расширенный протокол HTTP (HyperText Transfer Protocol Secure) |
| IP | — | межсетевой протокол (Internet Protocol) |
| LAN | — | локальная вычислительная сеть (Local Area Network) |
| LDAP | — | облегчённый протокол доступа к каталогам (Lightweight Directory Access Protocol) |
| LRO | — | сетевая разгрузка (Large Receive Offload) |
| MBR | — | главная загрузочная запись (Master Boot Record) |
| QR | — | код быстрого реагирования (Quick Response Code) |

RFC — рабочее предложение (Request for Comments)

SNMP — простой протокол сетевого управления (Simple Network Management Protocol)

SPAN — анализатор коммутируемых портов (Switch Port Analyzer)

SSD — твердотельный накопитель (Solid-State Drive)

SSH — безопасная оболочка (Secure Shell)

SSL — уровень защищённых сокетов (Secure Sockets Layer )

TCP — протокол управления передачей (Transmission Control Protocol)

TLS — протокол защиты транспортного уровня (Transport Layer Security)

TOTP — алгоритм создания одноразовых паролей (Time Based One Time Password)

TSO — разгрузка сегментированием на уровне TCP (TCP Segmentation Offload)

USB — универсальная последовательная шина (Universal Serial Bus)

VGA — компонентный видеоинтерфейс (Video Graphics Array)

VLAN — виртуальная локальная сеть (Virtual Local Area Network)

WAN — глобальная вычислительная сеть (Wide Area Network)

# ВВЕДЕНИЕ

| | |
|---|---|
| Название документа | Программный комплекс InfoWatch ARMA Industrial Firewall (далее ПК «InfoWatch ARMA Industrial Firewall»). Руководство администратора |
| Версия документа | Версия 40 |
| Дата редакции документа | 18.03.2020 |
| Ключевые слова | Межсетевой экран, система обнаружения вторжений |

Руководство администратора содержит описание процедур, необходимых для установки, запуска и первоначальной конфигурации ПК «InfoWatch ARMA Industrial Firewall». Руководство администратора предназначено для администратора, который устанавливает ПК «InfoWatch ARMA Industrial Firewall» на аппаратное обеспечение, проводит начальную настройку, устанавливает в инфраструктуру предприятия, создает пользователей и назначает им привилегии. Роль пользователя и администратора может выполнять один сотрудник предприятия.

# 1. Требования к среде функционирования

Установка ПК «InfoWatch ARMA Industrial Firewall» производится на следующие типы платформ:

- аппаратная;
- виртуальная (гипервизор).

Установка на аппаратную платформу выполняется с использованием USB-накопителя, на который должен быть записан образ ПК «InfoWatch ARMA Industrial Firewall» в формате «*.IMG».

Установка на виртуальную платформу (гипервизор) производится с помощью образа в формате «*.ISO».

## 1.1. Требования к аппаратной платформе

При установке ПК «InfoWatch ARMA Industrial Firewall» на аппаратную платформу необходимо использовать микропроцессорную архитектуру x86 или x64.

Для аппаратной платформы, на которую устанавливается ПК «InfoWatch ARMA Industrial Firewall» достаточно руководствоваться минимальными требованиями к аппаратному обеспечению.

Для обеспечения корректного функционирования ПО и общей пропускной способности ПК «InfoWatch ARMA Industrial Firewall» 150 Мбит/секунду при работе функций межсетевого экрана, системы предотвращения вторжений (СОВ) с размером базы решающих правил в количестве 20000 сигнатур к оборудованию предъявляются минимальные требования, которые представлены в таблице (таблица 1).

**Таблица 1 — Минимальные требования к оборудованию**

| Название оборудования | Требования |
|---|---|
| Процессор | 2,0 ГГц, двухъядерный |

| | |
|---|---|
| ОЗУ | 8 ГБ |
| Интерфейсы, необходимые для установки программного обеспечения | Последовательная консоль или видео-выход (VGA или DVI) с USB (или PS/2) интерфейсами для подключения клавиатуры |
| Жесткий диск | 120 ГБ, SSD |
| Сетевые интерфейсы | Не менее 2 x Ethernet 10/100/1000 Мбит/сек |

Для подключения графического интерфейса поддерживаются следующие web-браузеры:

для ОС семейства Windows:

Chrome, Firefox, Internet Explorer (v8-v11);

для ОС семейства Linux:

Chrome для Linux, Firefox для Linux.

## 1.2. Требования к виртуальной платформе

Виртуализация ПК «InfoWatch ARMA Industrial Firewall» поддерживается для следующих виртуальных платформ (гипервизоров):

- HyperV Generation 1 и 2;
- KVM версии 53 и выше;
- Bhyve версии 11.1 и выше;
- VirtualBox версии 6.0.4 и выше;
- VMware ESXi версии 5.5 обновления 2 и выше.

ПК «InfoWatch ARMA Industrial Firewall» может быть установлено на все среды виртуализации, которые поддерживают FreeBSD версии 11.1.

Для запуска ПК «InfoWatch ARMA Industrial Firewall» предъявляются следующие минимальные требования к виртуальной среде ПК «InfoWatch ARMA Industrial Firewall»:

– количество процессоров: 1;

– объем оперативной памяти: 4 ГБ;

– размер виртуального диска: 25 ГБ

– количество сетевых интерфейсов: не менее 2.

В такой конфигурации производительность ПК «InfoWatch ARMA Industrial Firewall» обеспечивает обработку трафика не более 30 Мбит/секунду при работе функций межсетевого экрана, системы предотвращения вторжений (СОВ) с размером базы решающих правил в количестве 20000 сигнатур. При необходимости хранения большого количества записей журналов, необходимо руководствоваться минимальными требованиями к аппаратной платформе в разделе 1.1.

Для корректного отображения веб-интерфейса к веб-браузерам предъявляются следующие требования:

для ОС Windows:

Chrome, Firefox, Internet Explorer (v8-v11);

для ОС Linux:

Chrome для Linux, Firefox для Linux.

### 1.2.1. Требования к настройке среды виртуализации

Для возможности работы виртуальных машин, на физической платформе необходимо:

1. В BIOS - активировать поддержку виртуализации. Для этого необходимо:

– перезагрузить компьютер и войти в системное меню BIOS (обычно с помощью комбинаций клавиш «Alt» + «F4» или «Delete»);

– перейти к секции «Processor» и включить «Intel®Virtualization Technology» (в некоторых системах может называться «Virtualization Extensions») или «AMD-V»;

– сохранить изменения;

– выключить компьютер и отключить источник питания;

– выполнить команду cat /proc/cpuinfo | grep vmx svm и убедиться, что вывод команды пуст (иначе имеются ошибки в настройках или в системе отсутствуют необходимые расширения).

2. В операционной системе семейства Windows - убедиться в поддержке виртуализации, руководствуясь документацией на данную операционную систему, либо успешной попыткой запуска произвольной виртуальной машины.

# 2. Инструкция по установке системы и первоначальной настройке

ПК «InfoWatch ARMA Industrial Firewall» предназначен для установки только на платформах с поддержкой микропроцессорных архитектур x86 и x64.

## 2.1. Инструкция по установке

Для записи установочного образа ПК «InfoWatch ARMA Industrial Firewall» в формате «*.IMG» на USB-накопитель необходимо использовать ПО для установки образа на внешние накопители, например, ПК «InfoWatch ARMA Industrial Firewall»может быть использовано ПО «Rufus» (https://rufus-usb.ru.uptodown.com/windows) или его аналог. Производить запись образа необходимо в соответствии с описанием по использованию данного ПО.

ПК «InfoWatch ARMA Industrial Firewall» может работать в режиме «live» с USB-накопителя. Режим «live» позволяет подключаться к веб-интерфейсу в целях ознакомления с функциональными возможностями ПО без непосредственной установки. При первоначальной загрузке с USB-накопителя система будет работать в данном режиме.

Для начала работы в режиме «live» с USB-накопителя в консольном интерфейсе после появления приглашения на вход после надписи «login:» необходимо ввести имя пользователя «root» и нажать «ENTER», а в «password:» - «root» и нажать клавишу «ENTER». По умолчанию веб-интерфейс будет доступен по адресу «https://192.168.1.1/». Для входа в веб-интерфейс в браузере, после перехода по адресу «https://192.168.1.1/» в форме авторизации в поле «Username:» ввести «root», в поле «Password» ввести «root» и нажать кнопку «Login». Все изменения, сделанные в режиме загрузки ПК «InfoWatch ARMA Industrial Firewall» с USB Flash будут потеряны после перезагрузки, однако при установке без перезагрузки все изменения, внесенные в конфигурацию ПО будут сохранены на жестком диске.

Для того, чтобы произвести установку на целевую платформу в консольном интерфейсе нужно выйти из текущего пользователя (если до этого

был произведен вход с именем учетной записи пользователя «root») используя комбинацию клавиш «Ctrl+D». Затем после появления приглашения на вход после надписи «login:» необходимо ввести имя пользователя и нажать «ENTER», а в «password:» - «root» и нажать клавишу «ENTER».

В консольном интерфейсе управление происходит только с использованием клавиатуры. После нажатия клавиши «ENTER» появится приветственное сообщение. Для того, чтобы продолжить установку, необходимо выбрать «Ok, let’s go» (для этого нажать клавишу «ENTER») (рисунок 1).

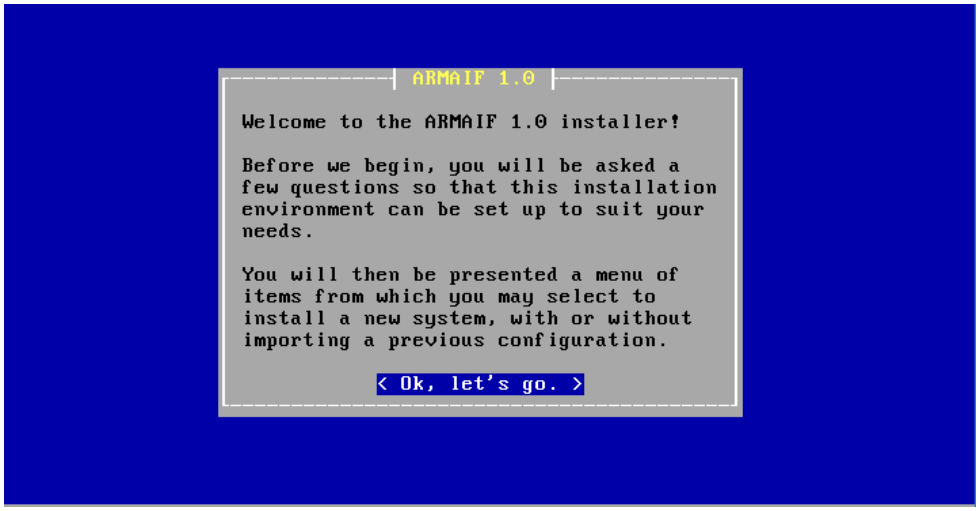



**Рисунок 1 — Приветственное сообщение**

Далее появится экран настройки консоли. Все доступные варианты настройки представлены в таблице (таблица 2). Выбор производится с помощью клавиш со стрелками вверх и вниз. Подтверждение выбора осуществляется с помощью нажатия клавиши «ENTER». Если нет необходимости изменять раскладку клавиатуры, рекомендуется выбрать «accept these settings» (рисунок 2).


**Рисунок 2 — Настройка консоли**

**Таблица 2 — Настройка консоли**

| Название настройки | Описание |
|---|---|
| Accept these Setting | Принять настройки по умолчанию |
| Change Keymap | Изменить раскладку клавиатуры |
| Change Video Font | Изменить шифры текста (то есть способ начертания символа и его размер) |

На следующем экране необходимо выбрать задачу. Все доступные варианты задач представлены в таблица 3. Выбор производится с помощью клавиш со стрелками вверх и вниз. Подтверждение выбора осуществляется с помощью нажатия клавиши «ENTER». Для продолжения установки ПК «InfoWatch ARMA Industrial Firewall», необходимо выбрать «Guided installation» (рисунок 3). Полный список возможных действий представлен в таблице (таблица 3).

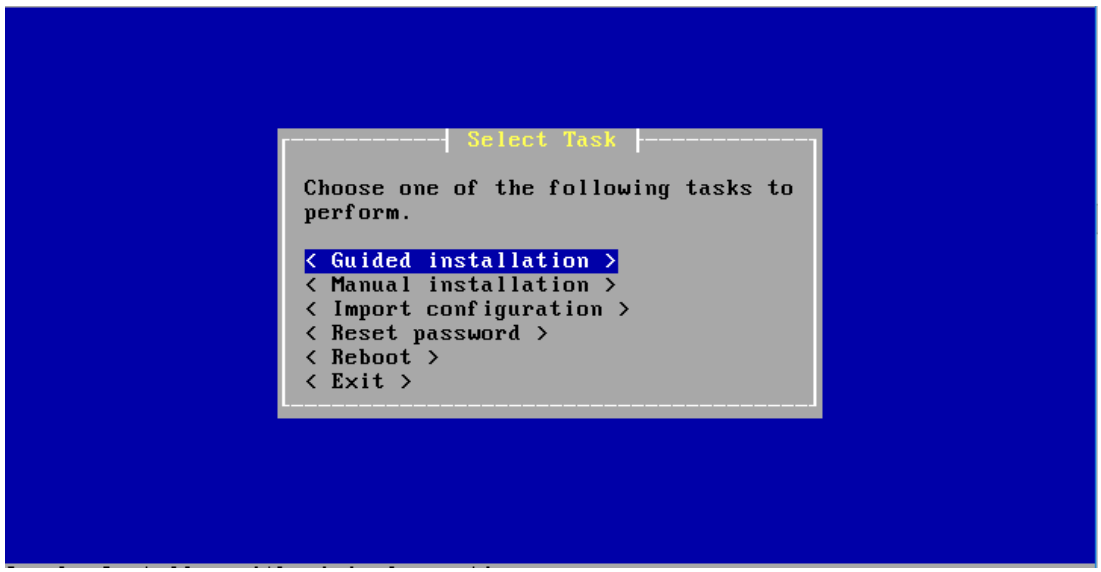



**Рисунок 3 — Выбор задачи**

**Таблица 3 — Выбор задачи**

| **Название задачи** | **Описание** |
|---|---|
| Guided installation | Установить |
| Manual installation | Установить вручную |
| Import configuration | Импортировать конфигурацию |
| Reset password | Сбросить пароль |
| Reboot | Перезагрузить |
| Exit | Выйти |

Следующим шагом необходимо выбрать диск, на который будет устанавливаться система. Выбор производится с помощью клавиш со стрелками вверх и вниз. Подтверждение выбора осуществляется с помощью нажатия клавиши «ENTER». Чтобы вернуться назад в окно «Выбор задачи» необходимо выбрать «Return to Select Task» (рисунок 4). Для продолжения установки ПК «InfoWatch ARMA Industrial Firewall», необходимо выбрать целевой накопитель для установки ПО.

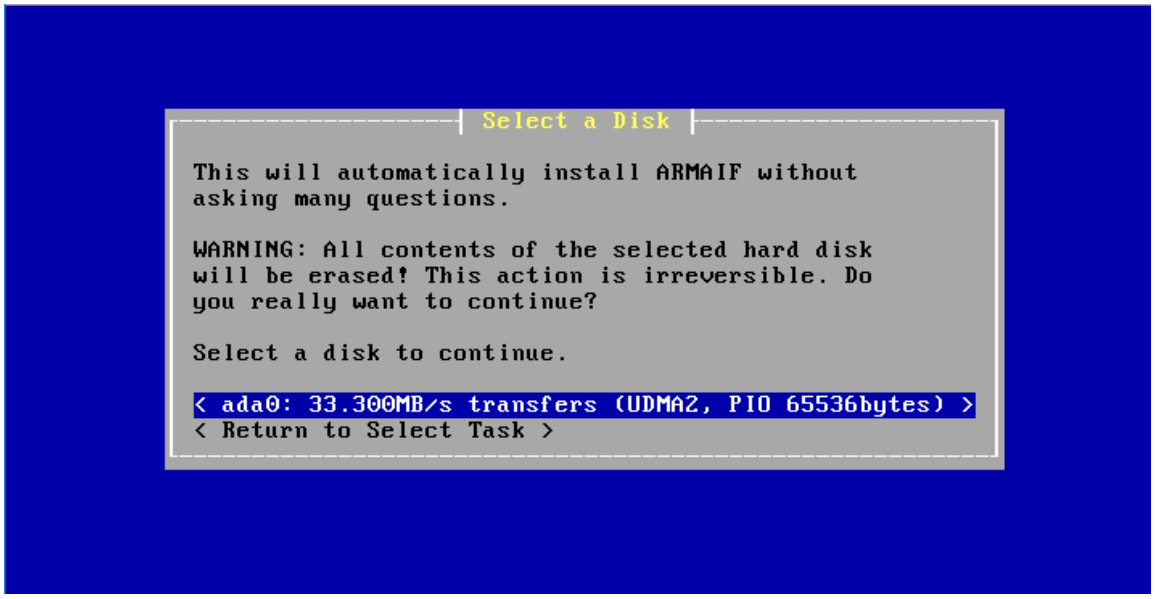



**Рисунок 4 — Выбор диска**

Далее необходимо выбрать режим установки ПК «InfoWatch ARMA Industrial Firewall», все доступные варианты режимов записи на диск представлены в таблице (таблица 4). Выбор производится с помощью клавиш со стрелками вверх и вниз. Подтверждение выбора осуществляется с помощью нажатия клавиши «ENTER». Для продолжения установки ПК «InfoWatch ARMA Industrial Firewall», необходимо выбрать «GPT/UEFI mode». Для возвращения в окно «Выбор диска» необходимо выбрать «Return to Select Disk» (рисунок 5).

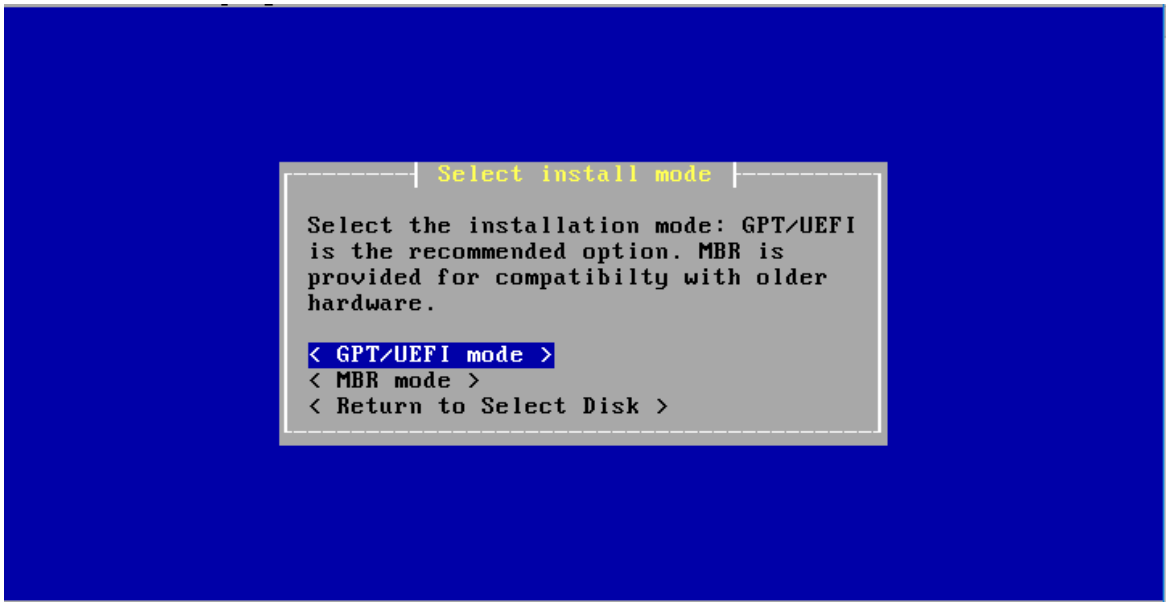



**Рисунок 5 — Выбор режима установки**

**Таблица 4 — Выбор режима установки**

| Название режима установки | Описание |
|---|---|
| GPT/UEFI mode | Запись в раздел GPT/UEFI жесткого диска |
| MBR mode | Запись в раздел MBR жесткого диска |

После настройка параметров необходимо дождаться окончания установки системы. При необходимости прервать установку нужно выбрать «Cancel», и нажать клавишу «ENTER» (рисунок 6).

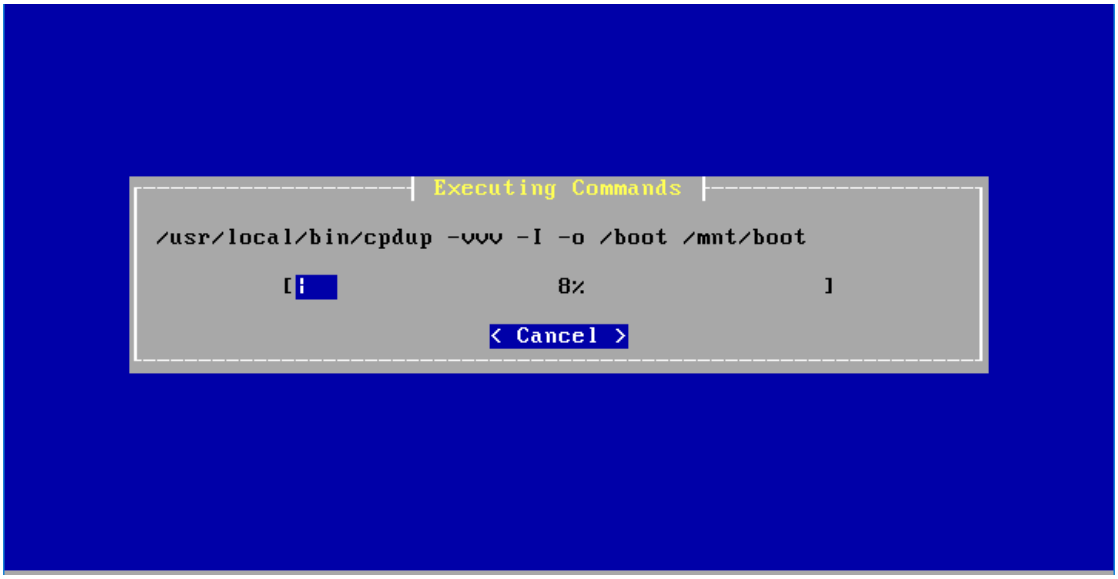



**Рисунок 6 — Установка системы**

После установки ПК «InfoWatch ARMA Industrial Firewall» необходимо ввести новый пароль пользовательской учетной записи «root» в поле «Root Password», нажать клавишу «ENTER» и повторить этот пароль в поле «Re-type Root Password», нажать клавишу «ENTER». После ввода пароля необходимо выбрать «Accept and Set Password», нажатием клавиши «ENTER» (рисунок 7).

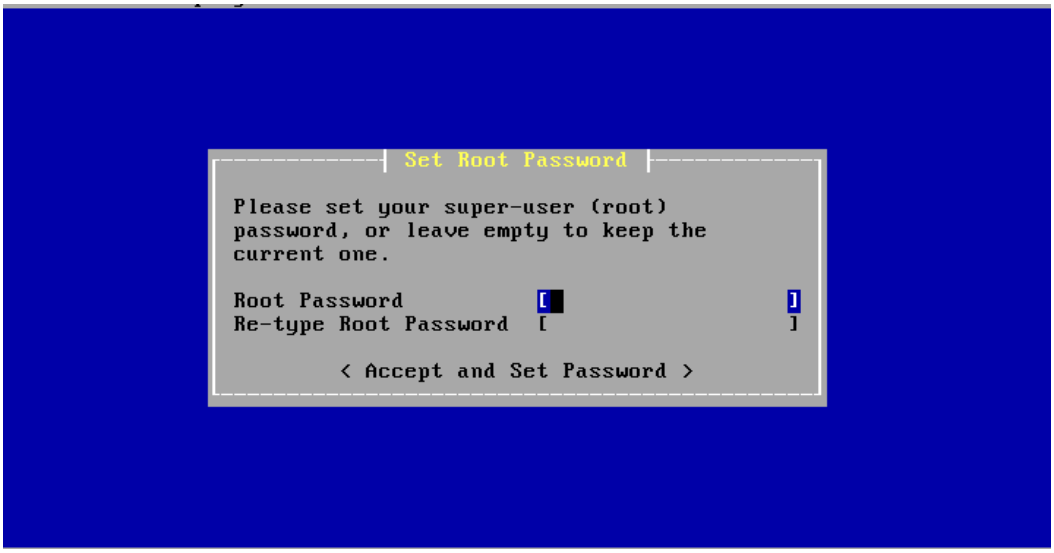



**Рисунок 7 — Выбор пароля**

После окончания установки будет представлен экран с вариантами дальнейших действий. Чтобы вернуться в окно «Выбор задачи» (рисунок 3), необходимо выбрать «Return to Select Task» (рисунок 8). Для перезагрузки необходимо выбрать «reboot». Выбор производится с помощью клавиш со стрелками вверх и вниз. Подтверждение выбора осуществляется с помощью нажатия клавиши «ENTER». После чего извлечь Flash USB носитель.

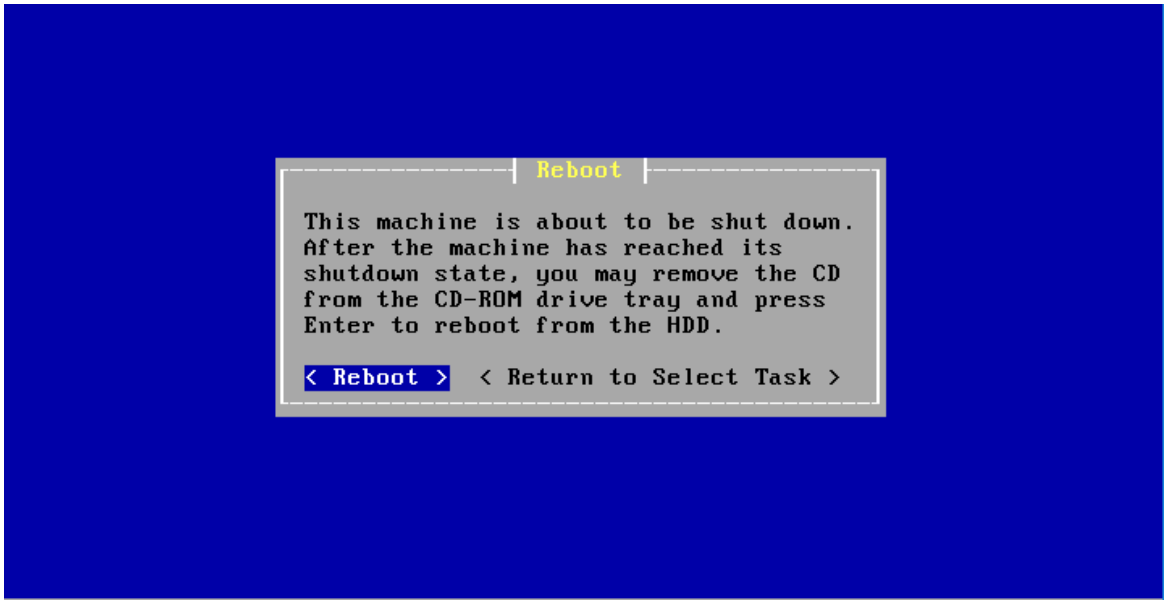



**Рисунок 8 — Перезагрузка**

## 2.2. Первоначальная настройка

Если производится первый запуск системы после установки, то необходимо убедиться, что установочный носитель ПК «InfoWatch ARMA Industrial Firewall» извлечен. При первой загрузке ПК «InfoWatch ARMA Industrial Firewall» будет представлена возможность настроить физические интерфейсы (рисунок 9). Для этого после появления надписи на экране «Press any key to start the manual interface assignment:» необходимо нажать любую клавишу в течение 5 секунд после появления надписи, если проигнорировать это сообщение, то будут применены настройки по умолчанию:

– первый определенный системой сетевой порт (или сетевой адаптер среды виртуализации) будет назначен как сетевой интерфейс WAN;

– второй определенный системой сетевой порт (или сетевой адаптер среды виртуализации) будет назначен как сетевой интерфейс LAN.

Назначение физических интерфейсов подробнее описано в подразделе 2.2.2 настоящего руководства.

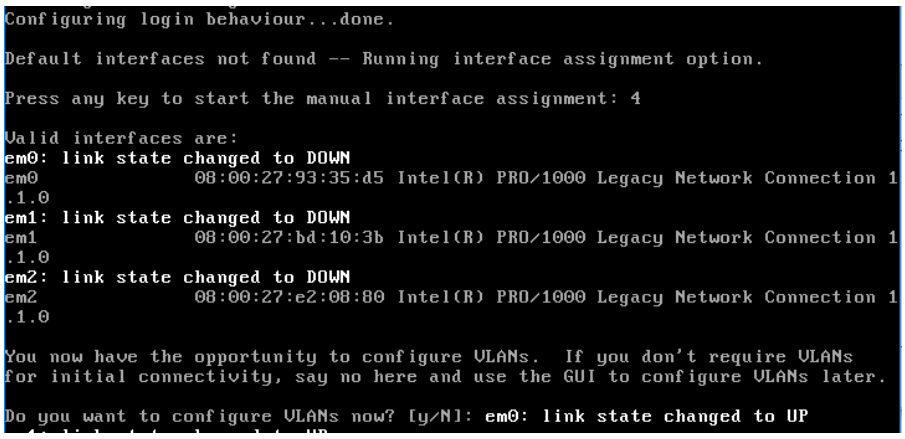



**Рисунок 9 — Назначение физических интерфейсов при загрузке системы**

Загрузка системы завершается приглашением для входа (рисунок 10).


**Рисунок 10 — Приглашение для входа в консольное меню**

Для входа в консольный интерфейс после появления приглашения на вход после надписи «login:» необходимо ввести имя пользователя «root» и

нажать «ENTER», а в «password:» - «root» или заданный при установке на этапе задания нового пароля (рисунок 7) и нажать клавишу «ENTER».

Консольное меню отображает 14 параметров показанных в таблице (таблица 5).

**Таблица 5 — Консольное меню**

| | |
|---|---|
| 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) Update from console |
| 6) Reboot system | 13) Restore a backup |

Если лицензия ранее не была установлена, дополнительно будет присутствовать пункт меню «14) Setup license».

### 2.2.1. Назначение физических интерфейсов

Для назначения физических интерфейсов вручную, необходимо ввести команду «1». Каждое из представленных имён сетевых интерфейсов соответствует физическому интерфейсу. Сопоставление физических интерфейсов с именами производится на уровне системы. Далее физическим интерфейсам назначаются соответствующие сетевые интерфейсы в стандартной последовательности:

– VLAN — необходимо учитывать, что настройка VLAN является необязательной, если VLAN не используется, необходимо ввести «n»;

– WAN — если нет необходимости настраивать WAN, необходимо нажать клавишу «ENTER», иначе необходимо ввести соответствующее имя физического интерфейса, например, «em0» и нажать клавишу «ENTER» (рисунок 11);

– LAN — если нет необходимости настраивать LAN, необходимо нажать клавишу «ENTER», иначе необходимо ввести соответствующее имя физического интерфейса, например, «em1» и нажать клавишу «ENTER»;

– OPT[номер дополнительного сетевого интерфейса] — если нет необходимости настраивать OPT[номер дополнительного сетевого интерфейса], необходимо нажать клавишу «ENTER», иначе необходимо ввести соответствующее имя физического интерфейса, например, «em2» и нажать клавишу «ENTER» (рисунок 11).

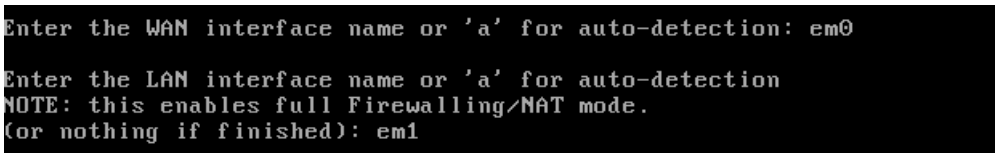



**Рисунок 11 — Настройка интерфейсов**

Если на аппаратной или виртуальной платформе (машине) имеются другие доступные физические интерфейсы, то необходимо по аналогии с выбором предыдущих интерфейсов определить их. Эти интерфейсы назначаются как сетевые интерфейсы с именем OPT ([OPT [номер дополнительного сетевого интерфейса]]). Если назначены все физические интерфейсы, необходимо нажать клавишу «ENTER» на вопрос о назначении последующего сетевого интерфейса. Необходимо проверить правильность настройки и подтвердить настройки после сообщения «Do you want proceed?», ввести «y» и нажать клавишу «ENTER». ПК «InfoWatch ARMA Industrial Firewall» настроит физические интерфейсы и представит приглашение для входа в систему по завершении.

### 2.2.2. Настройка IP-адресов

При необходимости настройки IP-адресов на назначенных сетевых интерфейсах необходимо выбрать опцию «2) Set interface(s) IP address». Данная операция может быть выполнена и через графический интерфейс пользователя.

**Настройка IPv4-адресов**

Для настройки IPv4 адреса после выбора пункта меню «2) Set interface(s) IP address» необходимо выбрать сетевой интерфейс (WAN, LAN, OPT, OPT1 и т.п.), для которого производится настройка IPv4-адреса. Далее необходимо

выбрать способ задания IPv4-адреса для выбранного интерфейса: с помощью DHCP-сервера или вручную.

Для этого необходимо на вопрос «Configure IPv4 address [Название интерфейса] via DHCP? [y/N]» ввести «y» и нажать клавишу «ENTER» при необходимости задания адреса для выбранного интерфейса с помощью DHCP-сервера (IPv4-адрес будет назначен выбранному интерфейсу автоматически), в противном случае, для задания адреса вручную, необходимо ввести «n» и нажать клавишу «ENTER».

Для настройки IPv4-адреса вручную после вопроса «Enter the new [Название интерфейса] IPv4 address. Press «ENTER» for none:» необходимо ввести IPv4-адрес выбранного интерфейса и нажать клавишу «ENTER». Далее необходимо ввести маску подсети IPv4-адреса (255.255.255.255 = 32, 255.255.255.0 =24, 255.255.0.0 = 16, 255.0.0.0 = 8) после «Enter the new [название интерфейса] IPv4 subnet bit count (1 to 32)» и нажать клавишу «ENTER».

При настройке IPv4-адреса WAN интерфейса есть возможность выбрать сетевой шлюз. Для этого необходимо ввести сетевой шлюз после «For a WAN, enter the new [Название интерфейса] IPv4 upsteream gateway address» и нажать клавишу «ENTER». При необходимости пропустить настройку сетевого шлюза необходимо нажать клавишу «ENTER».

**Настройка IPv6-адресов**

Для настройки IPv6 адреса после выбора пункта меню «2) Set interface(s) IP address» необходимо выбрать сетевой интерфейс (WAN, LAN, OPT, OPT1 и т.п.), для которого производится настройка IPv6-адреса. Далее необходимо выбрать способ задания IPv6-адреса для выбранного интерфейса: с помощью DHCP-сервера или вручную.

При необходимости задания IPv6-адреса с помощью DHCP-сервера после вопроса «Configure IPv6 address [Название интерфейса] via DHCPv6? [y/N]» необходимо ввести «y» (IPv6-адрес будет назначен выбранному интерфейсу автоматически) и нажать клавишу «ENTER». Для задания адреса вручную, необходимо ввести «n» и нажать клавишу «ENTER».

Для настройки IPv6-адреса вручную после «Enter the new [Название интерфейса] IPv6 address. Press «ENTER» for none:» необходимо ввести IPv6-адрес выбранного интерфейса и нажать клавишу «ENTER». Далее необходимо ввести маску подсети IPv6-адреса (ffff:ffff:ffff:ffff:ffff:ffff:ffff:ff00 = 120, ffff:ffff:ffff:ffff:ffff:ffff:ffff:0=112, ffff:ffff:ffff:ffff:ffff:ffff:0:0= 96, ffff:ffff:ffff:ffff:ffff:0:0:0= 80, ffff:ffff:ffff:ffff:0:0:0:0= 64) после «Enter the new [название интерфейса] IPv4 subnet bit count (1 to 128)» и нажать клавишу «ENTER».

При настройке IPv6-адреса WAN интерфейса есть возможность выбрать сетевой шлюз. Для этого необходимо ввести сетевой шлюз после «For a WAN, enter the new [название интерфейса] IPv6 upsteream gateway address» и нажать клавишу «ENTER». При необходимости пропустить настройку сетевого шлюза необходимо нажать клавишу «ENTER».

После настройки рекомендуется перезагрузить систему. Для этого необходимо в меню действий выбрать «6) Reboot system» (ввести «6» и нажать клавишу «ENTER»). Для перезагрузки системы необходимо ввести «y» после «The system will reboot. Do you want to proceed? [y/N]» и нажать клавишу «ENTER».

## 2.3. Настройки сервера посредством веб-интерфейс

### 2.3.1. Подключение к веб-интерфейсу

Для подключения к веб-интерфейсу необходимо открыть веб-браузер Chrome, Firefox либо Internet Explorer (версии веб-браузеров описаны в подразделе 1.1 настоящего руководства) и ввести IP-адрес, указанный в консольном интерфейсе, (по умолчанию 192.168.1.1) (рисунок 12).

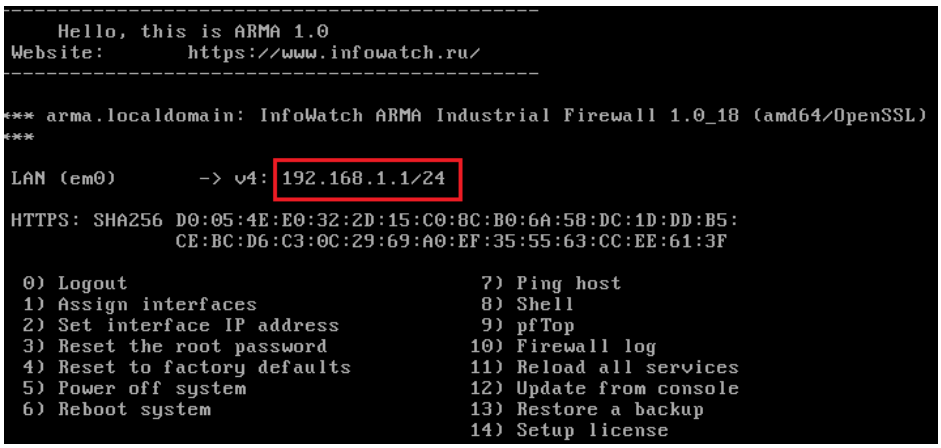



**Рисунок 12 — IP-адрес веб-интерфейса**

Для начала работы с ПК «InfoWatch ARMA Industrial Firewall» необходимо авторизоваться (рисунок 13). Для этого выполнить следующие действия:

– в поле «Username:» необходимо ввести «root»;

– в поле «Password» необходимо ввести «root» или пароль, который был задан при установке ПК «InfoWatch ARMA Industrial Firewall» (рисунок 13).

– нажать кнопку «Login» для входа в систему.

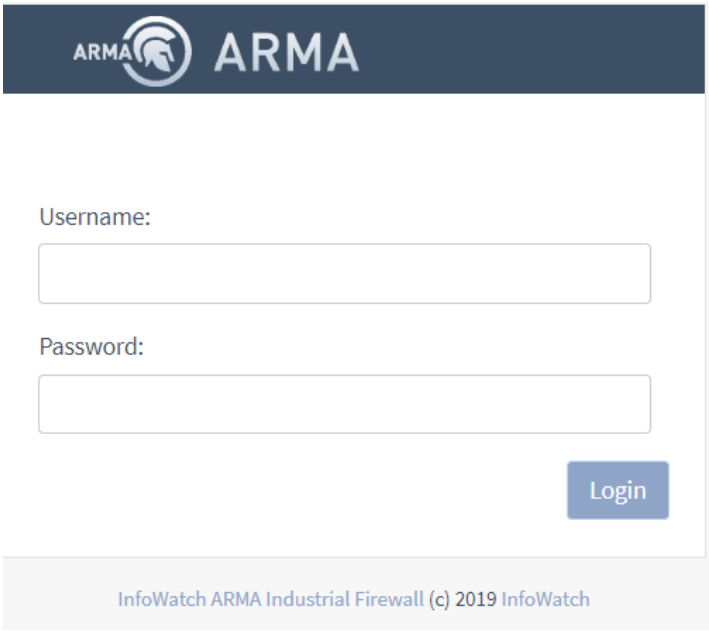



**Рисунок 13 — Вход в систему**

### 2.3.2. Включение русского языка

Для включения русского языка необходимо перейти в раздел общих настроек ПК «InfoWatch ARMA Industrial Firewall» «System» - «Setting» -

«General» и в поле «Language» выбрать язык «Russian» после чего внизу страницы нажать на кнопку «Save» (рисунок 14). Далее по документу приведено описание действий для веб-интерфейса на русском языке.

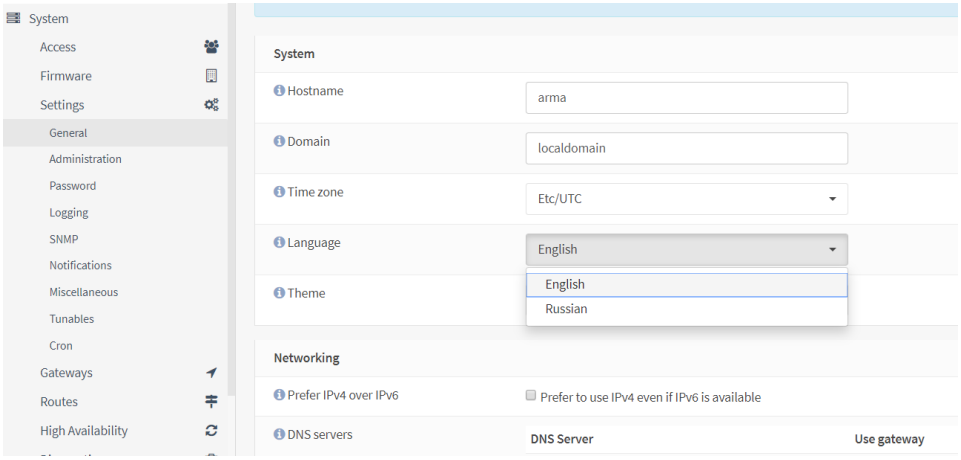



**Рисунок 14 — Включение русского языка**

### 2.3.3. Оптимизация веб-сервера

После установки ПК «InfoWatch ARMA Industrial Firewall» для оптимизации веб-сервера необходимо перейти в разделе меню настроек сетевых интерфейсов «Интерфейсы» - «Настройки» и отключить CRC, TSO, LRO. CRC — это расчет контрольной суммы Ethernet-кадра средствами сетевой карты без участия ЦП. TSO — это сегментирование TCP-пакета без участия ЦП с помощью аппаратных возможностей сетевой карты. LRO — это буферизация входящих пакетов и их передача сетевому стеку в агрегированном виде с целью избежать неэффективной передачи каждого пакета в отдельности. Для отключения CRC, TSO, LRO необходимо поставить флажок напротив (рисунок 15):

– CRC аппаратного обеспечения;
– TSO аппаратного обеспечения;
– LRO аппаратного обеспечения.

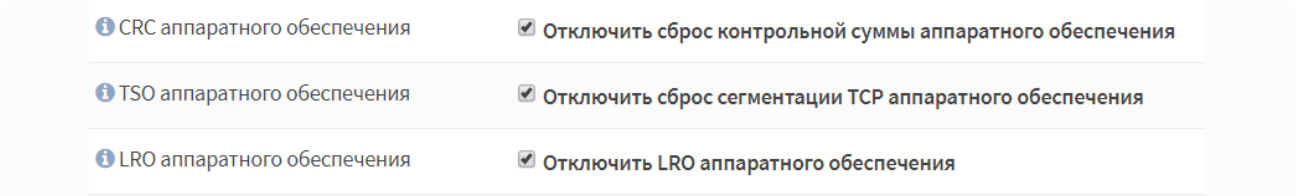



**Рисунок 15 — Обеспечение оптимальной производительности**

После внесения изменений в разделе необходимо нажать кнопку «Сохранить» внизу страницы.

### 2.3.4. Настройки безопасности

В данном разделе указываются настройки, позволяющие ограничить доступ по некоторым из каналов (интерфейсов) управления.

**Настройка подключения по протоколу HTTP/ HTTPS**

В рамках проведения диагностики неисправностей, имеется возможность изменения протокола подключения к веб-интерфейсу с HTTPS на HTTP. Для изменения протокола подключения к веб-интерфейсу (по умолчанию используется протокол подключения HTTPS) необходимо перейти в раздел настроек ПК «InfoWatch ARMA Industrial Firewall» «Система» - «Настройки» - «Администрирование», в группе настроек «Веб-интерфейс» в «Протокол» выбрать нужный протокол (рисунок 16) и нажать кнопку «Сохранить» внизу страницы.

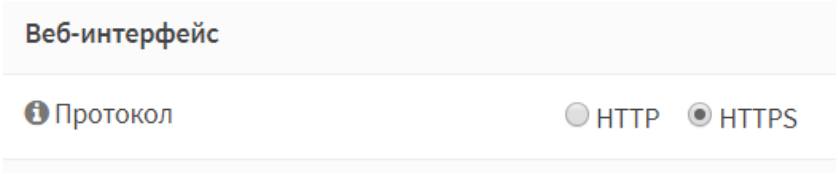



**Рисунок 16 — Настройка подключения по протоколу HTTP/HTTPS**

Предусмотрена возможность отключения HTTPS и через консоль управления. Для этого в консольном интерфейсе необходимо ввести «2» и нажать клавишу «ENTER». Далее выберите интерфейс, через который подключается веб-интерфейс (чаще всего это «LAN»), для этого необходимо ввести номер нужного интерфейса и нажать клавишу «ENTER». Появится настройка выбранного интерфейса. Необходимо произвести настройку адресации для интерфейса, после чего на вопрос «Do you want to revert to HTTP as the web GUI protocol? [y/N]», для подключения по протоколу HTTP необходимо ввести«y» и нажать клавишу «ENTER».

Во всех других режимах для подключения необходимо использовать

только протокол HTTPS.

**Настройка доступа по SSH**

По умолчанию доступ по SSH отключен. Для настройки доступа по SSH необходимо перейти в веб-интерфейсе в раздел меню настроек ПК «InfoWatch ARMA Industrial Firewall» «Система» - «Настройки» - «Администрирование». Для включения SSH-сервера в группе настроек «SSH» в графе «SSH-сервер» установите флажок «Включите SSH». В поле «Группа логина» для удаленного подключения по SSH необходимо выбрать разрешенные группы пользователей. Для разрешения входа пользователя «root» через SSH в поле «Вход суперпользователей (root) в учетную запись» необходимо установить флажок «Разрешить парольный вход в учетную запись». Для разрешения парольного входа в учетную запись в графе «Метод аутентификации» необходимо установить флажок «Разрешить парольный вход в учетную запись». В поле «Порт SSH» необходимо ввести порт для подключения по SSH или оставить значение по умолчанию (22 порт). В поле «Прослушиваемые интерфейсы» необходимо выбрать сетевые интерфейсы, по которым будет разрешен доступ через SSH (рисунок 17). Для сохранения настроек доступа SSH нажать кнопку «Сохранить» внизу страницы.

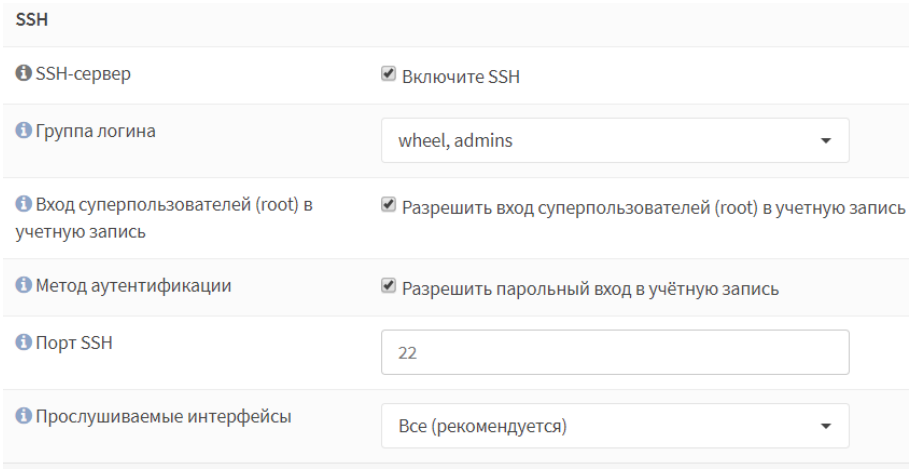



**Рисунок 17 — Доступ по SSH**

**Настройка доступа к локальному консольному интерфейсу**

Для настройки доступа к локальному консольному интерфейсу необходимо перейти в раздел меню настроек ПК «InfoWatch ARMA Industrial Firewall» «Система» - «Настройки» - «Администрирование». Для использования драйвера виртуального терминала в группе настроек «Консоль» в «Драйвер консоли» установить флажок напротив «Использовать драйвер виртуального терминала». В поле «Главная консоль» необходимо выбрать основную консоль, которая будет показывать вывод сценариев загрузки. В поле «Вспомогательная консоль» выбрать вспомогательные консоли, которые будут отображать сообщения загрузчика ОС, сообщения консоли и меню консоли. В поле «Скорость последовательного порта» ввести значение пропускной способности последовательного порта консоли. Для использования USB-порта в графе «USB-порт» установить флажок. Для защиты паролем консольного меню в графе «Меню консоли» напротив пункта «Защита паролем меню консоли» установить флажок (рисунок 18). После внесения необходимых изменений в конфигурацию для сохранения настроек необходимо нажать кнопку «Сохранить» внизу страницы.

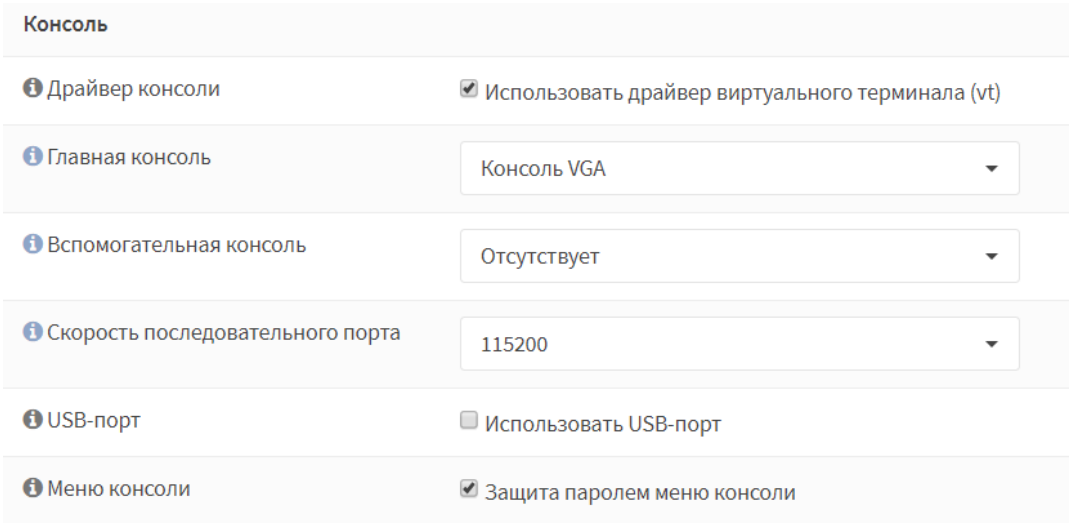



**Рисунок 18 — Доступ к локальному консольному интерфейсу**

## 2.4. Проверка работоспособности

Для проверки работоспособности ПК «InfoWatch ARMA Industrial Firewall» в веб-интерфейс необходимо перейти в раздел меню настроенных служб «Система» - «Диагностика» - Службы» и убедиться в том, что системные службы запущены, то есть напротив каждой службы значок «Запуск»  отображается зеленым цветом (рисунок 19). Ниже приведен список системных служб, ПК «InfoWatch ARMA Industrial Firewall»:

– configd;
– login;
– ntpd;
– pf;
– syslog.

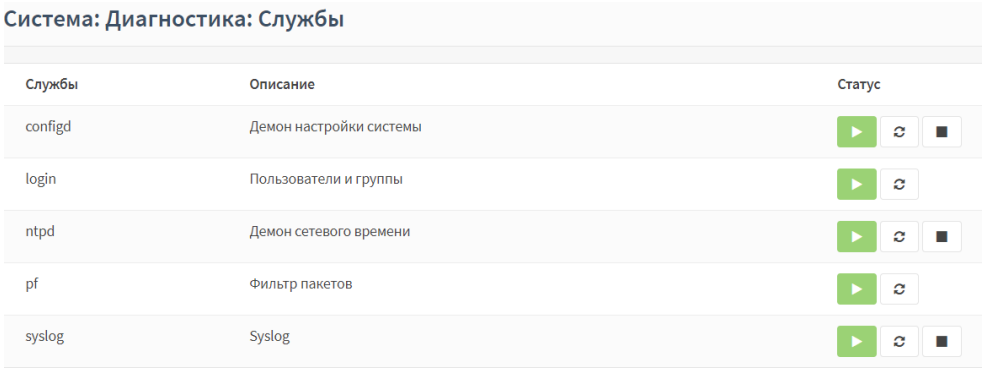



**Рисунок 19 — Проверка работоспособности**

# 3. Варианты развертывания

ПК «InfoWatch ARMA Industrial Firewall» предусматривает установку в сеть в одном из четырех вариантов (режимов работы). Режим работы определяется настройками сетевых интерфейсов:

– режим маршрутизации;

– режим прозрачного моста;

– режим sniffing mode (обнаружение вторжений путем анализа копии сетевого трафика, снятого со SPAN порта);

– режим отказоустойчивого кластера.

Каждый вариант отличается настройкой сетевых интерфейсов, а не самого устройства.

## 3.1. Маршрутизация

В режиме маршрутизации ПК «InfoWatch ARMA Industrial Firewall» функционирует как межсетевой экран с функциями обнаружения и предотвращения вторжений, обеспечивая защиту передачи информации на уровне L3 с возможностью маршрутизации. Режим маршрутизации может использоваться при объединении подсетей, имеющих разное адресное пространство. Общая схема подключения ПК «InfoWatch ARMA Industrial Firewall» в режиме маршрутизации показана на рисунке (рисунок 20).

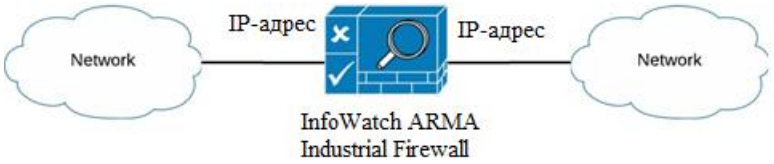



**Рисунок 20 — Режим маршрутизации**

## 3.2. Прозрачный мост

В режиме прозрачного моста ПК «InfoWatch ARMA Industrial Firewall» функционирует как система обнаружения и предотвращения вторжений в прозрачном режиме с возможностью блокировки вредоносных пакетов.

Интерфейсы при этом соединены в сетевой мост. Такой режим предназначен для фильтрации трафика между сетями одного адресного пространства. При обнаружении подозрительного либо вредоносного трафика, информация о нем отправляется на веб-интерфейс для последующего отображения и информирования пользователей и при необходимости блокируется. Общая схема подключения ПК «InfoWatch ARMA Industrial Firewall» в режиме прозрачного моста показана на рисунке (рисунок 21).

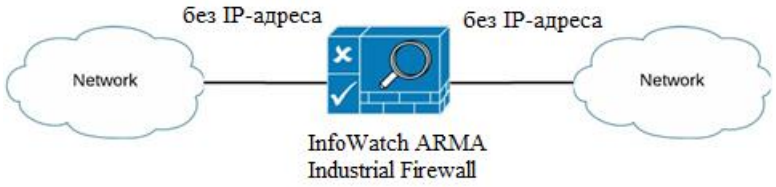



**Рисунок 21 — Режим прозрачного моста**

## 3.3. Sniffing mode

В режиме sniffing mode (мониторинга) ПК «InfoWatch ARMA Industrial Firewall» функционирует в качестве системы обнаружения вторжений, которая анализирует копии сетевого трафика, снятого со SPAN порта. Для подключения ПК «InfoWatch ARMA Industrial Firewall» в качестве СОВ необходимо настроить перенаправление на него всего сетевого трафика из основной сети на коммутаторе с помощью технологии SPAN или аналогичной (зеркалированный порт). Такой коммутатор должен обладать как минимум одним свободным портом для подключения ПК «InfoWatch ARMA Industrial Firewall». ПК «InfoWatch ARMA Industrial Firewall» проводит глубокий анализ пакетов (DPI) и, в случае необходимости, уведомляет администратора о событиях информационной безопасности. Общая схема подключения ПК «InfoWatch ARMA Industrial Firewall» в режиме sniffing mode (мониторинга) показана на рисунке (рисунок 22).

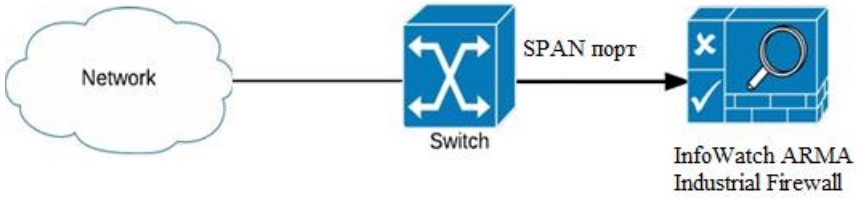



**Рисунок 22 — Режим sniffing mode**

## 3.4. Отказоустойчивый кластер

В режиме отказоустойчивого кластера несколько ПК «InfoWatch ARMA Indstrial Firewall» объединяются в единый кластер в режиме active-passive. В каждый момент времени, только одно устройство в кластере (ведущее) обрабатывает весь трафик. Подчиненные (резервные) устройства постоянно синхронизируют свое состояние и конфигурацию с ведущим (мастер-устройством). В случае отказа или отключения ведущего устройства, резервное устройство начинает обрабатывать сетевой трафик и становится ведущим. В случае, если первоначальное ведущее устройство возвращается в рабочее состояние, то текущее ведущее устройство переходит в состояние резервного устройства. Общая схема подключения ПК «InfoWatch ARMA Industrial Firewall» в режиме отказоустойчивого кластера показана на рисунке (рисунок 23).

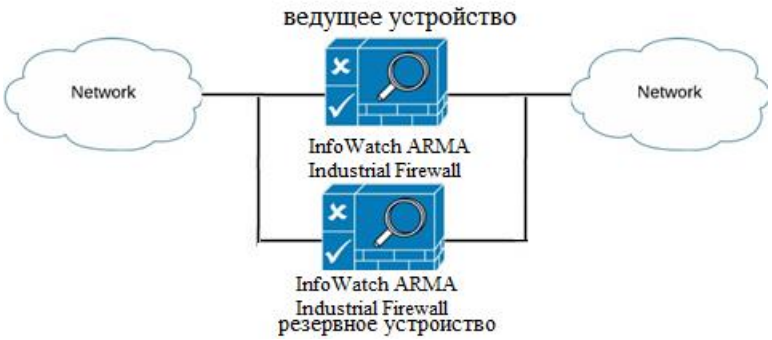



**Рисунок 23 — Режим отказоустойчивого кластера**

# 4. Контроль управления доступом

## 4.1. Аутентификация

Аутентификация пользователей производится с использованием локальной (внутренний сервер) или внешней (внешние серверы) базы пользователей.

В состав ПК «InfoWatch ARMA Industrial Firewall» входит локальная база данных пользователей.

К дополнительным мерам защиты при аутентификации с использованием внутренних серверов относится ваучер-сервер.

ПК «InfoWatch ARMA Industrial Firewall» поддерживает работу со следующими внешними серверами:

– LDAP (OpenLDAP, MS Active Directory, Novell eDirectory);

– Radius.

К дополнительным мерам защиты при аутентификации с использованием внешних серверов относится сервис двухфакторной аутентификации.

Для авторизации и предоставления соответствующих привилегий пользовательской учетной записи, настроенной с помощью внешнего сервера, необходимо импортировать пользовательскую учетную запись в локальную базу пользователей ПК «InfoWatch ARMA Industrial Firewall».

### 4.1.1. Локальная база данных пользователей

Локальная база данных пользователей используется по умолчанию после установки системы для хранения учетных записей пользователей (например, запись пользователя по умолчанию «root»). Для настройки параметров локальной базы данных необходимо перейти в раздел меню настройки серверов аутентификации «Система» - «Доступ» - «Серверы» и нажать на значок «Редактировать»  в строке «Локальная база данных». В режиме редактирования необходимо задать настройки пароля для всех пользователей

локальной базы пользователей, а именно — в поле «Длина» задать необходимую длину пароля, в графе «Сложность пароля» 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 (рисунок 24).

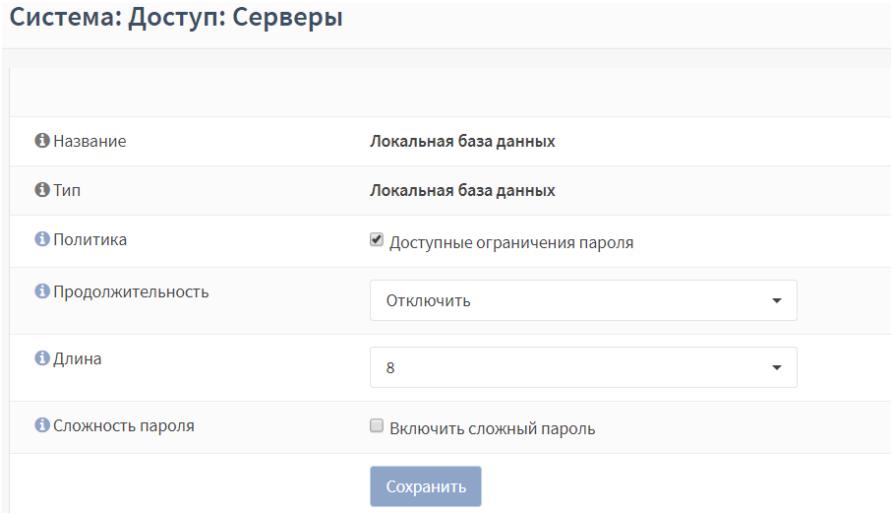



**Рисунок 24 — Локальная база данных (редактирование)**

### 4.1.2. Ваучер-сервер

Для обеспечения аутентификации в Портале авторизации в ПК «InfoWatch ARMA Industrial Firewall» используется ваучер-сервер.

Ваучер — это запись с логином и паролем, которую ПК «InfoWatch ARMA Industrial Firewall» генерирует по запросу. Ваучеры имеют настраиваемый срок жизни. По его истечении пользователю необходимо получить новый ваучер.

Для настройки ваучер-сервера необходимо перейти в раздел настройки серверов аутентификации «Система» - «Доступ» - «Серверы» и нажать на значок «Редактировать»  в строке имеющегося ваучер-сервера или нажать кнопку 

для добавления нового сервера. В поле «Название» необходимо ввести название сервера, в поле «Тип» необходимо выбрать «Ваучер», в графе «Использовать простые пароли (менее безопасные)» необходимо установить которые удовлетворяют требованиям по наличию:

– специального символа;

– цифры;

– строчной буквы;

– прописной буквы.

В поле «Общий секретный ключ» необходимо ввести секретный ключ, в поле «Длина имени пользователя» необходимо ввести длину имени пользователя для создания ваучеров, в поле «Длина пароля» необходимо ввести длину пароля для создания ваучеров. Для сохранения настроек необходимо нажать кнопку «Сохранить» (рисунок 25).

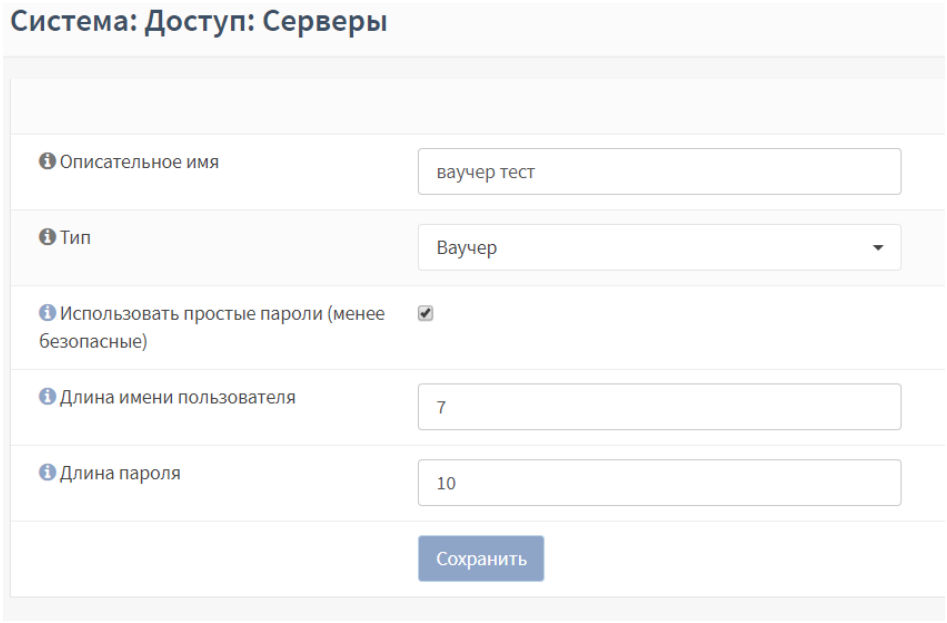



**Рисунок 25 — Ваучер-сервер (редактирование)**

Для использования ваучер-сервера в Портале авторизации необходимо перейти в раздел меню настройки портала авторизации «Службы» - «Портал авторизации» - «Администрирование» - «Зоны» и нажать на + для создания новой зоны. В «Включить» необходимо поставить флажок для включения редактируемой зоны Портала авторизации. В поле «Интерфейсы» выбрать интерфейсы, для которых необходимо включить Портал авторизации. В поле «Аутентификация через» выбрать созданный ваучер сервер. В поле «Описание» необходимо ввести описание и нажать «Сохранить». Далее необходимо перейти в «Службы» - «Портал авторизации» - «Ваучеры» и нажать на кнопку «Создать

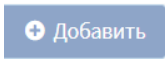
Ваучеры». При нажатии на кнопку «Создать Ваучеры» ПК «InfoWatch ARMA Industrial Firewall» создаст ваучер и автоматически скачает его в формате «.CSV». Скаченный ваучер позволяет успешно аутентифицироваться через Портал авторизации.

### 4.1.3. LDAP

Для аутентификации пользователей, ПК «InfoWatch ARMA Industrial Firewall» поддерживает использование внешнего LDAP-сервера. При использовании LDAP для графического веб-интерфейса необходимо определить необходимые привилегии пользователей, для чего требуется импорт пользовательских учетных записей из источника LDAP-сервера.

Для настройки внешнего LDAP-сервера для ПК «InfoWatch ARMA Industrial Firewall» необходимо иметь сетевой доступ к такому серверу. Далее приводятся шаги по настройке и использованию внешнего LDAP-сервера.

**Шаг 1 — Добавление сервера LDAP**

Для добавления сервера LDAP необходимо перейти в раздел настроек серверов аутентификации «Система» - «Доступ» - «Серверы» и нажать 

в верхнем правом углу, после чего необходимо заполнить поля в соответствии с таблицей (таблица 6).

**Таблица 6 — Добавление сервера LDAP**

| Поле | Значение | Комментарий |
|---|---|---|
| Название | ws2012 | Название сервера |
| Тип | LDAP | - |
| Имя хоста или IP-адрес | 10.10.2.1 | IP-адрес сервера LDAP |
| Значение порта | 389 | Номер порта, 389 по |

| | | |
|---|---|---|
| | | умолчанию |
| Транспортный протокол | TCP — стандартный | Стандартный или Зашифрованный |
| Центр сертификации пиров | Не выбрано | При использовании SSL-шифрования необходимо выбрать CA |
| Версия протокола | 3 | - |
| Привязать параметры доступа | Уникальное имя пользователя = arma@opc.local, пароль = TVKLcWM6 | - |
| Область поиска | Целое поддерево | - |
| Базовый DN: | DC = opc, DC = local | - |
| Контейнеры аутентификации | Выбрать | Необходимо нажать кнопку «Выбрать» и выбрать группы пользователей из списка, например, «CN=Users,DC=opc,DC=local» (Рисунок 26) |
| Расширенный запрос | - | Расширить запрос, ограничить результаты для лиц |

| | | |
|---|---|---|
| Начальный шаблон | Microsoft AD | Тип сервера LDAP |
| Атрибут присвоения имени пользователя | SamAccountName | Автозаполнение на основе начального шаблона |

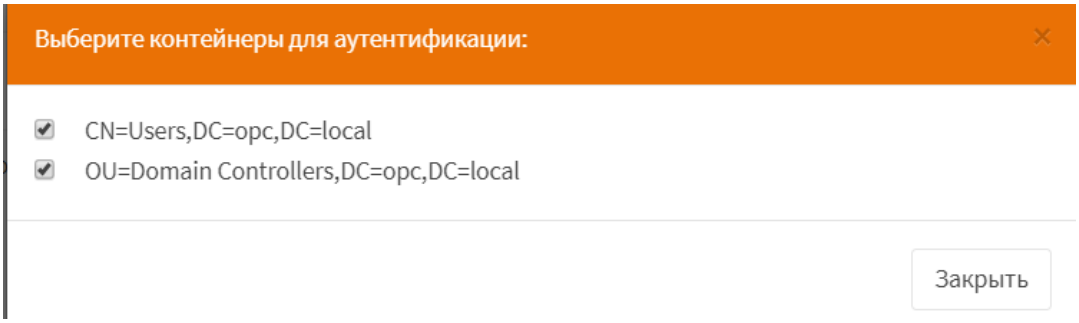



**Рисунок 26 — Контейнеры для аутентификации**

После внесения изменений необходимо нажать кнопку «Сохранить» для сохранения настроек (рисунок 27, рисунок 28)

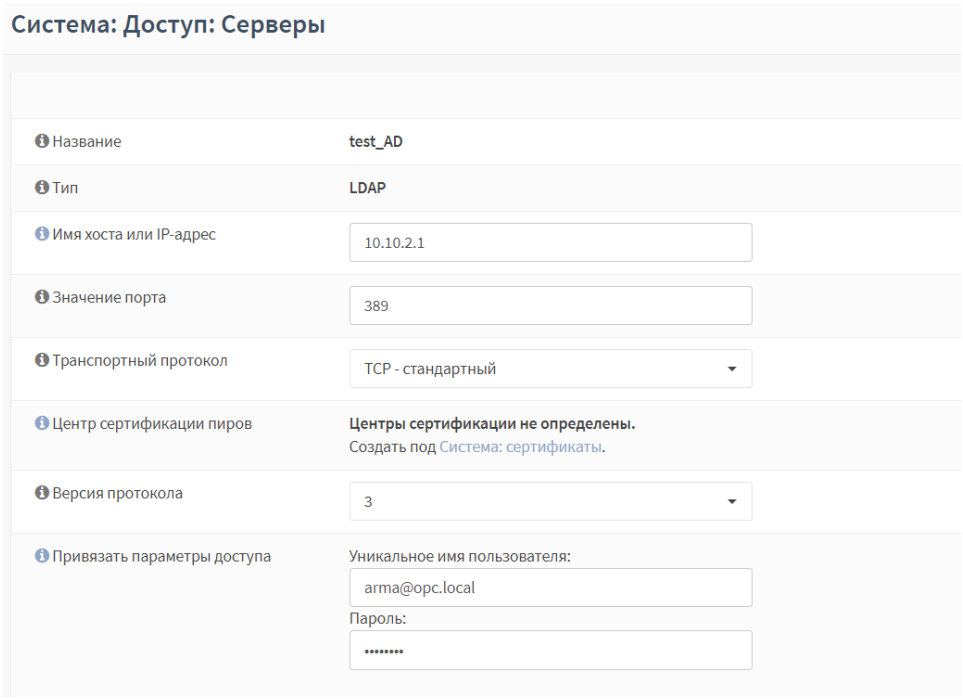



**Рисунок 27 — Настройка Active Directory LDAP-сервера (1)**

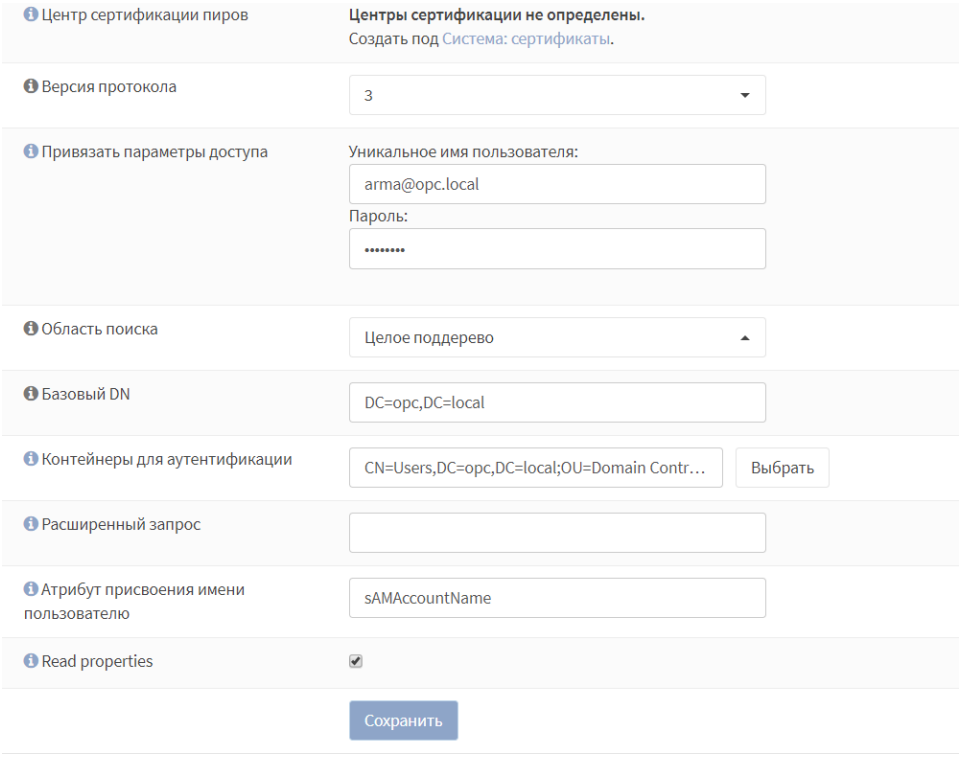



**Рисунок 28 — Настройка Active Directory LDAP-сервера (2)**

## Шаг 2 — Тест

Для проверки правильности настройки сервера необходимо перейти в раздел меню настроек серверов аутентификации «Система» - «Доступ» - «Средство проверки». В поле «Сервер аутентификации» необходимо выбрать созданный на шаге 1 LDAP-сервер и ввести существующие пользовательские учетные данные, например, «arma», в поле «Имя пользователя» и пароль, например, «TVKLcWM6», в поле «Пароль». Для проверки правильности настройки сервера необходимо нажать кнопку «Проверка», если настройка сервера корректна, появится уведомление об успешной проверке (рисунок 29).


**Рисунок 29 — Успешная аутентификация**

В ином случае (или если введены неверные учетные данные), будет отображена ошибка (рисунок 30).

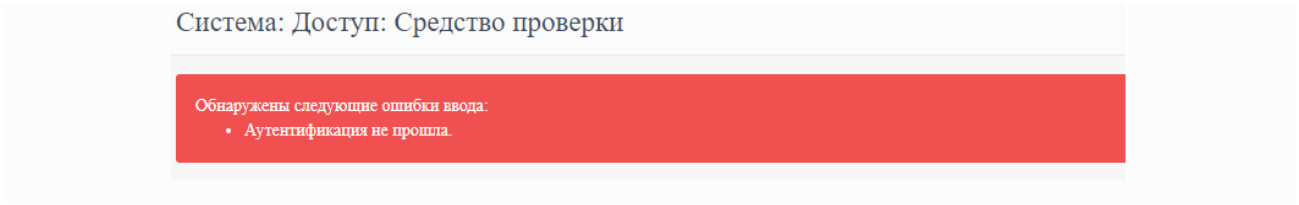



**Рисунок 30 — Ошибка аутентификации**

Также подключение можно проверить через консольное меню интерфейсе ПК «InfoWatch ARMA Industrial Firewall» выбрать пункт меню "8)" и ввести:

– ldapsearch -W -h 10.10.2.1 -D "uid=arma,dc=opc,dc=local" -b "dc=example,dc=com".

И ввести пароль. В случае успешной аутентификации появится сообщение об этом.

**Шаг 3 — Импорт пользовательских учетных записей**

Для предоставления доступа к графическому веб-интерфейсу пользовательским учетным записям LDAP-сервера, необходимо их импортировать. В разделе меню настроек пользователей «Система» - «Доступ» - «Пользователи», появится значок импорта  в правом нижнем углу формы (рисунок 31).

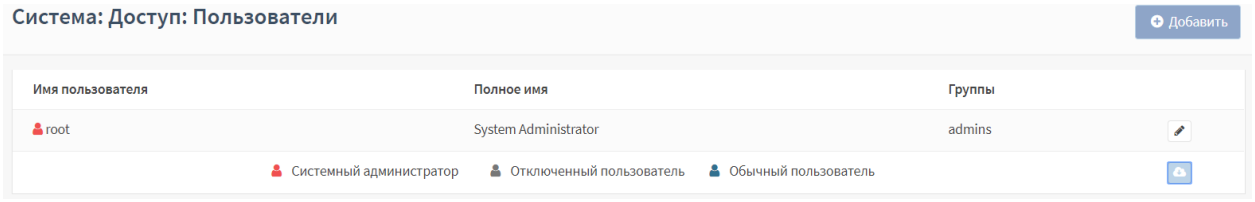



**Рисунок 31 — Импорт пользовательских учетных записей**

Необходимо нажать на значок импорта, чтобы импортировать пользовательские учетные записи (рисунок 32). Импорт произведен успешно, если после нажатия кнопки не появилось сообщений об ошибке.

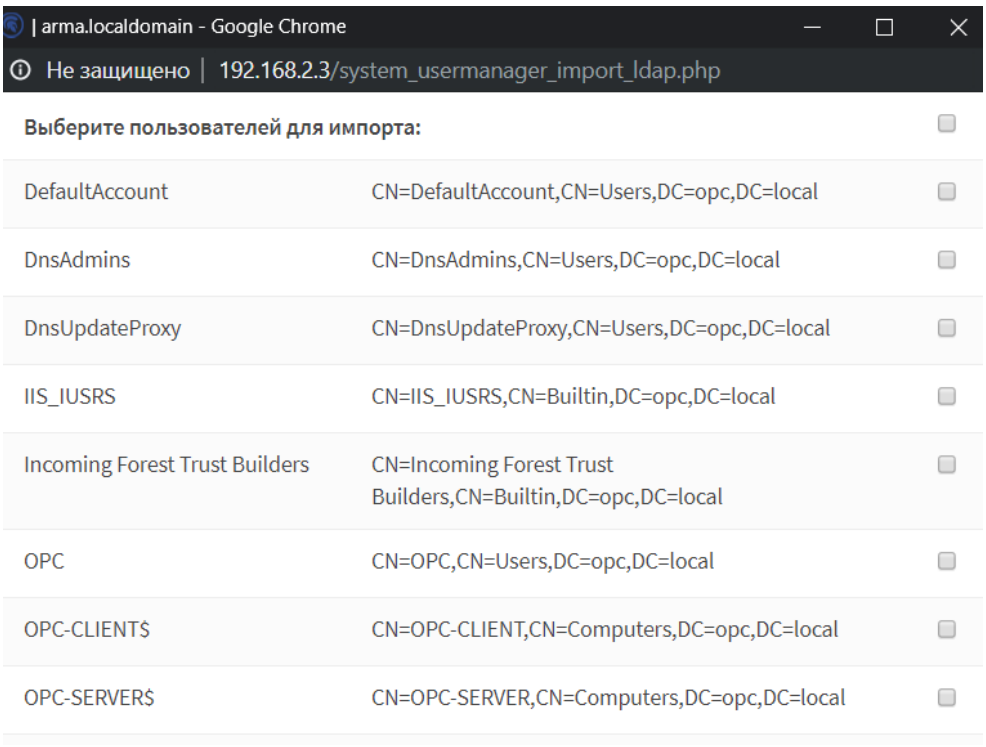



**Рисунок 32 — Выбор импортируемых пользовательских учетных записей**

**Шаг 4 — Обновление пользовательской учетной записи LDAP**

Далее необходимо перейти в раздел меню настроек пользователей «Система» - «Доступ» - «Пользователи». Необходимо убедиться, что в данном разделе будут отображены все учетные записи, включая импортированные из LDAP-сервера.

**Шаг 5 — Обновление настроек доступа к системе**

На данном шаге необходимо изменить настройки по умолчанию, чтобы пользовательские учетные записи LDAP получили доступ к системе.

В разделе меню настроек ПК «InfoWatch ARMA Industrial Firewall» «Система» - «Настройки» - «Администрирование» необходимо изменить сервер аутентификации на подключенный сервер LDAP в пункте «Сервер». После внесения изменений для сохранения настроек необходимо нажать кнопку «Сохранить».

### 4.1.4. Radius

Для аутентификации пользователей, ПК «InfoWatch ARMA Industrial Firewall» также поддерживает использование внешнего Radius -сервера.

Для добавления сервера Radius необходимо перейти в раздел настроек серверов аутентификации ПК «InfoWatch ARMA Industrial Firewall» «Система» - «Доступ» - «Серверы» и нажать Добавить в верхнем правом углу, после чего необходимо заполнить появившиеся поля (рисунок 33). В поле «Название» необходимо ввести название сервера, в поле «Тип» необходимо выбрать «Radius», в поле «Имя хоста или IP» необходимо ввести IP-адрес Radius сервера, в поле «Общий секретный ключ» необходимо ввести секретный ключ, в поле «Предложенные службы» необходимо выбрать «Аутентификация» или «Аутентификация и учет», в поле «Значение порта аутентификации» необходимо выбрать порт сервера Radius, в поле «Значение порта учета» необходимо ввести порт для учета, в поле «Тайм-аут аутентификации» необходимо ввести значение времени в секундах, за которое сервер RADIUS отвечает на запрос аутентификации, если поле оставлено пустым, то значение по умолчанию равно 5 секундам.

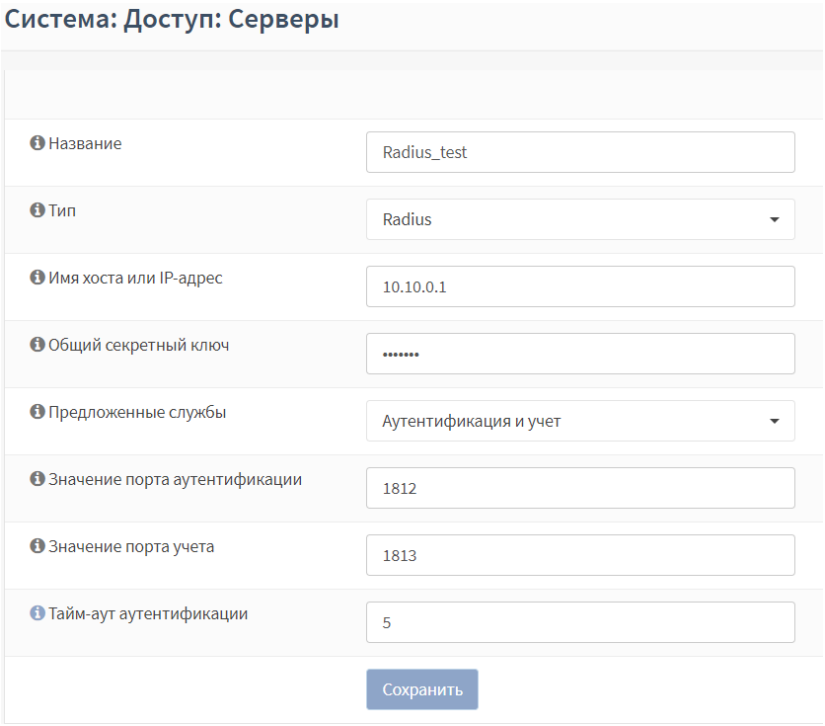



**Рисунок 33 — Настройка Radius**

После внесения изменений необходимо нажать кнопку «Сохранить».

Для тестирования правильности настройки Radius-сервера необходимо перейти в раздел меню настроек серверов аутентификации «Система» - «Доступ»

- «Средство проверки». В поле «Сервер аутентификации» необходимо выбрать созданный ранее сервер. В поле «Имя пользователя» необходимо ввести существующую пользовательскую учетную запись Radius-сервера. В поле «Пароль» необходимо ввести пароль без пробелов и нажать кнопку «Проверка», если настройка сервера правильная, появится уведомление об успешной проверке (рисунок 29).

Если введены некорректные данные или Radius-сервер настроен неправильно, будет отображена ошибка (рисунок 30).

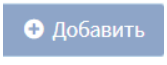
### 4.1.5. Двухфакторная аутентификация

Двухфакторная аутентификация в ПК «InfoWatch ARMA Industrial Firewall» — это аутентификация, при которой пользователь вводит помимо своего постоянного пароля от локальной учетной записи, ещё и временный одноразовый пароль (Time-based One-Time Password).

Для генерации одноразовых паролей ПК «InfoWatch ARMA Industrial Firewall» поддерживает RFC 6238. Для поддержки двухфакторной аутентификации используются мобильные приложения, совместимые с RFC 6238.

Ниже описаны шаги настройки и использования двухфакторной аутентификации.

**Шаг 1 — Добавление сервера аутентификации**

Для добавления сервера двухфакторной аутентификации, в настройках ПК «InfoWatch ARMA Industrial Firewall» необходимо перейти в раздел меню настроек серверов аутентификации «Система» - «Доступ» - «Серверы» и нажать 

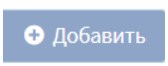
в верхнем правом углу. Далее необходимо заполнить поля в соответствии с таблицей (таблица 7).

**Таблица 7 — Добавление сервера аутентификации**

| Поле | Значение | Комментарий |
|---|---|---|
| Название | Сервер TOTP | Необходимо ввести название сервера |
| Тип | Локальный + Синхронизованный по времени одноразовый пароль | - |
| Длина токена | 6 | - |
| Интервал времени | - | - |
| Разрешенный период регистрации | - | - |
| Обратный порядок токена | Не выбрано | - |

После внесения изменений необходимо нажать кнопку «Сохранить».

**Шаг 2 — Добавление или настройка пользовательской учетной записи**

Для добавления пользовательской учетной записи необходимо перейти в раздел меню настроек пользователей «Система» - «Доступ» - «Пользователи» и нажать 

в правом верхнем углу.

В поле «Имя пользователя» необходимо ввести имя учетной записи и в поле «Пароль» ввести пароль учетной записи. Затем в «Выдача одноразовых паролей» поставьте флажок «Сгенерировать новый ключ (160 бит)».

После внесения изменений необходимо нажать кнопку «Сохранить».

**Шаг 3 — Активация одноразовый пароль**

Для активации нового одноразового пароля, необходимо перейти в режим редактирования созданной на шаге 2 пользовательской учетной записи. Для этого необходимо нажать на значок «Редактирование» напротив соответствующей учетной записи. В режиме редактирования необходимо нажать на кнопку «Нажмите, чтобы показать» напротив «OTP QR код» (рисунок 34).

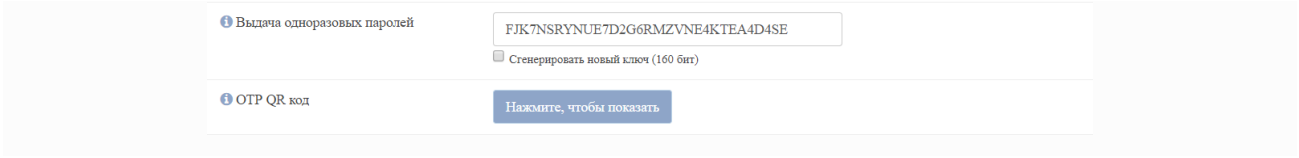



**Рисунок 34 — Активизация одноразового пароля**

После нажатия появится QR-код. Указанный код по безопасному коммуникационному каналу необходимо передать соответствующему пользователю.

При невозможности передачи кода, администратор может выслать пользователю одноразовый пароль, указанный в поле «Выдача одноразовых паролей» (рисунок 34).

Далее пользователю на мобильном устройстве, подключенном к сети Интернет, необходимо открыть определенное администратором приложение, например, FreeOTP для ОС Android (https://freeotp.github.io/) и отсканировать QR-код или, при необходимости, ввести одноразовый пароль, ).

После сканирования QR-кода в приложении мобильного устройства откроется окно, где будут представлен результат сканирования и распознавания кода, - тот же одноразовый пароль. Необходимо подтвердить правильность сканирования QR-кода. Далее откроется окно, в котором будет указан токен.

**Шаг 4 — Проверка токена**

Для тестирования аутентификации пользователя, в настройках ПК

«InfoWatch ARMA Industrial Firewall» необходимо перейти в раздел меню «Система» - «Доступ» - «Средство проверки». В поле «Сервер аутентификации» необходимо выбрать созданный на Шаге 1 сервер и ввести существующую пользовательскую учетную запись в поле «Имя пользователя», далее ввести полученный пользователем токен в поле «Токен» и пароль в поле «Пароль». Для проверки правильности настройки сервера необходимо нажать кнопку «Проверка», если настройка сервера правильная, то появится уведомление об успешной проверке (рисунок 29).

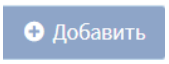
В ином случае (или если введены некорректные учетные данные), будет показана ошибка (рисунок 30).

## 4.2. Пользовательские учетные записи, группы и привилегии

Для пользовательской учетной записи или определенной группы пользователей можно определить набор привилегий используя локальную базу пользователей, в том числе в сочетании с внешним сервером проверки подлинности. Назначить привилегии пользовательской учетной записи можно при создании или редактировании пользовательской учетной записи (см. подраздел 4.3). Назначить привилегии группе пользователей также можно при создании и редактировании группы пользователей (см. подраздел 4.4).

Системные учетные записи, используемые в различных целях на уровне ОС создаются по умолчанию при установке ПК «InfoWatch ARMA Industrial Firewall». Системные учетные записи не видны в настройках ПК «InfoWatch ARMA Industrial Firewall» и используются только для обеспечения системных требований, их права не могут быть присвоены пользовательским учетным записям (часть прав доступа являются системной, часть присвоена администратору). Список всех системных учетных записей приведен в Приложении А.

## 4.3. Добавление пользовательских учетных записей и их привилегий

Для добавления пользовательской учетной записи необходимо перейти в раздел меню ПК «InfoWatch ARMA Industrial Firewall «Система» - «Доступ» - «Пользователи» и нажать на кнопку 

в правом верхнем углу формы. В режиме редактирования пользовательской учетной записи ввести имя пользовательской учетной записи в поле «Имя пользователя». В поле «Пароль» ввести пароль и повторить ввод пароля, который будет использоваться при аутентификации. В поле «Полное имя пользователя» необходимо ввести полное имя пользователя. В поле «E-mail» ввести E-mail пользователя. В поле «Предпочтительная целевая страница» ввести адрес домашней страницы, на которую будет перенаправлен пользователь после авторизации в системе. В поле «Оболочка входа» выбрать оболочку консоли при подключении по SSH или к локальной консоли используя учетную запись создаваемого пользователя. В поле «Дата окончания срока действия данного пользователя» ввести дату окончания срока действия данной пользовательской учетной записи. В поле «Членство в группе» добавить пользователя в существующую(-ие) группы пользователей. В поле «Сертификат» создать сертификат пользователя, нажав на флажок напротив данного поля. В поле «Выдача одноразовых паролей» сгенерировать одноразовый пароль (например, при использовании двухфакторной аутентификации), нажав на флажок напротив «Сгенерировать одноразовый новый ключ (160 бит)». В поле «Авторизованные ключи» ввести ssh-ключи (рисунок 35, рисунок 36).

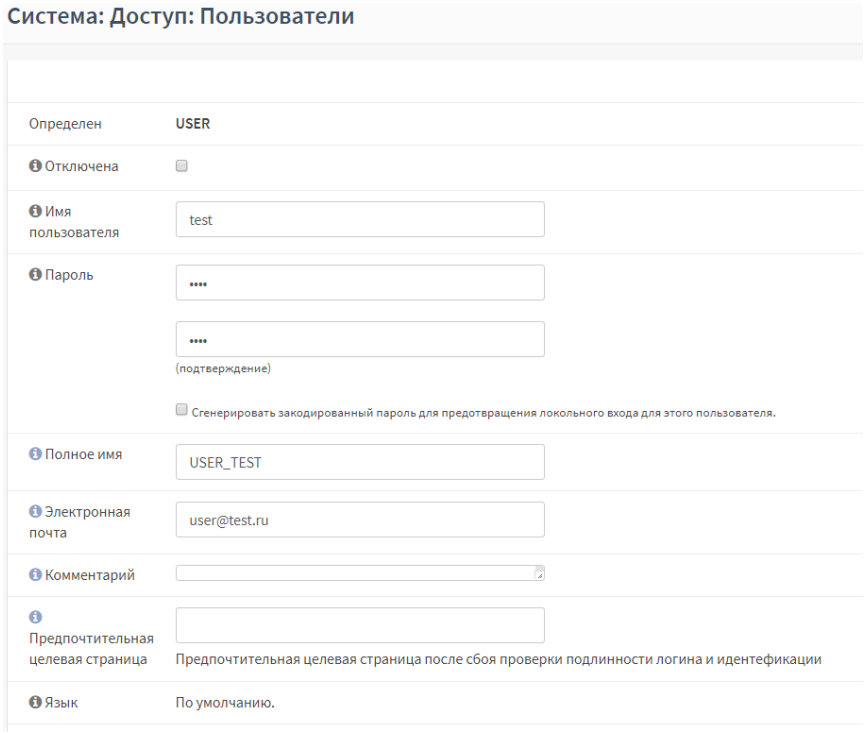



**Рисунок 35 — Создание пользовательской учетной записи (часть 1)**

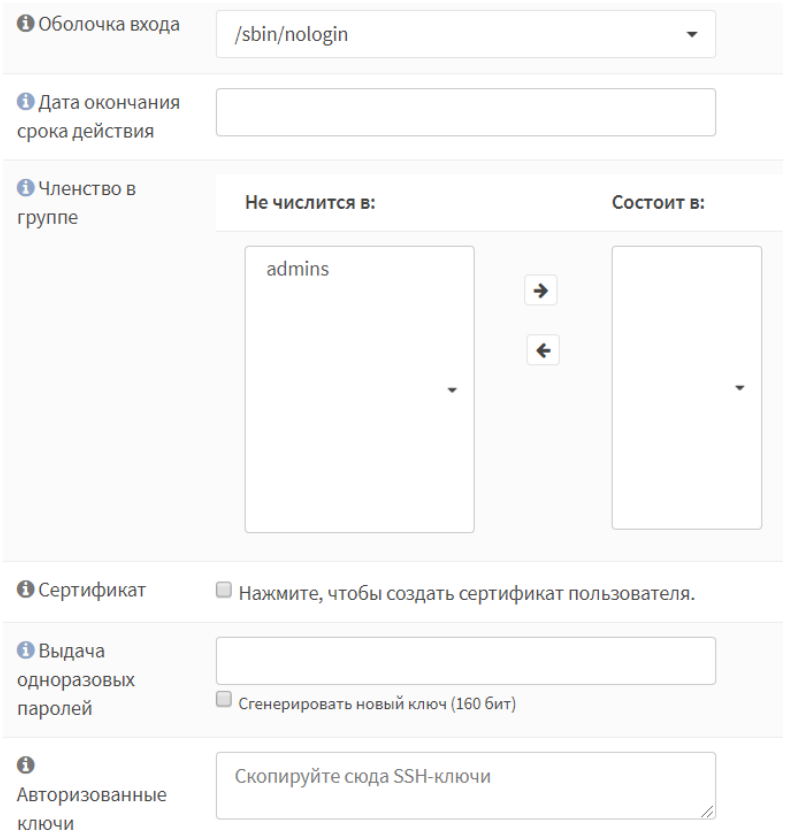



**Рисунок 36 — Создание пользовательской учетной записи (часть 2)**

Для определения привилегий пользовательской учетной записи необходимо сохранить изменения нажатием кнопки «Сохранить» и войти в

редактирование пользовательской учетной записи, для которой необходимо установить привилегии. Для этого необходимо перейти в раздел меню настроек пользователей «Система» - «Доступ» - «Пользователи» и нажать на значок «Редактировать»  напротив нужной пользовательской учетной записи. В поле «Действующие привилегии» необходимо нажать на значок «Редактировать»  для редактирования привилегий. В появившимся окне необходимо выбрать страницы, доступ к которым пользователю будет разрешен и нажать кнопку «Сохранить» (рисунок 37):

- доступ к сервисным AJAX (Get Service Providers);
- доступ к сервисным AJAX (Get Starts);
- все страницы;
- Инструментальная панель (все);
- Инструментальная панель (только виджеты);
- Интерфейсы: Диагностика: Сканирование ARP;
- Интерфейсы: Диагностика: ARP-таблица;
- Система: Доступ: Средство проверки;
- Система: Конфигурация: Резервное копирование;
- Система: Конфигурация: История изменений;
- Система: Конфигурация: Значение по умолчанию;
- Система: Питание: Выключение;
- Межсетевой экран: Ограничитель трафика: Статус;
- Службы: DHCPv4: Журнал;
- Межсетевой экран: Журналы: В реальном времени;
- Межсетевой экран: Журналы: Журнал pflog;
- Межсетевой экран: Журналы: Обзор;
- Система: Шлюзы: Журнал;
- Система: Настройки: Журналирование;
- Система: Журналы: Общие настройки;
- Интерфейсы: Диагностика: NDP-таблица;

- Анализ: Netflow;
- Анализ: Анализ Netflow;
- Интерфейсы: Диагностика: Захват пакетов;
- Межсетевой экран: Диагностика: pfTables;
- Межсетевой экран: Диагностика: pfInfo;
- Межсетевой экран: Диагностика: pfTop;
- Интерфейсы: Диагностика: Ping;
- Система: Питание: Перезагрузка;
- Межсетевой экран: Диагностика: Сброс состояний;
- Система: Маршруты: Статус;
- Межсетевой экран: Диагностика: Снимок состояний;
- Межсетевой экран: Диагностика: Сокеты;
- Межсетевой экран: Диагностика: Сводка состояний;
- Система: Диагностика: Активность;
- Анализ: Состояние;
- Интерфейсы: Диагностика: Проверка порта;
- Интерфейсы: Диагностика: Trace route;
- Межсетевой экран: Псевдонимы: Вид: Добавление правила;
- Межсетевой экран: Псевдонимы;
- Межсетевой экран: NAT: Один к одному;
- Межсетевой экран: NAT: Один к одному: Добавление правила;
- Межсетевой экран: NAT: NPTv6;
- Межсетевой экран: NAT: NPTv6: Добавление правила;
- Межсетевой экран: NAT: Исходящий;
- Межсетевой экран: NAT: Исходящий: Добавление правила;
- Межсетевой экран: NAT: Переадресация портов;
- Межсетевой экран: NAT: Переадресация портов: Добавление правила;
- Межсетевой экран: Настройки: Нормализация;
- Межсетевой экран: Правила;

– Межсетевой экран: Правила: Добавление правила;
– Межсетевой экран: Настройки: Расписания;
– Межсетевой экран: Настройки: Расписания: Добавление нового расписания;
– Межсетевой экран: Ограничитель трафика;
– Межсетевой экран: Виртуальные IP-адреса: Настройки: Добавление нового IP-адреса;
– Межсетевой экран: Виртуальные IP-адреса;
– Обнаружение вторжений: Администрирование;
– Обнаружение вторжений: Контроль уровня приложений;
– Обнаружение вторжений: Журнал;
– Интерфейсы: Назначение портов;
– Интерфейсы: Другие типы: Сетевой мост;
– Интерфейсы: Другие типы: Сетевой мост: Добавить интерфейс;
– Интерфейсы: Другие типы: GIF;
– Интерфейсы: Другие типы: GIF: Добавить интерфейс;
– Интерфейсы: Другие типы: GRE;
– Интерфейсы: Другие типы: GRE: Добавить интерфейс;
– Межсетевой экран: Группы;
– Межсетевой экран: Группы: Добавление группы;
– Интерфейсы: Другие типы: LAGG;
– Интерфейсы: Другие типы: LAGG: Добавить интерфейс;
– Интерфейсы: Другие типы: VLAN;
– Интерфейсы: Другие типы: VLAN: Добавить интерфейс;
– Интерфейсы: WAN;
– Авторизация, Система: Питание: Выход, Инструментальная панель;
– Блокирование прав на аутентификацию в проксисервере;
– Службы: Портал авторизации;
– Службы: DHCPv4: Ретрансляция;
– Службы: DHCPv4;

– Службы: DHCPv4: Добавление статической маршрутизации через DHCPv4;
– Службы: DHCPv6: Ретрансляция;
– Службы: DHCPv6;
– Службы: DHCPv6: Добавление статической маршрутизации через DHCPv6;
– Система: Настройки: SNMP;
– Службы: Синхронизация времени;
– Службы: Прокси;
– Система: Маршруты: Конфигурация;
– Сеть: Анализ трафика;
– Межсетевой экран: Виртуальные IP-адреса: Статус;
– Службы: DHCPv4: Аренда адресов;
– Службы: DHCPv6: Аренда адресов;
– Система: Уровень высокой доступности: Статус;
– Интерфейсы: Обзор;
– Службы: Синхронизация времени: Статус;
– Службы: Синхронизация времени: GPS-приемник;
– Службы: Синхронизация времени: PPS;
– Система: Диагностика: Службы;
– Службы: Портал авторизации: Журнал;
– Службы: Синхронизация времени: Журнал;
– Система: Маршруты: Журнал;
– Анализ: Трафик;
– Система: Мастер;
– Доступ администратора ко всем страницам;
– Межсетевой экран;
– Система: Настройки: Прочее;
– Интерфейсы: Настройки;
– Система: Настройки: Параметры;
– Система: Доступ: Серверы;

- Система: Доверенные сертификаты: Полномочия;
- Система: Доверенные сертификаты;
- Система: Прошивка: Средство создания отчетов;
- Система: Доверенные сертификаты: Отзыв сертификатов;
- Просматривать конфигурационные файлы, но не изменять;
- Система: Шлюзы: Группы;
- Система: Шлюзы;
- Система: Шлюзы: Единичный: Добавление шлюза;
- Система: Шлюзы: Группы: Добавление группы шлюзов;
- Система: Настройки: Общие настройки;
- Система: Доступ: Группы;
- Система: Доступ: Группы: Добавление привилегий;
- Система: Уровень высокой доступности;
- Система: Настройки: Планировщик задач Cron;
- Система: Маршруты;
- Система: Доступ: Пользователи;
- Система: Доступ: Пользователи: Добавление привилегий;
- Система: Доступ: Серверы: Установка сложности паролей;
- Обнаружение вторжений: Контроль уровня приложений;
- Система: Прошивка: Контроль целостности;
- Службы: Monit;
- Возможность правки служб запросов по протоколу XMLRPC;
- Маршрутизация;
- Возможность очистки журнала Syslog;
- Возможность очистки журнала Backend;
- Возможность очистки журнала событий веб-интерфейса;
- Возможность очистки журнала изменения настроек шлюза;
- Возможность очистки журнала маршрутизации;
- Возможность очистки журнала системных событий;

– Возможность очистки журнала событий безопасности;
– Возможность очистки журнала необработанных событий от pf;
– Возможность очистки журнала Портала авторизации;
– Возможность очистки журнала DHCPv4;
– Возможность очистки журнала системы обнаружения вторжений;
– Возможность очистки журнала инцидентов системы обнаружения вторжений;
– Возможность очистки журнала NTP;
– Возможность очистки журнала прокси-сервера (Кэш);
– Возможность очистки журнала прокси-сервера (Доступ).

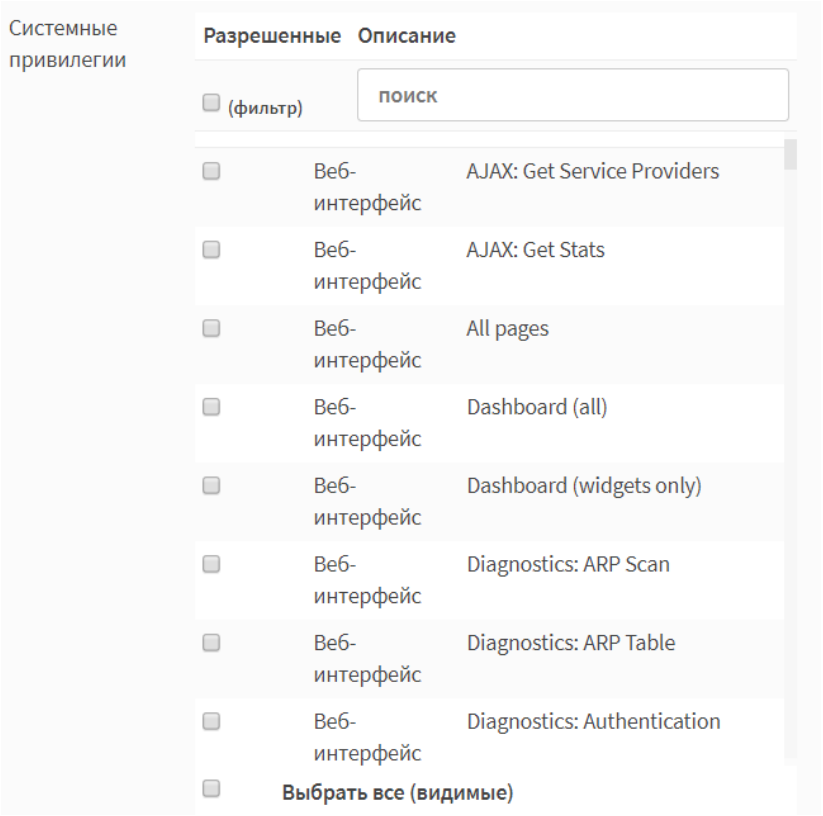
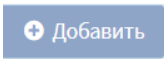



**Рисунок 37 — Привилегии пользовательской учетной записи**

## 4.4. Создание группы и добавление им привилегий

Для создания группы пользователей необходимо перейти в раздел меню настроек групп пользователей «Система» - «Доступ» - «Группы» и нажать

кнопку 

в правом верхнем углу формы.

В поле «Имя группы» необходимо ввести название группы. В поле «Описание» необходимо ввести описание группы пользователей. В поле «Членство в группе» необходимо выбрать из правого окна пользователя, нажать на него, далее нажать на стрелку  , чтобы добавить пользователя к создаваемой группе. После внесения изменений необходимо нажать кнопку «Сохранить», чтобы сохранить изменения (рисунок 38).

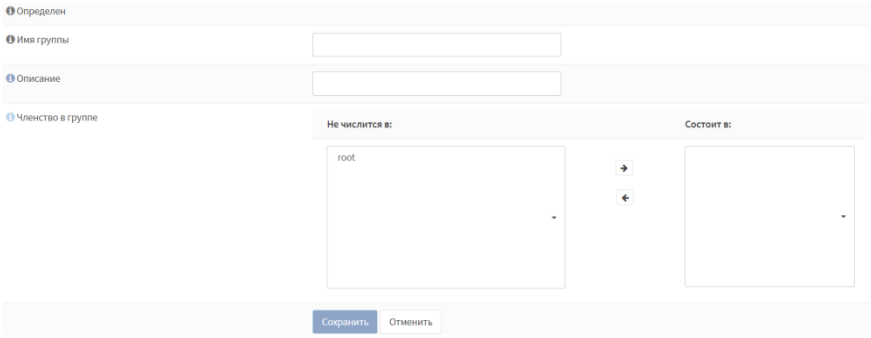



**Рисунок 38 — Создание группы пользователей**

Для изменения привилегий группы пользователей необходимо перейти в раздел меню настроек групп пользователей «Система» - «Доступ» - «Группы» и нажать на значок «Редактировать»  напротив группы, которой необходимо добавить привилегии. В поле «Действующие привилегии» необходимо нажать на значок «Редактировать»  . В появившимся окне необходимо выбрать страницы, доступ к которым группам пользователей будет разрешен. Для сохранения изменений необходимо нажать кнопку «Сохранить» (рисунок 39):

- доступ к сервисным AJAX (Get Service Providers);
- доступ к сервисным AJAX (Get Starts);
- все страницы;
- Инструментальная панель (все);
- Инструментальная панель (только виджеты);
- Интерфейсы: Диагностика: Сканирование ARP;
- Интерфейсы: Диагностика: ARP-таблица;
- Система: Доступ: Средство проверки;

– Система: Конфигурация: Резервное копирование;
– Система: Конфигурация: История изменений;
– Система: Конфигурация: Значение по умолчанию;
– Система: Питание: Выключение;
– Межсетевой экран: Ограничитель трафика: Статус;
– Службы: DHCPv4: Журнал;
– Межсетевой экран: Журналы: В реальном времени;
– Межсетевой экран: Журналы: Журнал pflog;
– Межсетевой экран: Журналы: Обзор;
– Система: Шлюзы: Журнал;
– Система: Настройки: Журналирование;
– Система: Журналы: Общие настройки;
– Интерфейсы: Диагностика: NDP-таблица;
– Анализ: Netflow;
– Анализ: Анализ Netflow;
– Интерфейсы: Диагностика: Захват пакетов;
– Межсетевой экран: Диагностика: pfTables;
– Межсетевой экран: Диагностика: pfInfo;
– Межсетевой экран: Диагностика: pfTop;
– Интерфейсы: Диагностика: Ping;
– Система: Питание: Перезагрузка;
– Межсетевой экран: Диагностика: Сброс состояний;
– Система: Маршруты: Статус;
– Межсетевой экран: Диагностика: Снимок состояний;
– Межсетевой экран: Диагностика: Сокеты;
– Межсетевой экран: Диагностика: Сводка состояний;
– Система: Диагностика: Активность;
– Анализ: Состояние;
– Интерфейсы: Диагностика: Проверка порта;

- Интерфейсы: Диагностика: Trace route;
- Межсетевой экран: Псевдонимы: Вид: Добавление правила;
- Межсетевой экран: Псевдонимы;
- Межсетевой экран: NAT: Один к одному;
- Межсетевой экран: NAT: Один к одному: Добавление правила;
- Межсетевой экран: NAT: NPTv6;
- Межсетевой экран: NAT: NPTv6: Добавление правила;
- Межсетевой экран: NAT: Исходящий;
- Межсетевой экран: NAT: Исходящий: Добавление правила;
- Межсетевой экран: NAT: Переадресация портов;
- Межсетевой экран: NAT: Переадресация портов: Добавление правила;
- Межсетевой экран: Настройки: Нормализация;
- Межсетевой экран: Правила;
- Межсетевой экран: Правила: Добавление правила;
- Межсетевой экран: Настройки: Расписания;
- Межсетевой экран: Настройки: Расписания: Добавление нового расписания;
- Межсетевой экран: Ограничитель трафика;
- Межсетевой экран: Виртуальные IP-адреса: Настройки: Добавление нового IP-адреса;
- Межсетевой экран: Виртуальные IP-адреса;
- Обнаружение вторжений: Администрирование;
- Обнаружение вторжений: Контроль уровня приложений;
- Обнаружение вторжений: Журнал;
- Интерфейсы: Назначение портов;
- Интерфейсы: Другие типы: Сетевой мост;
- Интерфейсы: Другие типы: Сетевой мост: Добавить интерфейс;
- Интерфейсы: Другие типы: GIF;
- Интерфейсы: Другие типы: GIF: Добавить интерфейс;
- Интерфейсы: Другие типы: GRE;

– Интерфейсы: Другие типы: GRE: Добавить интерфейс;
– Межсетевой экран: Группы;
– Межсетевой экран: Группы: Добавление группы;
– Интерфейсы: Другие типы: LAGG;
– Интерфейсы: Другие типы: LAGG: Добавить интерфейс;
– Интерфейсы: Другие типы: VLAN;
– Интерфейсы: Другие типы: VLAN: Добавить интерфейс;
– Интерфейсы: WAN;
– Авторизация, Система: Питание: Выход, Инструментальная панель;
– Блокирование прав на аутентификацию в проксисервере;
– Службы: Портал авторизации;
– Службы: DHCPv4: Ретрансляция;
– Службы: DHCPv4;
– Службы: DHCPv4: Добавление статической маршрутизации через DHCPv4;
– Службы: DHCPv6: Ретрансляция;
– Службы: DHCPv6;
– Службы: DHCPv6: Добавление статической маршрутизации через DHCPv6;
– Система: Настройки: SNMP;
– Службы: Синхронизация времени;
– Службы: Прокси;
– Система: Маршруты: Конфигурация;
– Сеть: Анализ трафика;
– Межсетевой экран: Виртуальные IP-адреса: Статус;
– Службы: DHCPv4: Аренда адресов;
– Службы: DHCPv6: Аренда адресов;
– Система: Уровень высокой доступности: Статус;
– Интерфейсы: Обзор;
– Службы: Синхронизация времени: Статус;
– Службы: Синхронизация времени: GPS-приемник;

- Службы: Синхронизация времени: PPS;
- Система: Диагностика: Службы;
- Службы: Портал авторизации: Журнал;
- Службы: Синхронизация времени: Журнал;
- Система: Маршруты: Журнал;
- Анализ: Трафик;
- Система: Мастер;
- Доступ администратора ко всем страницам;
- Межсетевой экран;
- Система: Настройки: Прочее;
- Интерфейсы: Настройки;
- Система: Настройки: Параметры;
- Система: Доступ: Серверы;
- Система: Доверенные сертификаты: Полномочия;
- Система: Доверенные сертификаты;
- Система: Прошивка: Средство создания отчетов;
- Система: Доверенные сертификаты: Отзыв сертификатов;
- Просматривать конфигурационные файлы, но не изменять;
- Система: Шлюзы: Группы;
- Система: Шлюзы;
- Система: Шлюзы: Единичный: Добавление шлюза;
- Система: Шлюзы: Группы: Добавление группы шлюзов;
- Система: Настройки: Общие настройки;
- Система: Доступ: Группы;
- Система: Доступ: Группы: Добавление привилегий;
- Система: Уровень высокой доступности;
- Система: Настройки: Планировщик задач Cron;
- Система: Маршруты;
- Система: Доступ: Пользователи;

- Система: Доступ: Пользователи: Добавление привилегий;
- Система: Доступ: Серверы: Установка сложности паролей;
- Обнаружение вторжений: Контроль уровня приложений;
- Система: Прошивка: Контроль целостности;
- Службы: Monit;
- Возможность правки служб запросов по протоколу XMLRPC;
- Маршрутизация;
- Возможность очистки журнала Syslog;
- Возможность очистки журнала Backend;
- Возможность очистки журнала событий веб-интерфейса;
- Возможность очистки журнала изменения настроек шлюза;
- Возможность очистки журнала маршрутизации;
- Возможность очистки журнала системных событий;
- Возможность очистки журнала событий безопасности;
- Возможность очистки журнала необработанных событий от pf;
- Возможность очистки журнала Портала авторизации;
- Возможность очистки журнала DHCPv4;
- Возможность очистки журнала системы обнаружения вторжений;
- Возможность очистки журнала инцидентов системы обнаружения вторжений;
- Возможность очистки журнала NTP;
- Возможность очистки журнала прокси-сервера (Кэш);
- Возможность очистки журнала прокси-сервера (Доступ);
- Возможность очистки всех журналов.

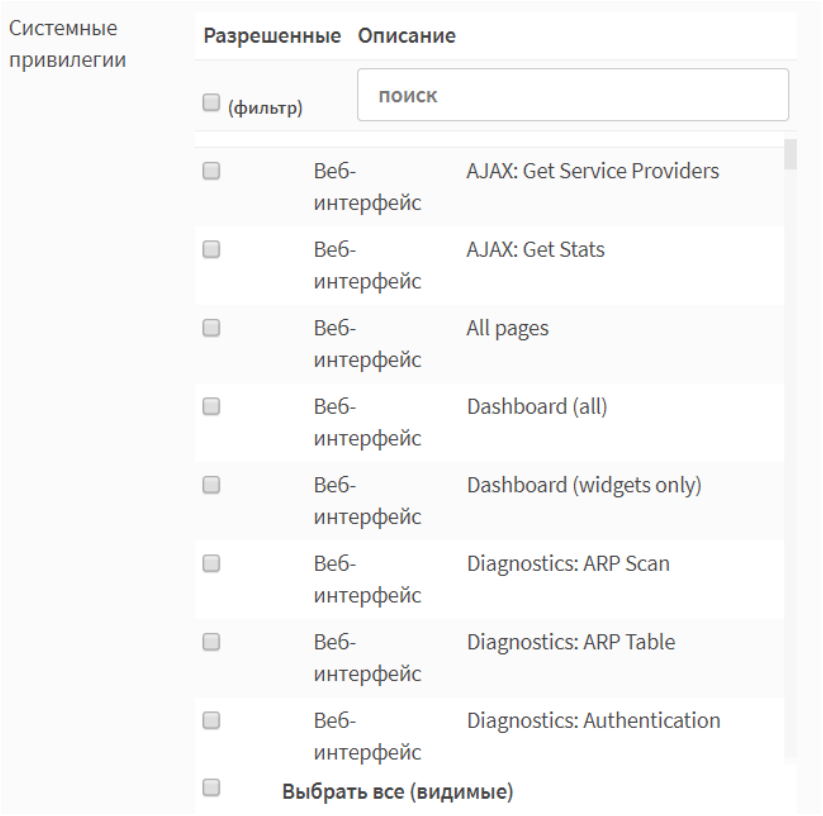



**Рисунок 39 — Привилегии группы пользователей**

# 5. Сервисы

## 5.1. Маршрутизация

ПК «InfoWatch ARMA Industrial Firewall» поддерживает статическую и динамическую маршрутизацию.

**Статическая маршрутизация**

Настройка статической маршрутизации описана в документе Руководство пользователя в разделе 6, подразделе 6.5.

**Динамическая маршрутизация**

Протоколы маршрутизации, используемые в ПК «InfoWatch ARMA Industrial Firewall»:

- OSPF и OSPFv3;
- RIPv1 и RIPv2;
- BGPv4.

Настройка динамической маршрутизации описана в документе Руководство пользователя в разделе 8.

## 5.2. Прокси

Веб-прокси позволяет производить контент-фильтрацию и управление передачи трафика от одного хоста к другому.

Прокси поддерживает ряд методов аутентификации:

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

Настройка прокси-сервера описана в документе Руководство пользователя в разделе 10, подразделе 10.2, 10.17 и в разделе 9, подразделе 9.6.

## 5.3. DHCP

DHCP доступен как для клиентов IPv4, так и для клиентов IPv6. Сервисы называются DHCPv4 и DHCPv6 соответственно.

Настройка DHCP-сервера описана в документе Руководство пользователя в разделе 9, подразделах 9.2, 9.3.

## 5.4. Сервисы мониторинга

### 5.4.1. Syslog

Syslog — стандарт отправки и регистрации сообщений о происходящих в системе событиях. ПК «InfoWatch ARMA Industrial Firewall» формирует текстовые сообщения о происходящих в нем событиях, инцидентах безопасности с точной меткой времени и идентификационными данными ПК «InfoWatch ARMA Industrial Firewall» и передает их на обработку серверу Syslog. Формат событий МЭ — IPFW, формат событий СОВ — Suricata.

Настройка Syslog описана в документе Руководство пользователя в разделе 6, подразделе 6.3.4.

### 5.4.2. SNMP

SNMP позволяет осуществлять удаленный мониторинг состояния ПК «InfoWatch ARMA Industrial Firewall», что позволяет использовать данные о состоянии ПК «InfoWatch ARMA Industrial Firewall» в различных системах мониторинга. Функции удаленного мониторинга SNMP включают:

– регистрация устройств сети, их сетевых адресов и идентификаторов;

– определение параметров сетевой операционной системы и описание конфигурации элементов сети, а также протоколов сетевых взаимодействий;

– графическое отображение схемы сети;

– контроль доступа и управление полномочиями пользователей;

– контроль и управление параметрами межсетевого взаимодействия;

– защита от несанкционированного доступа извне;

– управление целостностью данных (архивированием и энергопитанием);

– регистрация лицензий и учет использования программных средств и сетевых ресурсов;

– управление приоритетами пользователей и прикладных задач;

– поиск, обнаружение, локализация и устранение неисправностей и ошибок;

– предупреждение и профилактика сбоев;

– наблюдение за кабельной системой;

– мониторинг удаленных сегментов и межсетевых связей;

– сбор и анализ статистических данных о функционировании сети, анализ трафика;

– планирование и оценка эффективности использования ресурсов сети;

– анализ и интерпретация протоколов;

– планирование развития сети, управление сегментацией.

Настройка мониторинга по SNMP описана в документе Руководство пользователя в разделе 6, подразделе 6.3.5.

# 6. Описание локального (консольного) интерфейса

Меню локального (консольного) интерфейса отображает 14 параметров показанных в таблице (таблица 8). Это меню доступно после входа в консоль с использованием существующей учетной записи пользователя.

**Таблица 8 — Консольное меню**

| | |
|---|---|
| 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) Update from console | |
| 6) Reboot system | 13) Restore a backup |

Управление в консольном интерфейсе происходит только с использованием клавиатуры. Для выбора одного из пунктов меню необходимо ввести номер этого пункта с клавиатуры и нажать клавишу «ENTER».

## 6.1. Выход из консольного интерфейса

Для выхода из меню и возвращения к форме входа необходимо выбрать пункт меню «0) Logout» (ввести «0» и нажать клавишу «ENTER»).

## 6.2. Назначение сетевых интерфейсов и настройка VLAN

Для ручного назначения соответствия физических и логических сетевых интерфейсов необходимо выбрать пункт меню «1) Assing interfaces» (ввести «1» и нажать клавишу «ENTER»).

В случае если необходимо настроить VLAN для определенного сетевого интерфейса после «Do you want to Configure VLANs now?» необходимо ввести «y» и нажать клавишу «ENTER». После ввода появится список физических сетевых интерфейсов после надписи «VLAN-capable interface» из которого необходимо выбрать сетевой интерфейс для настройки VLAN и ввести его имя (например, em0) после «Enter the parent interface name for the new VLAN (or nothing if

finished):» и нажать клавишу «ENTER» или если необходимо прервать настройку VLAN, то необходимо нажать на кнопку клавишу «ENTER» не вводя имя сетевого интерфейса. После ввода имени сетевого интерфейса необходимо ввести тег VLAN интерфейса, то имеется идентификатор принадлежности трафика к VLAN интерфейсу, после «Enter the VLAN tag (1-4094):» и нажать клавишу «ENTER». Далее в консольном интерфейсе снова отобразится список доступных для настройки VLAN сетевых интерфейсов. Настройки следующих VLAN интерфейсов производятся аналогично настройке первого VLAN интерфейса. По завершении настройки необходимых VLAN интерфейсов и для перехода к настройкам других сетевых интерфейсов необходимо нажать на кнопку клавишу «ENTER» без ввода имени интерфейса после «Enter the parent interface name for the new VLAN (or nothing if finished):» (рисунок 40).

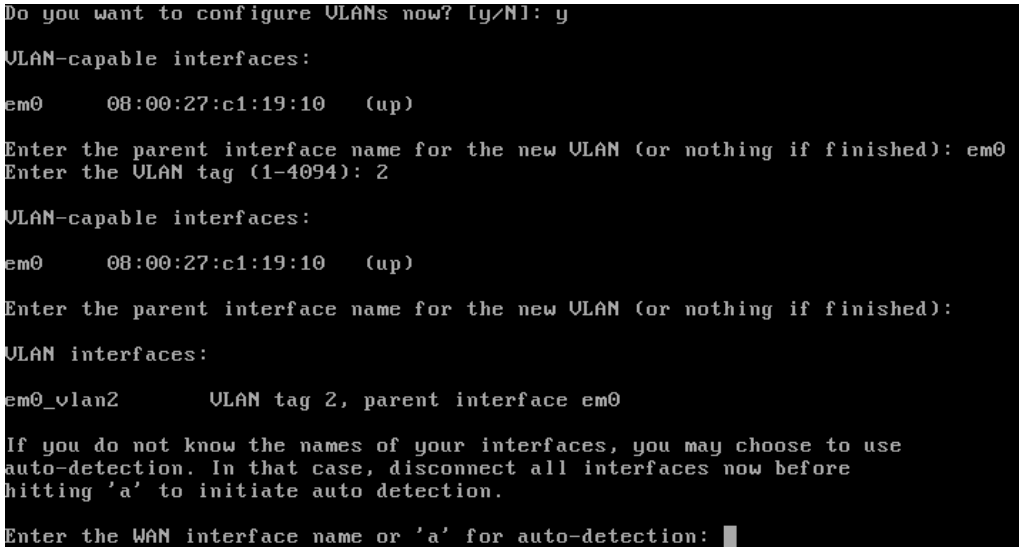



**Рисунок 40 — Настройка VLAN**

Необходимо учитывать, что настройка VLAN является необязательной. Если VLAN не используется, то на запрос «Do you want to Configure VLANs now?» необходимо ввести «n» и нажать клавишу «ENTER».

Каждое из представленных имён сетевых интерфейсов соответствует физическому интерфейсу. Сопоставление физических интерфейсов с именами производится на уровне системы. Далее физическим интерфейсам назначаются соответствующие сетевые интерфейсы в стандартной последовательности:

– WAN — необходимо ввести соответствующее имя физического интерфейса после «Enter the WAN interface name or ‘a’ for auto-detection:», например, «em0», или для автоматической настройки необходимо ввести «a», если нет необходимости настраивать WAN, необходимо нажать на кнопку клавишу «ENTER» (рисунок 41);

– LAN — необходимо ввести соответствующее имя физического интерфейса после «Enter the LAN interface name or ‘a’ for auto-detection:», например, «em1», или для автоматической настройки необходимо ввести «a», если нет необходимости настраивать LAN, необходимо нажать на кнопку клавишу «ENTER» (рисунок 41).

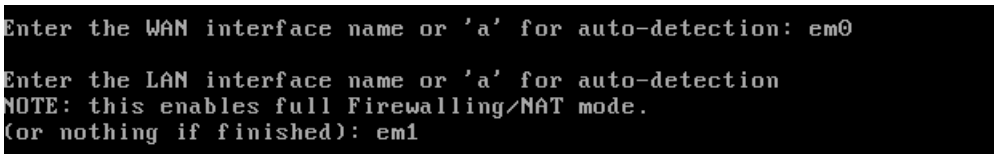



**Рисунок 41 — Настройка интерфейсов**

Если на аппаратной или виртуальной платформе (машине) имеются другие доступные физические интерфейсы, то необходимо по аналогии с выбором предыдущих интерфейсов определить их. Эти интерфейсы назначаются как сетевые интерфейсы с именем OPT ([OPT [номер дополнительного сетевого интерфейса]]). Если назначены все физические интерфейсы, необходимо нажать на кнопку клавишу «ENTER» на вопрос о назначении последующего сетевого интерфейса. Необходимо проверить правильность настройки и подтвердить настройки после сообщения «Do you want proceed?», ввести «y» и нажать клавишу «ENTER». ПК «InfoWatch ARMA Industrial Firewall» настроит физические интерфейсы и представит приглашение для входа в систему по завершении.

## 6.3. Настройка IPv4 адреса

При необходимости настройки IP-адресов на назначенных сетевых интерфейсах необходимо выбрать опцию «2) Set interface(s) IP address».

После выбора пункта меню необходимо выбрать способ задания IPv4-адреса для выбранного интерфейса: с помощью DHCP-сервера или вручную.

Для этого необходимо на вопрос «Configure IPv4 address [Название интерфейса] via DHCP? [y/N]» ввести «y» и нажать клавишу «ENTER» при необходимости задания адреса для выбранного интерфейса с помощью DHCP-сервера (IPv4-адрес будет назначен выбранному интерфейсу автоматически), в противном случае, для задания адреса вручную, необходимо ввести «n» и нажать клавишу «ENTER».

Для настройки IPv4-адреса вручную после вопроса «Enter the new [Название интерфейса] IPv4 address. Press «ENTER» for none:» необходимо ввести IPv4-адрес выбранного интерфейса и нажать клавишу «ENTER». Далее необходимо ввести маску подсети IPv4-адреса (255.255.255.255 = 32, 255.255.255.0 =24, 255.255.0.0 = 16, 255.0.0.0 = 8) после «Enter the new [название интерфейса] IPv4 subnet bit count (1 to 32)» и нажать клавишу «ENTER».

При настройке IPv4-адреса WAN интерфейса имеется возможность выбрать сетевой шлюз. Для этого необходимо ввести сетевой шлюз после «For a WAN, enter the new [Название интерфейса] IPv4 upsteream gateway address» и нажать клавишу «ENTER». При необходимости пропустить настройку сетевого шлюза необходимо нажать на кнопку клавишу «ENTER».

## 6.4. Настройка IPv6 адреса

Для настройки IPv6 адреса после выбора пункта меню «2) Set interface(s) IP address» необходимо выбрать сетевой интерфейс (WAN, LAN, OPT, OPT1 и т.п.), для которого производится настройка IPv6-адреса. Далее необходимо выбрать способ задания IPv6-адреса для выбранного интерфейса: с помощью DHCP-сервера или вручную.

При необходимости задания IPv6-адреса с помощью DHCP-сервера после вопроса «Configure IPv6 address [Название интерфейса] via DHCPv6? [y/N]» необходимо ввести «y» (IPv6-адрес будет назначен выбранному интерфейсу

автоматически) и нажать клавишу «ENTER». Для задания адреса вручную, необходимо ввести «n» и нажать клавишу «ENTER».

Для настройки IPv6-адреса вручную после «Enter the new [Название интерфейса] IPv6 address. Press «ENTER» for none:» необходимо ввести IPv6-адрес выбранного интерфейса и нажать клавишу «ENTER». Далее необходимо ввести маску подсети IPv6-адреса (ffff:ffff:ffff:ffff:ffff:ffff:ffff:ff00 = 120, ffff:ffff:ffff:ffff:ffff:ffff:ffff:0=112, ffff:ffff:ffff:ffff:ffff:ffff:0:0= 96, ffff:ffff:ffff:ffff:ffff:0:0:0= 80, ffff:ffff:ffff:ffff:0:0:0:0= 64) после «Enter the new [название интерфейса] IPv4 subnet bit count (1 to 128)» и нажать клавишу «ENTER».

При настройке IPv6-адреса WAN интерфейса имеется возможность выбрать сетевой шлюз. Для этого необходимо ввести сетевой шлюз после «For a WAN, enter the new [название интерфейса] IPv6 upsteream gateway address» и нажать клавишу «ENTER». При необходимости пропустить настройку сетевого шлюза необходимо нажать на кнопку клавишу «ENTER».

После настройки рекомендуется перезагрузить систему. Для этого необходимо в меню действий выбрать «6) Reboot system» (ввести «6» и нажать клавишу «ENTER»). Для перезагрузки системы необходимо ввести «y» после «The system will reboot. Do you want to proceed? [y/N]» и нажать клавишу «ENTER».

## 6.5. Сброс пароля

Для сброса пароля необходимо выбрать пункт меню «3) Reset the root password» (ввести «3» и нажать клавишу «ENTER»). Для обновления пароля необходимо ввести «y» после «Do you want to proceed? [y/N]» и нажать клавишу «ENTER». Необходимо ввести новый пароль после «Type a new password» и нажать клавишу «ENTER». Далее необходимо повторить новый пароль после «Confirm new password» и нажать клавишу «ENTER».

## 6.6. Восстановление настроек по умолчанию

Для сброса всех настроек ПК «InfoWatch ARMA Industrial Firewall» необходимо выбрать пункт меню «4) Reset to factory defaults» (ввести «4» и нажать клавишу «ENTER»). Для восстановления настроек ПК «InfoWatch ARMA Industrial Firewall» по умолчанию необходимо ввести «y» после «Do you want to proceed? [y/N]» и нажать клавишу «ENTER».

## 6.7. Выключение ПК

Для выключения ПК «InfoWatch ARMA Industrial Firewall» необходимо выбрать пункт меню «5) Power off system» (ввести «5» и нажать клавишу «ENTER»). Для выключения системы необходимо ввести «y» после «The system will halt and power off. Do you want to proceed? [y/N]» и нажать клавишу «ENTER».

## 6.8. Перезагрузка ПК

Для перезагрузки ПК «InfoWatch ARMA Industrial Firewall» необходимо выбрать пункт меню «6) Reboot system» (ввести «6» и нажать клавишу «ENTER»). Для перезагрузки системы необходимо ввести «y» после «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 «7» и нажать клавишу «ENTER»). Необходимо ввести IP-адрес хоста после «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» (ввести «8» и нажать клавишу «ENTER») пользователю будет доступен. Для выхода необходимо нажать на кнопку одновременно клавиши «Ctrl» и «D».

## 6.11. Просмотр состояния пакетного фильтра

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

## 6.12. Просмотр журнала ПК

Для просмотра журнала межсетевого экрана необходимо выбрать пункт меню «10) Firewall log» (ввести «10» и нажать клавишу «ENTER»). Для выхода необходимо нажать на кнопку одновременно клавиши «Ctrl» и «C».

## 6.13. Перезапуск сервисов

Для перезапуска всех настроенных сервисов необходимо выбрать пункт меню «11) Reload all services» (ввести «11» и нажать клавишу «ENTER»).

## 6.14. Обновление ПО

Перед обновлением ПК «InfoWatch ARMA Industrial Firewall» целесообразно проверить файл обновления в соответствии с политикой в компании. С помощью пункта меню «12) Update from console» производится обновление ПК «InfoWatch ARMA Industrial Firewall». Для обновления ПК «InfoWatch ARMA Industrial Firewall» необходимо вставить USB носитель с записанными обновлениями в USB порт ПК «InfoWatch ARMA Industrial Firewall». Ввести команду «12» и нажать клавишу «ENTER». Далее необходимо выбрать раздел диска, на котором находится файл обновления ПК «InfoWatch ARMA Industrial Firewall». Для этого после «Choose device partition number with update packages or press enter to update list:» необходимо ввести номер раздела диска из списка и нажать клавишу «ENTER». Если при обновлении ПК «InfoWatch ARMA Industrial Firewall» обновляет ядро ОС (kernel) или обновление ПК «InfoWatch ARMA Industrial Firewall» вносит существенные изменения в пакет ПК «InfoWatch ARMA Industrial Firewall», то в консольном интерфейсе

отобразится информация об этих изменения. Необходимо подтвердить эти изменения для продолжения обновления ПК «InfoWatch ARMA Industrial Firewall». Для этого необходимо ввести «y» после вопроса «Proceed with this action [y/N]» и нажать клавишу «ENTER».

## 6.15. Восстановление из резервной копии

Для восстановления системы необходимо выбрать пункт меню «13) Restore a backup» (ввести «13» и нажать клавишу «ENTER») (рисунок 42).

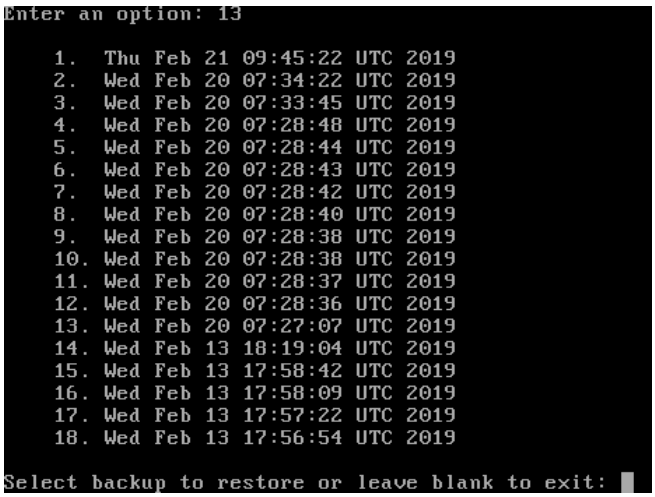



**Рисунок 42 — Восстановление из резервной копии**

В случае если нет необходимости восстанавливать конфигурацию из резервной копии, необходимо оставить поле ввода пустым и нажать клавишу «ENTER». Для выбора резервной копии ПК «InfoWatch ARMA Industrial Firewall» необходимо ввести ее номер после «Select backup to restore or leave blank to exit:» и нажать клавишу «ENTER». После выбора резервной копии ПК «InfoWatch ARMA Industrial Firewall» система будет восстановлена и перезагружена. Для этого необходимо нажать на кнопку «y» после «Do you want to reboot to apply the backup cleanly? [y/N]» и клавишу «ENTER».

# 7. Обслуживание

## 7.1. Установка и проверка лицензии

В ПК «InfoWatch ARMA Industrial Firewall» предусмотрена система лицензирования и защиты от копирования. Файл программной лицензии ПО ПК «InfoWatch ARMA Industrial Firewall» установлен на USB-токен, привязываемый также ПК «InfoWatch ARMA Industrial Firewall» к используемому аппаратному обеспечению. Это позволяет предотвратить несанкционированное копирование ПК «InfoWatch ARMA Industrial Firewall». Для активации лицензии и защиты от копирования необходимо:

1. вставить USB-токен в соответствующий порт оборудования;
2. вызвать процедуру привязки к USB-токену и оборудованию;
3. произвести проверку активации лицензии.

Для выполнения п.2 необходимо подключиться к консоли посредством последовательного интерфейса, SSH или монитора и клавиатуры и войти в консоль, используя необходимые учетные данные. Далее вставить USB-токен в ПК «InfoWatch ARMA Industrial Firewall». Для вызова процедуры привязки необходимо выбрать пункт «14) Setup license» (если пункт недоступен, это означает, что лицензия и защита от копирования уже была настроена). Затем необходимо выбрать тип лицензии:

– «USB key (usual USB key license)» (внешний USB для хранения ключа);

– «Virtual key (from virtual machines, i.e. USB is emulated by license service)» (локальный диск для хранения ключа).

Следующим шагом необходимо ввести номер USB-токена, в соответствии с позицией в списке, представленным в консоли.

Далее необходимо выбрать лицензию из следующих видов лицензии:

– «Demo» (лицензия с доступом ко всем страницам, имеющая ограничение по времени);

– «With IDS» (нет доступа к странице графического интерфейса «Обнаружение вторжений» - Контроль уровня приложений»);

– «With application control» (нет доступа к странице графического интерфейса «Обнаружение вторжений»);

– «With IDS and application control» (полная лицензия).

При выборе демо версии необходимо ввести время действия лицензии в днях после чего нажать клавишу «ENTER» (рисунок 43).

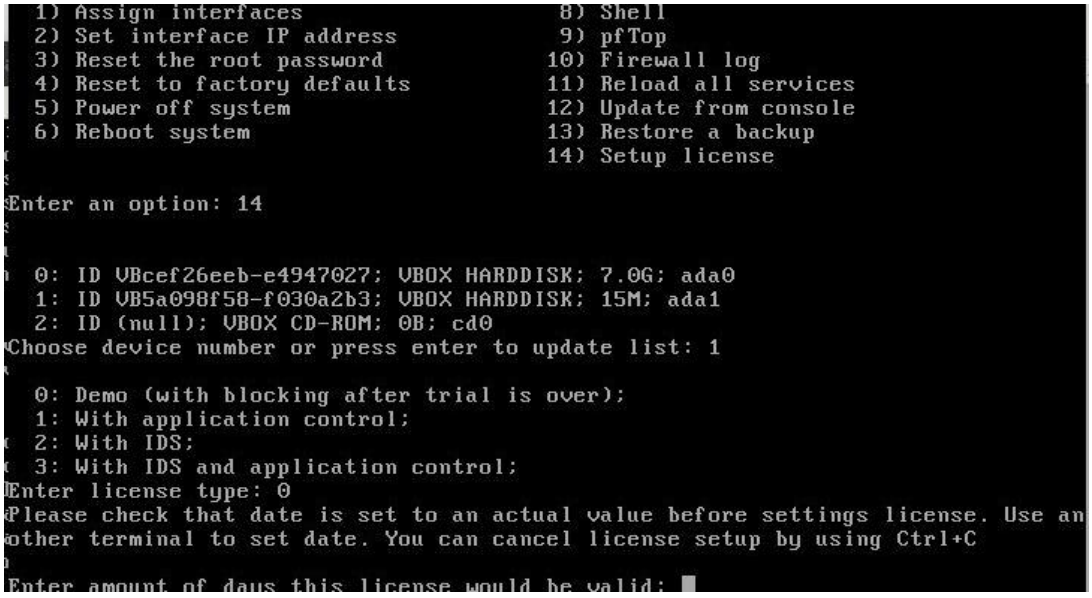



**Рисунок 43 — Установка лицензии**

После выполнения данных шагов будет выдано сообщение об успешной привязке, а пункт «14) Setup license» должен быть автоматически убран из списка меню. При истечении лицензии появится сообщение «license expired». При неправильном USB токене появится сообщение «license key is invalid».

Для проверки корректности установленной лицензии необходимо извлечь USB токен. В течение 1 минуты ПО в консоли укажет, что необходимо вставить USB токен («no USB key»). При этом к веб-серверу и через SSH подключения не будет, однако межсетевое экранирование и система обнаружения вторжений продолжат работать. Для продолжения работы необходимо снова вставить USB токен в порт устройства. В течение одной минуты устройство продолжит работать в нормальном режиме. Если этого не произойдет – необходимо перезагрузить ПК «InfoWatch ARMA Industrial Firewall».

## 7.2. Обновление программного обеспечения

Обновления ПО представляются разработчиком или технической поддержкой. Для обновления ПК «InfoWatch ARMA Industrial Firewall» необходимо файлы обновления поместить на USB Flash (накопитель должен иметь файловую систему FAT32). Далее подключить USB накопитель с файлом обновления к USB порту устройства, на котором развернуто ПК «InfoWatch ARMA Industrial Firewall».

Для обновления через консольный интерфейс необходимо войти в консольный интерфейс, используя действующую учетную запись пользователя и выбрать пункт «12) Update from console». Выбрать раздел диска, на котором находится файл обновления ПК «InfoWatch ARMA Industrial Firewall». Для этого после «Choose device partition number with update packages or press enter to update list:» необходимо ввести номер раздела диска из списка и нажать клавишу «ENTER». После вопроса «Proceed with this action [y/N]» необходимо ввести «y». Система произведет обновление (рисунок 44).

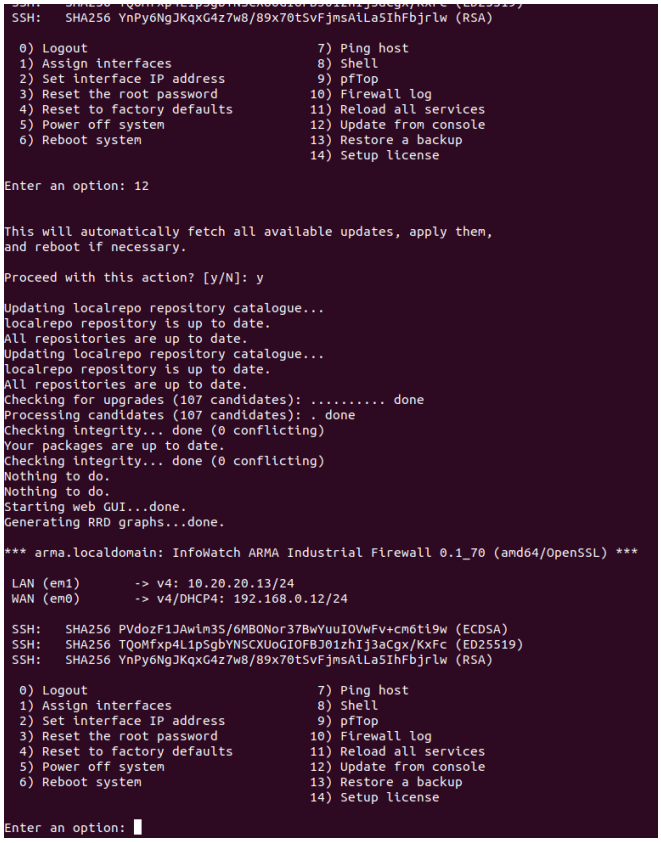



**Рисунок 44 — Обновление ПО: консольный интерфейс**

Для обновления через графический интерфейс необходимо перейти в «Система» - «Прошивка» - «Обновления» и нажать кнопку «Выбрать файл». Выбрать файл обновления с USB накопителя и нажать кнопку «Обновить сейчас». Система произведет обновление.

## 7.3. Резервное копирование и восстановление

Для сохранения на внешний носитель текущей конфигурации ПК «InfoWatch ARMA Industrial Firewall» в формате XML необходимо перейти в веб-интерфейсе в раздел настроек резервного копирования «Система» - «Конфигурация» - «Резервные копии», в группе настроек «Сохранение» и выбрать параметры сохранения конфигурации: «Не делать резервную копию данных анализа трафика» и «Зашифровать этот файл конфигурации» если это необходимо. Для сохранения конфигурации необходимо нажать на кнопку «Сохранить конфигурацию» (рисунок 45). После нажатия на кнопку ПК «InfoWatch ARMA Industrial Firewall» сгенерирует файл конфигурации и передаст его на скачивание в веб-браузере. Этот файл необходимо поместить в выделенный обслуживающим персоналом каталог хранения конфигураций ПК «InfoWatch ARMA Industrial Firewall».

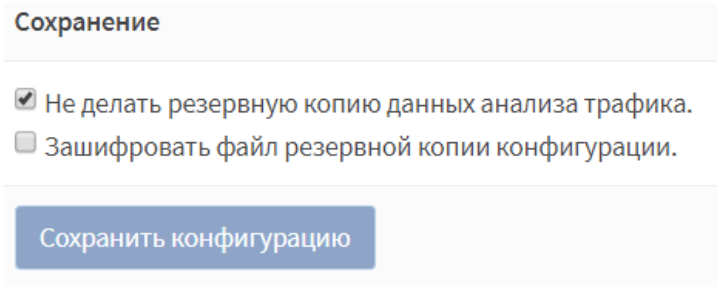



**Рисунок 45 — Сохранение текущей конфигурации**

Для восстановления конфигурации необходимо перейти в веб-интерфейсе в раздел настроек резервного копирования «Система» - «Конфигурация» - «Резервные копии». В группе настроек «Восстановить» в поле «Восстановить зону:» необходимо выбрать те разделы конфигурации, которые требуется восстановить. После выбора необходимых параметров восстановления необходимо нажать кнопку «Выберите файл», в и выбрать файл конфигурации

ПК «InfoWatch ARMA Industrial Firewall». При необходимости перезагрузить ПК «InfoWatch ARMA Industrial Firewall» после восстановления конфигурации необходимо установить флажок «Перезагрузить после восстановления». Если файл конфигурации зашифрован, необходимо установить флажок в графе «Файл конфигурации зашифрован» и в поле «Пароль» ввести пароль. Для восстановления необходимо нажать кнопку «Восстановить конфигурацию» (рисунок 46).

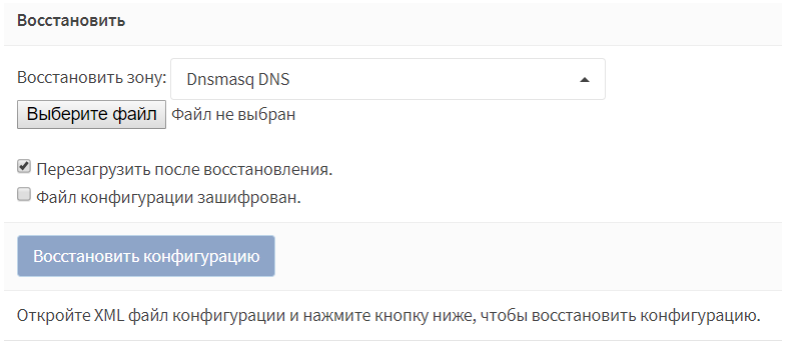



**Рисунок 46 — Восстановление конфигурации**

Обновление базы решающих правил системы обнаружения вторжений описано в документе Руководство пользователя в подразделе 5.1.2.

## 7.4. Экспорт конфигурации и набора баз решающих правил

Для настройки экспорта конфигурации и набора баз решающих правил необходимо перейти раздел «Система» - «Конфигурации» - «Настройки экспорта» - «Настройки».

Категория «Настройки экспорта» позволяет экспортировать текущую конфигурацию в формате «XML» на удаленный FTP-сервер и samba-сервер.

Для настройки подключения к FTP-серверу в поле «Протокол» необходимо выбрать «FTP». В поле «Адрес» необходимо ввести IP-адрес FTP-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения к FTP серверу. В поле «Путь к файлу» необходимо указать папку для экспорта конфигурации. В поле «Интервал ожидания» необходимо выбрать интервал времени в минутах, через который конфигурация будет экспортироваться повторно в случае неудачной попытки выгрузки.

Необходимо нажать кнопку «Выполнить» для сохранения настроек и экспорта конфигурации. При необходимости только сохранения настроек необходимо нажать кнопку «Применить» (рисунок 47).

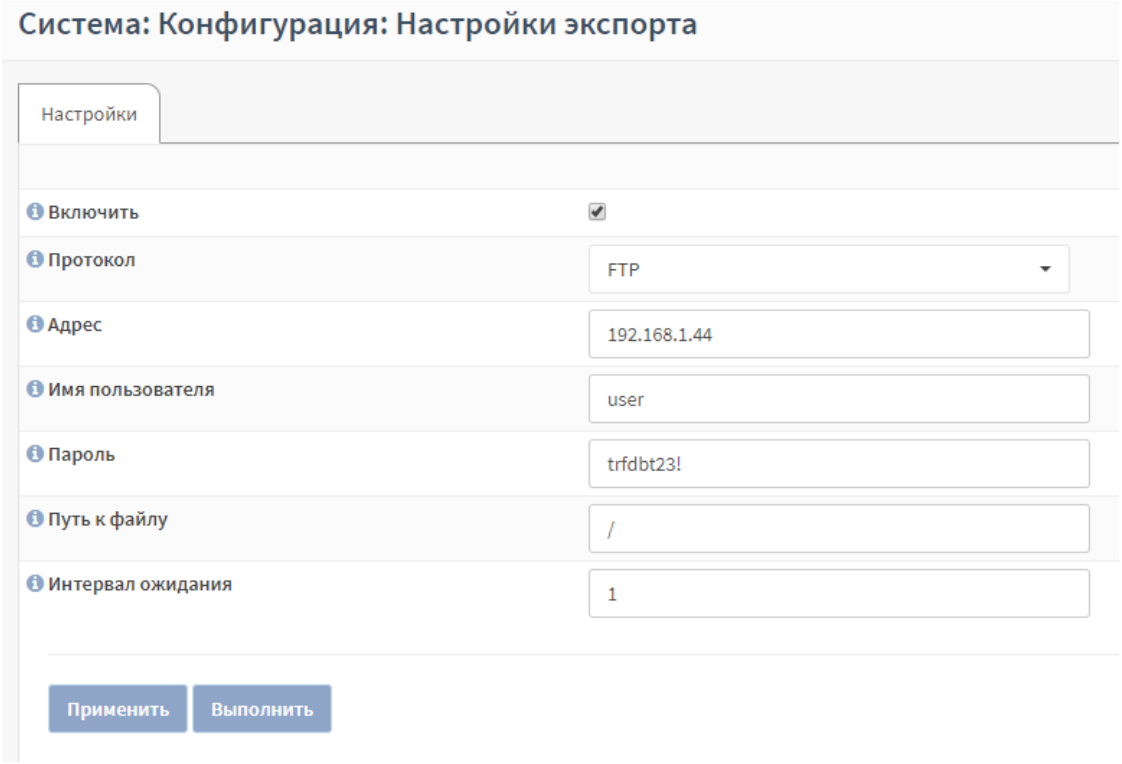



**Рисунок 47 — Система: Конфигурация: Экспорт конфигурации: Настройки (FTP)**

Для настройки подключения к samba-серверу в поле «Протокол» необходимо выбрать «SMB». В поле «Адрес» необходимо ввести IP-адрес samba-сервера. В поле «Samba сервис» необходимо ввести название samba-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения к samba-серверу. В поле «Путь к файлу» необходимо указать папку для экспорта конфигурации. В поле «Интервал ожидания» необходимо выбрать интервал времени в минутах, через который конфигурация будет экспортироваться повторно в случае неудачной попытки выгрузки.

Необходимо нажать кнопку «Выполнить» для сохранения настроек и экспорта конфигурации. При необходимости только сохранения настроек необходимо нажать кнопку «Применить» (рисунок 48).

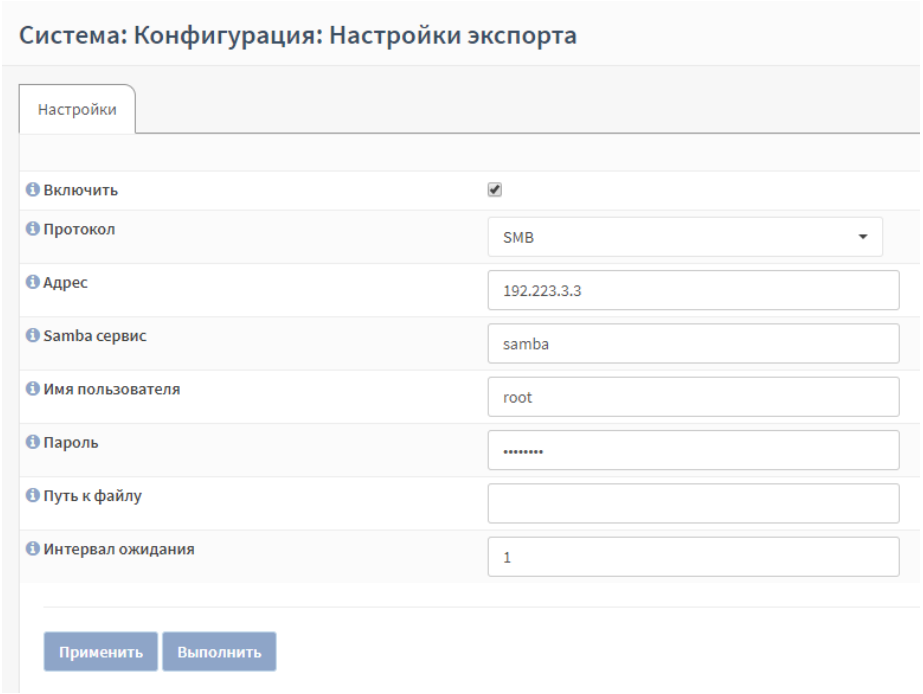



**Рисунок 48 — Система: Конфигурация: Экспорт конфигурации: Настройки (SMB)**

Для настройки расписания экспорта конфигурации и набора баз решающих правил необходимо перейти раздел «Система» - «Конфигурации» - «Настройки экспорта» - «Расписание».

При нажатии на категорию «Расписание» происходит автоматическое перенаправление в редактирование расписания системы предотвращения вторжений, которое находится в разделе «Система» - «Настройки» - «Планировщик задач Cron». При редактировании расписания в поле «Команда» необходимо выбрать «Экспорт конфигурации» (рисунок 49).

Остальные параметры расписания расписаны более подробно в Руководстве пользователя в подразделе (рисунок 49).

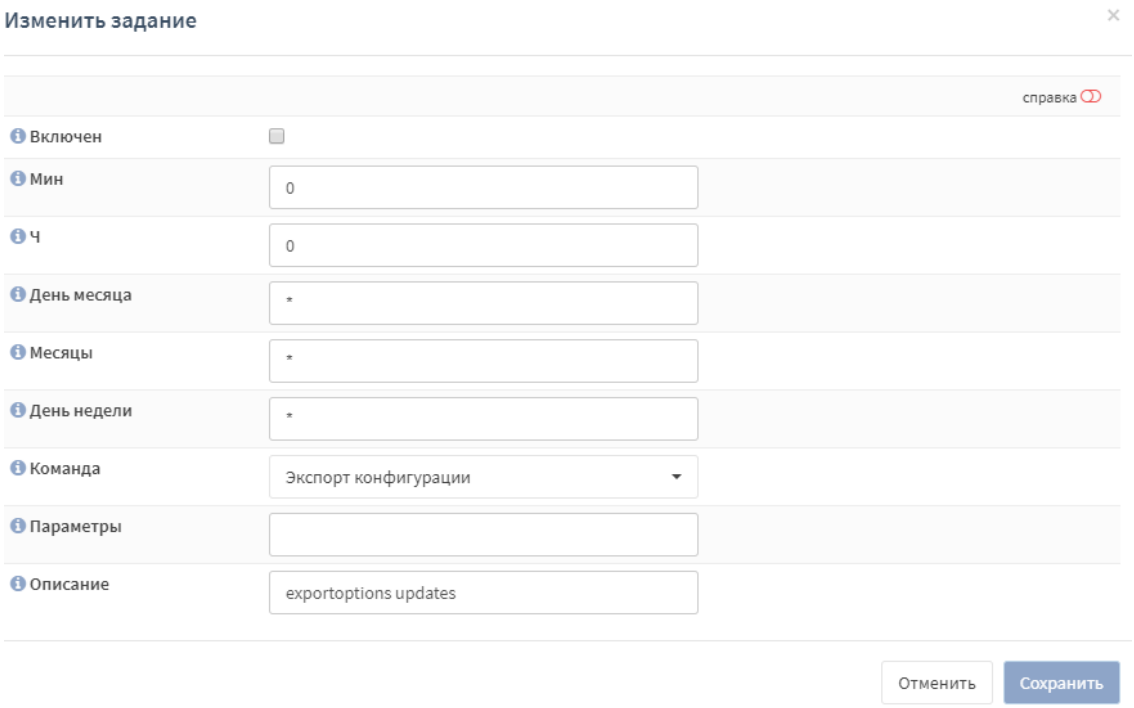



**Рисунок 49 — Система: Конфигурация: Экспорт конфигурации: Расписание**

# 8. Возможные ошибки и их решения

## 8.1. Ошибка копирования файла во время установки с использованием образа ISO

Ошибка копирования файла во время установки с использованием образа ISO чаще всего вызвана нехваткой памяти ОЗУ. Для предотвращения ошибки необходимо убедиться, что среда виртуализации, на которую устанавливается ПК «InfoWatch ARMA Industrial Firewall», имеет минимум 1 ГБ ОЗУ.

## 8.2. Ошибки диска на VMware

Ошибки диска на VMware чаще всего вызвана неисправным приводом (носителем). Для предотвращения ошибки необходимо изменить режимпривода на IDE.

## 8.3. Ошибка установки на KVM

Ошибка установки на KVM чаще всего происходит при использовании virtio для корневого диска. Для предотвращения ошибки необходимо переключиться в режим sata.

## 8.4. Проблемы с NAT на XenServer

Проблемы с NAT на XenServer чаще всего происходят при включенных контрольных суммах в domU и в VIFS. Для предотвращения ошибок необходимо отключить контрольную сумму в domU и в VIFS.

## 8.5. Ограничение трафика не работает на VMware

Если ограничение трафика не работает на VMware и в VMware используются драйверы vmxnet3 необходимо переключить драйверы на E1000.

## 8.6. Отсутствует доступ к веб-интерфейсу

Первой возможной причиной может является то, что в веб-браузере открывался веб-интерфейс через протокол HTTPS. Подключение через HTTP невозможно. Для подключения к веб-интерфейсу по протоколу HTTP необходимо очистить историю в веб-браузере или открыть страницу веб-браузера в режиме «Инкогнито».

Второй возможной причиной может являться то, что при использовании среды виртуализации порядок сетевых адаптеров, представленный в операционной системе может отличаться от порядка отображения в ПК «InfoWatch ARMA Industrial Firewall». Для решения данной ошибки необходимо дополнительно сопоставить MAC-адрес и название физических и сетевых интерфейсов.

## 8.7. Неверный пароль в консольном интерфейсе

Возможной причиной является то, что при изменении пароля в веб-интерфейсе на пароль, содержащий русские символы – невозможно авторизоваться в консольном интерфейсе, так как в консольном интерфейсе доступна только английская раскладка. Для решения данной ошибки необходимо поменять пароль в веб-интерфейсе на пароль, содержащий только символы английской раскладки.

## 8.8. Не работает FTP-прокси

Возможной причиной является то, что FTP-прокси будет работать только если сам прокси-сервер включен. FTP-прокси обрабатывает только незашифрованный FTP-трафик. Для решения данной ошибки необходимо перейти в раздел настройки прокси-сервера «Службы» - «Прокси» - «Основные настройки», поставить флажок напротив «Включен» и нажать кнопку «Применить».

## 8.9. Невозможно авторизоваться на прокси-сервере

Первой возможной причиной является то, что 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.

Второй возможной причиной является то, что Squid преднастроен таким образом, что разрешает проксирование запросов только к некоторому множеству портов, считающихся безопасными (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.

## 8.10. Не срабатывает правило межсетевого экрана

Первой возможной причиной является то, что все правила обрабатываются по порядку. При первом совпадении обработка правил прекращается. Для решения данной ошибки необходимо переместить нужное правило в начало списка.

Второй возможной причиной является то, что при работе с Microsoft AD существует проблема поиска пользователя в первичной группе (как правило, это группа Users). 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.

## 8.11. Отсутствует доступ к порталу авторизации

Первой возможной причиной является то, что нет разрешающих правил межсетевого экрана для портала авторизации по портам 8000-10000 и 53. Для решения данной ошибки необходимо добавить разрешающих правил по порту

8000-10000 и 53 в разделе настроек правил МЭ «Межсетевой экран» - «Правила» - «[Название сетевого интерфейса, на котором работает портал авторизации]».

Второй возможной причиной является то, что неправильно настроен DHCP-сервер. Для решения данной ошибки необходимо при настройке DHCP-сервера, указать DHCP-параметр DNS-серверы как IP-адрес LAN-интерфейса.

## 8.12. Не включается служба snmpd

Возможной причиной является то, что не указан IP-адрес для прослушивания. Для решения данной ошибки необходимо перейти в раздел настройки SNMP «Система» - «Настройки» - «SNMP» - «Общие настройки», вписать IP-адрес для мониторинга в поле «IP для прослушивания» и нажать кнопку «Сохранить».

## Приложение А

**Системные учетные записи**

| № | Имя системной учетной записи | Описание |
|---|---|---|
| 1 | root | Суперпользователь (System Administrator) |
| 2 | toor | Резервный пользователь с ID = 0, который имеет ровно те же возможности, что и root |
| 3 | installer | Учетная запись для установки ПК «InfoWatch ARMA Industrial Firewall» |
| 4 | daemon | От имени учетной записи daemon запускаются сервисы, которым необходима возможность записи файлов на диск |
| 5 | operator | Учетная запись предназначен для выполнения административных задач с низкими привилегиями |
| 6 | bin | Осуществляет запуск бинарных команд операционной системы |
| 7 | tty | Все устройства /dev/vca разрешают доступ на чтение и запись учетной записи из этой группы |
| 8 | kmem | Учетная запись, которой предоставляется доступ к виртуальной памяти ядра, для управления распределения оперативной памяти |
| 9 | man | Позволяет добавлять страницы в |

| | | |
|---|---|---|
| | | директорию /var/cache/man |
| 10 | sshd | Учетная запись для настройки доступа через SSH |
| 11 | smmsp | Является учетной записью по умолчанию, который использует Sendmail |
| 12 | mailnull | От данного учетной записи по умолчанию отправляются почтовые сообщения, учетная запись Sendmail |
| 13 | bind | Учетная запись по умолчанию сервиса Bind |
| 14 | unbound | Учетная запись для настройки и подключения кэширующий DNS |
| 15 | proxy | Используется прокси серверами, нет доступа записи файлов на диск |
| 16 | _pf logd | Учетная запись, от которой сохраняются события от pf |
| 17 | _dhcp | Учетная запись для подключения DHCP-сервера |
| 18 | uucp | Учетная запись для подключения по протоколу UUCP |
| 19 | pop | Учетная запись получения электронной почты |
| 20 | auditdistd | Демон распределения файлов журнала аудита |
| 21 | www | Учетная запись, которой обеспечивает подключение в веб-интерфейсу |
| 22 | _ypldap | Обеспечивает подключение к LDAP- |

| | | |
|---|---|---|
| | | серверу |
| 23 | hast | Обеспечивает работу HAST |
| 24 | nobody | Учетная запись без привилегий доступа |
| 25 | _flow | Учетная запись, разделяющая привилегии |
| 26 | frr | Учетная запись, обеспечивающая подключение пакета протоколов FFRouting |
| 27 | dhcpd | Демон DHCP |
| 28 | squid | Учетная запись, которая обеспечивает работу кэширующего прокси |