Руководство пользователя по эксплуатации

версия 65 ред. от 26.05.2022

Листов *335*

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем документе использованы определения, представленные в таблице (см. Таблица 1).

Таблица 1
Термины и сокращения

Термины и сокращения	Значение
ДСЧ	Датчик случайных чисел
ИБ	Информационная безопасность
МЭ	Межсетевой экран
ПО	Программное обеспечение
УЗ	Учётная запись
ПК	Персональный компьютер
СОВ	Система обнаружения вторжений
МП	Материнская плата
ЦП	Центральный процессор
API	Application Programming Interface – программный интерфейс приложения
ARMA IF	InfoWatch ARMA Industrial Firewall
ARMA MC	InfoWatch ARMA Management Console
Blacklists UT1	Список ограничения доступа к URL-адресам
CARP	Common Address Redundancy Protocol – протокол дупликации общего адреса
CIDR	Classless Inter-Domain Routing – бесклассовая междоменная маршрутизация
DCERPC	Distributed Computing Environment/Remote Procedure Calls, распределённая вычислительная среда/удалённые вызовы процедур – система удаленного вызова процедур, разработанная для Distributed Computing Environment
DHCP	Dynamic Host Configuration Protocol, протокол динамической настройки узла

Термины и сокращения	Значение
DNS	Domain Name System, система доменных имён – компьютерная распределённая система для получения информации о доменах
DUID	Уникальный идентификатор DHCP
ICMP	Internet Control Message Protocol, протокол межсетевых управляющих сообщений – сетевой протокол, входящий в стек протоколов TCP/IP
FQDN	Fully Qualified Domain Name, полностью определённое имя домена – имя домена, не имеющее неоднозначностей в определении
FTP	File Transfer Protocol – протокол передачи файлов по сети
GOOSE	Generic Object Oriented Substation Event – протокол передачи данных о событиях на подстанции
HTTP	HyperText Transfer Protocol, протокол передачи гипертекста – протокол прикладного уровня передачи данных
HTTPS	HyperText Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
ICAP	Internet Content Adaptation Protocol – протокол адаптации интернет-контента
ICMP	Internet Control Message Protocol – протокол межсетевых управляющих сообщений
ID	Идентификатор
IEC 60870-5-104	Стандарт, определяющий набор протоколов для контроля и управления с использованием постоянного соединения
IMAP	Internet Message Access Protocol – протокол прикладного уровня для доступа к электронной почте
IP	Internet Protocol, межсетевой протокол – маршрутизируемый протокол сетевого уровня стека TCP/IP
IPS	Intrusion Prevention System, система предотвращения вторжений – система сетевой безопасности, предназначенная для обнаружения

Термины и сокращения	Значение
	несанкционированных действий и атак, а также автоматизированного противодействия им
IPsec	IP Security – набор протоколов для обеспечения защиты данных
IPv4	Internet Protocol version 4 – четвёртая версия интернет-протокола IP
IPv6	Internet Protocol version 6 – шестая версия интернет-протокола IP
IP-адрес	Уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу TCP/IP
LAN	Local Area Network – локальная вычислительная сеть
LDAP	Lightweight Directory Access Protocol – легковесный протокол доступа к каталогам
MIB	Management Information Base, база управляющей информации – виртуальная база данных, используемая для управления объектами в сети связи
MMS	Протокол передачи данных реального времени и команд диспетчерского управления между сетевыми устройствами и/или программными приложениями
Modbus TCP	Открытый коммуникационный протокол, основанный на архитектуре ведущий – ведомый, используемый для передачи данных через сети TCP/IP
MS Active Directory	Служба каталогов корпорации Microsoft для операционных систем семейства Windows Server
NAT	Network Address Translation, преобразование сетевых адресов – механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов
NetBIOS	Network Basic Input/Output System – протокол для работы в локальных сетях на персональных ЭВМ типа IBM/PC, разработан в виде интерфейса, который не зависит от фирмы-производителя
NTP	Network Time Protocol, протокол сетевого времени – сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью

Термины и сокращения	Значение
OID	Идентификатор объектов MIB
OPC	Open Platform Communications – семейство программных технологий, предоставляющих единый интерфейс для управления объектами автоматизации и технологическими процессами
OPC DA	Open Platform Communications Data Access – стандарт OPC
OPC UA	Open Platform Communications Unified Architecture – стандарт OPC
OSPF	Open Shortest Path First – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры
POP3	Post Office Protocol Version 3, протокол почтового отделения, версия 3 – стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удалённого сервера по TCP-соединению
RFC	Request for Comments, рабочее предложение – документ из серии пронумерованных информационных документов Интернета
RIP	Routing Information Protocol – протокол маршрутной информации
RRD	Round-robin Database, циклическая база данных – база данных, объём хранимых данных которой не меняется со временем, поскольку количество записей постоянно, в процессе сохранения данных они используются циклически
S7 Communication	Протокол, предназначенный для обмена данными с контроллерами Siemens S7 и любым другим оборудованием, поддерживающим данный протокол
SDB	Подлежащие загрузке блоки
SMB	Server Message Block – сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия

Термины и сокращения	Значение
SNMP	Simple Network Management Protocol, простой протокол сетевого управления – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP
SSH	Secure Shell, безопасная оболочка – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
SSL	Secure Sockets Layer, уровень защищённых сокетов – криптографический протокол
TCP	Transmission Control Protocol, протокол управления передачей – один из основных протоколов передачи данных интернета
TFTP	Trivial File Transfer Protocol, простой протокол передачи файлов – используется главным образом для первоначальной загрузки бездисковых рабочих станций
TLS	Transport layer security – протокол защиты транспортного уровня
TUN/TAP	Виртуальные сетевые драйверы ядра системы
UDP	User Datagram Protocol, протокол пользовательских датаграмм – один из ключевых элементов набора сетевых протоколов для Интернета
UMAS	Собственный протокол Schneider Electric, который может интерпретироваться только процессором и некоторыми коммуникационными модулями
URL	Uniform Resource Locator, Унифицированный указатель ресурса – система унифицированных адресов электронных ресурсов, или единообразный определитель местонахождения ресурса
UUID	Universally unique identifier, универсальный уникальный идентификатор – стандарт идентификации, используемый в создании ПО
VLAN	Virtual Local Area Network – виртуальная локальная компьютерная сеть

Термины и сокращения	Значение
VOIP	Voice over Internet Protocol – телефонная связь по протоколу IP
VPN	Virtual Private Network, виртуальная частная сеть – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети
WAN	Wide Area Network – глобальная вычислительная сеть

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для технических специалистов и пользователей, выполняющих конфигурирование и мониторинг работы **ARMA Industrial Firewall v.3.7**.

Руководство пользователя по эксплуатации описывает принципы работы с **ARMA IF**, доступные функции, их подробное описание, настройку и использование.

Пользователю **ARMA IF** необходимо изучить настоящее руководство перед эксплуатацией.

1 МЕЖСЕТЕВОЙ ЭКРАН

Одной из основных функций **ARMA IF** является фильтрация трафика с помощью встроенного межсетевого экрана.

На рисунке (см. Рисунок 1) представлен стенд, в рамках которого будут создаваться правила МЭ. Необходимо получить доступ с ПК **«Admin»** к веб-серверу **«WebServer»** по протоколам HTTP и HTTPS.

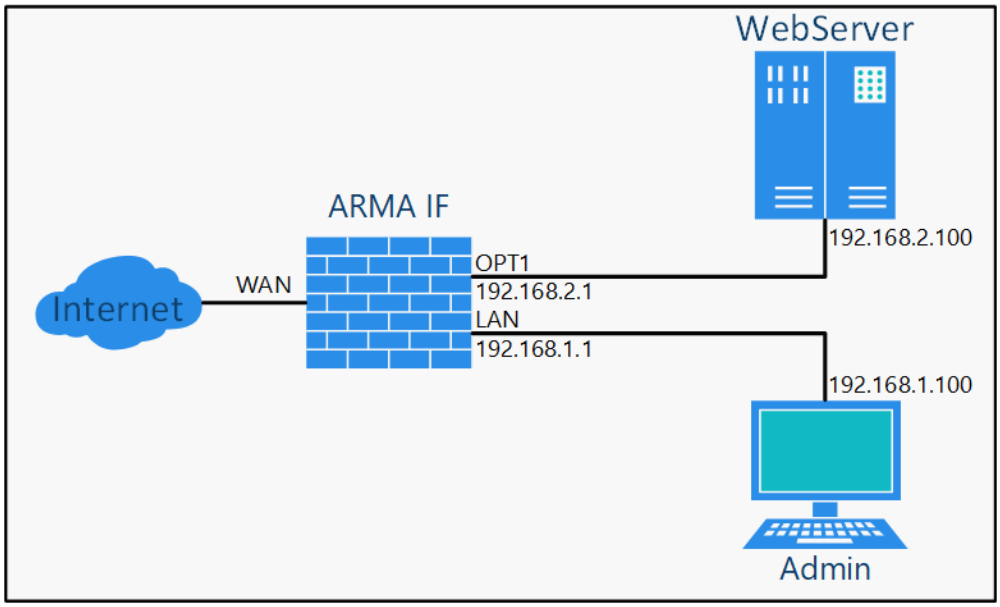

Рисунок 1 – Пример использования МЭ

Для получения доступа необходимо выполнить следующие шаги:

1. Убедиться в отсутствии доступа с ПК **«Admin»** к веб-серверу **«WebServer»**.
2. Понять общую последовательность работы правил МЭ (см. Раздел 1.1).
3. Создать правила МЭ для каждого из указанных протоколов (см. Раздел 1.1.1).
4. Убедиться в наличии доступа с ПК **«Admin»** к веб-серверу **«WebServer»** (см. Раздел 1.1.2).

Для проверки доступа необходимо открыть веб-браузер на ПК **«Admin»**, ввести в адресной строке «192.168.2.100» и нажать **клавишу «Enter»**. В результате откроется страница, указывающая на отсутствие доступа к веб-серверу (см. Рисунок 2).

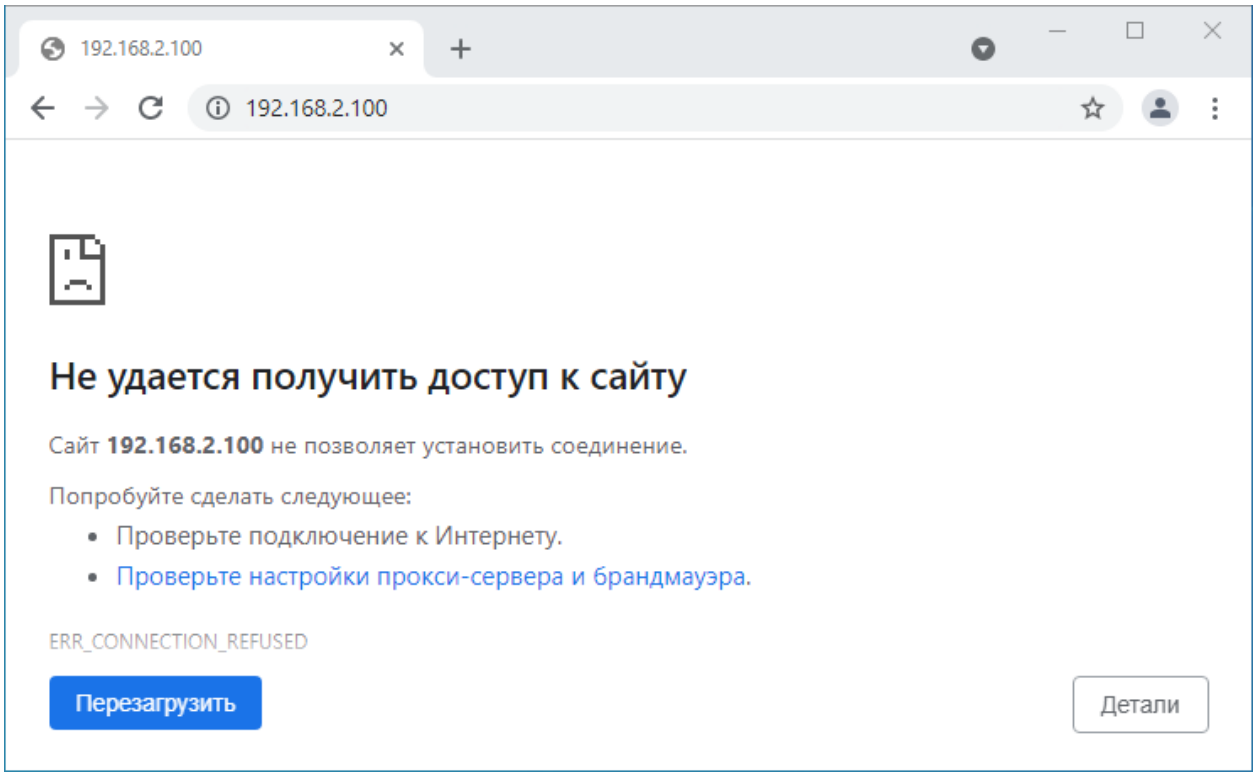

Рисунок 2 – Недоступность веб-сервера

1.1 Настройка правил МЭ

Перед созданием правил МЭ важно понимать алгоритм их работы.

Правила МЭ задаются отдельно для каждого сетевого интерфейса и располагаются в виде списка (см. Рисунок 3). По умолчанию предусмотрены автоматически сгенерированные правила. Для их просмотра необходимо нажать **кнопку «** 15 **»** в верхней правой части страницы. Перечень сгенерированных правил представлен в таблице (см. Таблица 2).

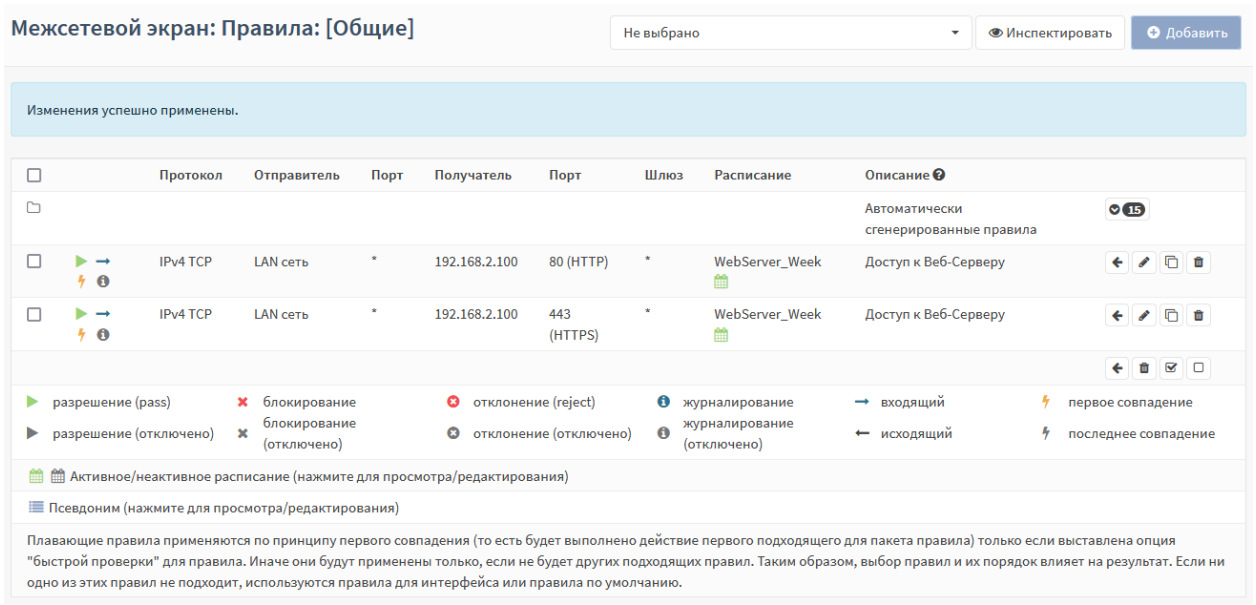

Рисунок 3 – Список правил

Порядок правил в списке имеет значение и им можно управлять с помощью **кнопки «»** напротив каждого из созданных правил. Сетевой пакет проверяется на совпадение с критериями правил по порядку, сверху вниз.

Возможны два принципа совпадения:

- **первого совпадения** – сразу происходит действие, указанное в первом совпавшем правиле, далее обработка сетевого пакета не производится;
- **последнего совпадения** – производится действие, указанное в последнем совпавшем правиле, далее обработка сетевого пакета не производится.

Принципы совпадения задаются в параметре правила **«Быстрая проверка»** (см. Рисунок 4) и отмечаются иконкой молнии в списке правил (см. Рисунок 3):

- **желтая молния «»** – принцип первого совпадения;
- **серая молния «»** – принцип последнего совпадения.

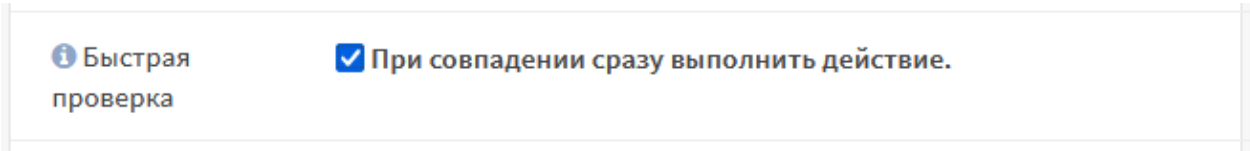

Рисунок 4 – Включение принципа первого совпадения

Если сетевой пакет не удовлетворяет критериям ни одного правила, то пакет блокируется.

Для интерфейсов правила проверяются в порядке, представленном на рисунке (см. Рисунок 5).

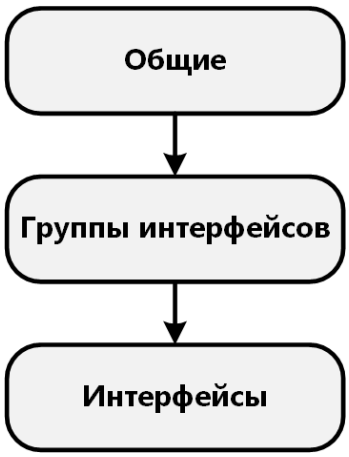

Рисунок 5 – Порядок применения правил для интерфейсов

По умолчанию во всех создаваемых правилах параметр **«Направление»** содержит значение **«Вх.»** – «Входящий трафик». Следует понимать, что это значение для интерфейса, первоначально принимающего трафик. Применение правил МЭ для исходящего трафика используется редко и для специфических целей.

В правиле возможны три действия над пакетом трафика:

- разрешить, **«Pass»** – разрешить движение пакета;
- блокировать, **«Drop»** – отбросить пакет;
- отклонить, **«Reject»** – отбросить пакет и отправить уведомление отправителю.

Таблица 2

Перечень автоматически сгенерированных правил МЭ

№	Название правила	Описание
Раздел [Общие]		
1	Default deny rule	Правило отбрасывает трафик, если для него не сработало ни одно из разрешающих правил. Правило работает по принципу «последнее совпадение». То есть, если правила №14 и №15, находящиеся ниже в таблице и тоже работают по принципу «последнее совпадение», или любое из «мгновенно применяемых правил» сработают, то такой трафик не будет отброшен. Во всех остальных случаях будет использовано это правило.
2	IPv6 requirements (ICMP)	Правила разрешают отправлять трафик по протоколу IPv6-ICMP с **ARMA IF** в локальную сеть (fe80::/10) и для групповой рассылки на адрес ff02::/16 (правило №3) и в обратном направлении (все кроме, правила №3).
3	IPv6 requirements (ICMP)	
4	IPv6 requirements (ICMP)	
5	IPv6 requirements (ICMP)	
6	IPv6 requirements (ICMP)	
7	Block all targetting from port 0	Правило блокирует все соединения с портом отправителя 0
8	Block all targetting to port 0	Правило блокирует все соединения с портом получателя 0.
9	Block CARP connection when CARP is disabled	Правило отбрасывает весь входящий трафик протокола CARP, если CARP на устройстве выключен. Если CARP включен, то данного правила не будет в списке
10	Allow CARP connection	Правило разрешает весь трафик CARP в двух направлениях. Правило не сработает, если CARP на устройстве выключен, так как сработает правило №9

№	Название правила	Описание
11	SSH lockout	Правила блокируют списки адресов/сетей из псевдонимов: • «sshlockout» • «webConfiguratorlockout» • «virusprot». Для срабатывания необходимо в разделе псевдонимов создать соответствующий псевдоним, например, «virusprot» и заполнить поля таблицы в pfTabl (**«Межсетевой экран»** - **«Диагностика»** - **«pfTables»**).
12	Web Configurator lockout	
13	Virusprot overload table (block all in alias <virusprot>)	
14	Let out anything from firewall host itself	Правило разрешает исходящий с **ARMA IF** трафик
15	Let out anything from firewall host itself (force gw)	Правило разрешает исходящий с **ARMA IF** трафик (принудительно для WAN-шлюза)
Раздел [LAN]		
1	Anti-lockout rule	Правило разрешает доступ к **ARMA IF** по HTTP(S) и SSH соединению
Раздел [WAN]		
1	Allow dhcpv6 client in WAN	Правила разрешают двусторонний обмен пакетами протокола DHCP для IPv6 сетей
2	Allow dhcpv6 client in WAN	
3	Allow dhcpv6 client in WAN	
4	Block bogon IPv4 networks from WAN	Правила блокируют IP-адреса Bogon-сетей IPv4/IPv6
5	Block bogon IPv6 networks from WAN	
6	Block private networks from WAN	Правила блокируют трафик, если адрес отправителя из локального сегмента адресов IPv4/IPv6
7	Block private networks from WAN	
8	Allow DHCP client on WAN	Правила разрешают двусторонний обмен пакетами протокола DHCP для IPv4 сетей
9	Allow DHCP client on WAN	

Количество автоматически сгенерированных правил может отличаться в зависимости от конфигурации **ARMA IF**. Например, если выключить IPv6, то в списке появятся правила блокировки IPv6 трафика, а если на интерфейсе включить DHCP,

то появятся разрешающие правила на двусторонний обмен пакетами DHCP по портам 546 и 547.

!Важно Помимо правил МЭ в **ARMA IF** присутствуют другие механизмы ограничения трафика, работающие в следующем порядке:

1. Правила ограничения трафика (см. Раздел 3).
2. Правила NAT (см. Раздел 2).
3. Правила МЭ (см. Раздел 1).
4. Правила СОВ (см. Раздел 5).
5. Ограничения портала авторизации (см. Раздел 20).

1.1.1 Создание правил межсетевого экранирования

Параметры создаваемого правила указаны в таблице (см. Таблица 3).

Таблица 3
Параметры создаваемого правила

Параметр	Значение	
Действие	Разрешить (Pass)	
Быстрая проверка	Да	
Интерфейс	LAN	
Направление	Вх.	
Протокол	TCP	
Отправитель	LAN сеть	
Получатель	Единственный хост или сеть	
	192.168.2.100/32	
Диапазон портов назначения	HTTP	HTTP
Описание	Доступ к веб-Серверу	

Для параметров **«Отправитель»** и **«Получатель»** существуют чек-боксы **«Инвертировать отправителя»** и **«Инвертировать получателя»** соответственно. При установке флажка в данных чек-боксах правило будет применено для всех отправителей/получателей, кроме значений, указанных в полях параметров **«Отправитель»**/**«Получатель»**.

Для создания правила МЭ необходимо выполнить следующие действия:

1. Перейти в подраздел общих правил МЭ (**«Межсетевой экран»** - **«Правила»** - **«[Общие]»**) (см. Рисунок 6).

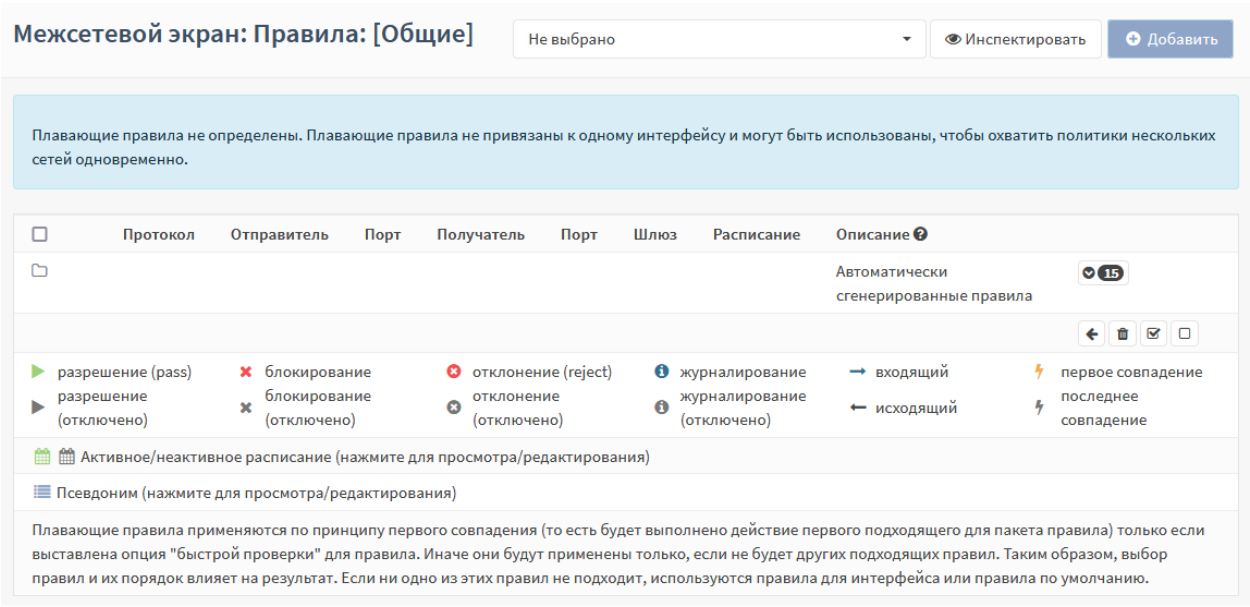

Рисунок 6 – Подраздел «Общие»

2. Нажать **кнопку «+Добавить»** и, в открывшейся форме (см. Рисунок 7), указать параметры из таблицы (см. Таблица 3). Остальные параметры оставить без изменения.

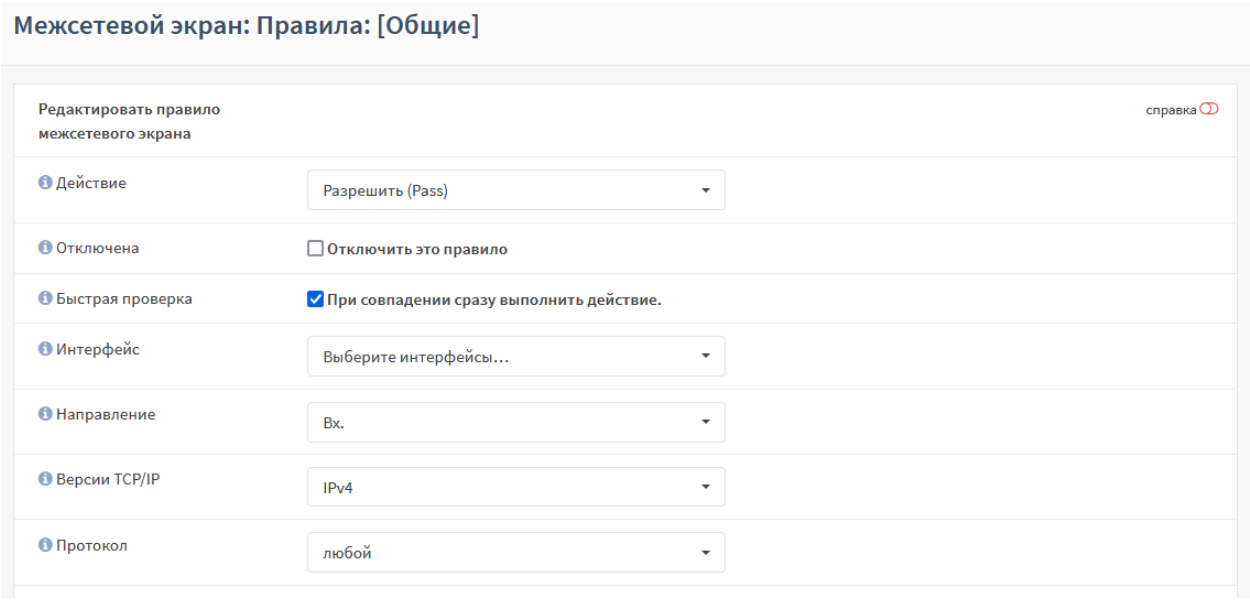

Рисунок 7 – Создание правила МЭ

3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»** (см. Рисунок 8).

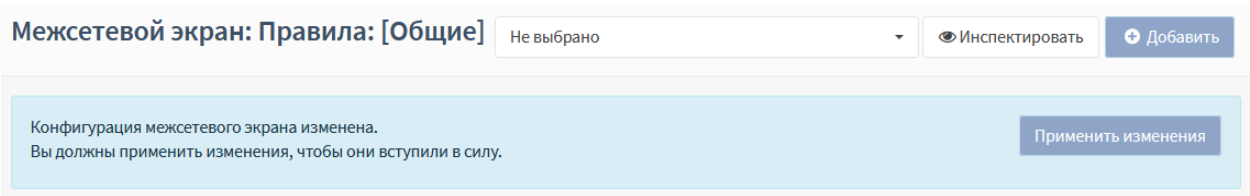

Рисунок 8 – Принятие изменений

4. В результате правило будет применено и отображено в списке правил (см. Рисунок 9).

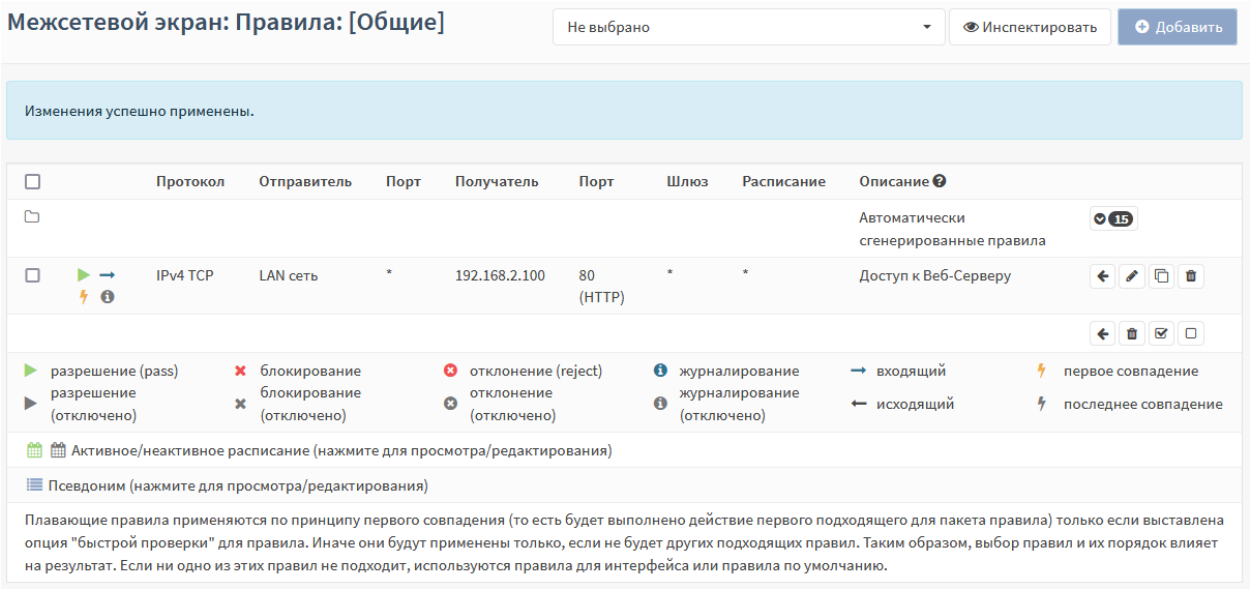

Рисунок 9 – Созданное правило в списке правил

Для копирования правила, например, для разрешения HTTPS-трафика, необходимо выполнить следующие действия:

1. Нажать **кнопку «**  **»** и, в открывшейся форме, изменить порт с HTTP на HTTPS (см. Рисунок 10).

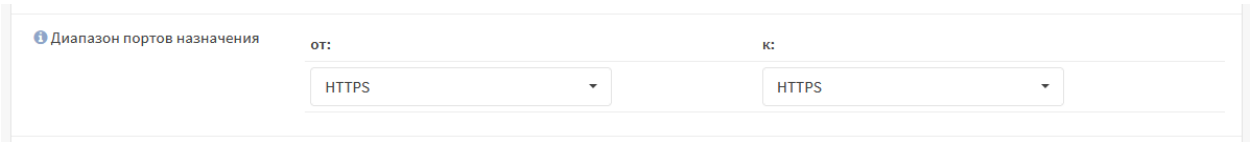

Рисунок 10 – Изменение диапазона портов

2. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.
3. В результате правило будет применено и отображено в списке правил.

В примере не используются дополнительные возможности правил МЭ и дополнительные параметры, доступные при нажатии **кнопки «Показать/скрыть»** (см. Рисунок 11). Данные возможности и параметры необходимы для более тонкой настройки правил МЭ.

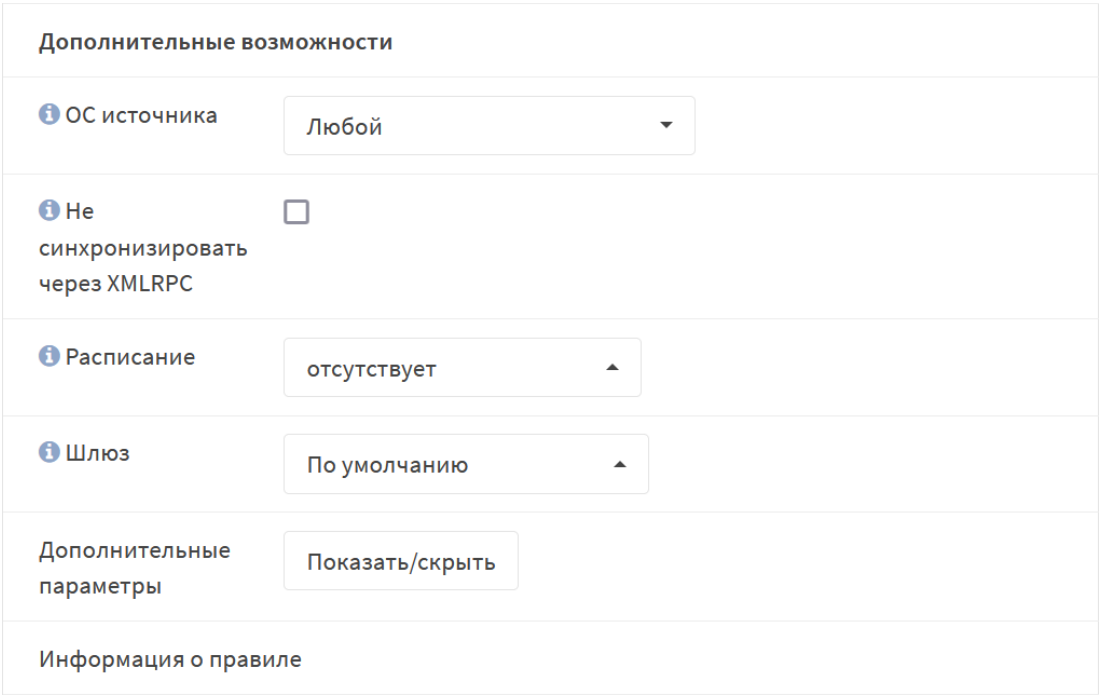

Рисунок 11 – Дополнительные возможности правил МЭ

1.1.2 Проверка созданных правил МЭ

Для проверки работы правил МЭ необходимо открыть веб-браузер на ПК **«Admin»**, ввести в адресной строке «192.168.2.100» и нажать **клавишу «Enter»**. В результате отобразиться стартовая страница веб-сервера (см. Рисунок 12).

Рисунок 12 – Стартовая страница веб-сервера

1.1.3 Создание псевдонимов

Псевдонимы – удобный инструмент объединения множества сетей, хостов и портов с целью дальнейшего использования в правилах МЭ, NAT, переадресации портов и других настройках **ARMA IF**.

Правильное использование псевдонимов улучшает читаемость правил МЭ и ускоряет добавление новых или изменение действующих правил.

Для создания псевдонима необходимо выполнить следующие действия:

1. Перейти в подраздел управления псевдонимами (**«Межсетевой экран»** - **«Псевдонимы»**) и нажать **кнопку «** **+** **»** (см. Рисунок 13).

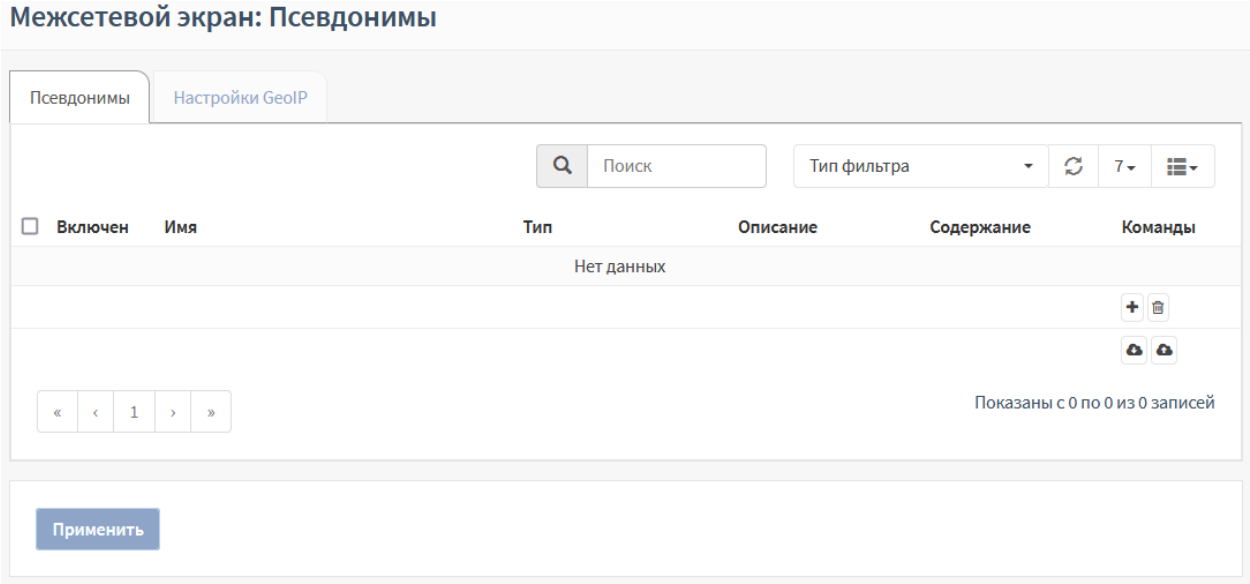

Рисунок 13 – Псевдонимы

2. В открывшейся форме (см. Рисунок 14) указать параметры и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить»**.

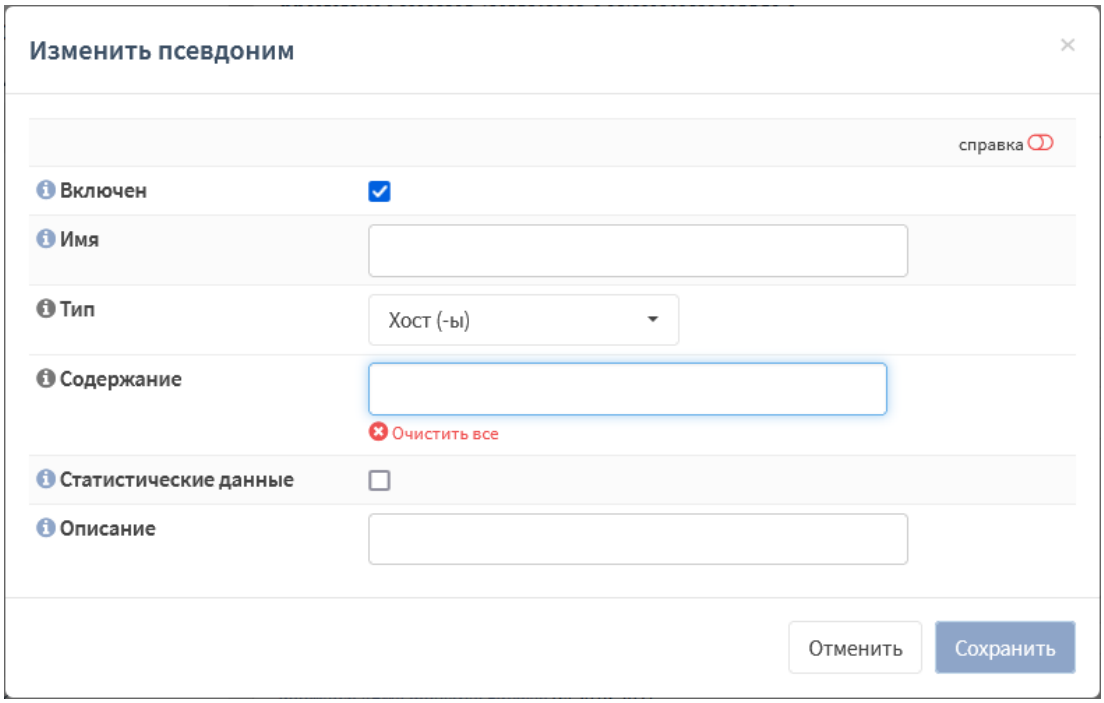

Рисунок 14 – Изменить псевдоним

Обязательными для создания псевдонима являются поля **«Имя»** и **«Тип»**. Типы псевдонимов, используемые в **ARMA IF**, и их краткое описание приведены в таблице (см. Таблица 4).

Таблица 4

Типы псевдонимов и их описание

Тип	Описание
Хост(-ы)	Один или более хостов указываются по IP-адресам или FQDN
Сеть(-и)	Одна или более сетей указываются в формате CIDR
Порт(-ы)	Один или более портов протоколов TCP и UDP указываются в форме списка или диапазона
URL (IP-адреса)	URL размещенного на каком-то веб-ресурсе списка IP-адресов. Список загружается и один раз
Таблица URL (IP-адреса)	URL размещенного на каком-то веб-ресурсе списка IP-адресов и периодичность обновления информации из списка. Список загружается с установленной периодичностью
GeoIP	Одна или более стран и регионов
Сетевая группа	Один или более псевдонимов типа **«Сеть(-и)»**
Внешний (расширенный)	Внешний псевдоним (только объявление)

Каждый псевдоним может содержать от одного, до нескольких значений (см. Рисунок 15).

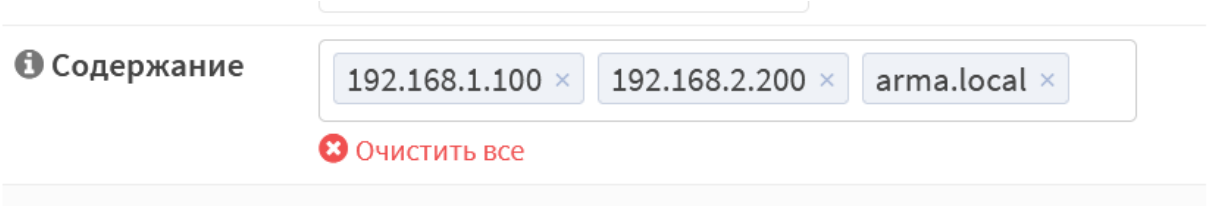

Рисунок 15 – Несколько значений в псевдониме

Большинство псевдонимов могут быть вложены в другие псевдонимы. Например, псевдоним, содержащий веб-серверы, и псевдоним, содержащий почтовые серверы, могут вместе входить в один более крупный псевдоним, содержащий все серверы.

1.1.3.1 Хост (-ы)

В содержании псевдонима данного типа возможно указать один или более хостов. Хосты задаются списком IP-адресов или полностью определенным доменным именем FQDN.

В случае использовании доменного имени для определения IP-адресов будет использоваться ответ DNS-сервера, опрос которого производится каждые 300 секунд. Интервал задаётся в параметре **«Интервал разрешения псевдонимов»** подраздела дополнительных настроек МЭ (**«Межсетевой экран»** - **«Настройки»** - **«Дополнительно»**).

1.1.3.2 Сеть (-и)

В содержании псевдонима данного типа возможно указать одну или более сетей IPv4 или IPv6.

Сети указываются в формате CIDR:

- <Адрес сети></><маска сети>, например, «192.168.1.0/24».

Используются списки сетей IPv4 и IPv6. Сети с масками «/32» для IPv4 и «/128» для IPv6 соответствуют одиночным хостам.

1.1.3.3 Порт (-ы)

В содержании псевдонима данного типа возможно указать один или более портов. Перечисляются одиночные порты, либо диапазоны портов, разделенные знаком «двоеточие».

Например, «420:500» будет соответствовать диапазону портов от 420 до 500.

1.1.3.4 URL (IP-адреса)

В содержании псевдонима данного типа возможно указать один или более URL со списком IP-адресов.

Список IP-адресов должен содержаться в текстовом файле, в котором каждый элемент списка (адрес отдельного хоста или сети) представлен отдельной строкой.

В списке IP-адресов могут быть указаны как отдельные IP-адреса, так и сети в формате CIDR.

URL задаются в следующей форме:

- <протокол><://><FQDN или IP-адрес хоста><путь к файлу списка>, например:
  - «https://www.spamhaus.org/drop/drop.txt»
  - «http://192.168.252.130/ip_list.txt»

После создания данного псевдонима список IP-адресов загружается однократно, после этого обновление списка не происходит.

1.1.3.5 Таблицы URL (IP-адреса)

В содержании псевдонима данного типа возможно указать один или более URL списком IP-адресов и периодичность обновления информации из указанного списка.

Параметры списков и URL идентичны параметрам псевдонима типа **«URL (IP-адреса)»** (см. Раздел 1.1.3.4).

Периодичность обновления информации из списка задается в форме количества дней и количества часов в полях **«Д»** и **«Ч»** соответственно. По истечении указанного периода времени будет произведена загрузка файла заново.

В состав псевдонима типа **«Таблица URL (IP-адреса)»** нельзя вложить никакой псевдоним, псевдоним типа **«Таблица URL (IP-адреса)»** так же не может быть вложен ни в один другой псевдоним.

1.1.3.6 GeoIP

В содержании псевдонима данного типа указывается одна или более стран и/или регионов. Задание значений псевдонима осуществляется выбором соответствующего пункта из выпадающих меню, а также добавлением ссылки на базу сопоставлений IP-адресов географическим регионам.

1.1.3.7 Сетевая группа

В содержании псевдонима данного типа указывается один или более существующих псевдонимов типа **«Сеть (-и)»** и/или **«Хост (-ы)»**. Функционально псевдоним выполняет ту же роль, что и псевдоним типа **«Сеть (-и)»**, но использует другой подход к отображению содержания псевдонима, что может упростить управление большим количеством псевдонимов типа **«Сеть (-и)»**.

1.1.3.8 Внешний (расширенный)

Содержание псевдонима данного типа нельзя указать средствами веб-интерфейса. В подразделе управления псевдонимами (**«Межсетевой экран»** - **«Псевдонимы»**) выполняется только объявление псевдонима для дальнейшего использования его в правилах межсетевого экрана. Содержание псевдонима управляется отдельными плагинами к **ARMA IF**, к функционалу которых относится псевдоним.

1.1.4 Создание групп интерфейсов

Данная функция позволяет создавать правила, применяемые к нескольким интерфейсам без дублирования правил (см. Рисунок 16).

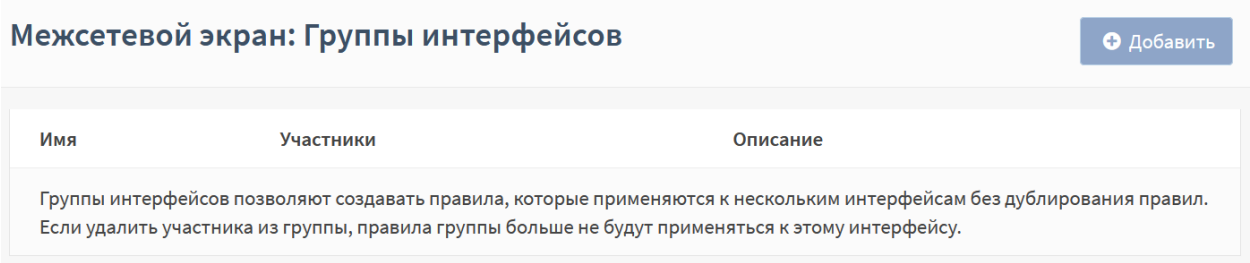

Рисунок 16 – Создание групп интерфейсов

В качестве примера использования групп интерфейсов подходит следующая задача:

- разрешить прохождение трафика ICMP по всем внутренним подсетям согласно схеме стенда, представленного на рисунке (см. Рисунок 1).

Для выполнения такой задачи необходимо объединить внутренние интерфейсы «OPT1» и «LAN» в группу и создать соответствующее правило.

Для создания группы интерфейсов необходимо выполнить следующие действия:

1. Перейти в подраздел настроек групп интерфейсов (**«Межсетевой экран»** - **«Группы интерфейсов»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок 17) указать следующие параметры:
    - поле **«Имя»** – «OPT1_LAN»;
    - поле **«Описание»** – «Внутренние интерфейсы»;
    - в списке **«Участники»** выбрать «LAN» и «OPT1».

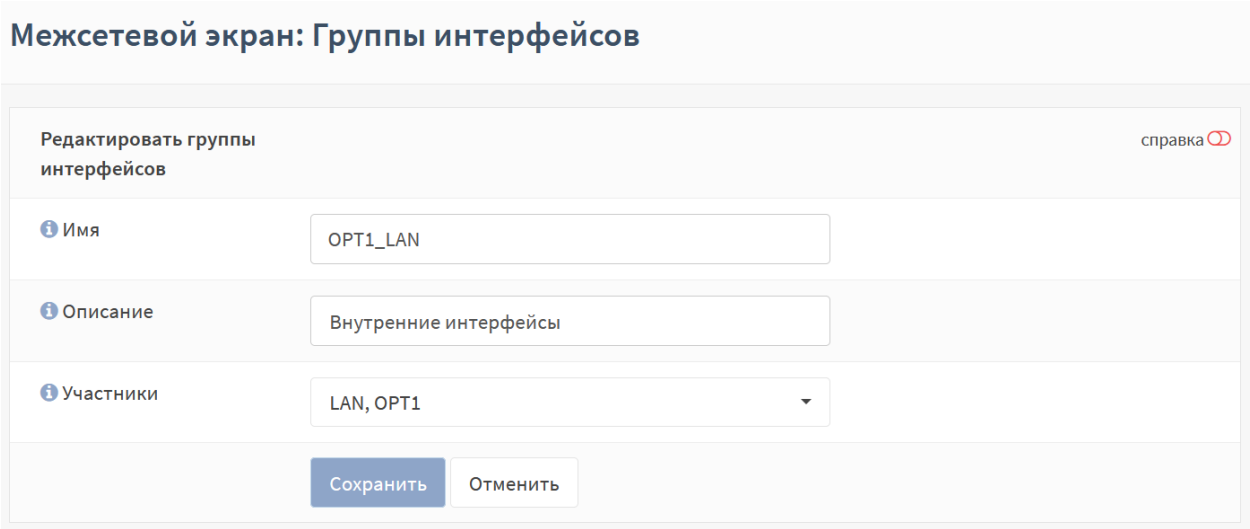

Рисунок 17 – Редактирование группы интерфейсов

3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.
4. В результате созданная группа интерфейсов появится в подразделе **«Правила»** (см. Рисунок 18).

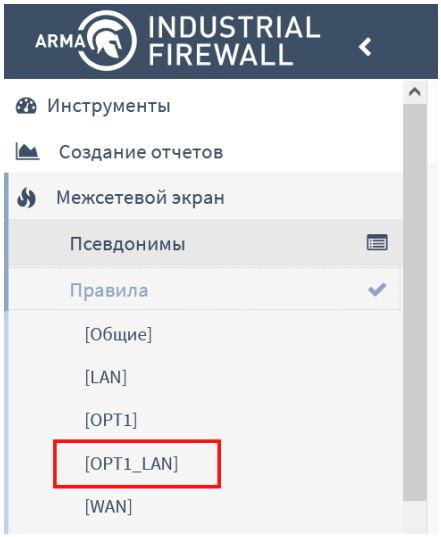

Рисунок 18 – Созданная группа интерфейсов

После этого необходимо создать правило (см. Раздел 1.1.1) для этой группы интерфейсов с параметрами, указанными в таблице (см. Таблица 5).

Таблица 5
Значения параметров правила для группы интерфейсов

Параметр	Значение
Действие	Разрешить (Pass)
Интерфейс	OPT1_LAN
Направление	Любой

Параметр	Значение
Протокол	ICMP

После сохранения и применения правила трафик ICMP будет доступен на внутренних интерфейсах (см. Рисунок 19).

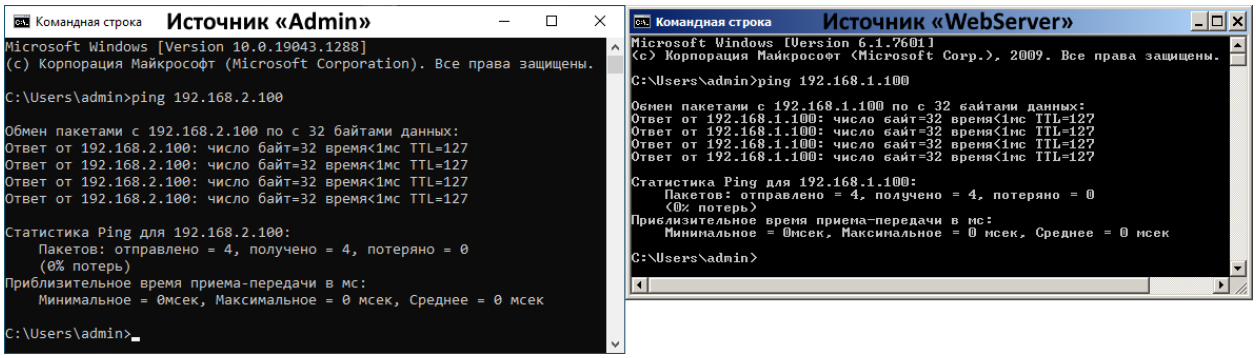

Рисунок 19 – Результат работы команды «Ping»

1.1.5 Создание расписания срабатывания правил

В некоторых случаях необходимо указать расписание работы правил МЭ. Например, требуется разрешить доступ к веб-серверу (см. Рисунок 1) только на рабочую неделю – с 25 по 29 октября 2021 года.

Для решения данной задачи необходимо создать расписание и изменить созданные ранее правила МЭ.

Для создания расписания необходимо выполнить следующие действия:

1. Перейти в подраздел управления расписаниями (**«Межсетевой экран»** - **«Настройки»** - **«Расписания»**) (см. Рисунок 20) и нажать **кнопку «+Добавить»**.

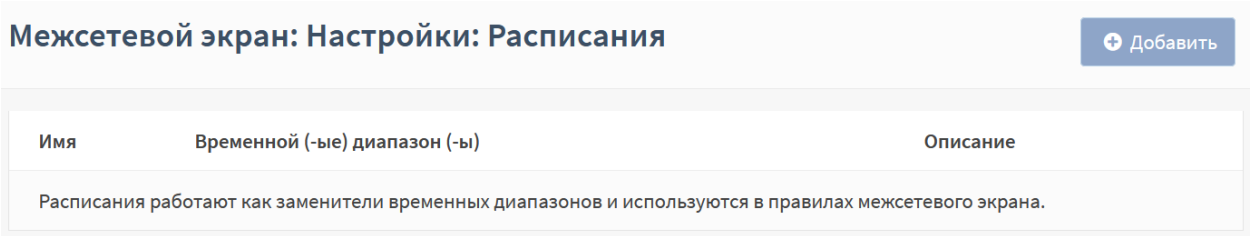

Рисунок 20 – Расписания для правил МЭ

2. В открывшейся форме (см. Рисунок 21) выполнить следующие действия:
   - в поле **«Имя»** указать значение «WebServer_Week»;
   - в списке **«Месяц»** выбрать «Октябрь 2021»;
   - нажать левой кнопкой мыши на 25-29 числа;
   - в поле **«Конечное время»** указать «23:59»;

- нажать **кнопку «Добавить время»**.

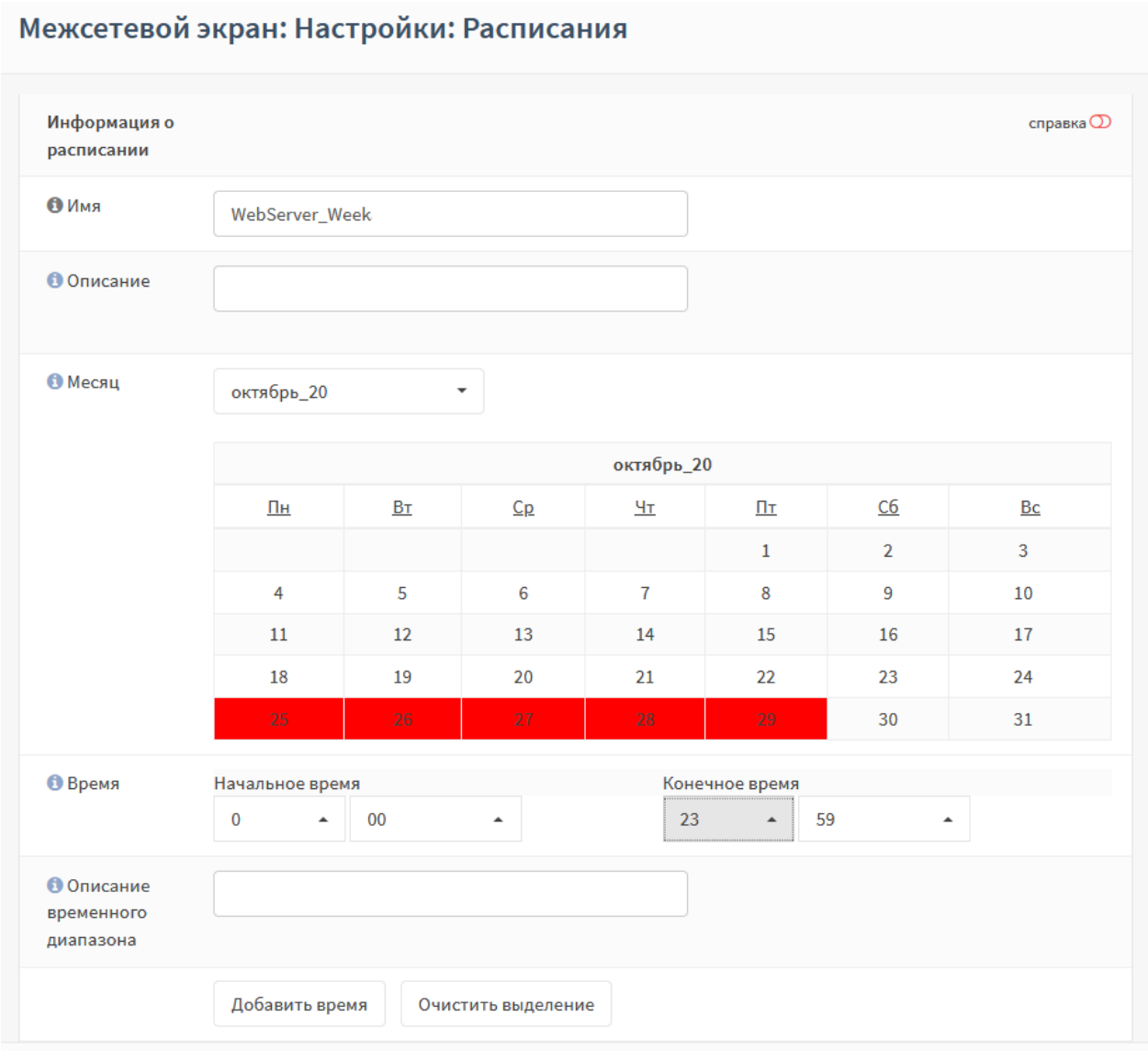

Рисунок 21 – Создание расписания для правил МЭ

3. В результате в блоке **«Повторение расписание»** формы будет отображено выбранное время (см. Рисунок 22).

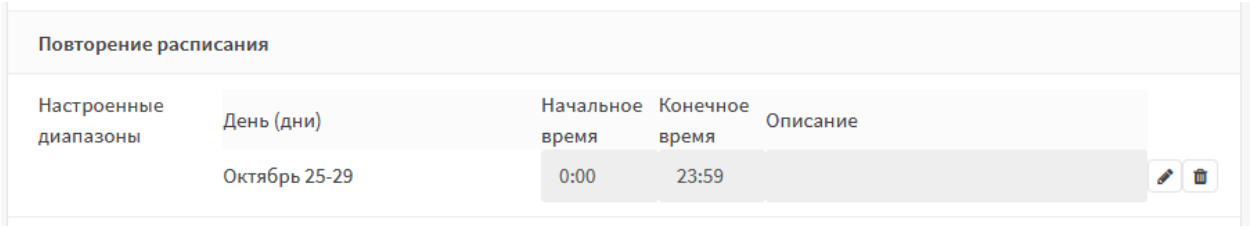

Рисунок 22 – Настроенные диапазоны

4. Нажать **кнопку «Сохранить»**.
5. В результате созданное расписание будет отображено в списке (см. Рисунок 23).

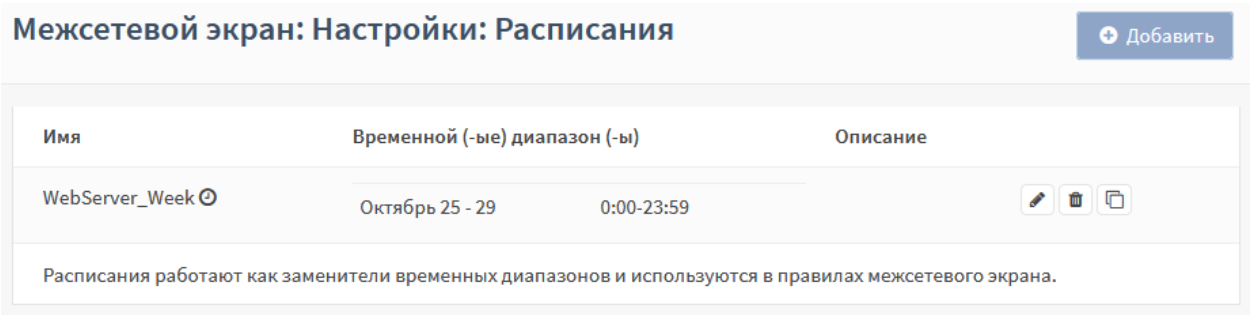

Рисунок 23 – Созданное расписание для правил МЭ

После создания расписания необходимо изменить правила МЭ для ограничения доступа к веб-серверу выполнив следующие действия:

1. Перейти в подраздел общих правил МЭ (**«Межсетевой экран»** - **«Правила»** - **«[Общие]»**) (см. Рисунок 6) и нажать **кнопку «** **»** напротив соответствующего правила.
2. В открывшейся форме (см. Рисунок 7) в поле **«Расписание»** выбрать значение **«WebServer_Week»** (см. Рисунок 24).

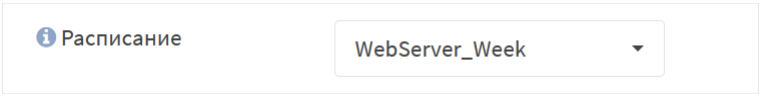

Рисунок 24 – Выбор расписания в правилах МЭ

3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.
4. В результате расписание будет применено к правилу и будет отображено в столбце **«Расписание»** в списке правил (см. Рисунок 25).

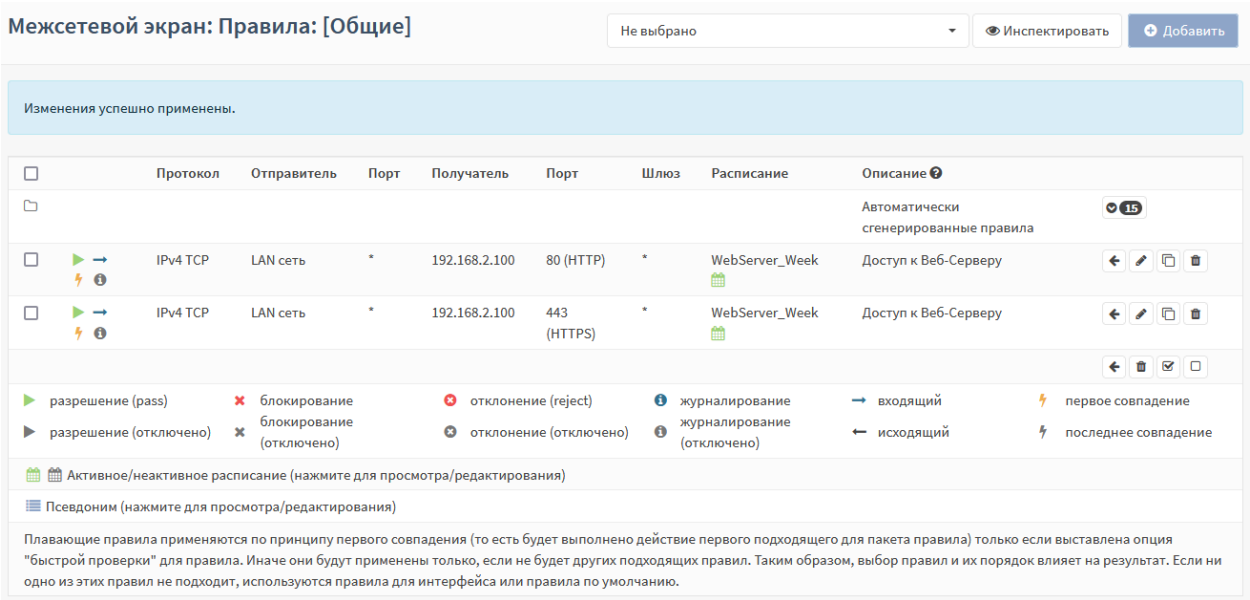

Рисунок 25 – Правила МЭ с расписанием

1.1.6 Создание правил API

Для управления извне **ARMA IF** необходимо создать соответствующие правила МЭ в подразделе управления правил API (**«Межсетевой экран»** - **«API правила»**).

Правила создаются по аналогии с другими правилами МЭ (см. Раздел 1.1.1)

Для создания правила API необходимо выполнить следующие действия:

1. Перейти в подраздел управления правил API (**«Межсетевой экран»** - **«API правила»**) и нажать **кнопку «+»**.
2. В открывшейся форме (см. Рисунок 26) задать параметры правила и нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

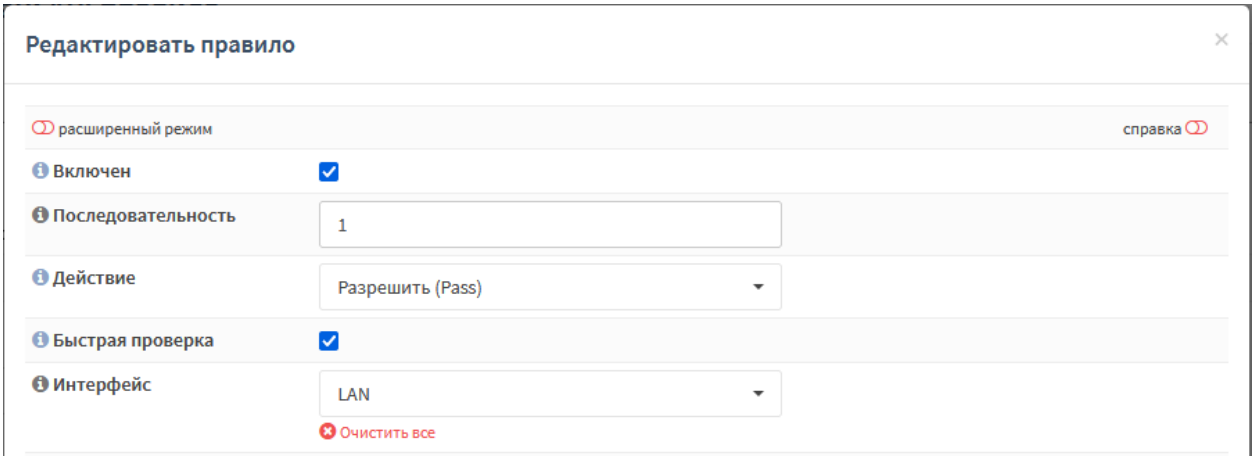

Рисунок 26 – Создание правила API

2 NAT

Трансляция сетевых адресов, сокращенно NAT – это технология преобразования IP-адресов внутренней сети «LAN» в IP-адреса внешней сети «WAN». Существуют следующие способы трансляции сетевых адресов:

- **переадресация портов** – позволяет получить доступ из внешней сети во внутреннюю сеть с перенаправлением на конкретный адрес и порт;
- **статический NAT, «Один-к-одному»** – позволяет каждому внутреннему IP-адресу присваивать уникальный внешний IP-адрес;
- **исходящий NAT, «Маскарадинг»** – позволяет множеству устройств, находящихся за NAT, выходить в сеть через один внешний IP-адрес. Скрывает структуру сети от внешнего мира.

Правила NAT задаются отдельно для каждого способа и располагаются в виде списка.

Порядок правил в списке имеет значение и им можно управлять с помощью **кнопки «»** напротив каждого из созданных правил. Сетевой пакет проверяется на совпадение с критериями правил по порядку, сверху вниз, по следующему принципу:

- **последнего совпадения** – производится действие, указанное в последнем совпавшем правиле, далее обработка сетевого пакета не производится.

2.1 Создание правила NAT «Переадресация портов»

Переадресация портов позволяет указать, что все запросы, приходящие на конкретный внешний адрес и конкретный порт маршрутизатора, должны быть перенаправлены на конкретный внутренний адрес и порт получателя.

Пример использования NAT «Переадресация портов» приведен на рисунке (см. Рисунок 27): все обращения на порт 8080 интерфейса «WAN» переадресовываются на порт 80 веб-сервера «WebServer».

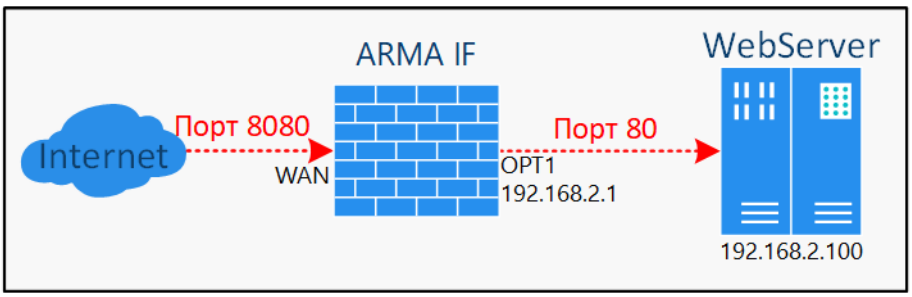

Рисунок 27 – NAT «Переадресация портов»

Для настройки переадресации портов необходимо выполнить следующие действия:

1. Перейти в подраздел управления переадресацией портов (**«Межсетевой экран»** - **«NAT»** - **«Переадресация портов»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок 28) указать следующие значения:
   - **«Интерфейс»** – «WAN»;
   - **«Версии TCP/IP»** – «IPv4»;
   - **«Протокол»** – «TCP»;
   - **«Отправитель»** – «любой»;
   - **«Диапазон портов источника»** – «любой»;
   - **«Получатель»** – «WAN адрес»;
   - **«Диапазон портов назначения»** – «от: (другое), 8080», «к: (другое), 8080»;
   - **«Целевой IP-адрес»** – «192.168.2.100»;
   - **«Целевой порт перенаправления»** – «HTTP».
3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.

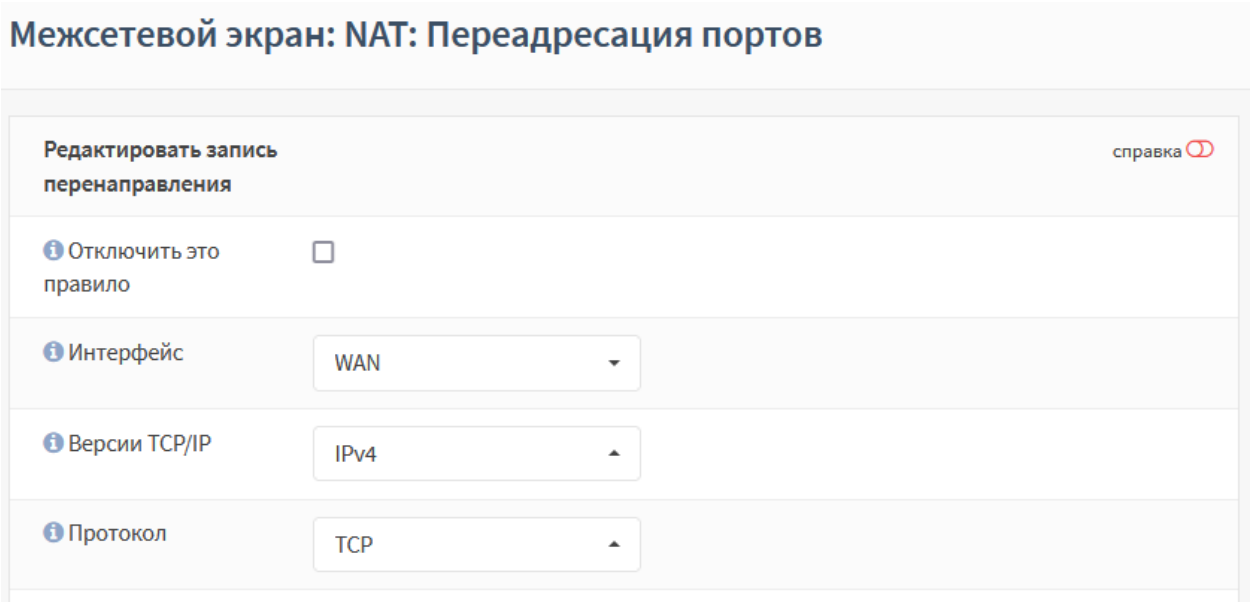

Рисунок 28 – Создание правила NAT «Переадресация портов»

2.1.1 Дополнительные параметры правила NAT «Переадресация портов»

Для параметров **«Отправитель»** и **«Получатель»** существуют чек-боксы **«Инвертировать отправителя»** и **«Инвертировать получателя»** соответственно. При установке флажка в данных чек-боксах правило будет применено для всех

отправителей/получателей, кроме значений, указанных в полях параметров **«Отправитель»**/**«Получатель»**.

Параметр **«Режим работы с сетью»** предназначен для выбора режима работы в случае использования конкретной сети в качестве целевого IP-адреса. По умолчанию используется циклический перебор транслируемых IP-адресов.

Поле **«Установить локальный тег»** предназначено для добавления внутреннего тэга пакетам, соответствующим критериям правила. Данный тэг могут проверять другие правила и фильтры NAT. Включение проверки тега осуществляется в поле **«Проверка на соответствие локального тега»**.

Параметр **«Не синхронизировать через XMLRPC»** предназначен для предотвращения передачи информации о записях состояния соединений другим участникам кластера межсетевых экранов.

Параметр **«Зеркальный NAT»** предназначен для включения/выключения возможности получить доступ к внешнему сервису из внутренней сети по публичному IP-адресу.

Параметр **«Ассоциация правила фильтрации»** необходим для создания правила МЭ разрешающего прохождение трафика перенаправления NAT. По умолчанию для параметра задано значение **«Rule»**, создающее правило МЭ, связанное с настраиваемым правилом NAT. Также доступны следующие параметры:

- **«отсутствует»** – правило МЭ создаваться не будет;
- **«добавить ассоциированное правило фильтрации»** – создаться правило МЭ, связанное с правилом NAT;
- **«добавить неассоциированное правило фильтрации»** – создаться правило МЭ, несвязанное с правилом NAT. При этом изменения, внесенные в правило NAT, необходимо будет вручную вносить в правило МЭ;
- **«разрешить (Pass)»** – разрешает прохождение трафика без правила МЭ.

2.2 Создание правила NAT «Один-к-одному»

Статический NAT «Один-к-одному» сопоставляет один внешний IP-адрес, в большинстве случаев общедоступный, с одним внутренним IP-адресом, в большинстве случаев частным. В **ARMA IF** предусмотрена настройка статического NAT двух типов:

- **«NAT»** – позволяет организовать связь между сетями одного размера, то есть применяется только в одном направлении.
- **«BINAT»** – позволяет организовать связь между разными подсетями без указания основного шлюза в настройках сетевого адаптера, то есть

определяет двунаправленное отображение между внешней и внутренней сетью и может быть использован в обоих направлениях.

Пример использования NAT «Один-к-одному» приведен на рисунке (см. Рисунок 29): все обращения на IP-адрес интерфейса «WAN» переадресовываются на IP-адрес ПК **«WebServer»**.

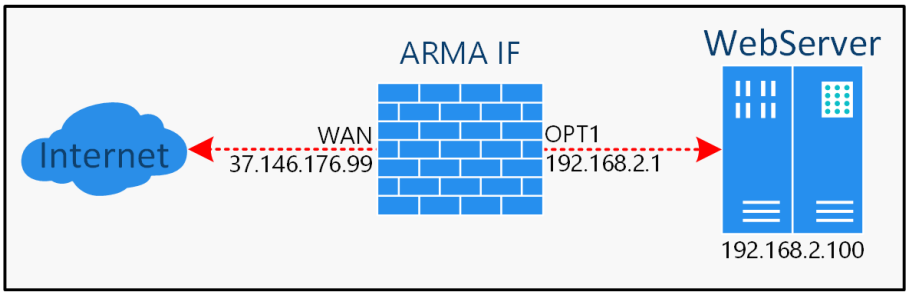

Рисунок 29 – NAT «Один-к-одному»

Для настройки статического NAT необходимо выполнить следующие действия:

1. Перейти в подраздел настроек NAT один-к-одному (**«Межсетевой экран»** - **«NAT»** - **«Один-к-одному»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок 30) указать следующие значения:
   - **«Интерфейс»** – «WAN»;
   - **«Тип»** – «BINAT»;
   - **«Внешняя сеть»** – «37.146.176.0»;
   - **«Отправитель»** – «Единственный хост или сеть, 192.168.2.100/32»;
3. Остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

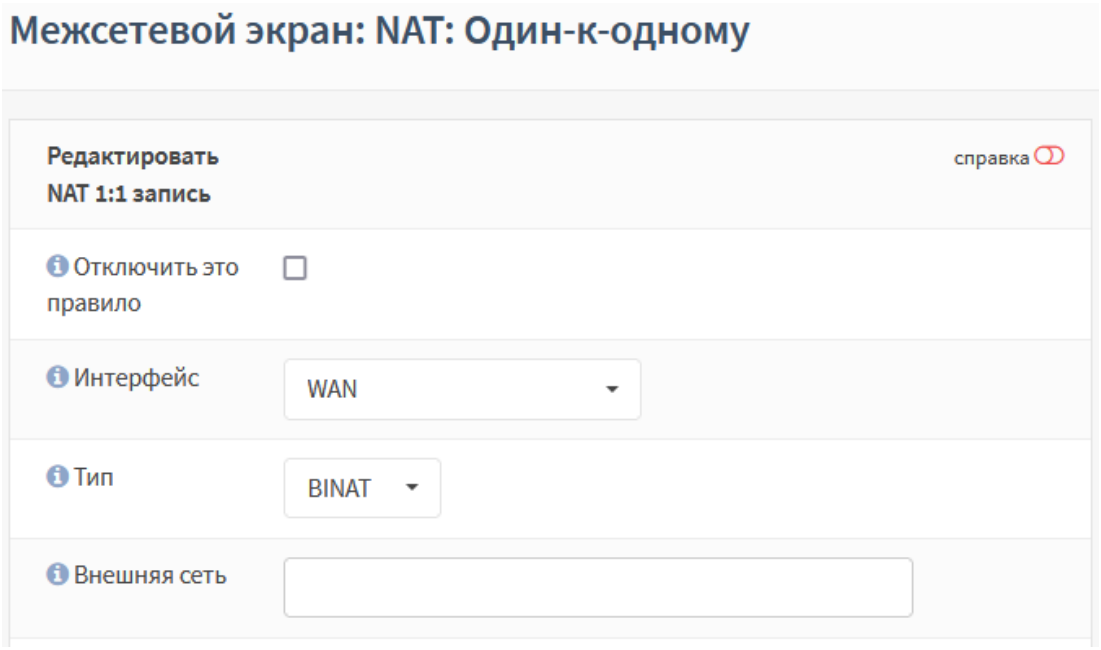

Рисунок 30 – Создание правила NAT «Один-к-одному»

2.3 Создание правила NAT «Исходящий»

В **ARMA IF** представлено четыре режима работы исходящего NAT:

- **«автоматическое создание правил исходящего NAT»** – запрет использования созданные вручную правил;
- **«ручное создание правил исходящего NAT»** – правила не будут созданы автоматически;
- **«смешанное создание правил исходящего NAT»** – автоматически созданные правила применяются после созданных вручную правил;
- **«отключить создание правил исходящего NAT»** – исходящий NAT отключен.

По умолчанию в **ARMA IF** используется режим **«Автоматическое создание правил исходящего NAT»**.

2.3.1 Автоматическое создание правил исходящего NAT

В режиме автоматического создания правил исходящего NAT система автоматически добавляет правила NAT, которые обеспечивают соединение между сетью «WAN» и внутренней сетью «LAN» (см. Рисунок 31).

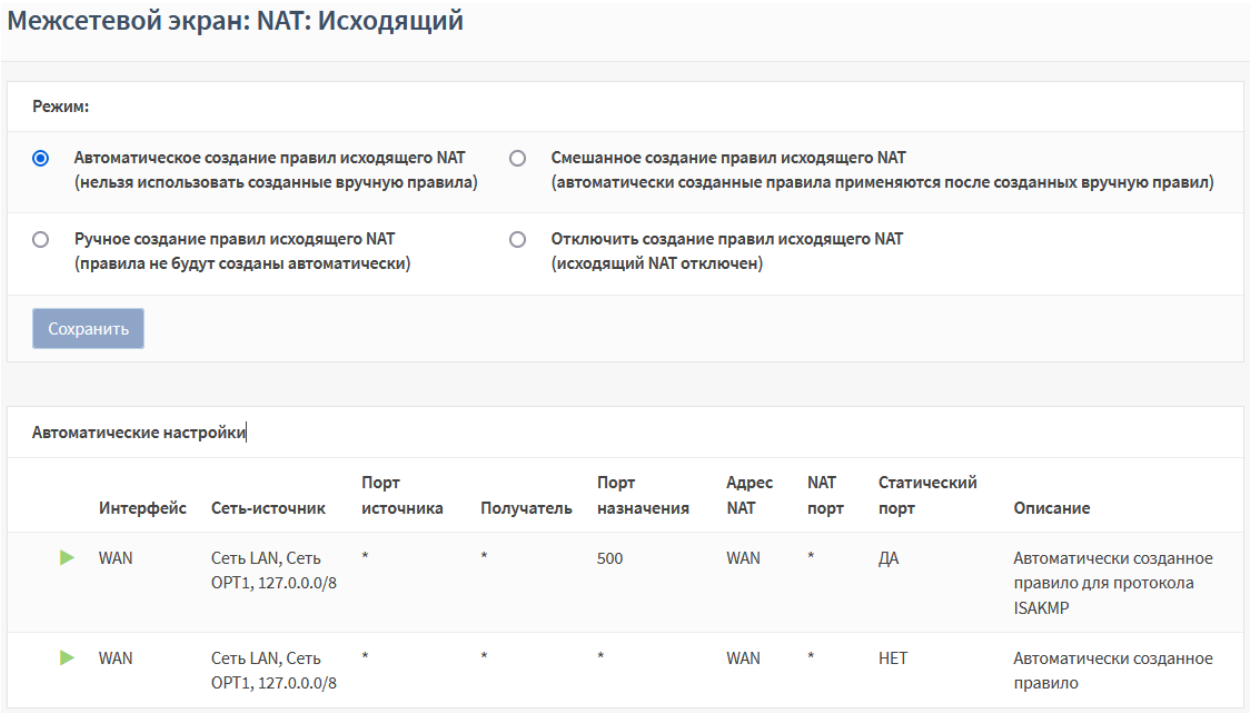

Рисунок 31 – Автоматический режим создания правил исходящего NAT

2.3.2 Ручное создание правил исходящего NAT

Режим ручного создания правил исходящего NAT позволяет вручную создавать правила исходящего NAT. Правила контролируют, как **ARMA IF** будет преобразовывать адрес источника и порты трафика, выходящего из интерфейса.

Для возможности создания правил необходимо выбрать режим ручного создания правил исходящего NAT в подразделе настроек исходящего NAT (**«Межсетевой экран»** - **«NAT»** - **«Исходящий»**) нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**. После этого появится **кнопка «+Добавить»** в правом верхнем углу страницы.

Для проверки работы созданных вручную правил исходящего NAT необходимо выполнить следующие шаги:

1. С помощью веб-браузера на ПК **«Admin»** (см. Рисунок 32) проверить доступность сайта «yandex.ru/internet».
2. Создать правило NAT со следующими основными параметрами:
   - **«Интерфейс»** – «WAN»;
   - **«IP-адрес источника»** – «LAN-сеть»;
   - **«Транслируемый IP-адрес/целевой IP-адрес»** – «WAN-адрес».
3. С помощью браузера на ПК **«Admin»** (см. Рисунок 32) проверить доступность сайта «yandex.ru/internet».

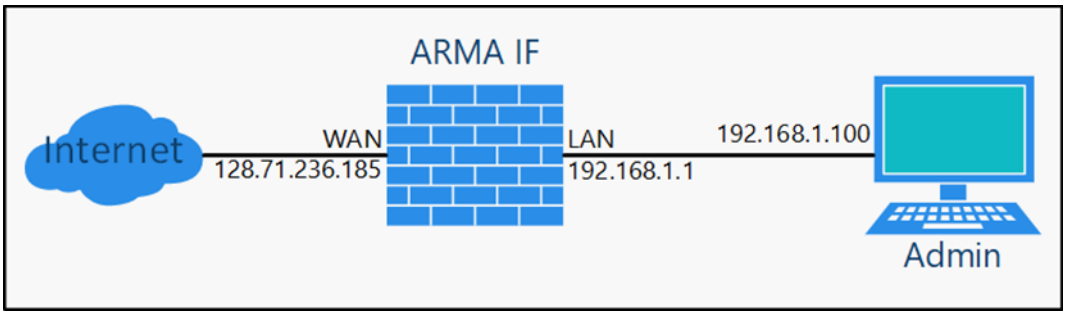

Рисунок 32 – Стенд для проверки созданных правил исходящего NAT

2.3.2.1 Проверка доступности сайта

В режиме ручного создания правил исходящего NAT правила исходящего NAT отсутствуют.

Для проверки доступности сайта необходимо открыть веб-браузер на ПК **«Admin»**, ввести в адресной строке «yandex.ru/internet» и нажать **клавишу «Enter»**. В результате откроется страница, указывающая на отсутствие доступа к сайту (см. Рисунок 33).

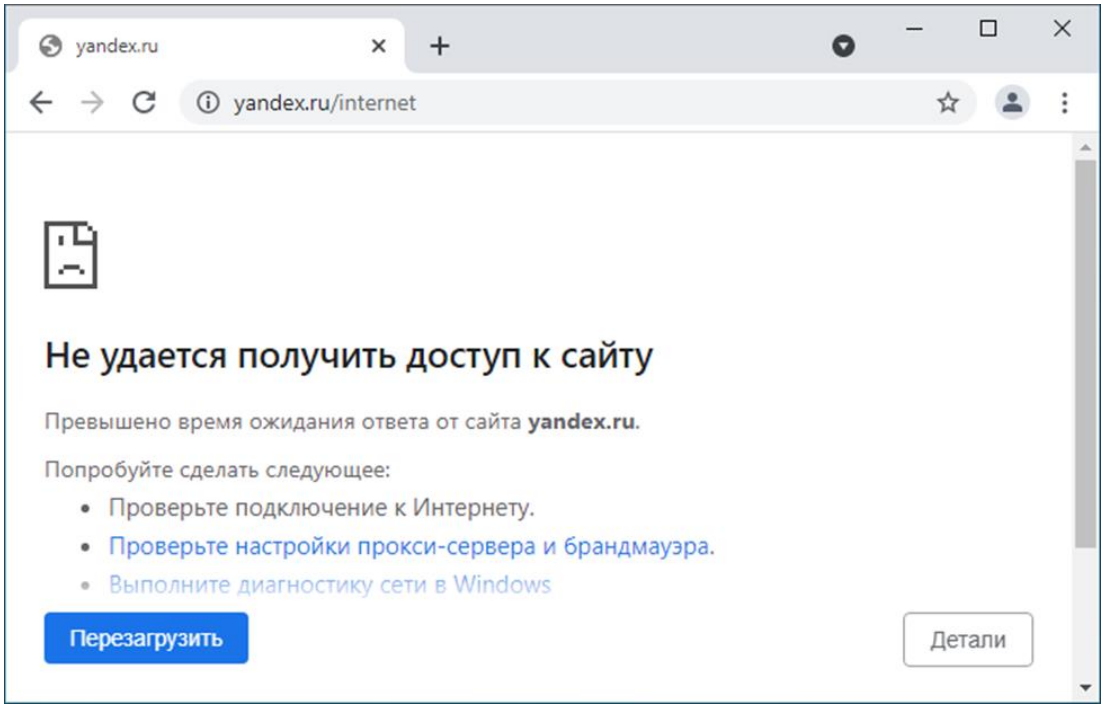

Рисунок 33 – Недоступность сайта

2.3.2.2 Создание правила NAT

Для создания правила необходимо выполнить следующие действия:

1. Перейти в подраздел настроек исходящего NAT (**«Межсетевой экран»** - **«NAT»** - **«Исходящий»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок 34) указать основные параметры указанные в примере (см. Раздел 2.3.2), нажать **кнопку «Сохранить»** и затем нажать **кнопку «Применить изменения»**.

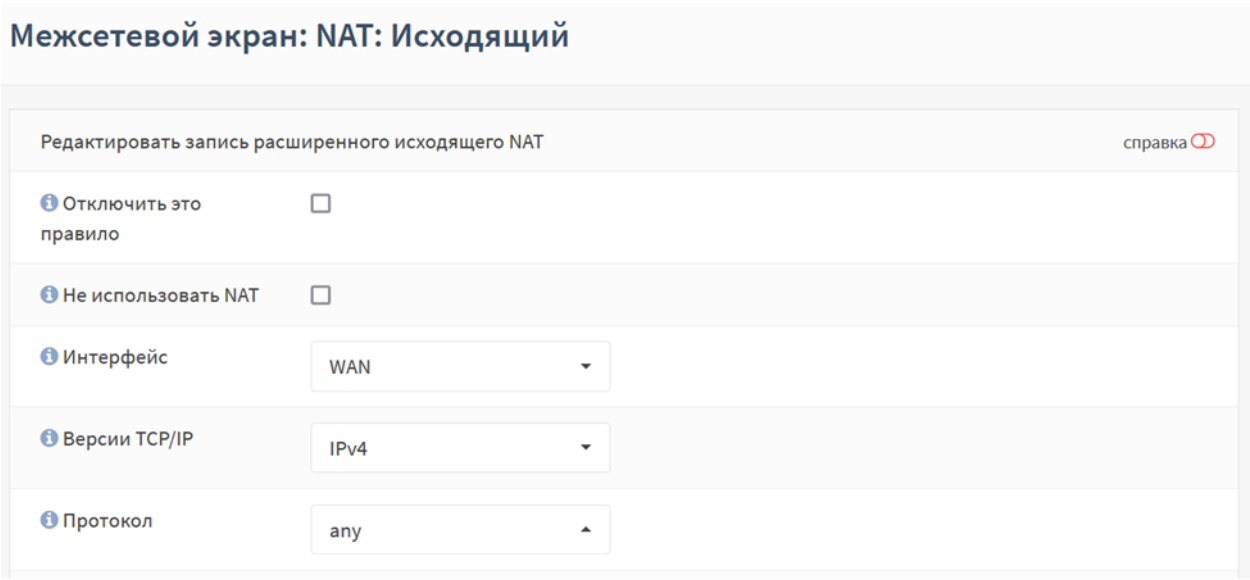

Рисунок 34 – Форма редактирования правил NAT

В результате правило исходящего NAT будет создано и отобразится в списке правил (см. Рисунок 35).

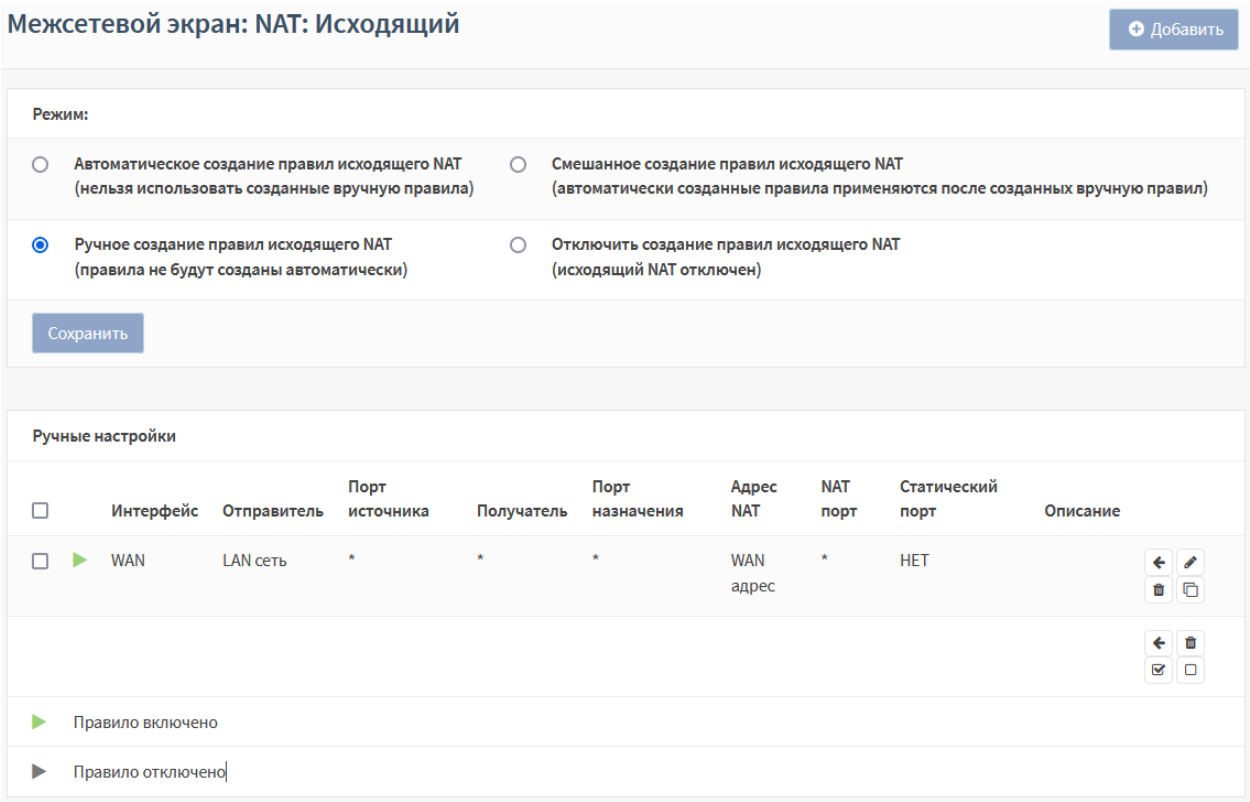

Рисунок 35 – Список правил исходящего NAT

В примере рассматриваются только основные настройки исходящего правила NAT. Остальные параметры необходимы для более тонкой настройки правил.

Порядок правил в списке имеет значение и им можно управлять с помощью **кнопки** «» напротив каждого из созданных правил. Правила обрабатываются начиная с самого верхнего и далее вниз по списку.

2.3.2.3 Проверка доступности сайта

В веб-браузере на ПК **«Admin»** ввести в адресной строке «yandex.ru/internet» и нажать **клавишу «Enter»**. В результате откроется страница с данными о внешнем IP-адресе интерфейса «WAN» (см. Рисунок 36).

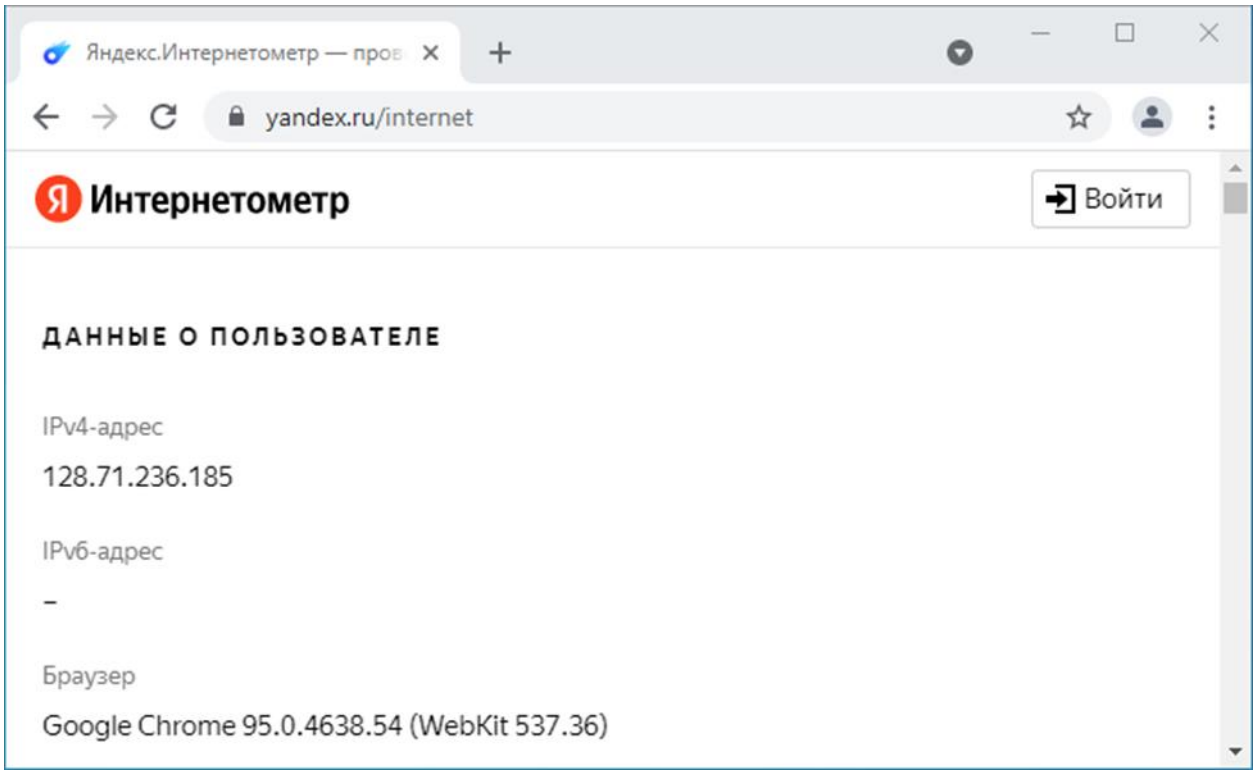

Рисунок 36 – Работа исходящего NAT

2.3.3 Смешанное создание правил исходящего NAT

Режим смешанного создания правил исходящего NAT позволяет создавать правила исходящего NAT, но также присутствуют автоматические правила исходящего NAT.

2.3.4 Отключить создание правил исходящего NAT

Режим отключения создания правил исходящего NAT отключает все правила исходящего NAT.

3 НАСТРОЙКИ ОГРАНИЧЕНИЯ ТРАФИКА

Функция ограничения трафика позволяет гибко настраивать пропускную способность канала, управлять приоритетом трафика для подсетей, хостов и приложений с целью обеспечения непрерывности критичных сетевых сервисов, в том числе в моменты пиковой сетевой нагрузки.

Примеры использования ограничения трафика:

- ограничение скорости входящего и исходящего соединений;
- ограничение максимальной пропускной способности на интерфейсе;
- приоритезация одного вида трафика перед другим.

В качестве примера настройки будет использоваться следующее ограничение трафика:

- **сегмент «LAN»** – 192.168.1.0/24, хост сегмента 192.168.1.100;
- **сегмент «WAN»** – 192.168.2.0/24, хост сегмента 192.168.2.100;
- **скорость входящего соединения** – 10 Мбит/с, из сегмента «WAN» в сегмент «LAN»;
- **скорость исходящего соединения** – 1 Мбит/с, из сегмента «LAN» в сегмент «WAN»;
- **равномерное распределение скорости** – между всеми хостами сегмента «LAN».

Для проверки корректности настройки будет использоваться утилита командной строки «iperf», не входящая в состав **ARMA IF**.

До момента настройки ограничений пропускная способность равна 431 Мбит/с и 456 Мбит/с для исходящего и входящего соединений соответственно (см. Рисунок 37).

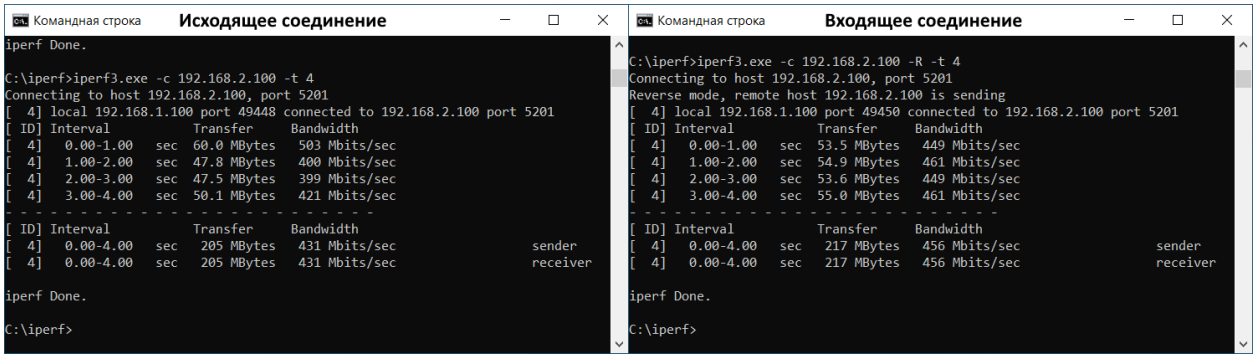

Рисунок 37 – Результат работы утилиты «iperf»

Утилита «iperf» запущена со следующими параметрами:

- в качестве сервера на хосте, находящимся в сети интерфейса «WAN»;

- в режиме измерения пропускной способности на хосте, находящимся в сети интерфейса «LAN».

3.1 Ограничение трафика

Подраздел ограничения трафика (**«Межсетевой экран»** - **«Ограничение трафика»**) содержит три вкладки (см. Рисунок 38):

- **«Каналы»** – настраиваются ограничения пропускной способности;
- **«Очереди»** – настраивается пропускная способность внутри канала и приоритет пропускной способности определённым приложениям;
- **«Правила»** – задаются правила, согласно которым будут применены ограничения трафика.

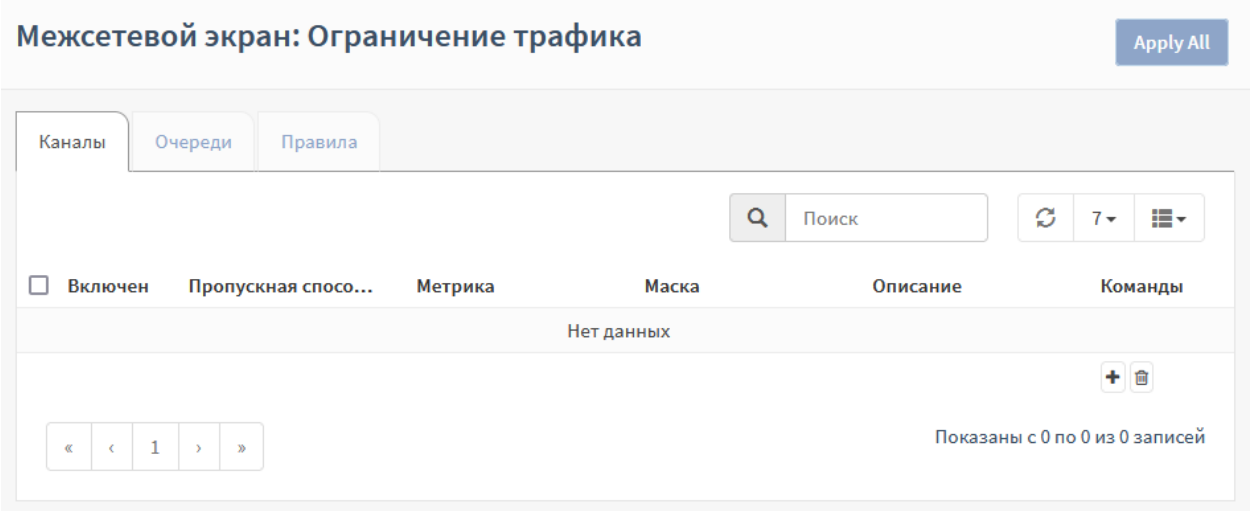

Рисунок 38 – Функция «Ограничение трафика»

3.1.1 Вкладка «Каналы»

Во вкладке настраиваются ограничения пропускной способности.

В данной вкладке необходимо создать два канала со следующими параметрами (см. Таблица 6):

Таблица 6
Значения параметров каналов

Параметр	Исходящий канал	Входящий канал
Пропускная способность	1	10
Единицы измерения пропускной способности	Мбит/с	Мбит/с
Описание	1Mbps_UP	10Mbps_Down

Для добавления канала необходимо выполнить следующие действия:

1. Нажать **кнопку «+»** в правой части формы.
2. В открывшейся форме (см. Рисунок 39) указать параметры (см. Таблица 6).

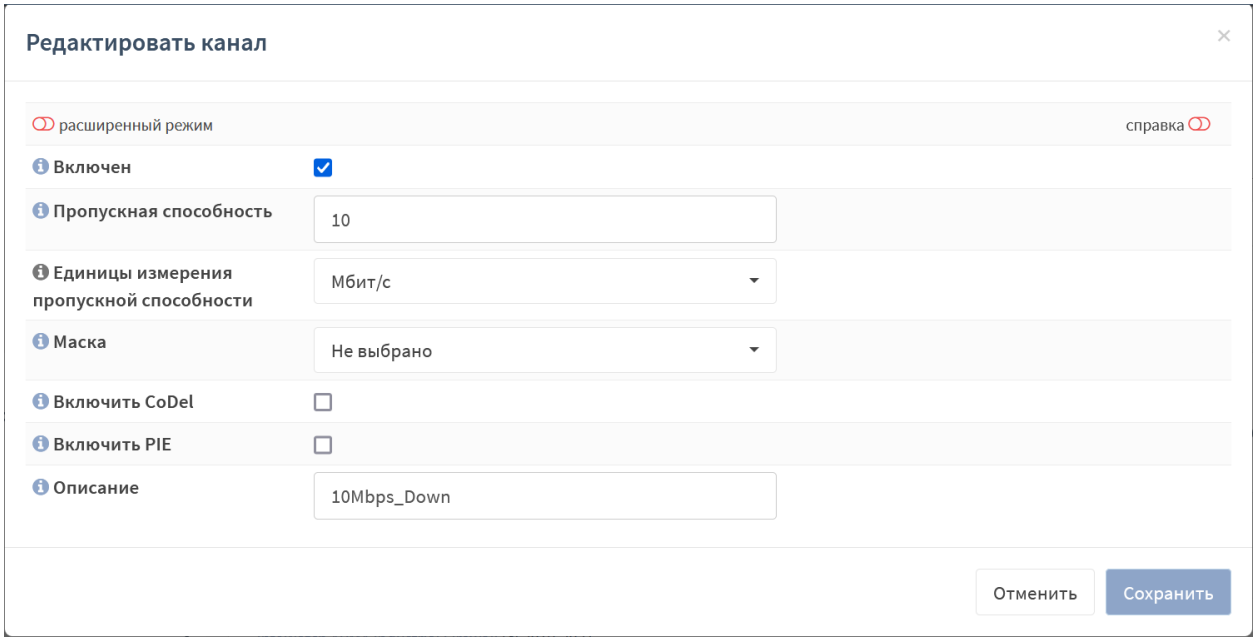

Рисунок 39 – Редактирование канала

3. Нажать **кнопку «Сохранить»**.
4. В результате канал будет добавлен в список (см. Рисунок 40).

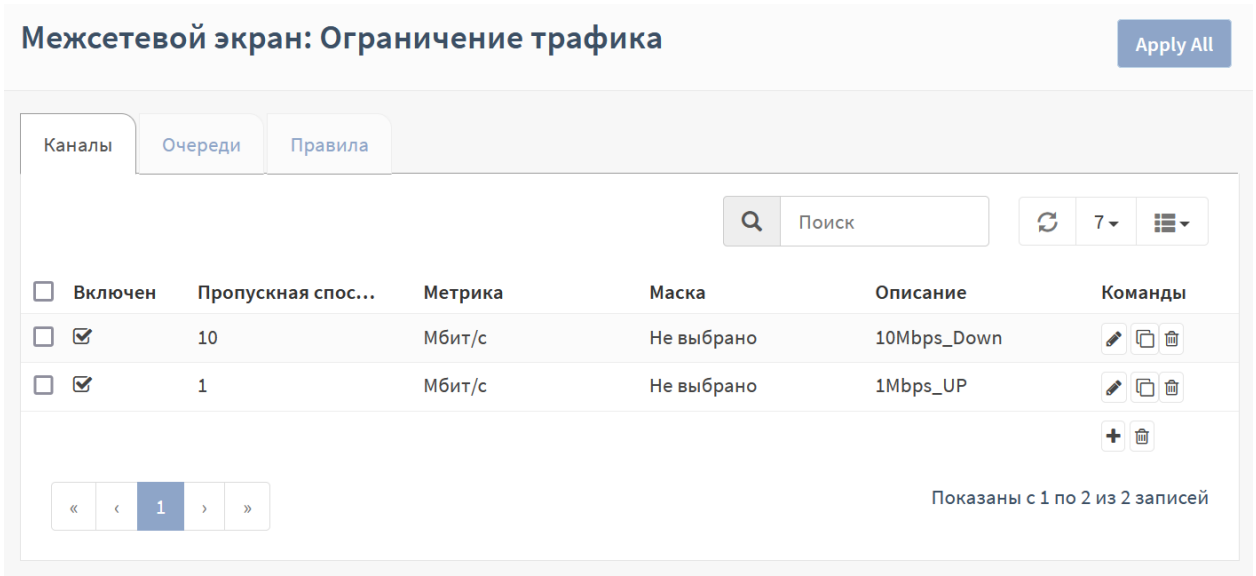

Рисунок 40 – Список каналов

При переключении выключателя **«Расширенный режим»** (см. Рисунок 39) в верхней левой части формы будут доступны дополнительные параметры для более тонкой настройки ограничений трафика:

- **«Очередь»**;
- **«Buckets»**;

- **«Тип планировщика»**;
- **«(FQ-)CoDel target»**;
- **«(FQ-)CoDel интервал»**;
- **«(FQ-)CoDel ECN»**;
- **«FQ-CoDel quantum»**;
- **«FQ-CoDel ограничение»**;
- **«FQ-CoDel потоки»**;
- **«Задержка»**.

3.1.2 Вкладка «Очереди»

В данной вкладке необходимо создать две очереди со следующими параметрами (см. Таблица 7):

Таблица 7
Значения параметров очереди

Параметр	Исходящий канал	Входящий канал
Канал	1Mbps_UP	10Mbps_Down
Весовой коэффициент	100	100
Описание	Queue_UP	Queue_Down

Для добавления очереди необходимо выполнить следующие действия:

1. Нажать **кнопку «** **»** в правой части формы.
2. В открывшейся форме (см. Рисунок 41) указать параметры (см. Таблица 7).

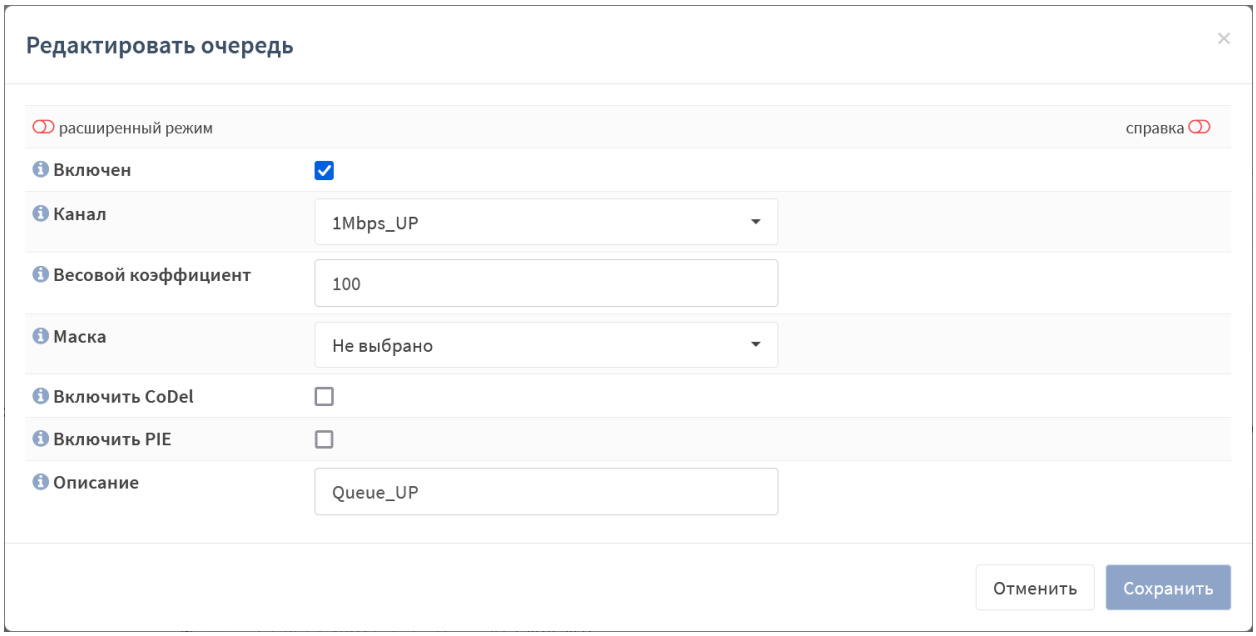

Рисунок 41 – Редактирование очереди

3. Нажать **кнопку «Сохранить»**.
4. В результате очередь будет добавлена в список (см. Рисунок 42).

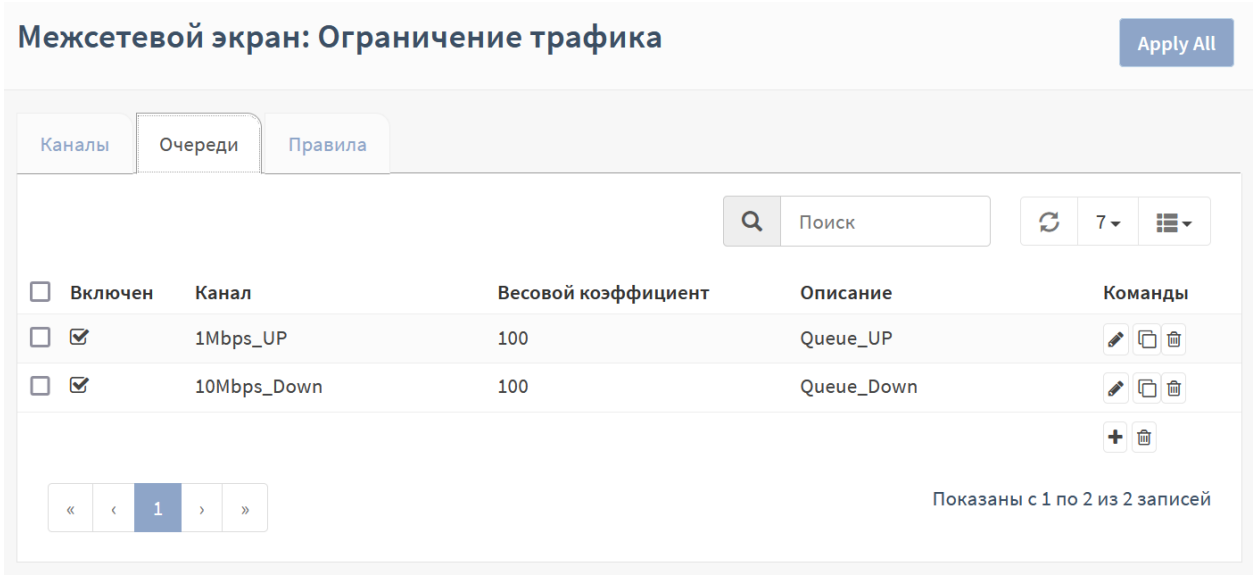

Рисунок 42 – Список очередей

При переключении выключателя **«Расширенный режим»** (см. Рисунок 41) в верхней левой части формы будут доступны дополнительные параметры очереди для более тонкой настройки ограничений трафика:

- **«Очередь»**;
- **«Buckets»**;
- **«Тип планировщика»**;
- **«(FQ-)CoDel target»**;

- **«(FQ-)CoDel интервал»**;
- **«(FQ-)CoDel ECN»**.

3.1.3 Вкладка «Правила»

В данной вкладке необходимо создать два правила со следующими параметрами (см. Таблица 8):

Таблица 8
Значения параметров правила

Параметр	Исходящий канал	Входящий канал
Интерфейс	WAN	WAN
Протокол	IP	IP
Отправитель	192.168.1.0/24	any
Порт источника	any	any
Получатель	any	192.168.1.0/24
Порт назначения	any	any
Канал/очередь	Queue_UP	Queue_Down
Описание	Upload	Download

Для добавления правила необходимо выполнить следующие действия:

1. Нажать **кнопку «** **+** **»** в правой части формы.
2. В открывшейся форме (см. Рисунок 43) указать параметры (см. Таблица 8).

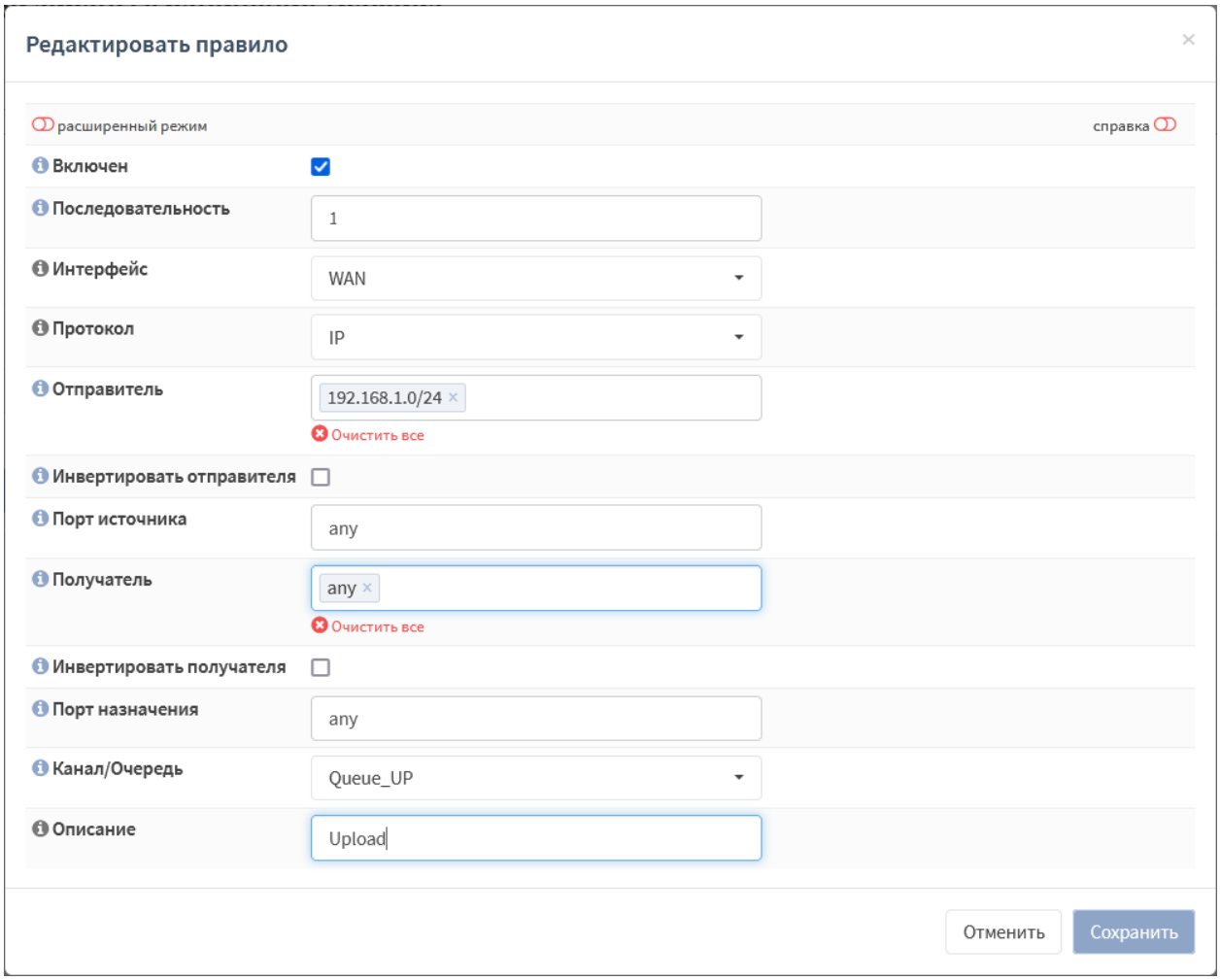

Рисунок 43 – Редактирование правила

3. Нажать **кнопку «Сохранить»**. В результате очередь будет добавлена в список (см. Рисунок 44).

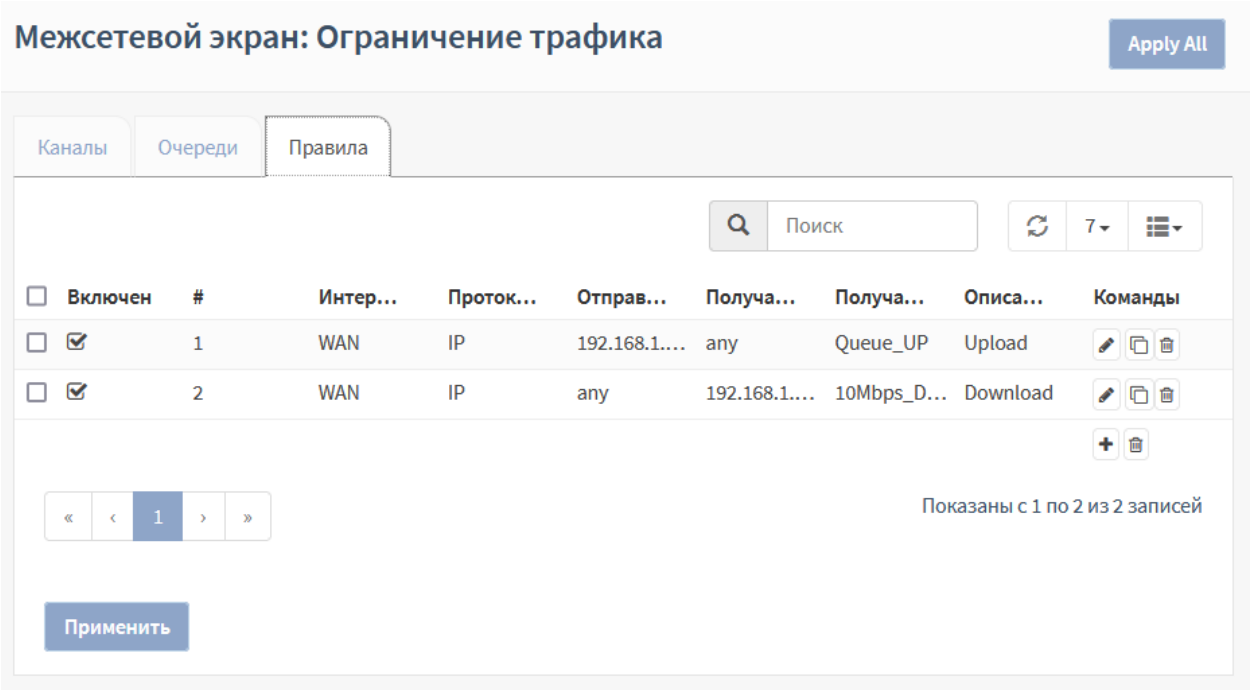

Рисунок 44 – Список правил

4. Нажать **кнопку «Apply All»** для применения ограничений.

При переключении выключателя **«Расширенный режим»** (см. Рисунок 44) в верхней левой части формы будут доступны дополнительные параметры правила для более тонкой настройки ограничений трафика:

- **«Интерфейс 2»**;
- **«DSCP»**;
- **«Направление»**.

3.1.4 Проверка ограничения трафика

Для проверки корректности настройки использоваться утилита командной строки «iperf», не входящая в состав **ARMA IF**.

После настройки и применения ограничений пропускная способность равна 1 Мбит/с и 10 Мбит/с для исходящего и входящего соединений соответственно (см. Рисунок 45).

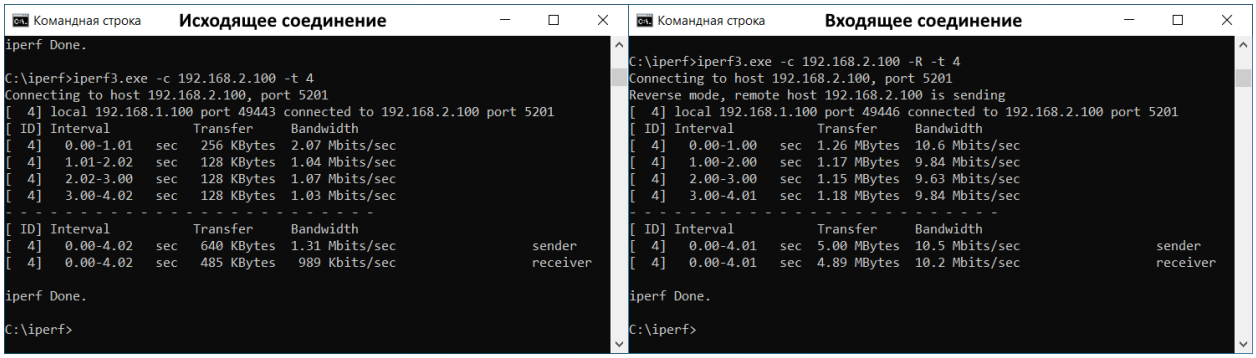

Рисунок 45 – Результат работы утилиты «iperf»

3.2 Статус

В подразделе отображаются настроенные ограничения и результаты их работы (см. Рисунок 46).

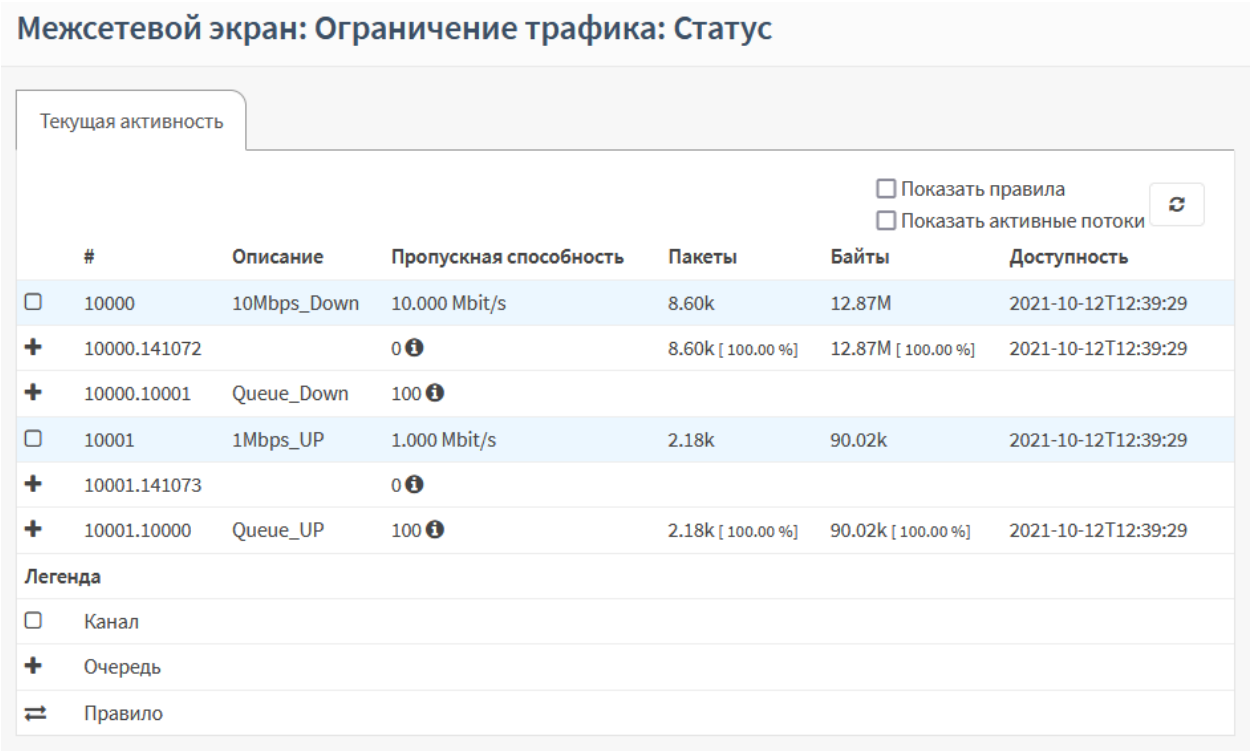

Рисунок 46 – Текущие ограничения трафика

При необходимости отобразить правила или активные потоки необходимо установить флажок напротив соответствующего значения в верхней правой части формы.

4 НАСТРОЙКА ОТКАЗОУСТОЙЧИВОГО КЛАСТЕРА

Кластер – это логическое и физическое объединение нескольких объектов со схожими функциями в одну группу с целью повышения эффективности.

В случае объединения двух **ARMA IF** в каждый момент времени только одно устройство **ARMA IF** в кластере обрабатывает весь трафик, такое устройство считается ведущим. Подчиненные, резервные устройства постоянно синхронизируют свое состояние с ведущим устройством. В случае выхода из строя ведущего устройства его подменяет одно из резервных устройств, которое само становится ведущим и начинает обрабатывать трафик. В случае если «старое» ведущее устройство вновь переходит в рабочее состояние, то текущие ведущее устройство возвращается в статус подчиненного резервного устройства.

Для настройки работы **ARMA IF** в режиме отказоустойчивого кластера используется схема, представленная на рисунке (Рисунок 47). Оба **ARMA IF** подключены к одним и тем же коммутаторам для обеспечения работы в режиме отказоустойчивого кластера, а между собой **ARMA IF** также соединены сетевым кабелем для обеспечения передачи состояния устройств.

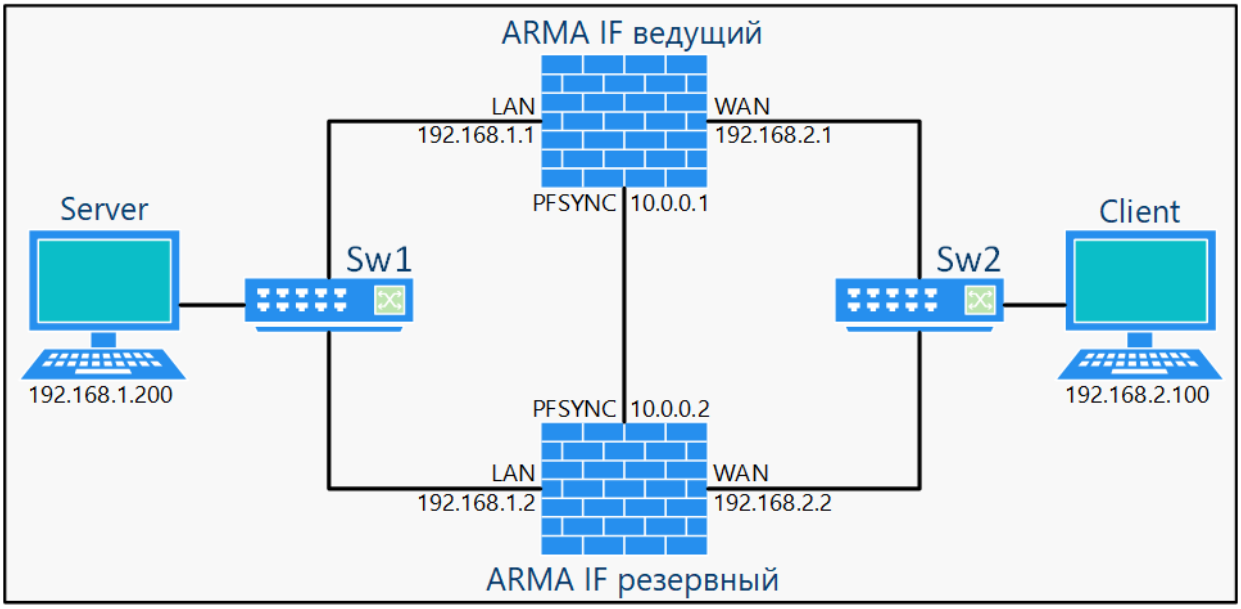

Рисунок 47 – Схема стенда для настройки режима отказоустойчивого кластера

Настройка и проверка работы **ARMA IF** в режиме отказоустойчивого кластера состоит из следующих этапов:

1. Добавить на ведущем устройстве виртуальные IP-адреса для сегментов сети.
2. Настроить режим отказоустойчивого кластера на резервном устройстве.
3. Настроить режим отказоустойчивого кластера на ведущем устройстве.
4. Выполнение проверки корректной работы устройств.

В примере у каждого экземпляра **ARMA IF** используются три сетевых интерфейса: «LAN», «WAN» и «PFSYNC». Каждый из интерфейсов имеет базовые настройки. В случае использования ВМ необходимо в настройках гипервизора включить режим **«Promiscuous mode»** на виртуальных сетевых интерфейсах для корректной работы кластера.

Сетевым интерфейсам необходимо назначить IP-адреса, указанные в таблице (см. Таблица 9). Настройка IP-адресов производится в разделе **«Интерфейсы»** (см. Раздел 14.2).

Таблица 9
IP-адреса для интерфейсов МЭ

Интерфейс	Ведущий ARMA IF	Резервный ARMA IF
LAN	192.168.1.1/24	192.168.1.2/24
WAN	192.168.2.1/24	192.168.2.2/24
PFSYNC	10.0.0.1/24	10.0.0.2/24

4.1 Настройка устройств кластера

4.1.1 Добавление виртуальных IP-адресов на ведущем устройстве

Для добавления IP-адресов на ведущем устройстве необходимо выполнить следующие действия:

1. Перейти в подраздел настроек виртуальных адресов (**«Межсетевой экран»** - **«Виртуальные IP-адреса»** - **«Настройки»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок 48) указать параметры IP-адреса для LAN-интерфейса и нажать **кнопку «Сохранить»**, затем вновь нажать **кнопку «+Добавить»**, указать параметры IP-адреса для WAN-интерфейса и нажать **кнопку «Сохранить»**. Данные для IP-адресов указаны в таблице (см. Таблица 10).

!Важно В случае, когда **ARMA IF** используется в подсети в качестве шлюза по умолчанию, необходимо изменить для клиентов шлюз по умолчанию на созданный виртуальный IP-адрес.

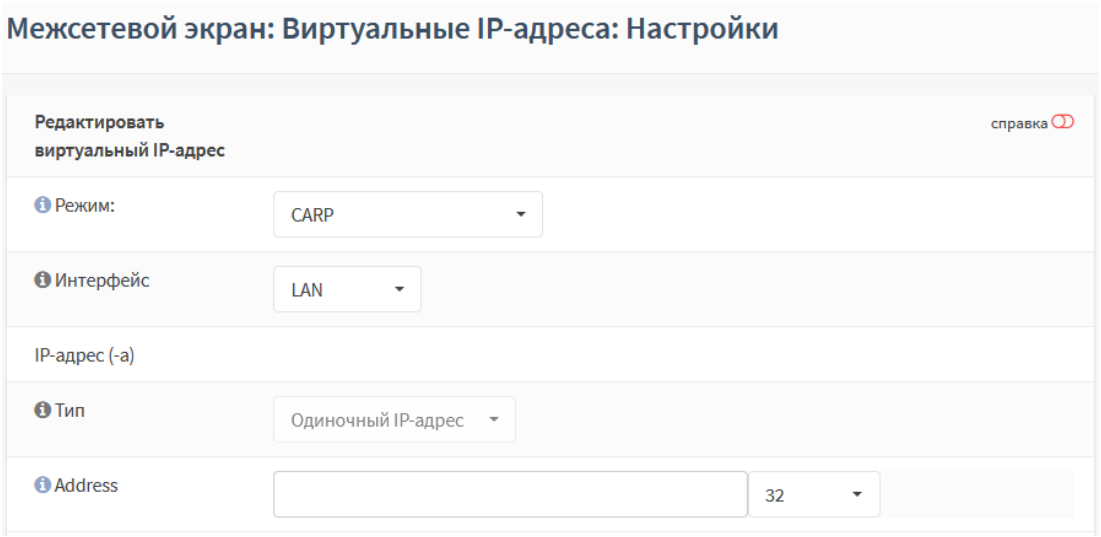

Рисунок 48 – Форма создания виртуального IP-адреса

Таблица 10
Параметры виртуальных IP-адресов

Параметр	Значения для IP-адреса LAN-интерфейса	Значения для IP-адреса WAN-интерфейса
Режим	CARP	CARP
Интерфейс	LAN	WAN
Адрес	192.168.1.254/24	192.168.2.254/24
Пароль*	1234	1234
Группа VHID*	1	2
Описание	Виртуальный IP-адрес на LAN стороне	Виртуальный IP-адрес на WAN стороне

***значение параметра **«Пароль»** указано в качестве примера, параметр **«Группа VHID»** должен отличаться для каждого интерфейса.

4.1.2 Порядок настройки резервного устройства

Для настройки режима работы **ARMA IF** в режиме отказоустойчивого кластера на резервном устройстве необходимо выполнить следующие действия:

1. Перейти в подраздел настроек синхронизации состояния (**«Система»** - **«Высокий уровень доступности»** - **«Настройки»**) и включить синхронизацию состояния установив флажок в параметре **«Синхронизация состояния»** (см. Рисунок 49).

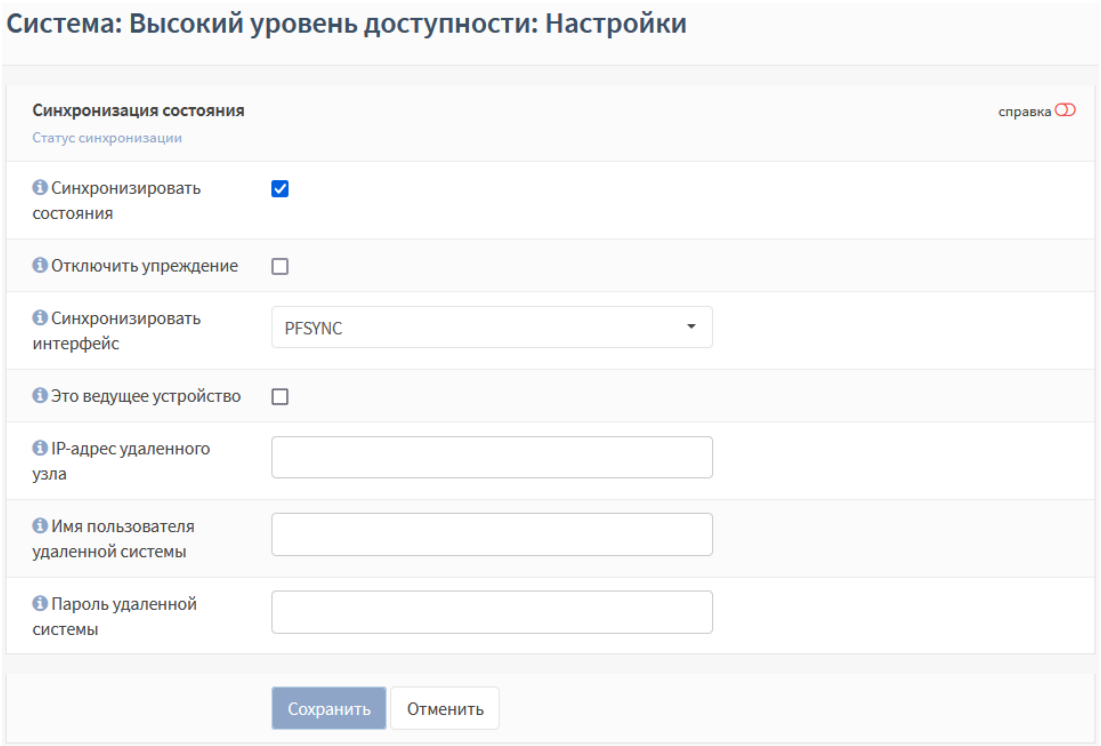

Рисунок 49 – Настройка синхронизации

2. Указать интерфейс синхронизации – **«PFSYNC»**.
3. Указать данные резервного устройства:
    - **«IP-адрес удаленного узла»** – «10.0.0.1»;
    - **«Имя пользователя удаленной системы»** – «root», значение по умолчанию;
    - **«Пароль удаленной системы»** – «root», значение по умолчанию.
4. Нажать **кнопку «Сохранить»**.

4.1.3 Порядок настройки ведущего устройства

Для настройки режима работы **ARMA IF** в режиме отказоустойчивого кластера на ведущем устройстве необходимо выполнить следующие действия:

1. Перейти в подраздел настроек синхронизации состояния (**«Система»** - **«Высокий уровень доступности»** - **«Настройки»**) и включить синхронизацию состояния установив флажок в параметре **«Синхронизация состояния»** (см. Рисунок 49).
2. Указать интерфейс синхронизации – **«PFSYNC»** и установить флажок в параметре **«Это ведущее устройство»**.
3. Указать данные резервного устройства:
    - **«IP-адрес удаленного узла»** – «10.0.0.2»;

- **«Имя пользователя удаленной системы»** – «root», значение по умолчанию;
- **«Пароль удаленной системы»** – «root», значение по умолчанию.

4. Нажать **кнопку «Сохранить»**.

После применения изменений в подразделе настроек виртуальных адресов на резервном устройстве (**«Межсетевой экран»** - **«Виртуальные IP-адреса»** - **«Настройки»**) появятся виртуальные IP-адреса, созданные на ведущем устройстве (Рисунок 50).

Рисунок 50 – Синхронизированные виртуальные IP-адреса

4.2 Проверка работы отказоустойчивого кластера

Статус работы кластера отображается в подразделе статуса виртуальных IP-адресов (**«Межсетевой экран»** - **«Виртуальные IP-адреса»** - **«Статус»**) (см. Рисунок 51 и Рисунок 52).

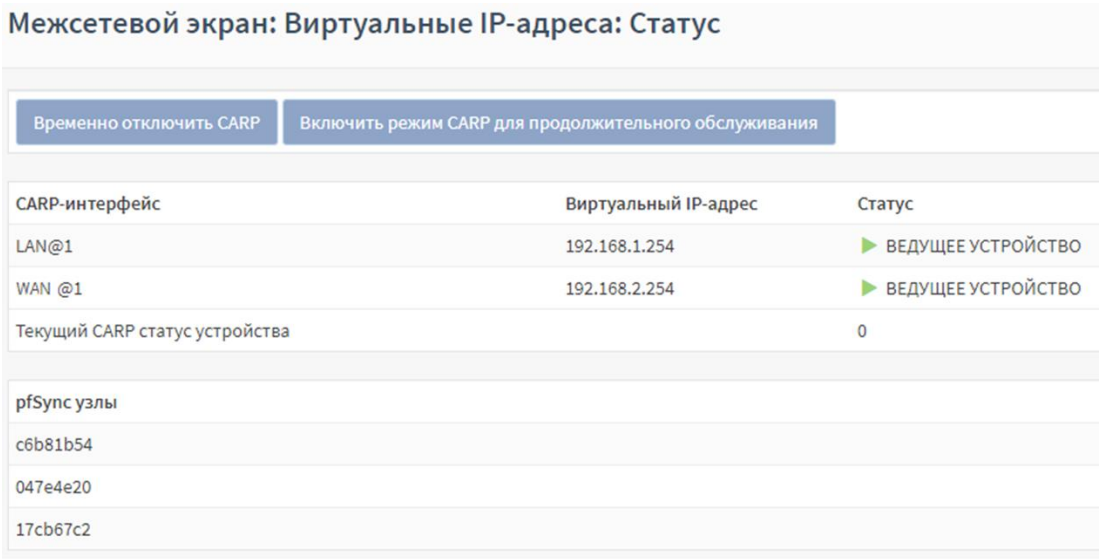

Рисунок 51 – Статус работы кластера на ведущем устройстве

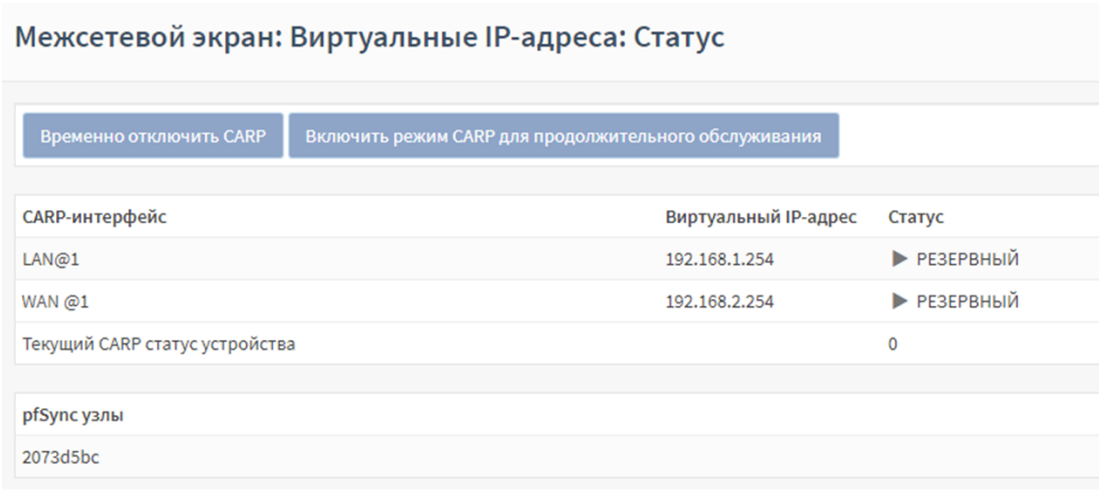

Рисунок 52 – Статус работы кластера на резервном устройстве

Проверка режима отказоустойчивого кластера считается успешно пройденной, когда после выключения ведущего устройства, значение статуса работы кластера резервного устройства поменяется с **«РЕЗЕРВНЫЙ»** на **«ВЕДУЩЕЕ УСТРОЙСТВО»**.

При переключении устройства возможен обрыв соединения продолжительностью примерно одна секунда.

!Важно В случае отключения интерфейса ведущего устройства путем снятия флажка в параметре **«Включен»** подраздела **«[Название интерфейса]»** (например, **«[WAN]»**) переключение устройств не произойдёт.

5 СИСТЕМА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

СОВ в **ARMA IF** основана на ПО «Suricata» с открытым исходным кодом и использует метод захвата пакетов «Netmap» для повышения производительности и минимизации нагрузки на ЦП.

СОВ в **ARMA IF** позволяет решать следующие задачи:

- обнаружение и предотвращение эксплуатирования уязвимостей в протоколах DNS, FTP, ICMP, IMAP, POP3, HTTP, NetBIOS, DCERPC, SNMP, TFTP, VOIP;
- обнаружение и предотвращение использования эксплойтов и уязвимостей сетевых приложений;
- обнаружение и блокировка DOS-атак;
- обнаружение и блокировка сетевого сканирования;
- блокировка трафика ботнетов;
- блокировка трафика от скомпрометированных хостов;
- блокировка трафика от хостов, зараженных троянским ПО и сетевыми червями.

!Важно Блокировка трафика производится только при включенном режиме IPS. При выключенном режиме IPS производятся только уведомления о блокировке трафика.

Правила СОВ отображаются во вкладке **«Правила»** подраздела администрирования СОВ (**«Обнаружение вторжений»** - **«Администрирование»**).

Правила обрабатываются в следующем порядке, зависящим от действия над пакетом трафика:

1. **«Pass»** – разрешить движение пакета;
2. **«Drop»** – отбросить пакет;
3. **«Reject»** – отклонить пакет;
4. **«Alert»** – оповестить о пакете.

5.1 Основные настройки СОВ

Перед использованием СОВ необходимо убедиться, что отключен режим «Hardware Offloading». Для выключения данного режима необходимо перейти в подраздел настройки интерфейсов (**«Интерфейсы»** - **«Настройки»**), установить флажки напротив параметров:

- **«CRC аппаратного обеспечения»**;
- **«TSO аппаратного обеспечения»**;

- **«LRO аппаратного обеспечения»**;

и нажать **кнопку «Сохранить»** внизу страницы (см. Рисунок 53).

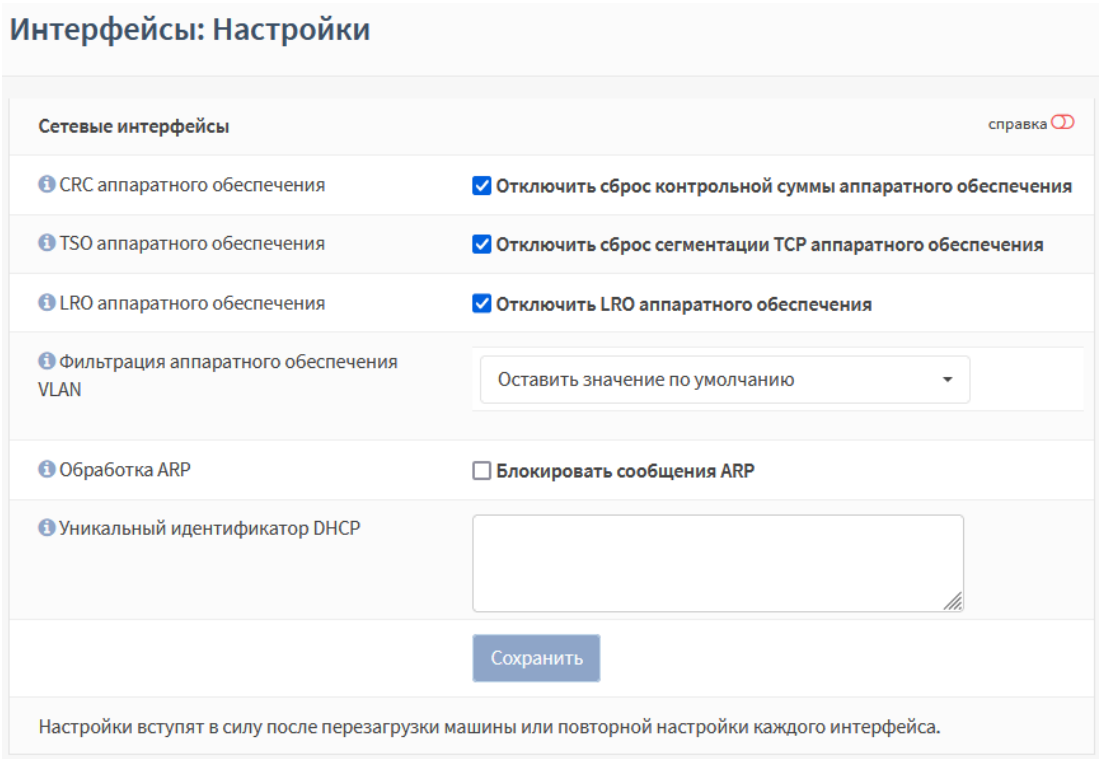

Рисунок 53 – Отключение режима Hardware Offloading

Для включения СОВ необходимо выполнить следующие действия:

1. Перейти в подраздел администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**) и, на вкладке **«Настройки»**, установить флажок для параметра **«Включен»** (см. Рисунок 54).
2. Выбрать интерфейсы, которые необходимо будет защищать в параметре **«Интерфейсы»**.
3. Включить переключатель **«Расширенный режим»**, указать значения используемых локальных подсетей в поле **«Домашние сети ($HOME_NET)»** и нажать **кнопку «Применить»**.

!Важно Для включения системы предотвращения вторжений необходимо установить флажок для параметра **«Режим IPS»**.

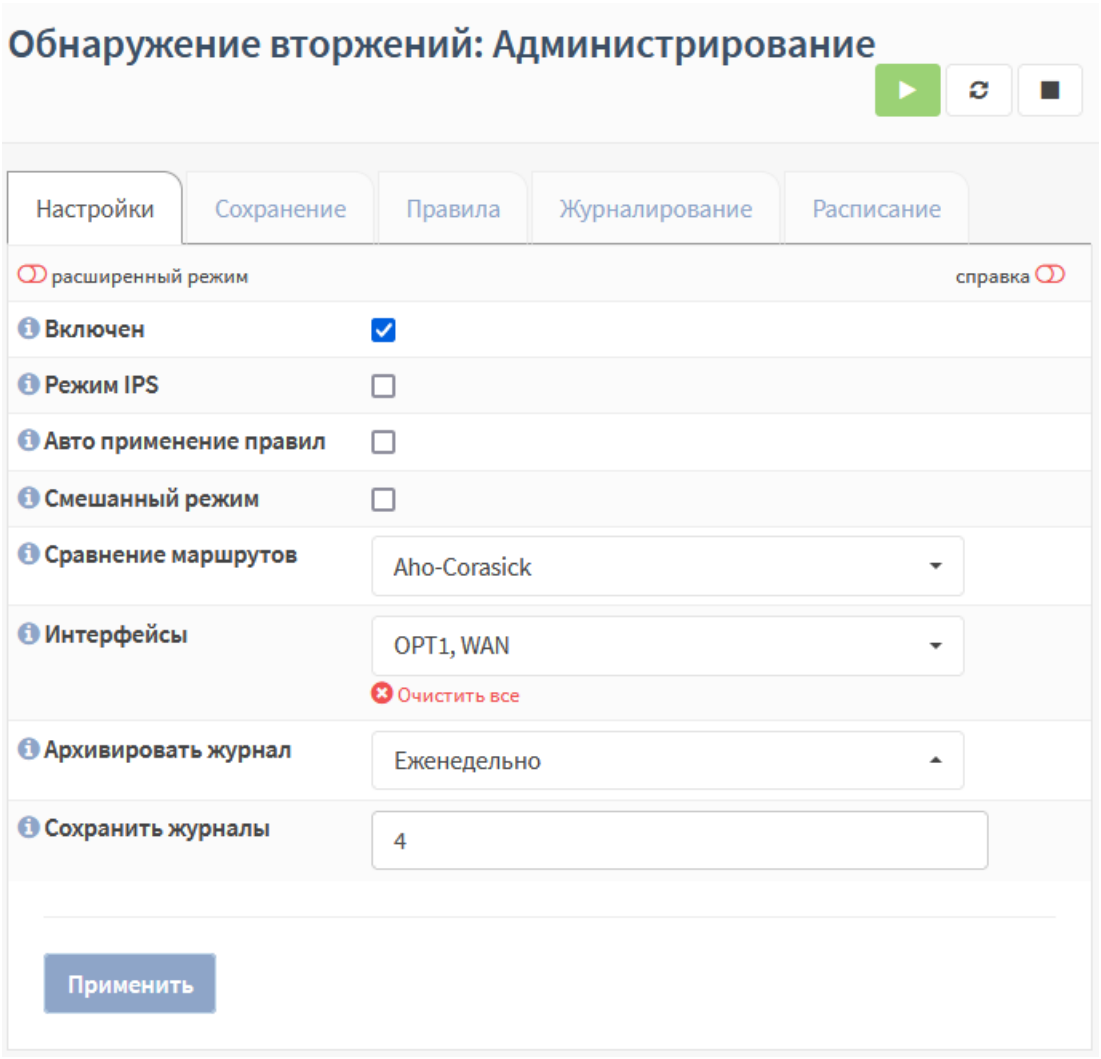

Рисунок 54 – Включение СОВ

После включения СОВ возможно будет просмотреть пакеты трафика, прошедшие через **ARMA IF** (см. Раздел 27.10)

Работу СОВ возможно проверить, настроив правило из раздела 5.5.1 настоящего руководства.

5.1.1 Дополнительные настройки СОВ

Часть дополнительных параметров доступна при включенном переключателе **«Расширенный режим»**.

Параметр **«Авто применение правил»** – включает автоматическое применение правил во время обновления.

Параметр **«Смешанный режим»** включает захват данных на физическом интерфейсе, например, на конфигурациях IPS с VLAN.

Параметр **«Сравнение маршрутов»** выбирается один из алгоритмов поиска подстроки при обработке пакетов:

- **«Aho-Corasick»** – алгоритм сопоставления «со словарем», находящий подстроки из «словаря» в пакетах. Используется по умолчанию;
- **«Hyperscan»** – высокопроизводительная библиотека сопоставления регулярных выражений от фирмы «Intel».

Параметр **«Размер пакета по умолчанию»** – задаёт размер пакетов по умолчанию в сети.

Параметры **«Архивировать журнал»** и **«Сохранить журналы»** отвечают за ведение журнала работы СОВ.

Параметры **«Содержимое пакета для журнала»** и **«Журналировать пакет»** отвечают за полноту информации о трафике, содержащейся в журнале работы СОВ.

Параметры **«Уровень приложения: Modbus порт(-ы)»** и **«Уровень приложения: MMS порт(-ы)»** задают значения портов, отличных от стандартных, для соответствующих протоколов.

5.2 Загрузка и включение наборов правил

Обновление базы решающих правил осуществляется путем импорта файла с сигнатурами в формате «Suricata» с помощью веб-интерфейса.

Включать/выключать, скачивать, обновлять и загружать локальные наборы правил необходимо во вкладке **«Сохранение»** подраздела администрирования СОВ (**«Обнаружение вторжений»** - **«Администрирование»**) (см. Рисунок 55).

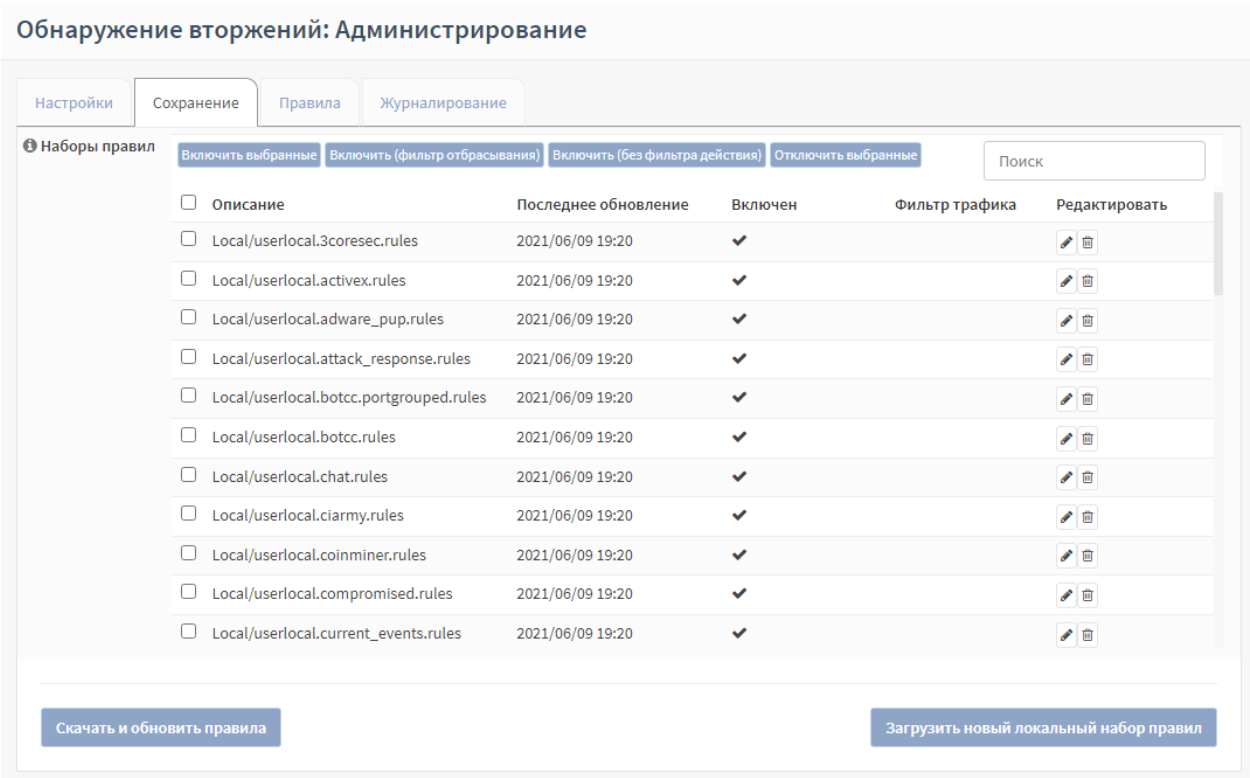

Рисунок 55 – Настройка импорта правил

!Важно В случае сброса **ARMA IF** к значениям по умолчанию, загруженные ранее правила сохраняются.

Возможна настройка автоматического обновления и перезагрузки правил СОВ с помощью планировщика задач Cron (см. Раздел 26). При создании задачи необходимо выбрать «Обновить и перезагрузить правила обнаружения вторжений» в параметре **«Команда»**.

!Важно В случае работы СОВ в режиме IPS, при выполнении расписания автоматического обновления и перезагрузки правил обнаружения вторжений, возможно пропадание трафика.

5.2.1 Пример импорта пользовательских решающих правил

В качестве примера будут использован файл набора прав «emerging-scan.rules», содержащий в себе правило, рассчитанное на обнаружение сетевого сканирования.

Для импорта пользовательских решающих правил необходимо выполнить следующие действия:

1. Во вкладке **«Сохранение»** подраздела администрирования СОВ (**«Обнаружение вторжений»** - **«Администрирование»**) нажать **кнопку «Загрузить новый локальный набор правил»**, в открывшейся форме выбрать файл «emerging-scan.rules» и нажать **кнопку «Открыть»**.
2. После успешной загрузки правил (см. Рисунок 56) необходимо нажать **кнопку «Закрыть»**, а затем **кнопку «Скачать и обновить правила»** чтобы изменения вступили в силу.

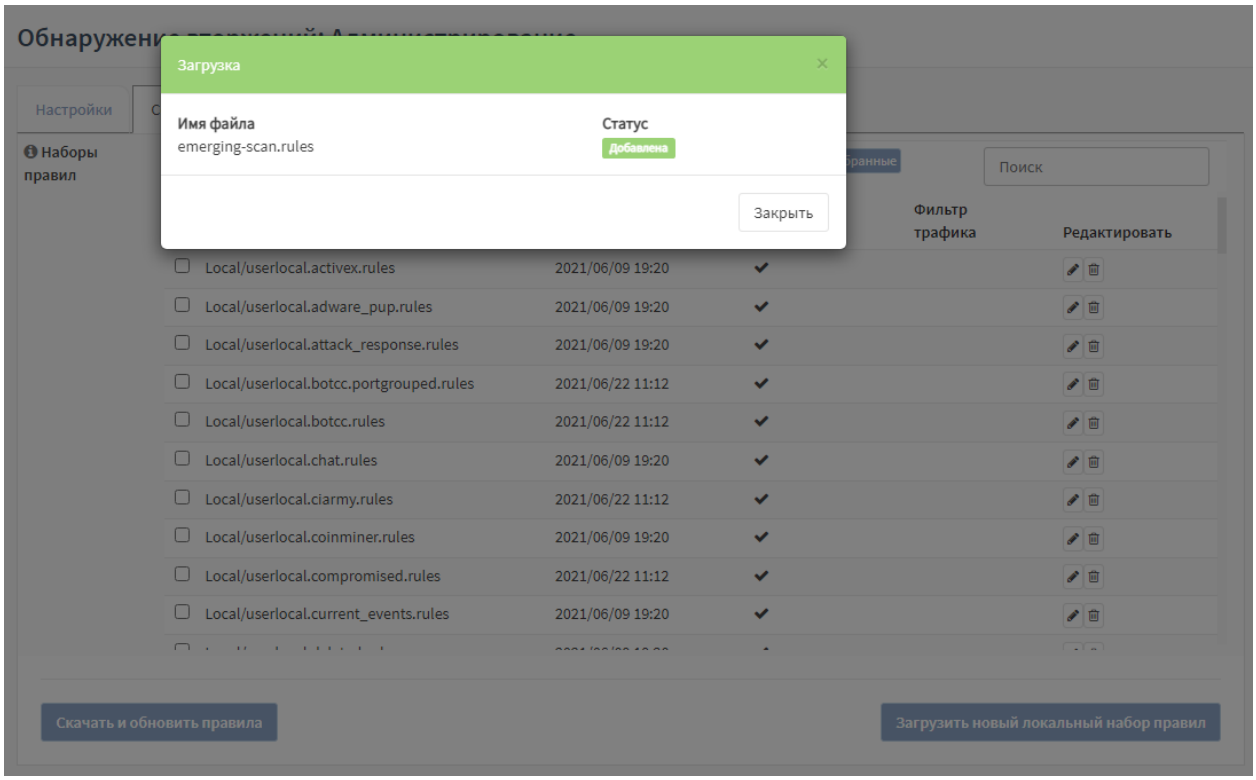

Рисунок 56 – Успешный импорт правил

3. Перейти во вкладку **«Правила»**, ввести в строку поиска **«NMAP –sS»**, установить флажок справа от **кнопки «** **»** для включения правил (см. Рисунок 57) и нажать **кнопку «Применить»**.

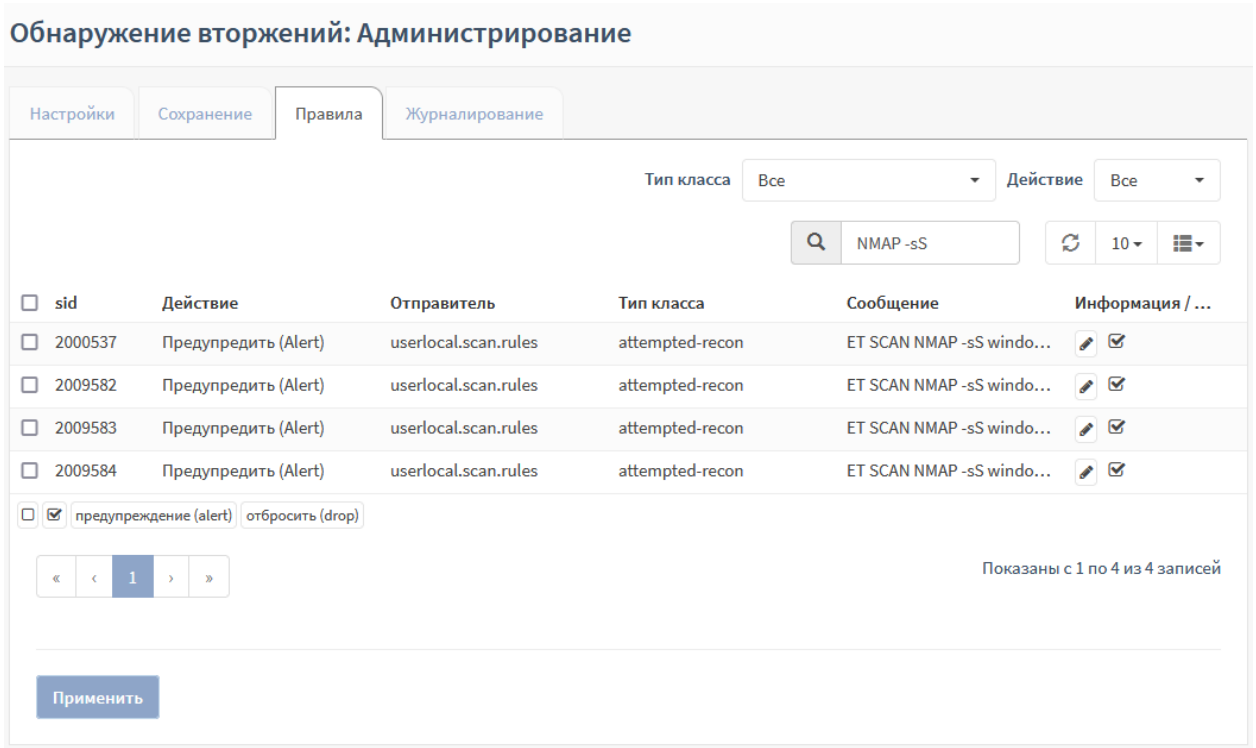

Рисунок 57 – Включение правил

5.2.2 Проверка загруженного набора правил

Для проверки срабатывания правил СОВ используется схема стенда, представленная на рисунке (см. Рисунок 58). На ПК **«Server»** установлено ПО «Zenmap».

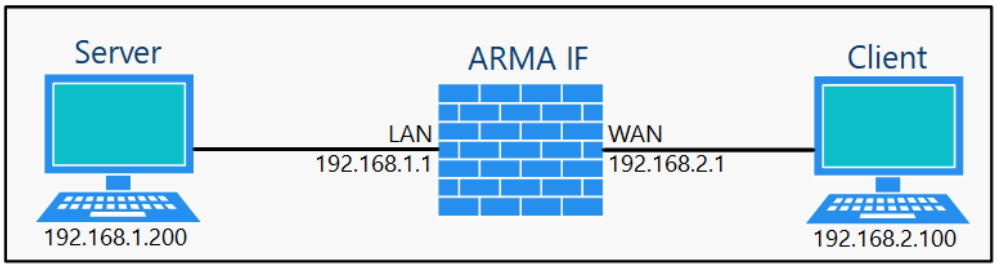

Рисунок 58 – Схема стенда для проверки срабатывания правил СОВ

Порядок проверки срабатывания загруженного набора правил:

1. В ПО «Zenmap» в поле **«Команда»** ввести строку **«nmap -sS 192.168.2.100»** и нажать **кнопку «Сканирование»** (см. Рисунок 59).

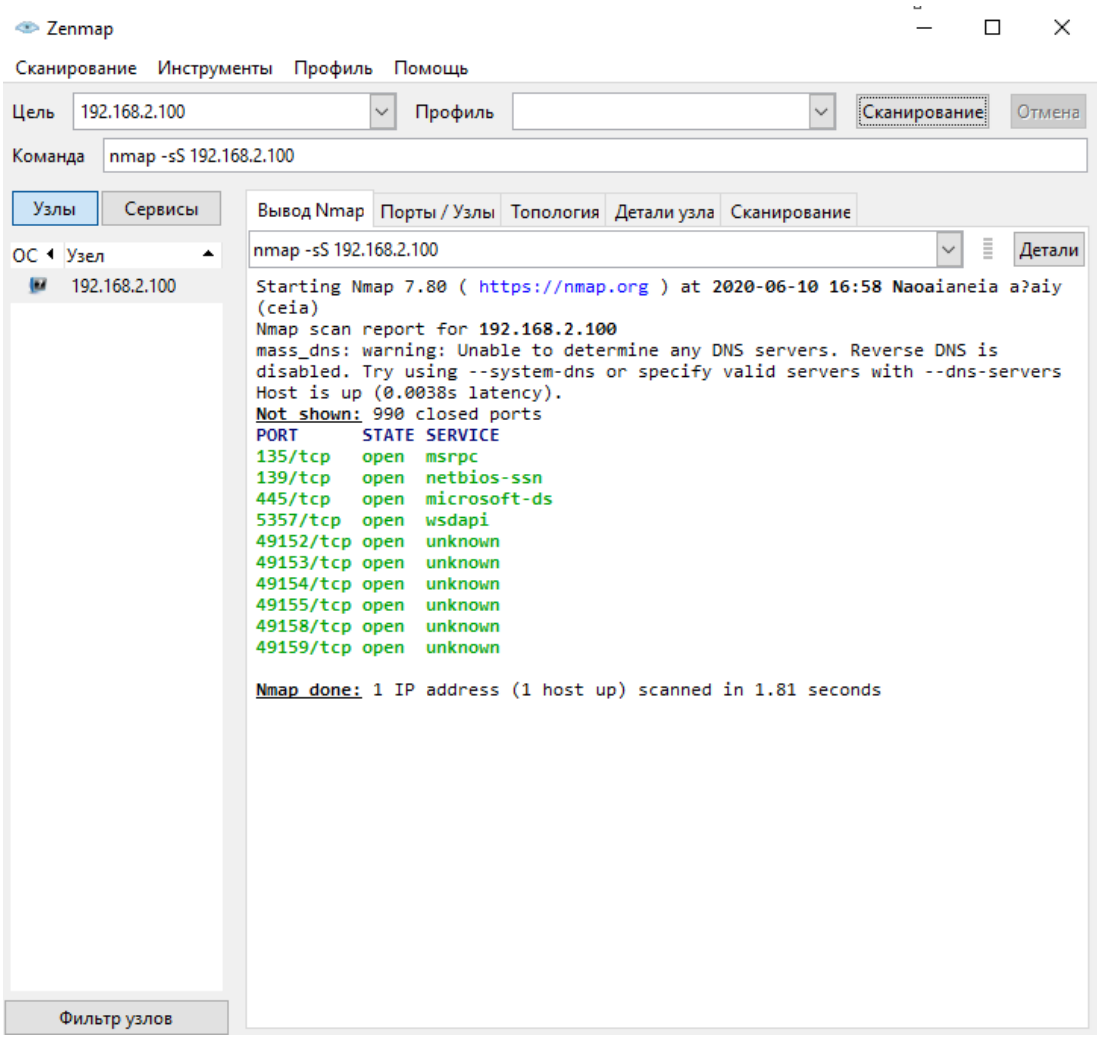

Рисунок 59 – Запуск сканирования с помощью программы Zenmap

2. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений»** -

«Предупреждения (Alerts)»), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:

- «ET SCAN NMAP» (см. Рисунок 60).

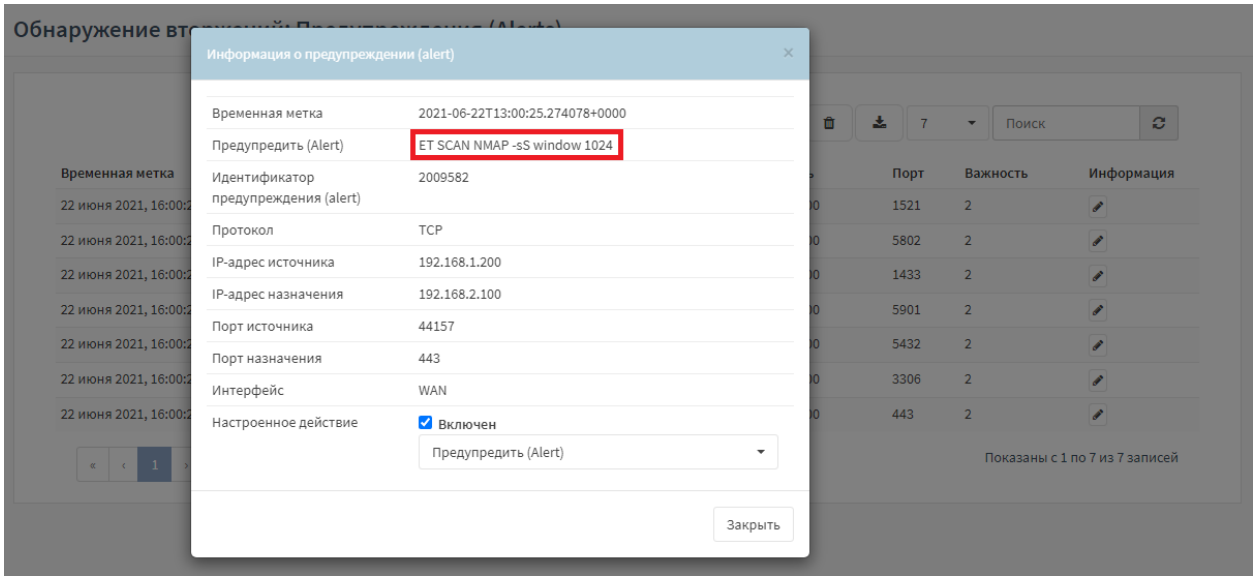

Рисунок 60 – Результаты сканирования

5.3 Настройка импорта правил

Импорт правил СОВ возможен с удаленных FTP/SMB-серверов.

При импорте правил используется архив наборов решающих правил формата **«tar.gz»**, название архива должно иметь следующий формат:

- «rulesets_[версия ARMA IF]_[версия правил].tar.gz», например «rulesets_3.6.rc.38_1.1.4.tar.gz»;

в процессе импорта правил выбирается файл правил с наиболее новой версией.

Архив наборов решающих правил должен находиться в каталоге, имеющим название следующего формата:

- «armaif_[версия ARMA IF]», например «armaif_3.6.rc.38».

Для настройки импорта правил необходимо выполнить следующие действия:

1. Перейти в подраздел настроек импорта правил (**«Обнаружение вторжений»** - **«Настройки импорта правил»**).
2. Установить флажок в параметре **«Включен»** и указать настройки импорта для требуемого протокола (см. Таблица 11).

Таблица 11
Значения параметров для импорта правил СОВ

Параметр	Значение для FTP	Значение для SMB
Протокол	FTP	SMB
Адрес	Адрес сервера: IP-адрес, хост, доменное имя	Адрес сервера: IP-адрес, хост, доменное имя
Общедоступный ресурс Samba	-	Имя общедоступного ресурса Samba
Имя пользователя	Учётные данные	Учётные данные
Пароль	Учетные данные	Учетные данные
Путь к корневой папке	Путь к каталогу с файлами правил. Путь должен начинаться с символа «\». Если каталог с архивом находится в корневой директории, необходимо оставить только символ «\».	Путь к каталогу с файлами правил. Путь должен начинаться с символа «\». Если каталог с архивом находится в корневой директории, необходимо оставить только символ «\».
Интервал	Интервал ожидания в случае неудачной попытки, задаётся в секундах	Интервал ожидания в случае неудачной попытки, задаётся в секундах

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

Результатом успешного импорта правил СОВ будет запись в журнале syslog (**«Система»** - **«Журналы» «Журнал Syslog»**) (см. Рисунок 61) и появление импортированных правил в подразделе СОВ (**«Обнаружение вторжений»** - **«Администрирование»** - **«Сохранение»**) (см. Рисунок 55).

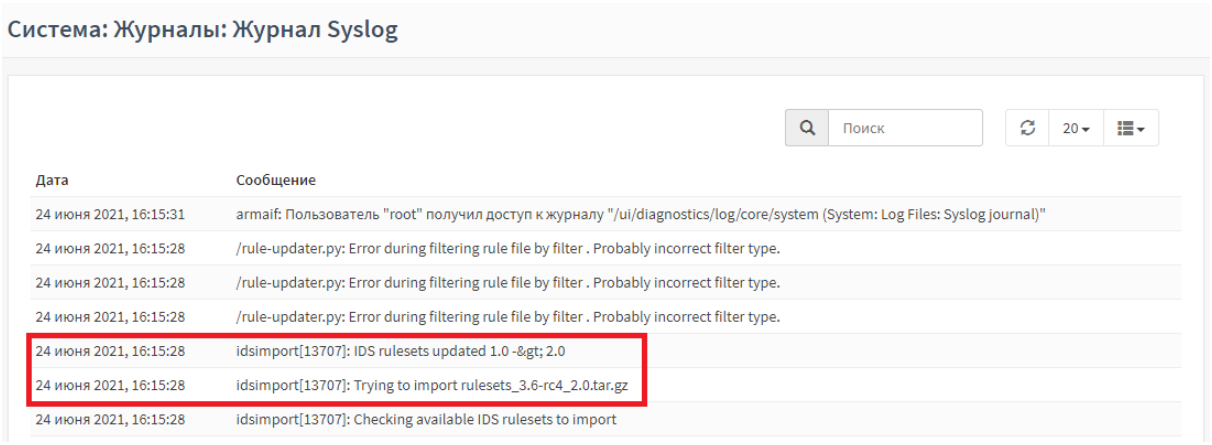

Рисунок 61 – Сообщения об успешном импорте правил СОВ

Для настроенного импорта возможно задать расписание выполнения с помощью планировщика задач Cron (см. Раздел 26). При создании задачи необходимо выбрать «Импорт правил СОВ» в параметре **«Команда»**.

5.4 Экспорт наборов правил СОВ

Существует возможность экспортировать наборы правил СОВ, загруженных ранее.

Для этого необходимо перейти в подраздел резервного копирования (**«Система»** - **«Конфигурация»** - **«Резервные копии»**) и, в блоке **«Скачать наборы правил СОВ»** (см. Рисунок 62), нажать **кнопку «Экспорт»**. Наборы правил СОВ будут скачены архивом формата **«tar.gz»**, название архива будет иметь следующий формат:

- «localrulesets-[полное доменное имя ARMA IF]-[Дата экспорта][Время экспорта].tar.gz».

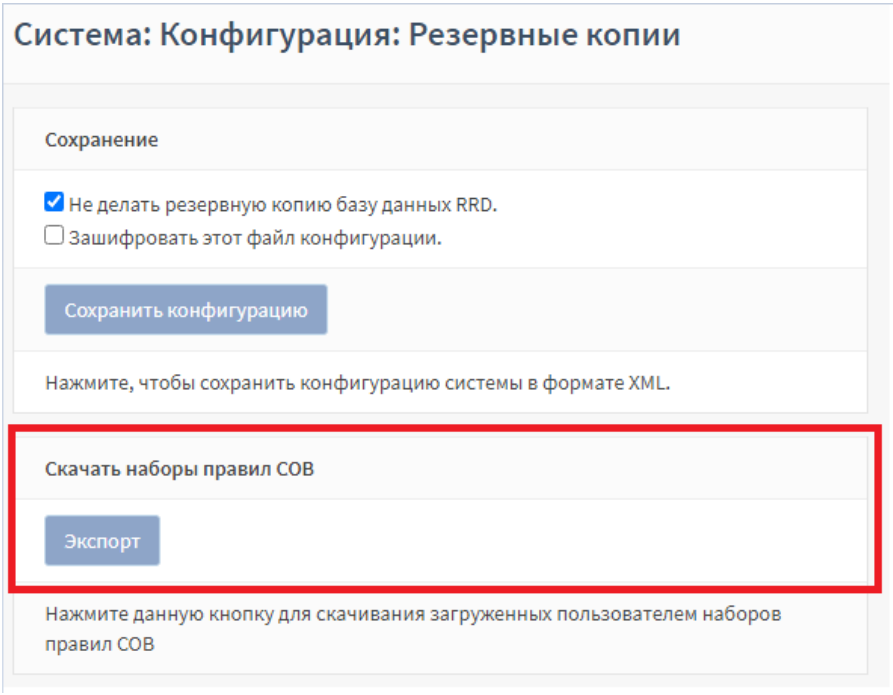

Рисунок 62 – Экспорт наборов правил СОВ

5.5 Подсистема «Контроль уровня приложений»

Подсистема контроля уровня приложений модуля СОВ реализована на базе технологии глубокой инспекции пакетов протоколов прикладного уровня, включая промышленные протоколы.

Функционал подсистемы контроля уровня приложений обеспечивает интеллектуальное распознавание протоколов прикладного уровня за счет сигнатурного анализа. Трафик будет распознан, даже если приложение ведет себя достаточно динамично и использует разные сетевые порты.

В таблице (см. Таблица 12) представлен список поддерживаемых протоколов, для которых представлены шаблоны форм и степень их разбора.

Таблица 12

Список поддерживаемых протоколов

Протокол	Стандарт	Степень разбора
Modbus TCP	MODBUS Application Protocol Specification V1.1b3	Для сообщений по протоколу Modbus TCP возможно задать правило обнаружения на основе признака совпадения: • свойство функции – код или категория функции; • тип доступа к данным – тип доступа и основная модель данных;

Протокол	Стандарт	Степень разбора
		• диапазон функции – ввод кода функции, адреса и значения переменной вручную. При обнаружении по свойству функции возможно задать дополнительные опции: • используемую функцию, подфункцию; • категория кодов функции. Категории кодов функции: • назначенная – коды функций, которые определены в Modbus спецификации; • неназначенная – общедоступная, стандартные и организационные коды; • пользовательская – два диапазона кодов, для которых возможно назначить произвольную функцию; • зарезервированная – коды функций, не являющимися стандартными; • все категории. При классификации по доступу к данным возможно задать следующие дополнительные опции: • тип доступа к данным – записать или считать. Модель данных: • «Регистры флагов (Coils)» – битовые данные, доступ чтение/запись; • «Регистры хранения (Holding Registers)» – 16 битовые данные, доступ чтение/запись; • «Дискретные входы (Discrete Inputs)» – битовые данные, доступ чтение;

Протокол	Стандарт	Степень разбора
		• «Регистры ввода (Input Registers)» – 16 битовые данные, доступ чтение.
IEC 60870-5-104	ГОСТ Р МЭК 60870-5-104-2004	Сообщения по протоколу IEC 60870-5-104 могут быть определены по типу пакета: • полный – APDU; • для целей управления – только поля APCI. При классификации по типу пакета APCI возможен выбор формата пакета: • любой; • «U-format (unnumbered control functions)» – функции управления без нумерации; • «S-format (numbered supervisory functions)» – функции контроля с нумерацией. При классификации по типу пакета ASDU возможно задание: • диапазона разрешенных входящих пакетов (RX); • диапазона разрешенных исходящих пакетов (TX); • типа ASDU; • причины передачи (ASDU cause of transfer)»; • числового значения ASDU адреса; • адреса объекта информации в формате диапазона; • значения IOA.
S7 Communication	Стандарт протокола связи коммуникационных модулей серий Siemens SIMATIC S7-300/400	Сообщения по протоколу S7Communication разделяются по функции: • CPUSERVICE; • SETUPCOMM; • READVAR; • WRITEVAR; • REQUESTDOWNLOAD; • DOWNLOADBLOCK; • DOWNLOADENDED;

Протокол	Стандарт	Степень разбора
		• STARTUPLOAD; • UPLOAD; • ENDUPLOAD; • PLCCONTROL; • PLCSTOP. При выборе в поле **«Функция»** функции «READVAR» необходимо выбрать тип области чтения и поля ввода имени области, типа данных, количества данных и смещения данных. При выборе в поле **«Функция»** функции «WRITEVAR» необходимо выбрать тип области чтения и поля ввода имени области, типа данных, количества данных и смещения данных, типа передаваемого значения, количество передаваемых данных, список значений данных. При выборе в поле **«Функция»** функции «REQUESTDOWNLOAD» появятся поле выбора типа блока, номера блока и целевой файловой системы. При выборе в поле **«Функция»** функции «DOWNLOADBLOCK» появятся поля выбора типа блока, номера блока и целевой файловой системы. При выборе в поле **«Функция»** функции «STARTUPLOAD» появятся поля выбора типа блока, номера блока и целевой файловой системы. При выборе в параметре **«Функция»** функции «PLCCONTROL» появится поле выбора функции управления ПЛК: • «INSE (Активация скаченного блока, параметром выступает имя блока)»; • «DELE (Удаление блока, параметром выступает имя блока)»;

Протокол	Стандарт	Степень разбора
		• «PPROGRAM (Запуск программы, параметром выступает имя программы)»; • «GARB (Сжатие памяти)»; • «MODU (Копирование RAM в ROM, параметр содержит идентификатор файловой системы A/E/P)»; • «OFF (Выключение ПЛК)»; • «ON (Включение ПЛК)».
OPC UA	IEC 62541	Сообщения по протоколу OPC UA разделяются по типу сообщения: • «HELLO» – маркер начала передачи данных между клиентом и сервером; • «ACKNOWLEDGE» – ответ на сообщение типа «HELLO»; • «OPEN – открытие канала передачи данных с предложенным методом шифрования данных; • «MESSAGE» – передаваемое сообщение; • «CLOSE» – конец сессии. При выборе «OPEN» появятся поле выбора политика безопасности. При выборе «MESSAGE» в поле появятся поле выбора типа запроса. При выборе «BROWSE» в поле **«Тип запроса»** появятся поле ввода диапазон запроса. При выборе «READ» в поле **«Тип запроса»** появятся поле ввода диапазон запроса. При выборе «WRITE» в поле **«Тип запроса»** появятся поле ввода диапазон запроса. При выборе «CALL» в поле **«Тип запроса»** появятся поле ввода

Протокол	Стандарт	Степень разбора
		идентификатора узла, содержащий вызываемую процедуру и поле ввода идентификатора узла вызываемой процедуры.
OPC DA	OLE for Process Control Data Access Automation Interface Standard v.2.0	Сообщения по протоколу OPC DA разделяются по типу сообщения: • REQUEST; • PING; • RESPONSE; • FAULT; • WORKING; • NOCALL; • REJECT; • ACK; • CI_CANCEL; • FACK; • CANCEL_ACK; • BIND; • BIND_ACK; • BIND_NACK; • ALTER_CONTEXT; • ALTER_CONTEXT_RESP; • SHUTDOWN; • AUTH3; • CO_CANCEL; • ORPHANED. При выборе «REQUEST» в поле появятся поля ввода идентификатора вызываемого объекта и ввода номера вызываемой функции объекта.
UMAS	Основан на протоколе Xway Unite. Протокол Umas используется для настройки и мониторинга ПЛК Schneider-Electric.	Сообщения по протоколу UMAS разделяются по функциям: • инициализация UMAS сессии; • чтение информации о проекте; • чтение внутренней информации ПЛК; • назначение ПЛК владельца; • инициализация загрузки – копирование с инженерного ПК на ПЛК;

Протокол	Стандарт	Степень разбора
		• завершение загрузки – копирования с инженерного ПК на ПЛК; • инициализация скачивания – копирование с ПЛК на инженерный ПК; • конец скачивания – копирования с ПЛК на инженерный ПК; • включение ПЛК; • выключение ПЛК.
MMS	IEC 61850-8-1	Сообщения по протоколу MMS разделяются по типу сообщения. Для типа сообщения «CONFIRMED_REQUEST» возможен выбор типа служб. Для службы «READ» возможен ввод имени переменной и адреса переменной для функции чтения. Для службы «WRITE» возможен ввод имени переменной для функции записи.
GOOSE	IEC 61850-8-1	Сообщения по протоколу GOOSE разделяются по: • идентификатору приложения; • значению поля «datset»; • значению поля «gocbref»; • значению поля «goid»; • значению поля «t».
KRUG	Круг ПК-контроллер	Сообщения по протоколу KRUG разделяются по: • значению поля «COMMAND»; • значению поля «CMD»; • значению поля «PORT»; • значению поля «ACCESS»; • значению поля «MODE»; • значению поля «ERRCODE».

Протоколы:

- Modbus;

- OPC DA;
- MMS;

будут анализироваться и обнаруживаться **ARMA IF** только в том случае, если **ARMA IF** выявит пакеты установления сессии по данным протоколам после запуска анализа и обнаружения. СОВ будет работать в рамках данной сессии.

В случае, когда установление сессии произошло до запуска анализа и обнаружения, пакеты данных протоколов будут игнорироваться.

5.5.1 Создание правила СОВ

Для создания пользовательских правил необходимо перейти в подраздел настроек правил (**«Обнаружение вторжений»** - **«Контроль уровня приложений»**) и нажать **кнопку «** **»**, в открывшейся форме (см. Рисунок 63) указать параметры правила и нажать **кнопку «Сохранить»**.

Для редактирования существующих правил необходимо перейти в подраздел настроек правил (**«Обнаружение вторжений»** - **«Контроль уровня приложений»**) и нажать **кнопку «** **»** напротив существующего правила, в открывшейся форме (см. Рисунок 63) изменить параметры правила и нажать **кнопку «Сохранить»**.

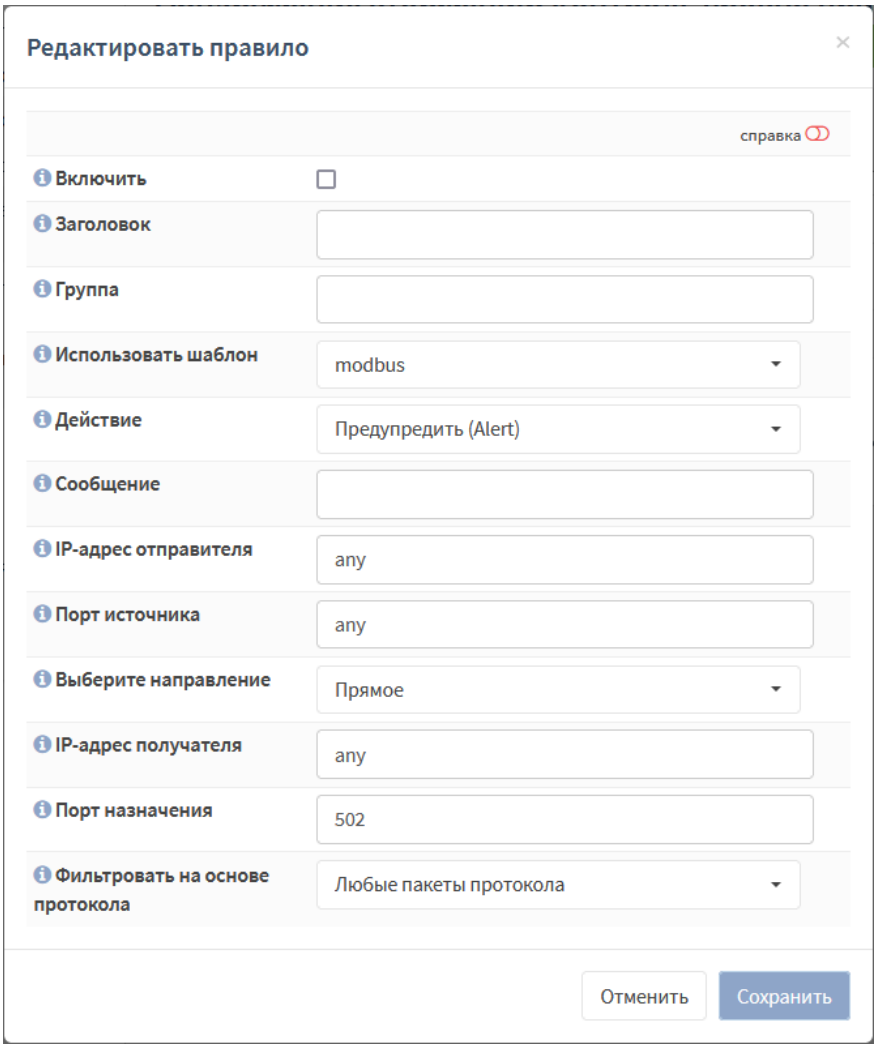

Рисунок 63 – Форма редактирования правила СОВ

При создании пользовательских правил доступны следующие варианты действий:

- **«Предупредить (Alert)»** –оповещение при срабатывании правила;
- **«Отклонить (Reject)»** – блокировка пакета при срабатывании правила и оповещение о блокировке отправителя;
- **«Отбросить (Drop)»** – блокировка пакета при срабатывании правила без уведомления о блокировке отправителя;
- **«Разрешить (Pass)»** – разрешение прохождения пакета при срабатывании правила.

!Важно При проверке срабатывания пользовательских правил необходимо убедиться, что СОВ включена (см. Раздел 5.1).

5.5.2 Создание пользовательских правил на основе собственного шаблона

В качестве примера работы правила СОВ будет рассмотрена имитация DOS-атаки. Схема стенда представлена на рисунке (см. Рисунок 64). На ПК **«Kali Linux»** установлено ОС Kali Linux.

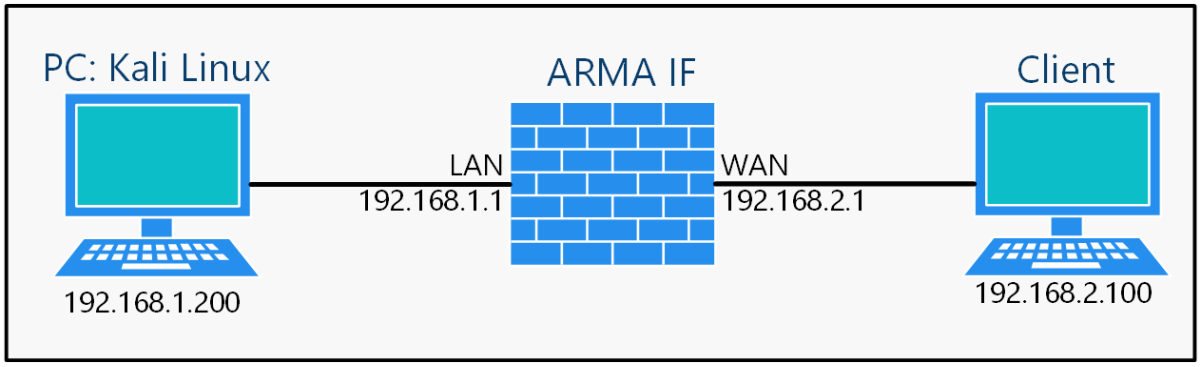

Рисунок 64 – Схема стенда для проверки срабатывания пользовательского правила на DOS- атаку

5.5.2.1 Пример создания правила СОВ

Необходимо создать пользовательское правило (см. Раздел 5.5.1) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «DOS-attack»;
- **«Использовать шаблон»** – «Настроенное пользователем»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «DOS-attack»;
- **«Протокол»** – «TCP»;
- **«Специфичная часть правила»** – «flow: stateless; threshold: type both, track by_dst,».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

Параметр **«Специфичная часть правила»** сконфигурирован в соответствии с форматом написания правил ПО «Suricata», дополнительные сведения представлены на официальном сайте ПО «Suricata» (см. https://suricata.readthedocs.io/en/suricata-6.0.0/rules/intro.html).

5.5.2.2 Проверка созданного правила СОВ

Для проверки правила СОВ необходимо выполнить следующие действия:

1. На ПК **«Kali Linux»** запустить терминал и выполнить команду:
   - «hping3 192.168.2.100 -S –flood»
2. Через 10 секунд остановить команду комбинацией **клавиш «Ctrl+C»**.
3. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений»** -

«Предупреждения (Alerts)»), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:

- «DOS-attack» (Рисунок 65).

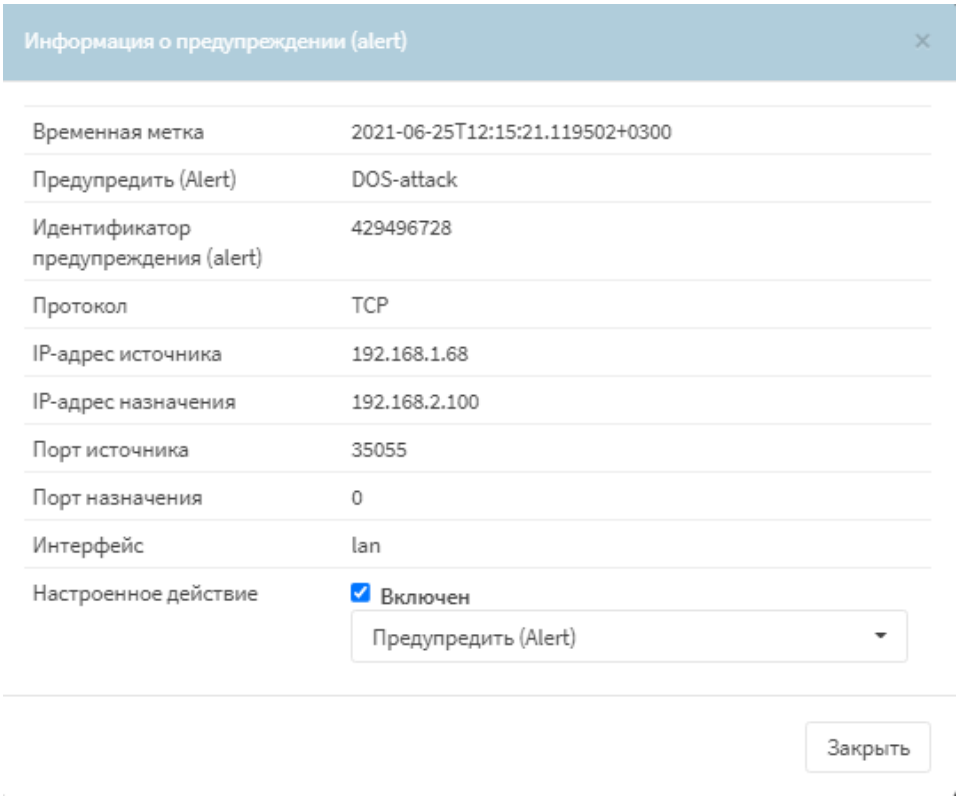

Рисунок 65 – Детальная информация. DOS-атака

5.5.3 Создание пользовательских правил СОВ на основе шаблонов промышленных протоколов

Для проверки срабатывания пользовательских правил СОВ на основе шаблонов промышленных протоколов используется стандартная схема стенда (см. Рисунок 66).

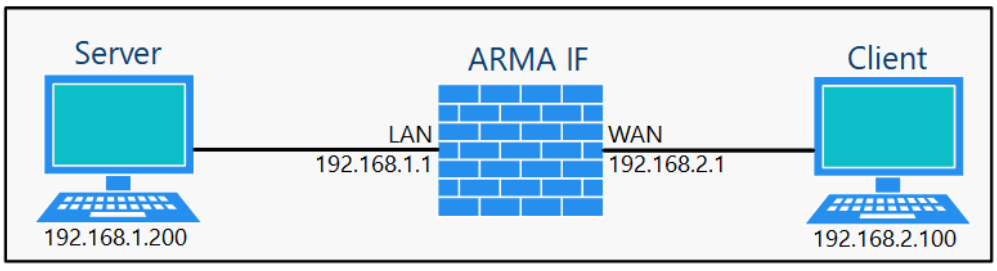

Рисунок 66 – Схема стенда для срабатывания пользовательских правил СОВ на основе шаблонов промышленных протоколов

!Важно При проверке срабатывания пользовательских правил на основе шаблонов промышленных протоколов необходимо убедиться, что создано соответствующее разрешающее правило МЭ (см. Раздел 1.1.1) и включена СОВ (см. Раздел 5.1). Основные параметры правил для протоколов приведены в таблице (см. Таблица 13).

Таблица 13
Значения параметров правила

Параметр	Значение
Действие	Разрешить (Pass)
Интерфейс	WAN
Протокол	TCP
Получатель	Единственный хост или сеть, 192.168.1.200/32
Диапазон портов назначения	Указывается в зависимости от протокола (см. Таблица 14)

Таблица 14
Значения портов по умолчанию для промышленных протоколов

Протокол	Порт по умолчанию
Modbus	502
IEC 104	2404
S7comm	102
OPC DA	135
OPC UA	4840, 4843
UMAS	502
MMS	102
GOOSE	Не используется. Рекомендуется использовать белые списки для интерфейса (см. Раздел 14.2.3)

5.5.3.1 Шаблон протокола Modbus

При создании пользовательского правила на основе шаблона промышленного протокола Modbus необходимо задать параметры протокола, выбрав в поле **«Фильтровать на основе протокола»** опцию «Указать дополнительные параметры».

При выборе «Указать дополнительные параметры» появятся поля **«Совпадение по»** и **«Код функции»**.

В поле **«Совпадение по»** доступно два признака совпадение правила:

- **«Функции»** – код или категория функции;
- **«Данные»** – тип доступа и основная таблица.

При выборе опции **«Функции»** появится поле **«Код функции»**, в котором необходимо выбрать код или категорию функции.

При выборе опции **«Данные»** появятся поля **«Код функции»**, **«Адрес»** и **«Значение»**, в которых необходимо ввести диапазоны функции/номеров адреса/значений:

- **«Код функции»** – принимает значения от «0» до «255»;
- **«Адрес»** – принимает значения от «0» до «65535»;
- **«Значение»** принимает значения от «0» до «65535».

5.5.3.1.1 Пример создания правила СОВ

Необходимо создать пользовательское правило (см. Раздел 5.5.1) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «Modbus»;
- **«Использовать шаблон»** – «modbus»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «Modbus»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»
- **«Совпадение по»** – «Функции»;
- **«Код функции»** – «06:Write Register».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.1.2 Проверка созданного правила СОВ

Для проверки срабатывания пользовательского правила на основе шаблона протокола Modbus на ПК **«Server»** должно быть установлено ПО «ModbusPal», а на ПК **«Client»** – ПО «qModMaster».

Для проверки правила СОВ необходимо выполнить следующие действия:

1. В ПО «ModbusPal» запустить сервис, нажав **кнопку «Run»**, затем в блоке **«Modbus slaves»** нажать **кнопку «Add»**, выбрать **«1»** и снова нажать **кнопку «Add»**.

2. Нажать **кнопку «**  **»** и путем нажатия **кнопки «Add»** добавить строки от «1» до «10» (см. Рисунок 67) для добавления десяти регистров со значениями «0».

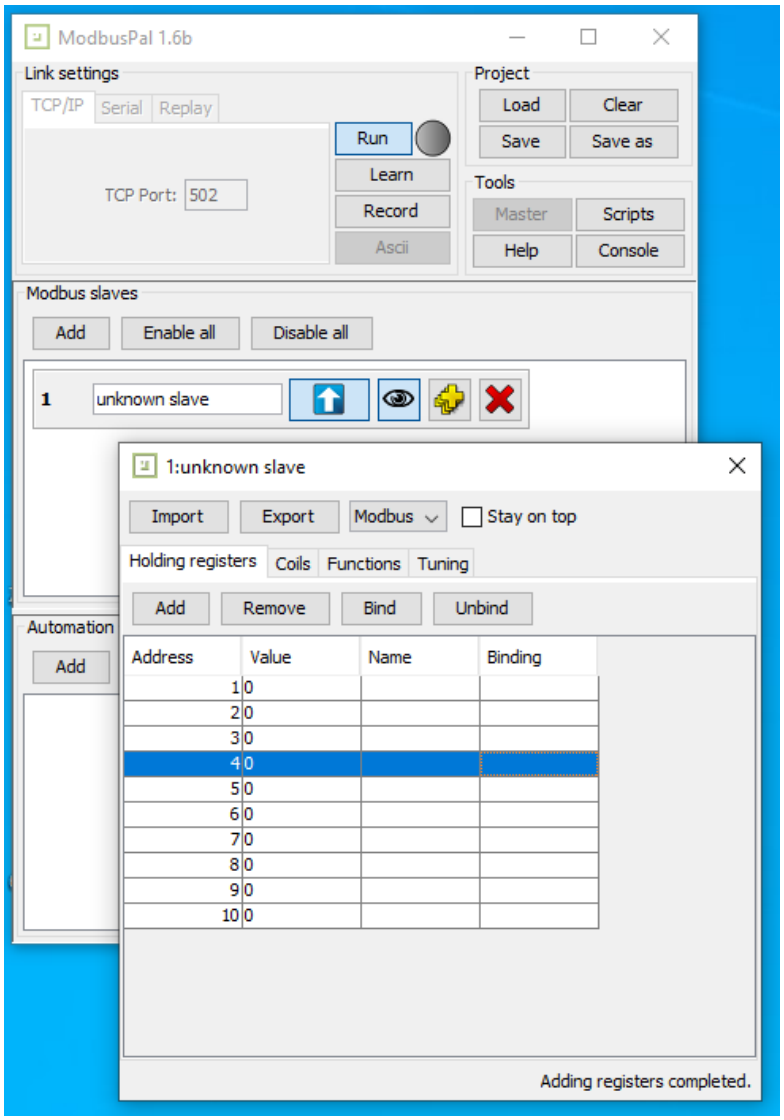

Рисунок 67 – Настройка ПО «ModbusPal»

3. В ПО «qModMaster» выполнить соединение с ПО «ModbusPal», для этого нажать **кнопку «**  **»**, ввести «192.168.1.100» и нажать **кнопку «**  **»** (**«Connect»**) для подключения к ПК **«Server»**.

4. Выбрать следующие значения в полях:
   - **«Modbus Mode»** – «TCP»;
   - **«Function code»** – «Write Single Register»;
   - **«Start Address»** – «7».

5. Выполнить функцию чтения/записи нажав **кнопку «**  **» – «Read/Write»**.

!Важно Внесенные данные в строку, указанную в поле **«Start Address»**, фактически будут отображаться со смещением на одну строку – то есть при внесении изменения в 7 строку данные появятся в 8.

6. В ПО «ModbusPal» убедиться, что внесенные данные отобразились (см. Рисунок 68).

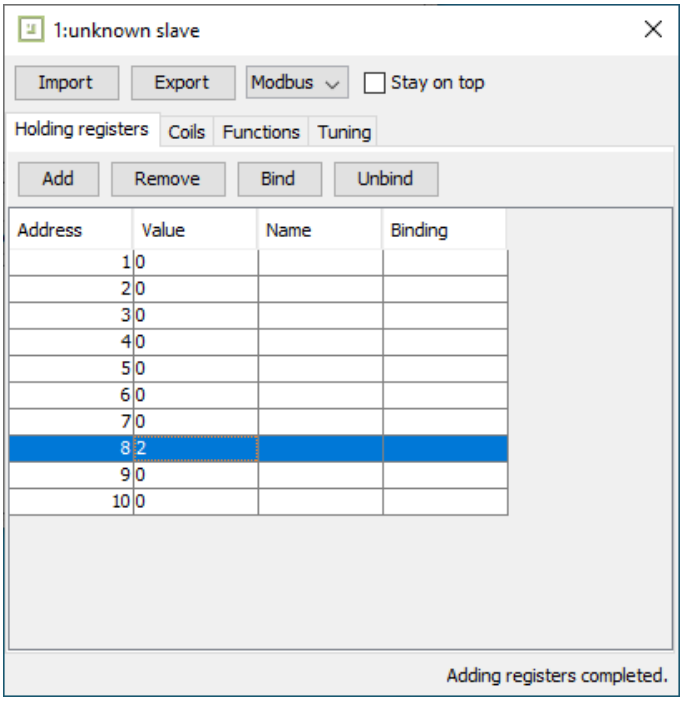

Рисунок 68 – Запись данных

7. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений»** - **«Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:
   - «Modbus» (см. Рисунок 69).

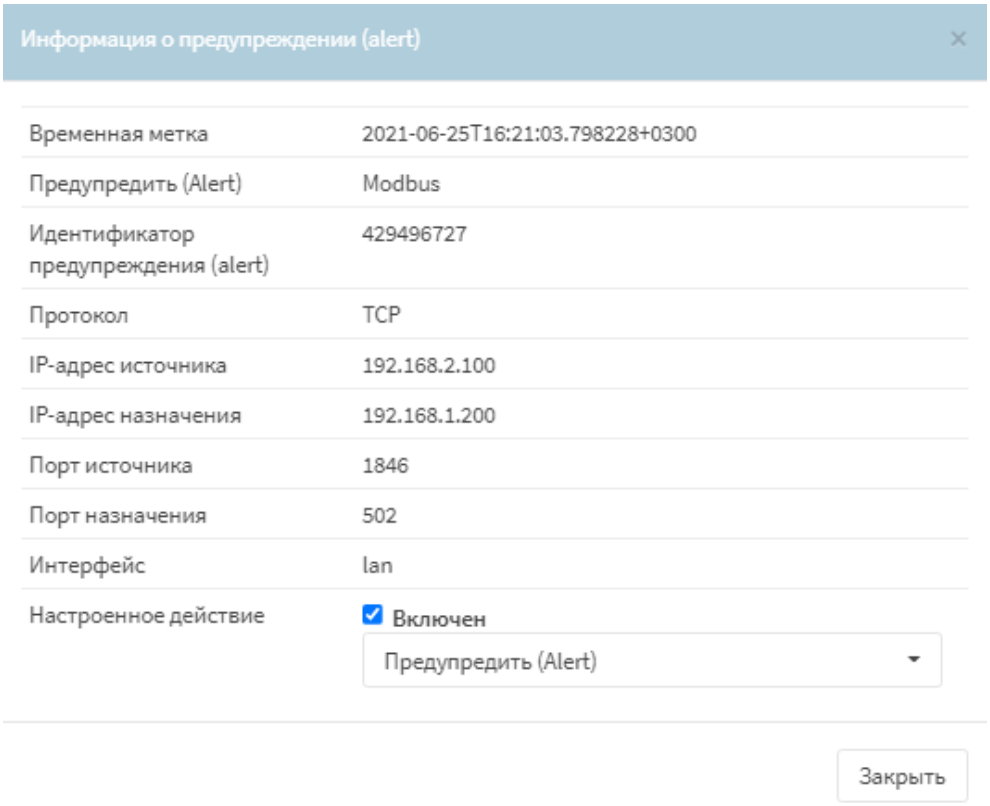

Рисунок 69 – Детальная информация, протокол Modbus

5.5.3.2 Шаблон протокола IEC 104

При создании пользовательского правила на основе шаблона промышленного протокола IEC 104 необходимо задать параметры протокола, выбрав в поле **«Фильтровать на основе протокола»** опцию «Указать дополнительные параметры».

При выборе опции «Указать дополнительные параметры» появится поле **«Функция приложения»**, в котором доступно два типа пакета:

- **«ASDU»** – блок данных прикладного уровня;
- **«APCI»** – управляющая информация прикладного уровня, включающий в каждый заголовок APCI такие маркировочные элементы, как стартовый символ и указание длины ASDU вместе с полем управления.

При выборе опции **«APCI (управляющая информация прикладного уровня)»** появится поле **«Формат»**, в котором доступно два формата:

- **«U-format (unnumbered control functions)»** – функции управления без нумерации;
- **«S-format (numbered supervisory functions)»** – функции контроля с нумерацией.

При выборе опции **«ASDU (блок данных прикладного уровня)»** появятся следующие поля:

- **«RX»**;
- **«TX»**;
- **«Тип ASDU»**;
- **«ASDU COT (cause of transfer)»**;
- **«AD (ASDU адрес)»**;
- **«IOA (адрес объекта информации)»**;
- **«IOA значение»**.

Диапазон разрешенных входящих и исходящих пакетов необходимо указать в полях **«RX»** и **«TX»** соответственно.

В поле **«Тип ASDU»** доступны типы ASDU, указанные в таблице (см. Таблица 15).

Таблица 15
Типы ASDU

Идентификатор типа	Описание	Метка ASDU
<0>	:= не определяется	
<1>	:= одноэлементная информация	M_SP_NA_1
<3>	:= двухэлементная информация	M_DP_NA_1
<5>	:= информация о положении отпаек	M_ST_NA_1
<7>	:= строка из 32 битов	M_BO_NA_1
<9>	:= значение измеряемой величины, нормализованное значение	M_ME_NA_1
<11>	:= значение измеряемой величины, масштабированное значение	M_ME_NB_1
<13>	:= значение измеряемой величины, короткий формат с плавающей запятой	M_ME_NC_1
<15>	:= интегральные суммы	M_IT_NA_1
<20>	:= упакованная одноэлементная информация с определением изменения состояния	M_PS_NA_1
<21>	:= значение измеряемой величины, нормализованное значение без описателя качества	M_ME_ND_1

Идентификатор типа	Описание	Метка ASDU
<22>..<29>	:= резерв для дальнейших совместимых определений	
<30>	:= одноэлементная информация с меткой времени CP56Время2a	M_SP_TB_1
<31>	:= двухэлементная информация с меткой времени CP56Время2a	M_DP_TB_1
<32>	:= информация о положении отпаек с меткой времени CP56Время2a	M_ST_TB_1
<33>	:= строка из 32 битов с меткой времени CP56Время2a	M_BO_TB_1
<34>	:= значение измеряемой величины, нормализованное значение с меткой времени CP56Время2a	M_ME_TD_1
<35>	:= значение измеряемой величины, масштабированное значение с меткой времени CP56Время2a	M_ME_TE_1
<36>	:= значение измеряемой величины, короткий формат с плавающей запятой с меткой времени CP56Время2a	M_ME_TF_1
<37>	:= интегральная сумма с меткой времени CP56Время2a	M_IT_TB 1
<38>	:= информация о работе релейной защиты с меткой времени CP56Время2a	M_EP_TD_1
<39>	:= упакованная информация о срабатывании пусковых органов защиты с меткой времени CP56Время2a	M_EP_TE_1
<40>	:= упакованная информация о срабатывании выходных цепей защиты с меткой времени CP56Время2a	M_EP_TF_1
<41>..<44>	:= резерв для дальнейших совместимых определений	
<45>	:= одноэлементная команда	C_SC_NA_1
<46>	:= двухэлементная команда	C_DC_NA_1

Идентификатор типа	Описание	Метка ASDU
<47>	:= команда пошагового регулирования	C_RC_NA_1
<48>	:= команда установки, нормализованное значение	C_SE_NA_1
<49>	:= команда установки, масштабированное значение	C_SE_NB_1
<50>	:= команда установки, короткое число с плавающей запятой	C_SE_NC_1
<51>	:= строка из 32 битов	C_BO_NA _1
<52>..<57>	:= резерв для дальнейших совместимых определений	
<58>	:= одноэлементная команда с меткой времени CP56Время2a	C_SC_TA_1
<59>	:= двухэлементная команда с меткой времени CP56Время2a	C_DC_TA_1
<60>	:= команда пошагового регулирования с меткой времени CP56Время2a	C_RC_TA_1
<61>	:= команда установки, нормализованное значение с меткой времени CP56Время2a	C_SE_TA_1
<62>	:= команда установки, масштабированное значение с меткой времени CP56Время2a	C_SE_TB_1
<63>	:= команда установки, короткое число с плавающей запятой с меткой времени CP56Время2a	C_SE_TC_1
<64>	:= строка из 32 битов с меткой времени CP56Время2a	C_BO_TA_1
<65>..<69>	:= резерв для дальнейших совместимых определений	
<70>	:= конец инициализации	M_EI_NA_1
<71>..<99>	:= резерв для дальнейших совместимых определений	M_EI_NA_1
<100>	:= команда опроса	C_IC_NA_1
<101>	:= команда опроса счетчика	C_CI_NA_1

Идентификатор типа	Описание	Метка ASDU
<102>	:= команда считывания	C_RD_NA_1
<103>	:= команда синхронизации времени (опция, см. 7.6)	C_CS_NA 1
<105>	:= команда установки процесса в исходное состояние	C_RP_NA_1
<107>	:= команда тестирования с меткой времени CP56Время2a	C_TS_NA_1
<108>..<109>	:= резерв для дальнейших совместимых определений	C_IC_NA_1
<110>	:= параметр измеряемой величины, нормализованное значение	P_ME_NA_1
<111>	:= параметр измеряемой величины, масштабированное значение	P_ME_NB_1
<112>	:= параметр измеряемой величины, короткий формат с плавающей запятой	P_ME_NC_1
<113>	:= параметр активации	P_AC_NA_1
<114>..<119>	:= резерв для дальнейших совместимых определений	P_AC_NA_1
<120>	:= файл готов	F_FR_NA_1
<121>	:= секция готова	F_SR_NA_1
<122>	:= вызов директории, выбор файла, вызов файла, вызов секции	F_SC_NA_1
<123>	:= последняя секция, последний сегмент	F_LS_NA_1
<124>	:= подтверждение файла, подтверждение секции	F_AF_NA_1
<125>	:= сегмент	F_SG_NA_1
<126>	:= директория	F_DR_TA_1

В поле **«ASDU COT (cause of transfer)»** доступны следующие причины передачи:

- 1:COT_CYCLIC (Cyclic data);
- 2:COT_BACKGROUND (Background scan);
- 3:COT_SPONTAN (Spontaneous data);

- 4:COT_INIT (End of initialization);
- 5:COT_REQ (Read request);
- 6:COT_ACT (Command activation);
- 7:COT_ACT_CON (Confirmation of command activation);
- 8:COT_DEACT (Command abortion);
- 9:COT_DEACT_CON (Confirmation of command abortion);
- 10:COT_ACT_TERM (Termination of command activation);
- 11:COT_RETREM (Response due to remote command);
- 12:COT_RETLOC (Response due to local command);
- 13:COT_FILE (File access);
- 14:COT_14;
- 15:COT_15;
- 16:COT_16;
- 17:COT_17;
- 18:COT_18;
- 19:COT_19;
- 20:COT_INROGEN (Station query (general));
- 21:COT_INRO1 (Station query for group 1);
- 22:COT_INRO2 (Station query for group 2);
- 23:COT_INRO3 (Station query for group 3);
- 24:COT_INRO4 (Station query for group 4);
- 25:COT_INRO5 (Station query for group 5);
- 26:COT_INRO6 (Station query for group 6);
- 27:COT_INRO7 (Station query for group 7);
- 28:COT_INRO8 (Station query for group 8);
- 29:COT_INRO9 (Station query for group 9);
- 30:COT_INRO10 (Station query for group 10);
- 31:COT_INRO11 (Station query for group 11);
- 32:COT_INRO12 (Station query for group 12);
- 33:COT_INRO13 (Station query for group 13);

- 34:COT_INRO14 (Station query for group 14);
- 35:COT_INRO15 (Station query for group 15);
- 36:COT_INRO16 (Station query for group 16);
- 37:COT_REQCOGEN (Counter query (general));
- 38:COT_ REQCO1 (Counter query for group 1);
- 39:COT_ REQCO2 (Counter query for group 2);
- 40:COT_ REQCO3 (Counter query for group 3);
- 41:COT_ REQCO4 (Counter query for group 4);
- 42:COT_42;
- 43:COT_43;
- 44:COT_UNKNOWN_TYPE (Unknown type);
- 45:COT_UNKNOWN_CAUSE (Unknown cause of transfer);
- 46:COT_UNKNOWN_ASDU_ADDRESS (Unknown common ASDU address);
- 47:COT_UNKNOWN_OBJECT_ADDRESS (Unknown object address);
- 48:COT_48;
- 49:COT_49;
- 50:COT_50;
- 51:COT_51;
- 52:COT_52;
- 53:COT_53;
- 54:COT_54;
- 55:COT_55;
- 56:COT_56;
- 57:COT_57;
- 58:COT_58;
- 59:COT_59;
- 60:COT_60;
- 61:COT_61;
- 62:COT_62;
- 63:COT_63.

5.5.3.2.1 Пример создания правила COB

Необходимо создать пользовательское правило (см. Раздел 5.5.1) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «IEC 104»;
- **«Использовать шаблон»** – «IEC 104»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «IEC 104»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»
- **«Функция приложения»** – «ASDU (блок данных прикладного уровня»;
- **«Тип ASDU»** – «45:C_SC_NA_1(Single command)»;
- **«IOA (адрес объекта информации)»** – установить флажок, «от 1 до 1».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.2.2 Проверка созданного правила COB

Для проверки срабатывания пользовательского правила на основе шаблона протокола IEC 104 на ПК **«Server»** должен быть установлен эмулятор протокола IEC 104 – ПО «IECServer», а на ПК **«Client»** – ПО «QTester104».

Для проверки правила COB необходимо выполнить следующие действия:

1. Запустить ПО «IECServer».
2. В выпадающем списке выбрать «C_SC_NA» и дважды нажать **кнопку «Add»**, а затем нажать **кнопку «StartServer»** (см. Рисунок 70).

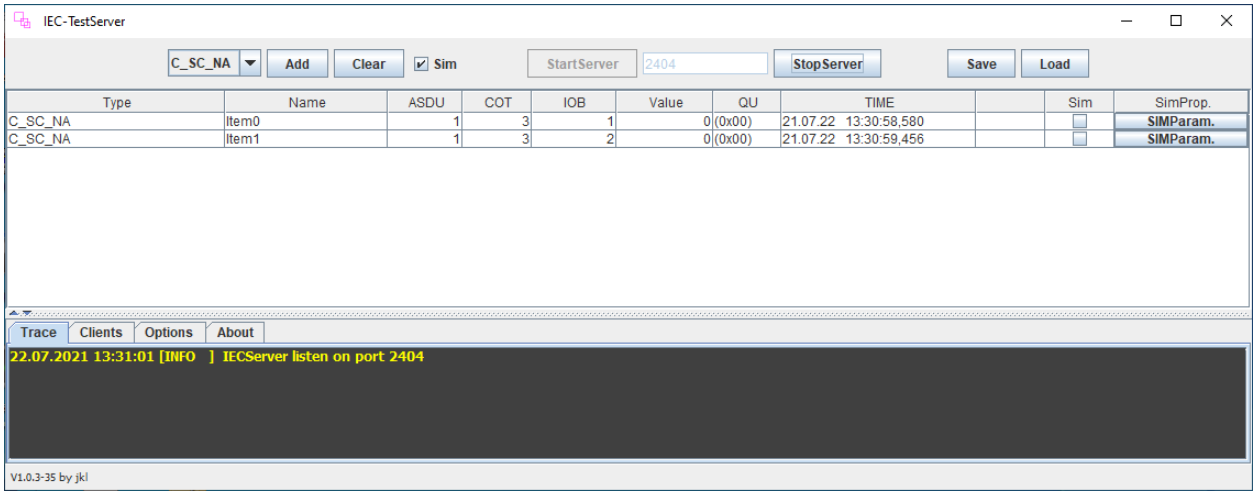

Рисунок 70 – Запуск IECServer

3. Запустить ПО «QTester104», указать в поле **«Remote IP Address»** значение «192.168.1.200» и нажать **кнопку «Connect»** для подключения к ПО «IECServer» (см. Рисунок 71).

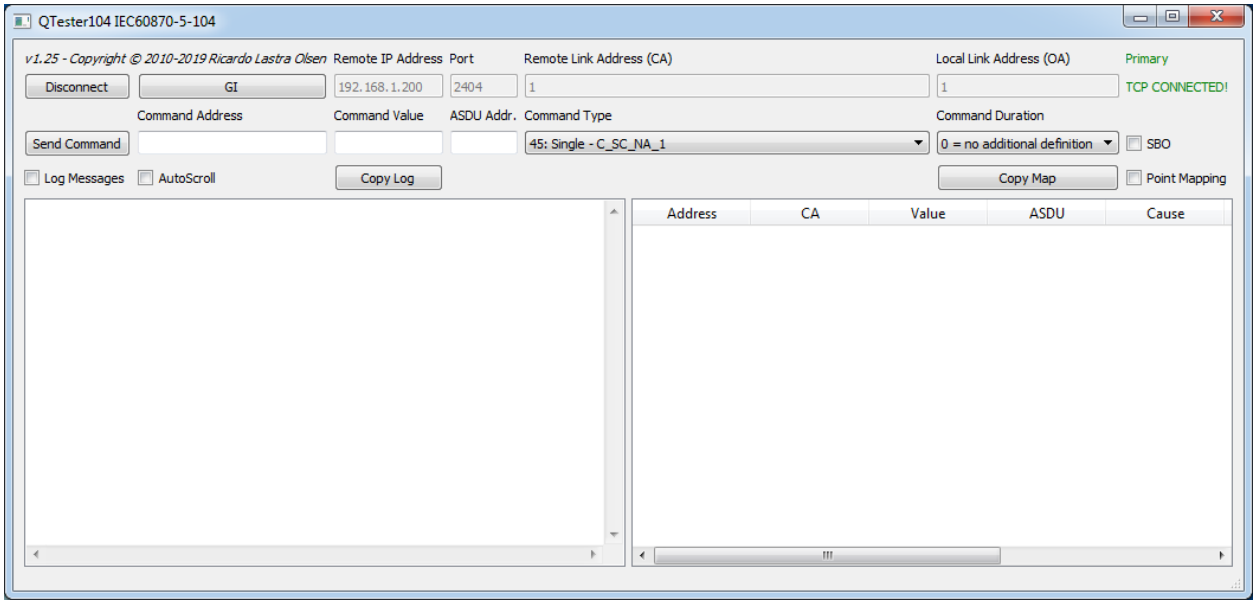

Рисунок 71 – Подключение к серверу в QTester104

4. Задать следующие значения в полях (см. Рисунок 72):
   - **«Command Address»** – 1;
   - **«Command Value»** – 2;
   - **«ASDU Addr.»** – 1.
5. Нажать **кнопку «Send Command»** для отправки команды на сервер.

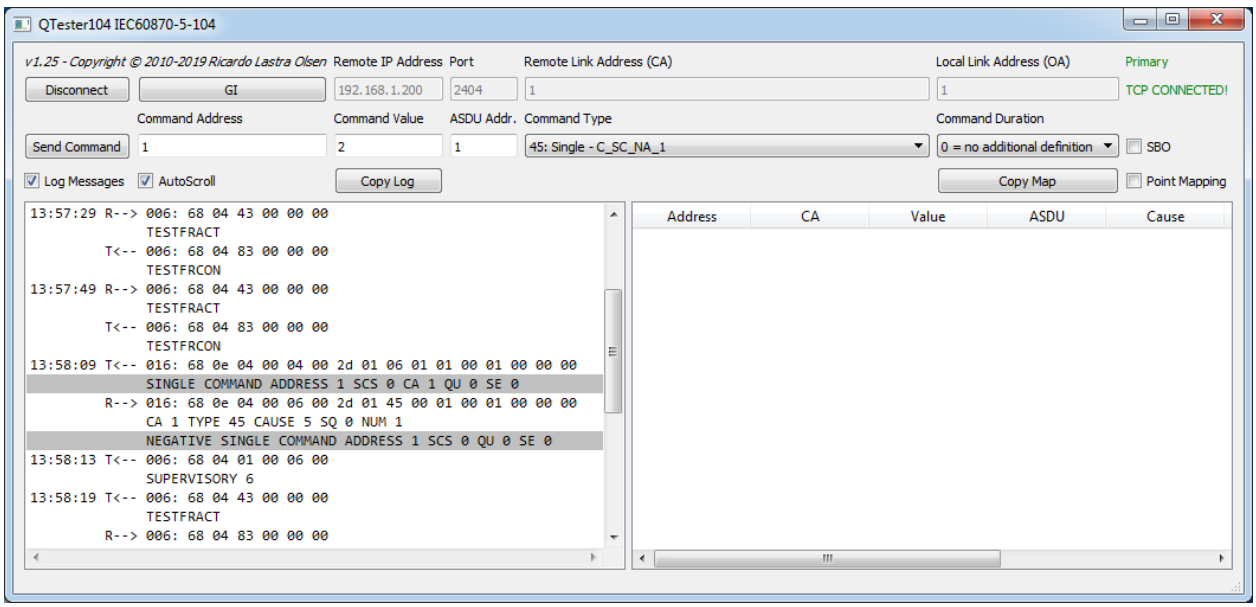

Рисунок 72 – Настройка значений в QTester104

6. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений»** -

«Предупреждения (Alerts)»), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:

- «IEC 104» (см. Рисунок 73).

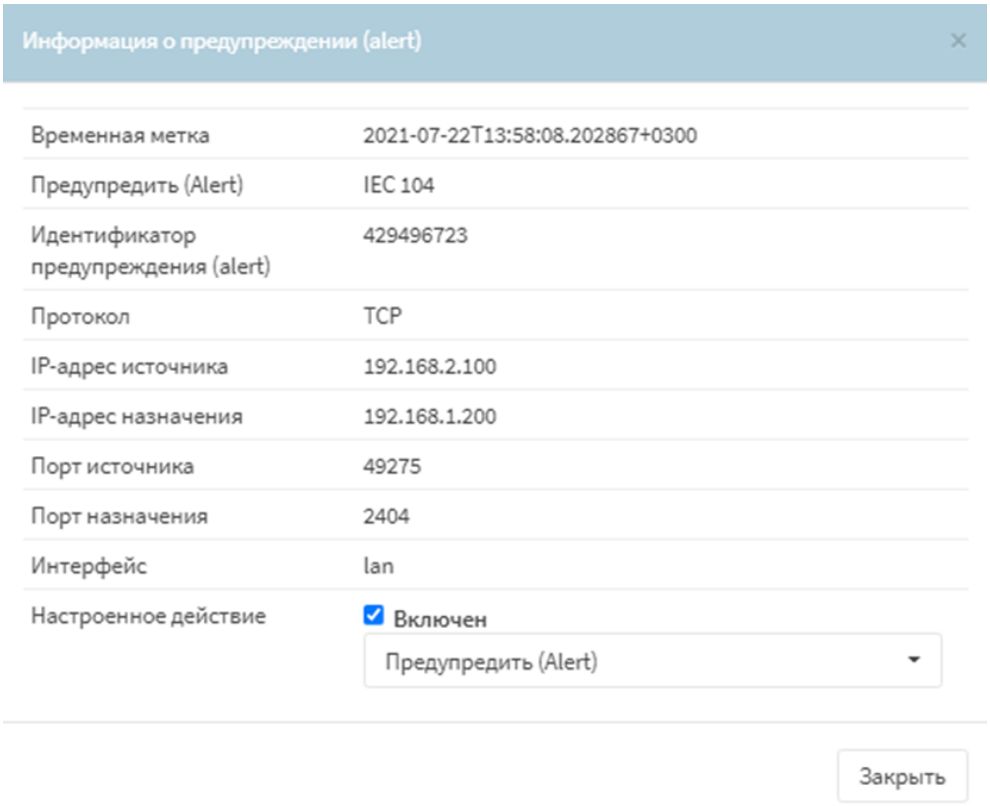

Рисунок 73 – Детальная информация, протокол IEC 104

5.5.3.3 Шаблон протокола S7comm

При создании пользовательского правила на основе шаблона промышленного протокола S7comm необходимо задать параметры протокола, выбрав в поле **«Фильтровать на основе протокола»** опцию «Указать дополнительные параметры».

При выборе опции «Указать дополнительные параметры» появится поле **«Тип сообщения»**, в котором доступно четыре типа сообщений:

- **«JOBREQUEST»** –пакет с запросом на выполнение функции;
- **«ACK»** – пакет с результатом выполнения операции;
- **«ACKDATA»** – пакет с ответом на запрос;
- **«USERDATA»** – пакет с данными пользователя.

При выборе типа сообщения «JOBREQUEST» появится поле **«Функция»**, в котором доступны следующие функции:

- **«CPUSERVICE»** – сервисы ЦП;

- **«SETUPCOMM»** – запрос на подключение к ПЛК;
- **«READVAR»** – запрос на чтение;
- **«WRITEVAR»** – запрос на запись;
- **«REQUESTDOWNLOAD»** – запрос на загрузку прошивки;
- **«DOWNLOADBLOCK»** – загрузка прошивки на ПЛК;
- **«DOWNLOADENDED»** – запрос на завершение загрузки прошивки на ПЛК;
- **«STARTUPLOAD»** – запрос на выгрузку прошивки;
- **«UPLOAD»** – выгрузка прошивки с ПЛК;
- **«ENDUPLOAD»** – окончание выгрузки прошивки с ПЛК;
- **«PLCCONTROL»** – управление ПЛК;
- **«PLCSTOP»** – остановка ПЛК.

При выборе функции «READVAR» или «WRITEVAR» появится поле **«Тип области»**, в котором будут доступны типы области чтения, указанные в таблице (см. Таблица 16).

Таблица 16
Типы области

Тип области	Описание
Любой	Любая область чтения
SI (System info)	Системная информация
SF (System flags)	Системные флаги
AI (Analog inputs)	Аналоговый ввод
AO (Analog outputs)	Аналоговый вывод
C (Counters)	Счетчики
T (Timers)	Таймеры
IC (IEC Counters)	Счетчики IEC
IT (IEC Timers)	Таймеры IEC
P (Directp peripheral access)	Прямой доступ к периферии
I (Inputs)	Ввод
Q (Outputs)	Вывод
M (Flags)	Флаги
DB (Data blocks)	Блоки данных

Тип области	Описание
DI (Instance data blocks)	Блоки данных экземпляра
LV (Local data)	Локальные данные

При выборе в поле **«Тип области»** любого значения, кроме значения «Любой», появятся поля:

- **«Имя области»**;
- **«Тип данных»**;
- **«Количество данных»**;
- **«Смещение данных»**.

Поле **«Имя области»** принимает значения от «0» до «65535».

В поле **«Тип данных»** доступны следующие типы данных:

- **«BIT»**;
- **«BYTE»**;
- **«CHAR»**;
- **«WORD»**;
- **«INT»**;
- **«DWORD»**;
- **«DINT»**;
- **«REAL»**;
- **«DATE»**;
- **«TOD»**;
- **«TIME»**;
- **«S5TIME»**;
- **«DATETIME»**;
- **«COUNTER»**;
- **«TIMER»**;
- **«IECTIMER»**;
- **«IECCOUNTER»**;
- **«HSCOUNTER»**.

Поле **«Смещение данных»** принимает целочисленное значение в шестнадцатеричной системе счисления в формате «0x000000».

При выборе функции «WRITEVAR» и любого значения в поле **«Тип области»**, кроме значения «Любой», появятся дополнительные поля:

- **«Тип передаваемого значения»**;
- **«Количество передаваемых данных»**;
- **«Список значений данных»**.

В поле **«Тип передаваемого значения»** доступны следующие типы значений:

- **«NULL»** – не выбрано;
- **«BIT»** – значение в битах;
- **«BYTE»** – значение в байтах;
- **«INT»** – целочисленное значение;
- **«REAL»** – вещественное;
- **«STR»** – строковое значение.

Поле **«Список значений данных»** принимает целочисленное значение в шестнадцатеричной системе счисления в формате «0x000000».

При выборе функций «REQUESTDOWNLOAD», «DOWNLOADBLOCK», «STARTUPLOAD» появится поле **«Тип блока»**, в котором будут доступны следующие типы блока скачивания:

- **«OB»** – организационный блок, хранит главные программы;
- **«DB»** – блок данных, хранит необходимые для ПЛК программ данные;
- **«SDB»** – блок данных системы, хранит необходимые для ПЛК программ данные;
- **«FC»** – функция, функции без состояния – не имеют собственной памяти), могут быть запущены из других программ;
- **«SFC»** – системная функция, функции без состояния – не имеют собственной памяти), могут быть вызваны из других программ;
- **«FB»** – блок функции, функции с состоянием, обычно имеют ассоциированный SDB;
- **«SFB»** – блок системной функции, функции с состоянием, обычно имеют ассоциированный SDB.

При выборе в поле **«Тип блока»** любого значения, кроме значения «Любой», появятся поля **«Номер блока»** и **«Целевая файловая система»**.

В поле **«Целевая файловая система»** доступны две опции:

- **«P»** – пассивная, блок требует активации после скачивания.
- **«A»** – активная, блок будет активизирован после скачивания.

При выборе функции «PLCCONTROL» появится поле **«Функция»**, в котором доступны следующие функции управления ПЛК:

- **«INSE»** – активация скаченного блока, параметром выступает имя блока;
- **«DELE»** – удаление блока, параметром выступает имя блока;
- **«PPROGRAM»** – запуск программы, параметром выступает имя программы;
- **«GARB»** – сжатие памяти;
- **«MODU»** – копирование RAM в ROM, параметр содержит идентификаторы файловой системы A/E/P;
- **«OFF»** – выключение ПЛК;
- **«ON»** – включение ПЛК.

5.5.3.3.1 Пример создания правила COB

Необходимо создать пользовательское правило (см. Раздел 5.5.1) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «S7Comm»;
- **«Использовать шаблон»** – «S7comm»;
- **«Действие»** – «Отклонить (Reject)»;
- **«Сообщение»** – «S7Comm»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»
- **«Тип сообщения»** – «JOBREQUEST»;
- **«Функция»** – «PLCSTOP».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.3.2 Проверка созданного правила COB

Для проверки срабатывания пользовательского правила на основе шаблона протокола S7comm на ПК **«Server»** должно быть установлено ПО «Snap7 Server Demo», а на ПК **«Client»** – ПО «Snap7 Client Demo».

Для проверки правила COB необходимо выполнить следующие действия:

1. В ПО «Snap7 Server Demo», в поле **«Local Address»** ввести «192.168.1.200» и нажать **кнопку «Start»** (см. Рисунок 74) для локального запуска сервиса.

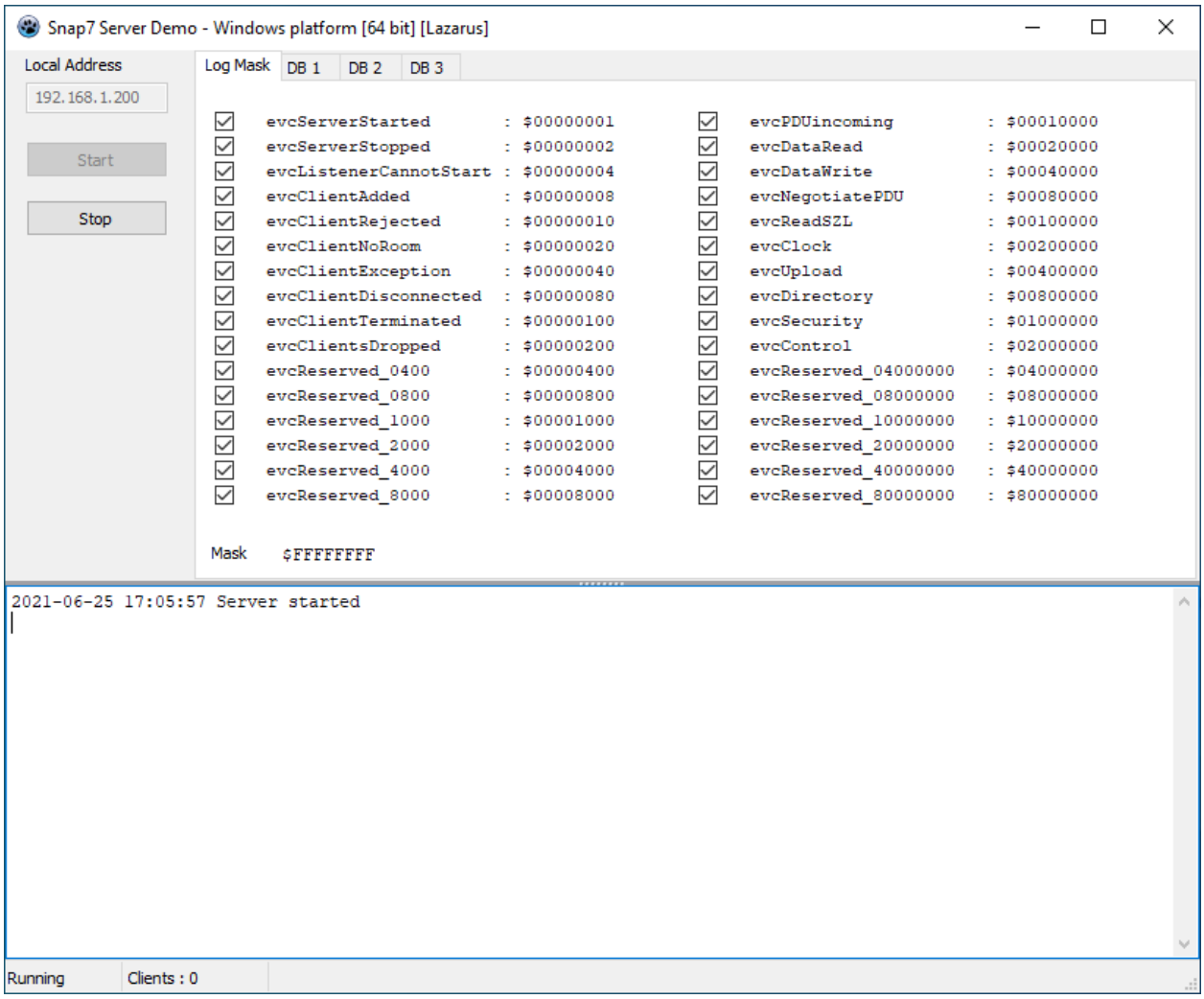

Рисунок 74 – Запуск ПО «Snap7 Server Demo»

2. Запустить ПО «Snap7 Client Demo», в поле **«IP»** ввести «192.168.1.200» и нажать **кнопку «Connect»** для подключения к «Snap7 Server Demo».
3. Убедиться, что во вкладке **«System info»** отображается информация о контроллере (см. Рисунок 75).

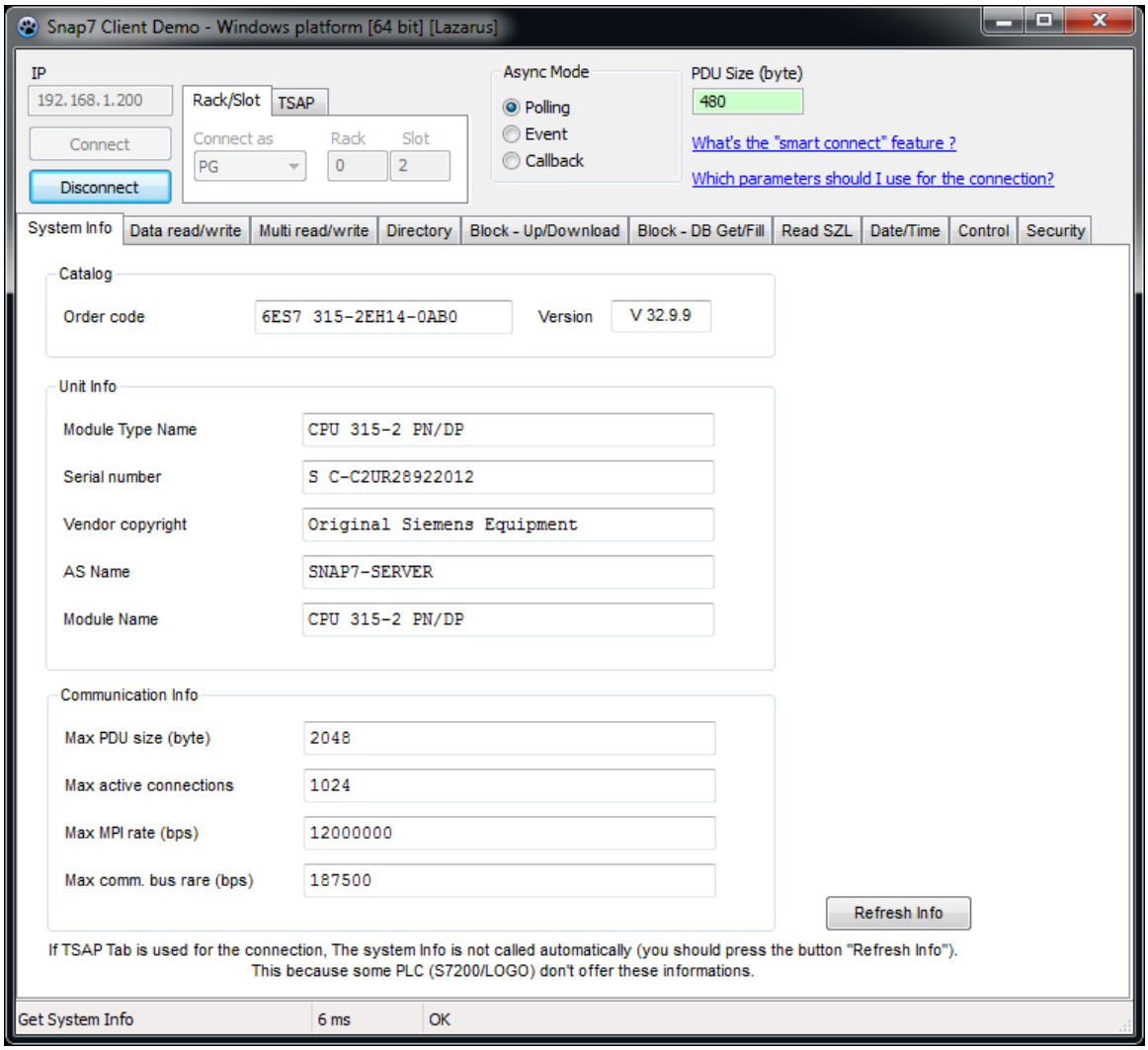

Рисунок 75 – Запуск ПО «Snap7 Client Demo»

4. Произвести запись в регистр, для этого перейти во вкладку **«Data read/write»**, ввести в регистр «0000/00» значение «1» и нажать **кнопку «Write»** (см. Рисунок 76).

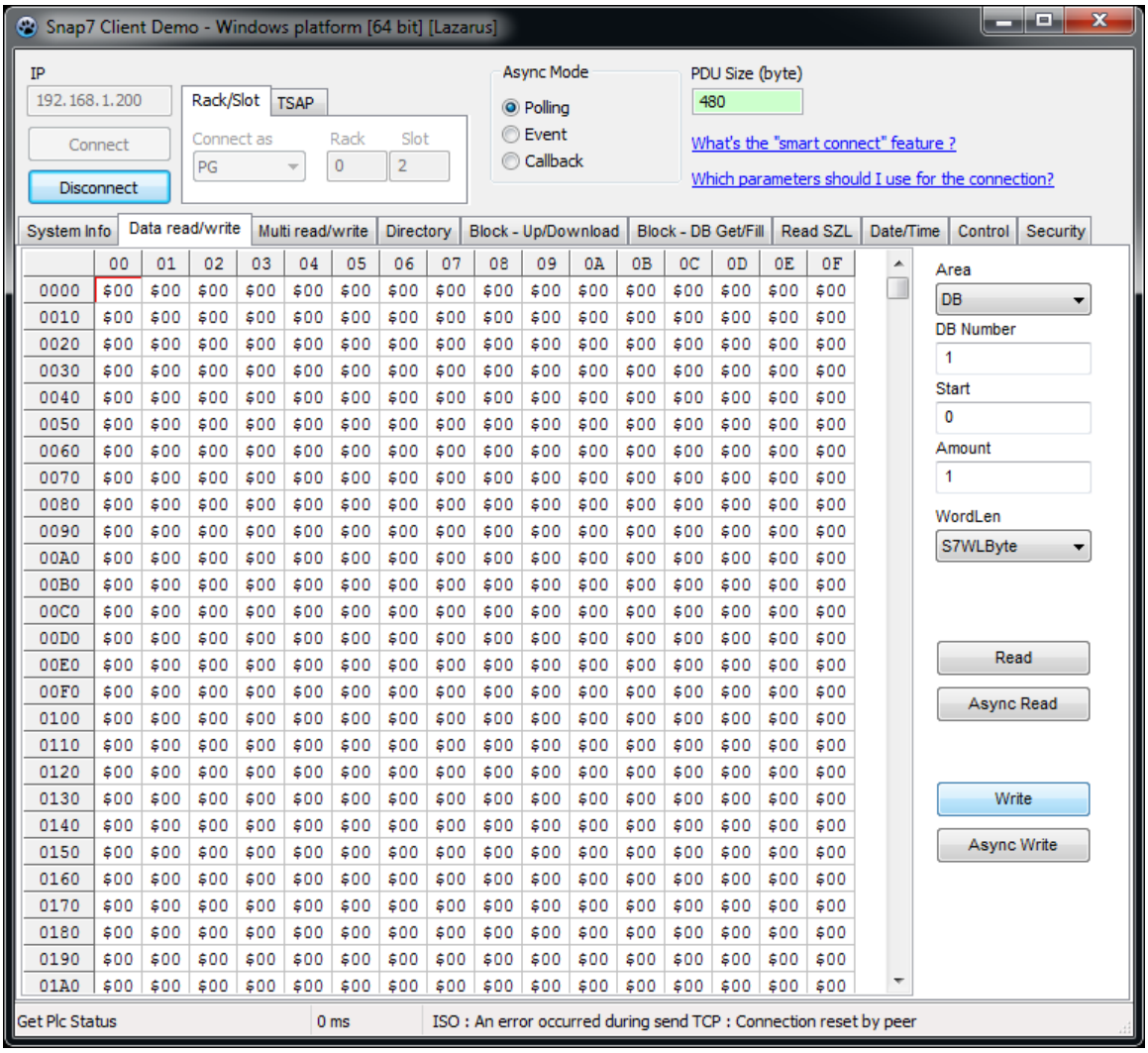

Рисунок 76 – Запись в регистр «0000/00»

5. Перейти во вкладку **«Control»**, нажать **кнопку «Stop»** для остановки работы контроллера и убедиться в изменении индикации с «RUN» на «Unknown» и недоступности **кнопки «Get status»** (см. Рисунок 77).

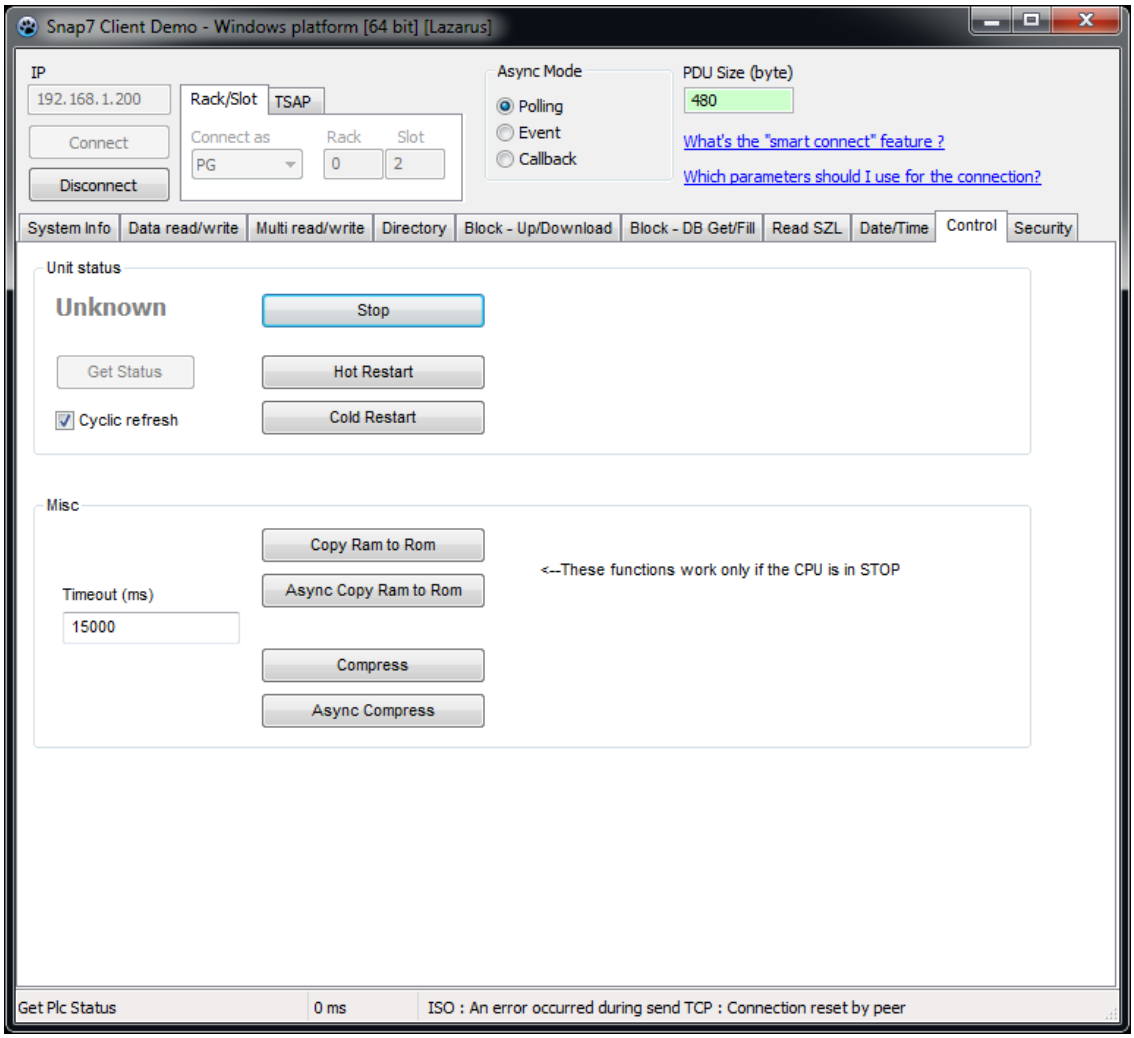

Рисунок 77 – Отключение контроллера

6. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений»** - **«Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:
    - «S7Comm» (см. Рисунок 78).

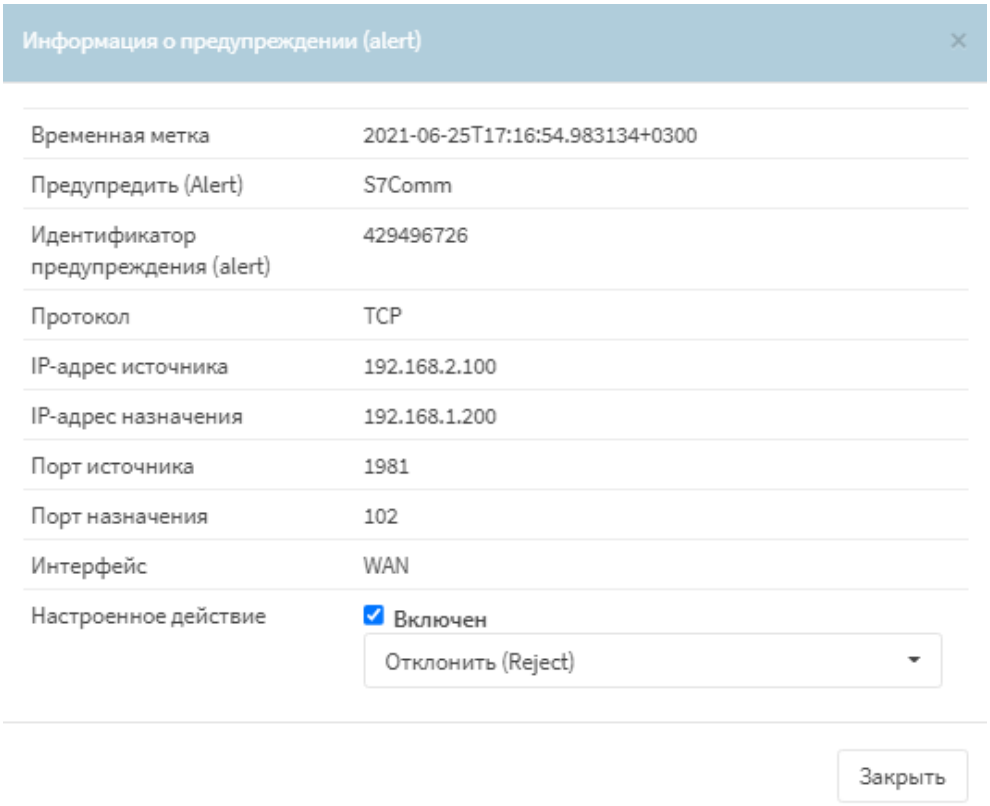

Рисунок 78 – Детальная информация, протокол S7comm

5.5.3.4 Шаблон протокола OPC DA

При создании пользовательского правила на основе шаблона промышленного протокола OPC DA необходимо задать параметры протокола, выбрав в поле **«Фильтровать на основе протокола»** опцию «Указать дополнительные параметры».

При выборе опции «Указать дополнительные параметры» появится поле **«Тип сообщения»**, в котором доступны типы сообщений, указанных в таблице (см. Таблица 17).

Таблица 17
Типы сообщений OPC DA

Тип сообщения	Описание
REQUEST	Сообщение запроса на операцию
PING	Сообщение запроса обратного вызова
RESPONSE	Сообщение ответа
FAULT	Сообщение сбоя
WORKING	Сообщение подтверждающее, что все исходящие пакеты получены

Тип сообщения	Описание
NOCALL	Ответ на команду PING
REJECT	Сообщение отклонения пакета
ACK	Подтверждение получения ответа
CI_CANCEL	Отмена операции
FACK	Если состояние вызова не STATE_SEND_FRAGS, отбросить пакет
CANCEL_ACK	Подтверждение отмены операции
BIND	Установка сессии
BIND_ACK	Подтверждение установки сессии
BIND_NACK	Отказ в установки сессии с выбранными параметрами
ALTER_CONTEXT	Изменение параметров сессии
ALTER_CONTEXT_RESP	Подтверждение изменения параметров сессии
SHUTDOWN	Сброс соединения
AUTH3	Обновление авторизации пользователя
CO_CANCEL	Передача команды отмены
ORPHANED	Флаг невозможности отмены операции

При выборе типа сообщения **«REQUEST»** появятся поля **«Идентификатор вызываемого интерфейса»** и **«Номер вызываемой функции объекта»**.

Пользовательские правила для протокола OPC DA возможно создать для действий над тегами и для заранее определенного UUID.

Набор заранее определенных UUID конечен и добавлен в **ARMA IF** в соответствии со спецификацией протокола OPC DA.

5.5.3.4.1 Пример создания правила COB

В качестве примера будет рассмотрено детектирование чтения тега «Intender_1» и выполнение функции номер «3» UUID «IOPCItemMgt».

Необходимо создать пользовательские правила (см. Раздел 5.5.1) для детектирования действия над тегом и детектирования выполнения функции UUID.

Для детектирования действия над тегом при создании правила необходимо указать следующие параметры правила:

- **«Включить»** – установлен флажок;

- **«Заголовок»** – «Test.Folder.Intender_1 Read»;
- **«Использовать шаблон»** – «OPC DA»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «Test.Folder.Intender_1 Read»;
- **«Фильтровать на основе протокола»** – «Операция над тегом»;
- **«Операция над тегом»** – «Считать»;
- **«Полный путь к тегу(-ам)»** – «Test.Folder.Intender_1». Данный параметр содержит в себе имя тега и все каталоги по пути к нему, разделённые точками.

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**.

Для детектирования выполнения функции UUID при создании правила необходимо указать следующие параметры правила:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «OPC DA IOPCItemMgt»;
- **«Использовать шаблон»** – «OPC DA»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «OPC DA IOPCItemMgt»;
- **«Фильтровать на основе протокола»** – «Дополнительные параметры»;
- **«Тип сообщения»** – «REQUEST»;
- **«Идентификатор вызываемого интерфейса»** – «[OPC DA] IOPCItemMgt»;
- **«Номер вызываемой функции объекта»** – «3». В случае, если данный параметр оставить пустым предупреждение будет сформировано для любой вызываемой функции UUID.

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.4.2 Проверка созданного правила СОВ

Для проверки срабатывания пользовательских правила на основе шаблона протокола OPC DA на ПК **«Server»** должен быть установлен и запущен эмулятор протокола OPC DA – «OPC DA Server», на ПК **«Client»** – «OPCtools».

Порядок проверки срабатывания пользовательских правил:

1. Запустить ПО «OPCtools» и выполнить подключение к серверу «OPC DA».
2. Выполнить чтение тега «Intender_1» (см. Рисунок 79).

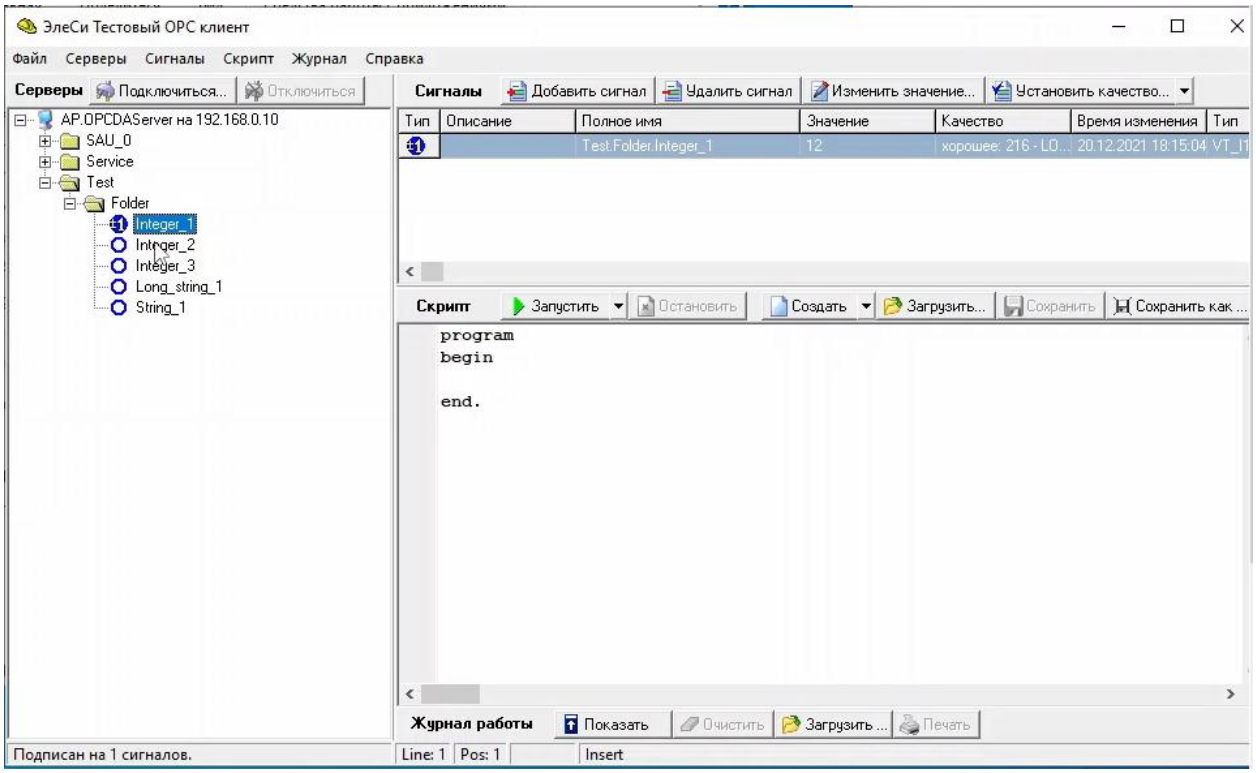

Рисунок 79 – Чтение тега «Intender_1» в ПО «OPCtools»

3. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений»** - **«Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:
    - **«Test.Folder.Intender_1 Read»** – для действия с тегом (см. Рисунок 80);
    - **«OPC DA IOPCItemMgt»** – для вызова функции UUID. (см. Рисунок 81).

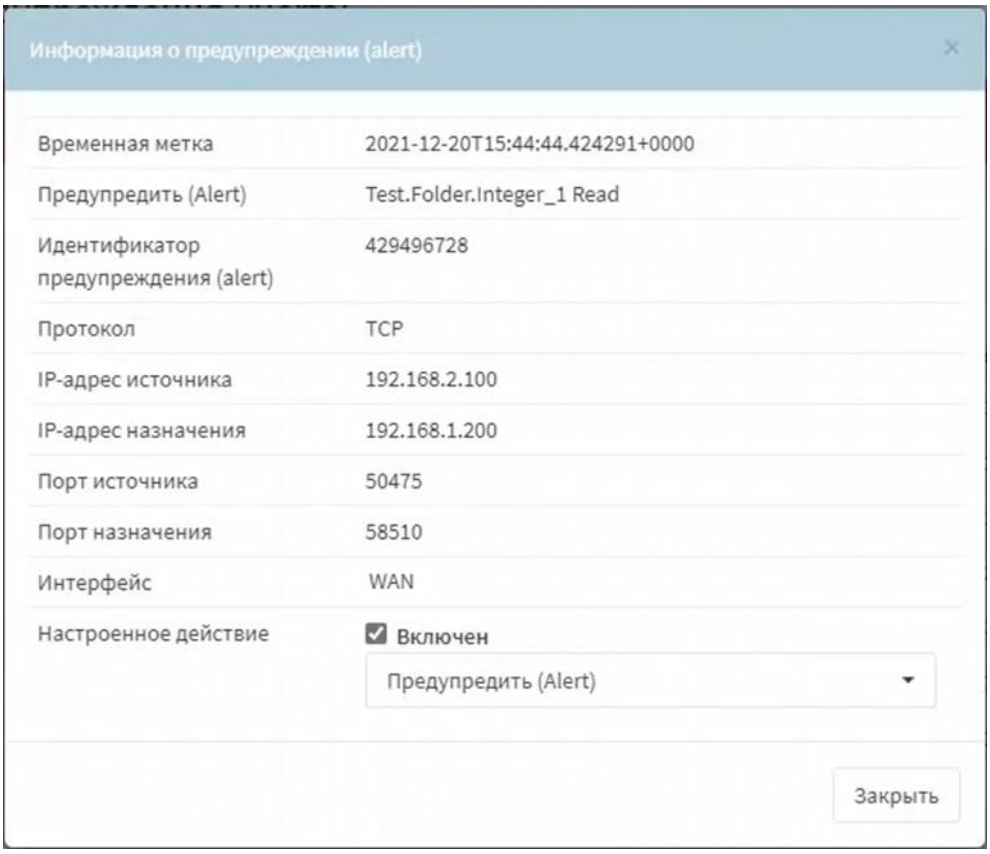

Рисунок 80 – Детальная информация, протокол OPC DA – чтение тега

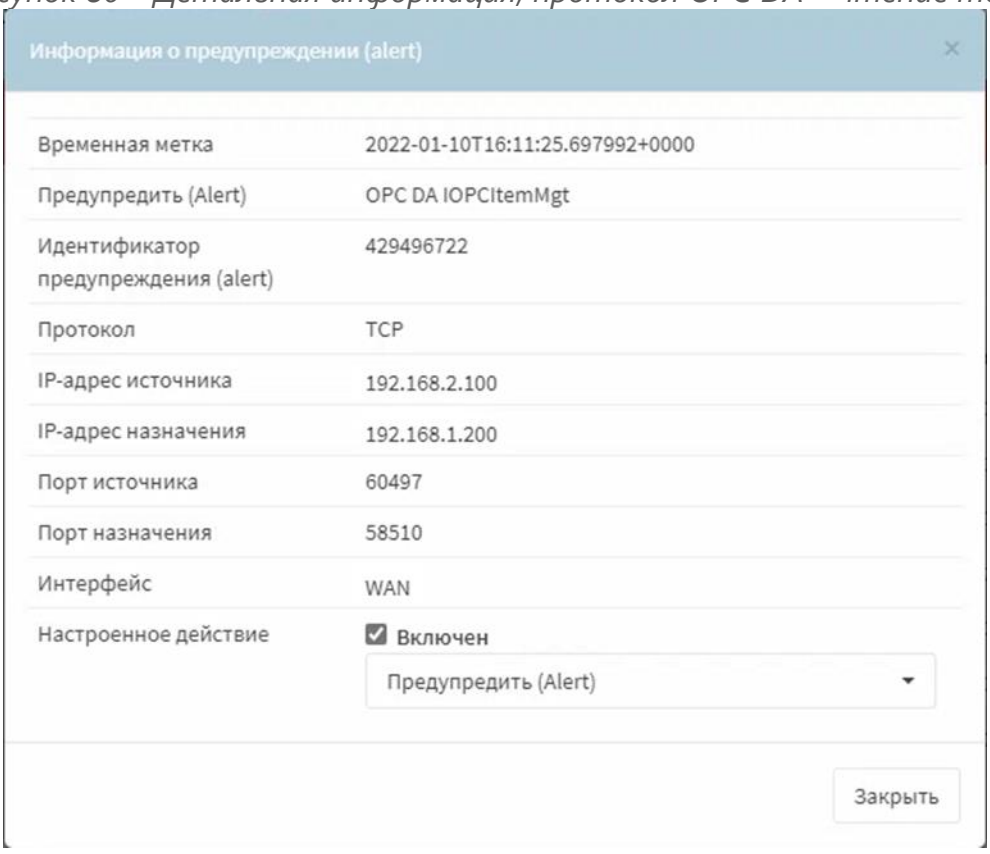

Рисунок 81 – Детальная информация, протокол OPC DA – вызов функции

5.5.3.5 Шаблон протокола OPC UA

При создании пользовательского правила на основе шаблона промышленного протокола OPC UA необходимо задать параметры протокола, выбрав в поле **«Фильтровать на основе протокола»** опцию «Указать дополнительные параметры».

При выборе опции «Указать дополнительные параметры» появятся поле **«Тип сообщения»**.

В поле **«Тип сообщения»** доступны следующие типы сообщений:

- **«HELLO»** – маркер начала передачи данных между клиентом и сервером;
- **«ACKNOWLEDGE»** – ответ на сообщение типа HELLO;
- **«OPEN»** – открытие канала передачи данных с предложенным методом шифрования данных;
- **«MESSAGE»** – передаваемое сообщение;
- **«CLOSE»** – конец сессии.

При выборе типа сообщения **«OPEN»** появится поле **«Политика безопасности»**, в котором доступны следующие политики безопасности:

- **«NONE»** – политика безопасности для конфигураций с самыми низкими требованиями безопасности, нет алгоритмов шифрования;
- **«BASIC128RSA15»** – политика безопасности для конфигураций со средними требованиями безопасности такие как:
    - проверка сертификата безопасности;
    - необходимо шифрование;
    - необходима безопасная подпись;
    - использование алгоритма шифрования SHA 1;
    - использование алгоритма шифрования AES 128 CBC;
    - использование алгоритма шифрования RSA-PKCS15-SHA1;
    - использование алгоритма шифрования RSA-PKCS15;
    - использование алгоритма получения ключа P-SHA1;
    - использование алгоритма подписи сертификата RSA-PKCS15-SHA1;
    - использование ограниченного алгоритма получения ключа RSA15;
- **«BASIC256»** – политика безопасности для конфигураций со средними требованиями безопасности такие как:

  - проверка сертификата безопасности;
  - необходимо шифрование;
  - необходима безопасная подпись;
  - использование алгоритма шифрования SHA 1;
  - использование алгоритма шифрования AES 128 CBC;
  - использование алгоритма шифрования RSA-PKCS15-SHA1;
  - использование алгоритма шифрования RSA-OAEP-SHA1;
  - использование алгоритма получения ключа P-SHA1;
  - использование алгоритма подписи сертификата RSA-PKCS15-SHA1;
  - использование ограниченного алгоритма получения ключа RSA15;
- **«BASIC256SHA256»** – политика безопасности для конфигураций со средними требованиями безопасности такие как:
  - проверка сертификата безопасности;
  - необходимо шифрование;
  - необходима безопасная подпись;
  - использование алгоритма шифрования SHA 2;
  - использование алгоритма шифрования AES 256 CBC;
  - использование алгоритма шифрования RSA-PKCS15-SHA2-256;
  - использование алгоритма шифрования RSA-OAEP-SHA1;
  - использование алгоритма получения ключа P-SHA2-256;
  - использование алгоритма подписи сертификата RSA-PKCS15-SHA2-256;
  - использование ограниченного алгоритма получения ключа SHA2-256;
- **«AES128_SHA256_RSAOAEP»** – политика безопасности для конфигураций со средними требованиями безопасности такие как:
  - проверка сертификата безопасности;
  - необходимо шифрование;
  - необходима безопасная подпись;
  - использование алгоритма шифрования AES 128 SHA-256;
- **«PUBSUB_AES128_CTR»** – политика безопасности для конфигураций со средними требованиями безопасности такие как:
  - необходимо шифрование;

  - необходима безопасная подпись;
  - использование алгоритма шифрования AES 128 CTR;
- **«PUBSUB_AES256_CTR»** – политика безопасности для конфигураций со средними требованиями безопасности такие как:
  - необходимо шифрование;
  - необходима безопасная подпись;
  - использование алгоритма шифрования AES 128 CTR.

При выборе типа сообщения **«MESSAGE»** появится поле **«Тип запроса»**, в котором доступны типы запросов, указанные в таблице (см. Таблица 18).

Таблица 18
Типы запросов OPC UA

№	Тип запроса	Описание
1	FINDSERVERS	Запрос известных серверов
2	FINDSERVERSONNETWORK	Запрос известных работающих серверов
3	GETENDPOINTS	Запрос на поддерживаемые сервером конечные точки
4	REGISTERSERVER	Запрос на регистрацию сервера
5	REGISTERSERVER2	Запрос на регистрацию сервера с дополнительной информации для FINDSERVERSONNETWORK
6	CREATESESSION	Запрос на создание сессии
7	ACTIVATESESSION	Запрос на создание сессии (передача идентификационных данных клиента)
8	CLOSESESSION	Запрос на завершение сессии
9	CANCEL	Запрос отмены невыполненных запросов на обслуживание
10	ADDNODES	Запрос на добавление узла как дочерний в адресное пространство
11	ADDREFERENCES	Запрос на добавление ссылки на узел
12	DELETENODES	Запрос на удаление узла из адресного пространства
13	DELETEREFERENCES	Запрос на удаление ссылки узла

№	Тип запроса	Описание
14	BROWSE	Запрос на просмотр узлов
15	BROWSENEXT	Запрос на продолжение просмотра результата запроса BROWSE, если результат этого запроса превышает максимального значения
16	TRANSLATEBROWSEPATHSTONODEIDS	Запрос на преобразование пути узла в идентификатор узла
17	REGISTERNODES	Запрос на регистрацию узла, например, узла, информация о котором пользователю известна
18	UNREGISTERNODES	Запрос на отмену регистрации узла
19	QUERYFIRST	Запрос просмотр данных из определенного экземпляра
20	QUERYNEXT	Запрос на продолжение просмотра результата запроса QUERYFIRST, если результат этого запроса превышает максимального значения
21	READ	Запрос на чтение данных
22	HISTORYREAD	Запрос на просмотр значений или событий узлов
23	WRITE	Запрос на изменение узла
24	HISTORYUPDATE	Запрос на обновление значений или событий узлов
25	CALLMETHOD	Запрос на получение результатов вызова удаленной процедуры
26	CALL	Запрос на вызов удаленной процедуры
27	MONITOREDITEMCREATE	Запрос на начало подписки на событие
28	CREATEMONITOREDITEMS	Запрос на подписку на событие
29	MONITOREDITEMMODIFY	Запрос на изменение параметров подписки на события
30	MODIFYMONITOREDITEMS	Запрос на изменение подписки

№	Тип запроса	Описание
31	SETMONITORINGMODE	Запрос на установку режима подписки
32	SETTRIGGERING	Запрос на создание связи между событием и узлом
33	DELETEMONITOREDITEMS	Запрос на завершение подписки
34	CREATESUBSCRIPTION	Запрос на создание подписки на событие
35	MODIFYSUBSCRIPTION	Запрос на изменение подписки на событие
36	SETPUBLISHINGMODE	Запрос на включение отправки уведомлений по подпискам на событие
37	PUBLISH	Запрос на подтверждение получения уведомлений по подпискам на события
38	REPUBLISH	Запрос на повторную отправку уведомлений по подпискам на события
39	TRANSFERSUBSCRIPTIONS	Запрос на передачу подписки на событие из одной сессии в другую
40	DELETESUBSCRIPTIONS	Запрос на удаление подписки на событие

При выборе типа запросов **«BROSE»**, **«READ»** и **«WRITE»** появится параметр **«Значение»**. В текущей версии **ARMA IF** поддерживается отслеживание только числовых значений данного параметра.

При выборе типа запроса **«CALL»** появятся поля **«Имя вызываемого объекта»** и **«Имя вызываемой процедуры»**.

5.5.3.5.1 Пример создания правила СОВ

Необходимо создать пользовательское правило (см. Раздел 5.5.1) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «OPC UA»;
- **«Использовать шаблон»** – «OPC UA»;

- **«Действие»** – «Отклонить (Reject)»;
- **«Сообщение»** – «OPC UA»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»
- **«Тип сообщения»** – «MASSAGE»;
- **«Функция»** – «WRITE».
- **«Значение»** – установить флажок, «от 6257 до 6257».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.5.2 Проверка созданного правила СОВ

Для проверки срабатывания пользовательского правила на основе шаблона протокола OPC UA на ПК **«Server»** должен быть установлен эмулятор протокола OPC UA – «OPC UA Server», на ПК **«Client»** – ПО «UaExpert».

Порядок проверки срабатывания пользовательских правил:

1. Запустить ПО «OPC UA Server» (см. Рисунок 82).

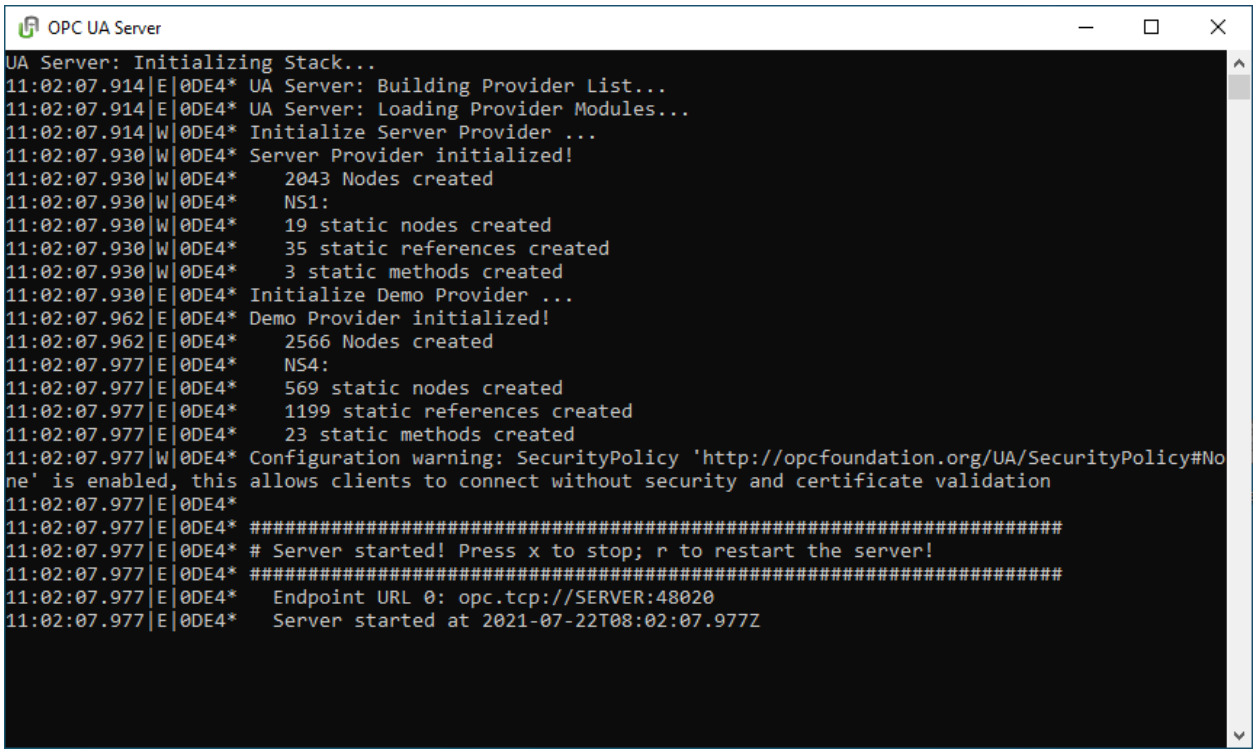

Рисунок 82 – Запуск OPC UA Server

2. Запустить ПО «UaExpert». При первом запуске необходимо будет создать сертификат, указав стандартную информацию SSL-ключа (см. Рисунок 83).

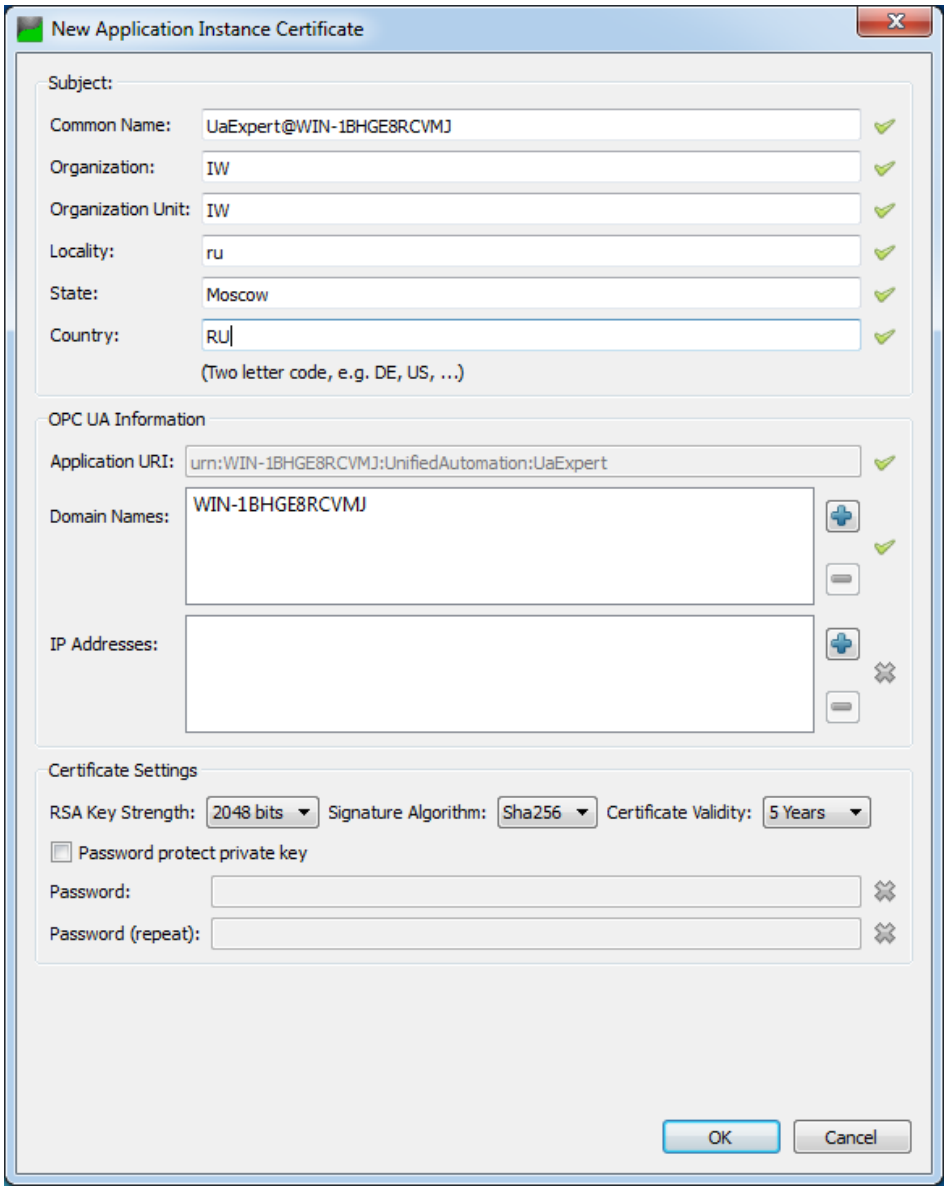

Рисунок 83 – Создание сертификата в UaExpert

3. Нажать **кнопку «**  **»** и добавить подключение к серверу «OPC UA Server» (см. Рисунок 84):

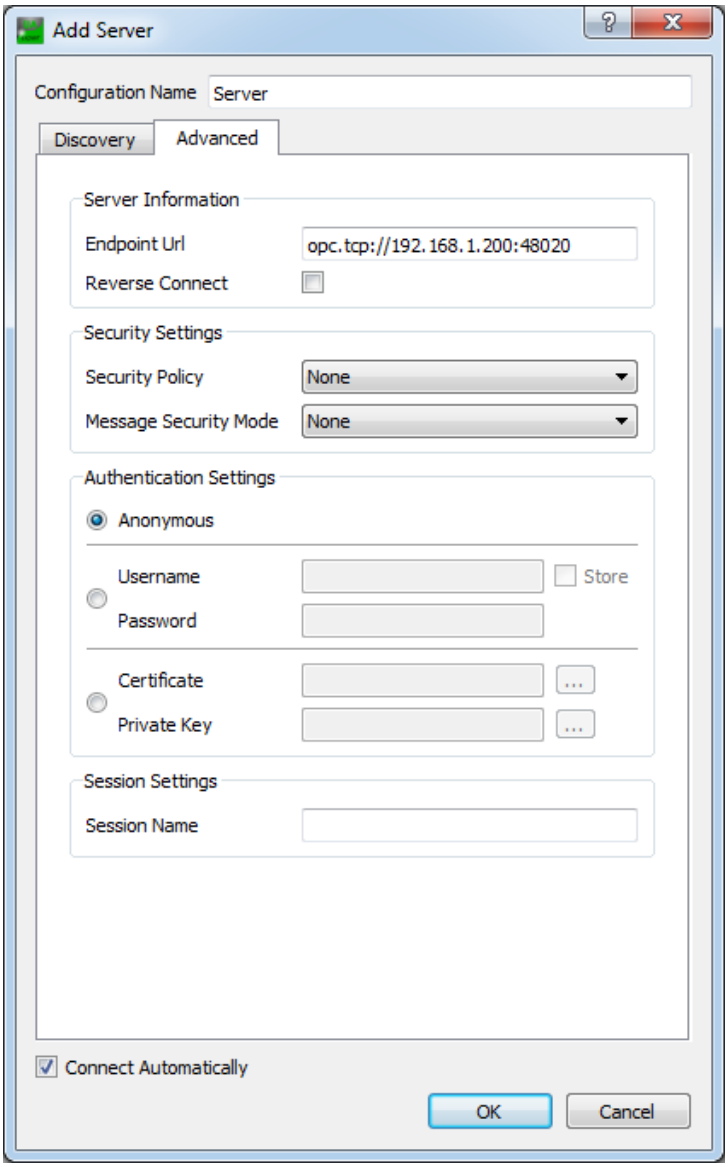

Рисунок 84 – Добавление сервера в UaExpert

4. Перейти в каталог «Root/Server/Machine» и перетащить мышью строку «HeaterSwitch» в окно «Data Access View». Затем нажать два раза **левой кнопкой мыши** по значению поля **«Value»** для перехода в режим редактирования значения переменной (см. Рисунок 85).

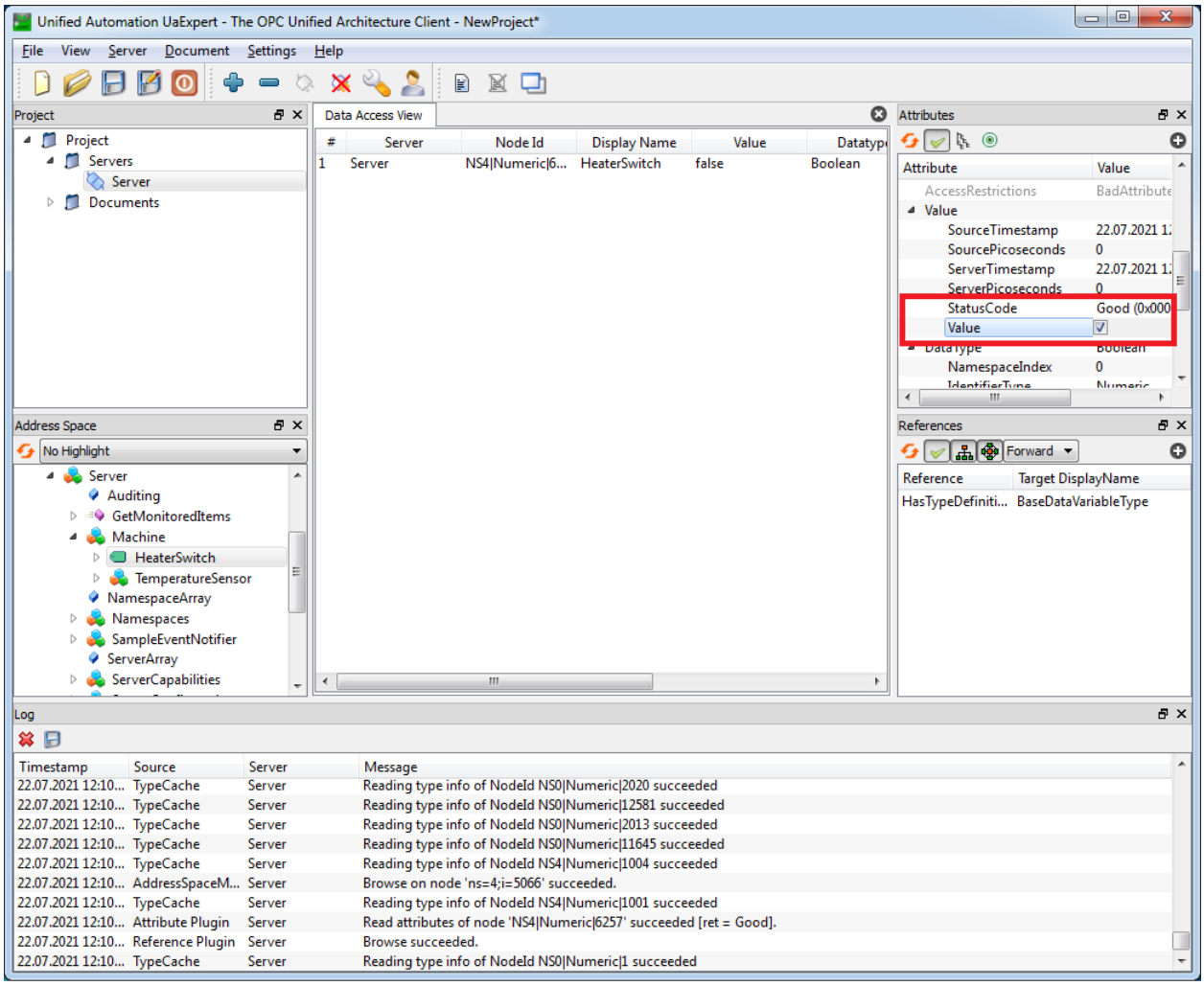

Рисунок 85 – Редактирование значения переменной

5. В блоке **«Log»** появится информация о неуспешной записи (см. Рисунок 86).

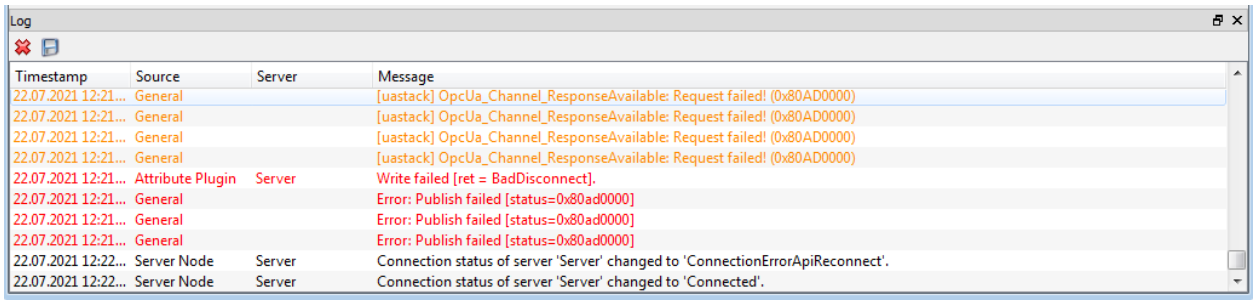

Рисунок 86 – Сообщение о неуспешной записи

6. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений»** - **«Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:

   - «OPC UA» (см. Рисунок 87).

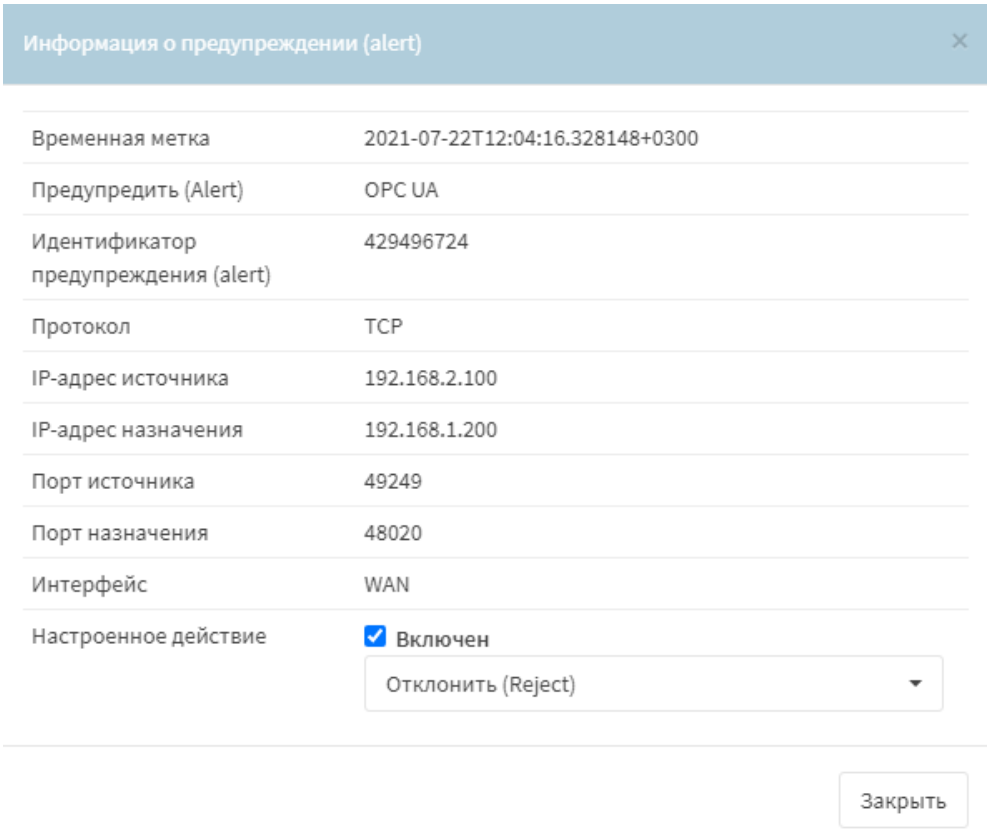

Рисунок 87 – Детальная информация, протокол OPC UA

5.5.3.6 Шаблон протокола UMAS

При создании пользовательского правила на основе шаблона промышленного протокола UMAS необходимо задать параметры протокола, выбрав в поле **«Фильтровать на основе протокола»** опцию «Указать дополнительные параметры».

При выборе опции «Указать дополнительные параметры» появится поле **«Функция»**, в которой доступны функции, указанные в таблице (см. Таблица 19).

Таблица 19
Функции протокола UMAS

Код	Название	Описание
0x01	INIT_COMM	Инициализация UMAS сессии
0x02	READ_ID	Запрос ПЛК ID
0x03	READ_PROJECT_INFO	Чтение информации о проекте
0x04	READ_PLC_INFO	Чтение внутренней информации ПЛК
0x06	READ_CARD_INFO	Чтение информации о внутренней SD карты ПЛК

Код	Название	Описание
0x0A	REPEAT	Отправить информацию обратно ПЛК. Используется для синхронизации
0x10	TAKE_PLC_RESERVATION	Назначить ПЛК владельца
0x11	RELEASE_PLC_RESERVATION	Снять владельца ПЛК
0x12	KEEP_ALIVE	Поддержка активного соединения
0x20	READ_MEMORY_BLOCK	Чтение блока памяти с ПЛК
0x22	READ_VARIABLES	Чтение системных битов, системных слов и переменных
0x23	WRITE_VARIABLES	Запись системных битов, системных слов и переменных
0x24	READ_COILS_REGISTERS	Чтение coils и регистров с ПЛК
0x25	WRITE_COILS_REGISTERS	Запись катушек и регистров в ПЛК
0x30	INITIALIZE_UPLOAD	Инициализация загрузки (копирование с инженерного ПК на ПЛК)
0x31	UPLOAD_BLOCK	Загрузка блока данных с инженерного ПК на ПЛК
0x32	END_STRATEGY_UPLOAD	Завершение загрузки (копирования с инженерного ПК на ПЛК)
0x33	INITIALIZE_DOWNLOAD	Инициализация скачивания (копирование с ПЛК на инженерный ПК)
0x34	DOWNLOAD_BLOCK	Скачивание блока данных с ПЛК на инженерный ПК
0x35	END_STRATEGY_DOWNLOAD	Конец скачивания (копирования с ПЛК на инженерный ПК)
0x39	READ_ETH_MASTER_DATA	Чтение Ethernet Master Data
0x40	START_PLC	Включение ПЛК
0x41	STOP_PLC	Выключение ПЛК
0x50	MONITOR_PLC	Мониторинг системных битов, системных слов и переменных
0x58	CHECK_PLC	Проверка статуса подключения ПЛК
0x70	READ_IO_OBJECT	Чтение IO объекта
0x71	WRITE_IO_OBJECT	Запись IO объекта

Код	Название	Описание
0x73	GET_STATUS_MODULE	Получение статуса модуля

При выборе «INIT_COMM», «READ_ID», «READ_PROJECT_INFO», «READ_PLC_INFO», «READ_CARD_INFO», «REPEAT», «TAKE_PLC_RESERVATION», «RELEASE_PLC_RESERVATION», «KEEP_ALIVE», «INITIALIZE_UPLOAD», «UPLOAD_BLOCK», «END_STRATEGY_UPLOAD», «INITIALIZE_DOWNLOAD», «DOWNLOAD_BLOCK», «END_STRATEGY_DOWNLOAD», «READ_ETH_MASTER_DATA», «START_PLC», «STOP_PLC», «MONITOR_PLC», «CHECK_PLC», «READ_IO_OBJECT», «WRITE_IO_OBJECT», «GET_STATUS_MODULE» появятся поля **«Информация о проекте»** и **«Тип сообщения»**.

В поле **«Тип сообщения»** доступно два типа сообщений:

- **«REQ»** – запрос.
- **«RES»** – ответ.

При выборе функции «READ_MEMORY_BLOCK» появятся поля:

- **«Номер блока»**;
- **«Количество данных»**;
- **«Смещение»**.

При выборе функции «READ_VARIABLES» появятся поля:

- **«Базовое смещение»**;
- **«Относительное смещение»**;
- **«Номер блока»**;
- **«Количество значений»**;
- **«Тип значений»**.

В поле **«Тип значений»** доступно три типа значений:

- **«BIT»**;
- **«WORD»**;
- **«DWORD»**.

При выборе функции «WRITE_VARIABLES» появятся поля:

- **«Номер блока»**;
- **«Смещение»**;
- **«Тип значений»**;

- **«Значение»**.

При выборе функций «READ_COILS_REGISTERS» и «WRITE_COILS_REGISTERS» появятся поля:

- **«Условие»**;
- **«Номер регистров флагов (Coils)»**;
- **«Смещение»**;
- **«Тип значений»**.

В поле **«Условие»** доступны следующие условия:

- **«отсутствует»**;
- **«больше чем»**;
- **«меньше чем»**;
- **«равно»**;
- **«отрицание»**.

В поле **«Тип значений»** доступно три типа значений:

- **«регистр»**;
- **«регистр флага (Coil)»**;
- **«отсутствует»**.

5.5.3.7 Шаблон протокола MMS

При создании пользовательского правила на основе шаблона промышленного протокола MMS необходимо задать параметры протокола, выбрав в поле **«Фильтровать на основе протокола»** опцию «Указать дополнительные параметры».

При выборе опции «Указать дополнительные параметры» появится поле **«Тип сообщения»**, в котором доступны следующие типы сообщений:

- **«CONFIRMED_REQUEST»**;
- **«CONFIRMED_RESPONSE»**;
- **«CONFIRMED_ERROR»**;
- **«UNCONFIRMED»**;
- **«REJECT»**;
- **«CANCEL_REQUEST»**;
- **«CANCEL_RESPONSE»**;

- **«CANCEL_ERROR»**;
- **«INITIATE_REQUEST»**;
- **«INITIATE_RESPONSE»**;
- **«INITIATE_ERROR»**;
- **«CONCLUDE_REQUEST»**;
- **«CONCLUDE_RESPONSE»**;
- **«CONCLUDE_ERROR»**.

При выборе типа сообщения «CONFIRMED_REQUEST» появится поле **«Тип службы»**, в котором доступны следующие типы используемых служб:

- **«STATUS»**;
- **«GETNAMELIST»**;
- **«IDENTIFY»**;
- **«RENAME»**;
- **«READ»**;
- **«WRITE»**;
- **«GETVARIABLEACCESSATTRIBUTES»**;
- **«DEFINENAMEDVARIABLE»**;
- **«DEFINESCATTEREDACCESS»**;
- **«GETSCATTEREDACCESSATTRIBUTES»**;
- **«DELETEVARIABLEACCESS»**;
- **«DEFINENAMEDVARIABLELIST»**;
- **«GETNAMEDVARIABLELISTATTRIBUTES»**;
- **«DELETENAMEDVARIABLELIST»**;
- **«DEFINENAMEDTYPE»**;
- **«GETNAMEDTYPEATTRIBUTES»**;
- **«DELETENAMEDTYPE»**;
- **«INPUT»**;
- **«OUTPUT»**;
- **«TAKECONTROL»**;
- **«RELINQUISHCONTROL»**;

- **«DEFINESEMAPHORE»**;
- **«DELETESEMAPHORE»**;
- **«REPORTSEMAPHORESTATUS»**;
- **«REPORTPOOLSEMAPHORESTATUS»**;
- **«REPORTSEMAPHOREENTRYSTATUS»**;
- **«INITIATEDOWNLOADSEQUENCE»**;
- **«DOWNLOADSEGMENT»**;
- **«TERMINATEDOWNLOADSEQUENCE»**;
- **«INITIATEUPLOADSEQUENCE»**;
- **«UPLOADSEGMENT»**;
- **«TERMINATEUPLOADSEQUENCE»**;
- **«REQUESTDOMAINDOWNLOAD»**;
- **«REQUESTDOMAINUPLOAD»**;
- **«LOADDOMAINCONTENT»**;
- **«STOREDOMAINCONTENT»**;
- **«DELETEDOMAIN»**;
- **«GETDOMAINATTRIBUTES»**;
- **«CREATEPROGRAMINVOCATION»**;
- **«DELETEPROGRAMINVOCATION»**;
- **«START»**;
- **«STOP»**;
- **«RESUME»**;
- **«RESET»**;
- **«KILL»**;
- **«GETPROGRAMINVOCATIONATTRIBUTES»**;
- **«OBTAINFILE»**;
- **«DEFINEEVENTCONDITION»**;
- **«DELETEEVENTCONDITION»**;
- **«GETEVENTCONDITIONATTRIBUTES»**;
- **«REPORTEVENTCONDITIONSTATUS»**;

- **«ALTEREVENTCONDITIONMONITORING»**;
- **«TRIGGEREVENT»**;
- **«DEFINEEVENTACTION»**;
- **«DELETEEVENTACTION»**;
- **«GETEVENTACTIONATTRIBUTES»**;
- **«REPORTEVENTACTIONSTATUS»**;
- **«DEFINEEVENTENROLLMENT»**;
- **«DELETEEVENTENROLLMENT»**;
- **«ALTEREVENTENROLLMENT»**;
- **«REPORTEVENTENROLLMENTSTATUS»**;
- **«GETEVENTENROLLMENTATTRIBUTES»**;
- **«ACKNOWLEDGEEVENTNOTIFICATION»**;
- **«GETALARMSUMMARY»**;
- **«GETALARMENROLLMENTSUMMARY»**;
- **«READJOURNAL»**;
- **«WRITEJOURNAL»**;
- **«INITIALIZEJOURNAL»**;
- **«REPORTJOURNALSTATUS»**;
- **«CREATEJOURNAL»**;
- **«DELETEJOURNAL»**;
- **«GETCAPABILITYLIST»**;
- **«FILEOPEN»**;
- **«FILEREAD»**;
- **«FILECLOSE»**;
- **«FILERENAME»**;
- **«FILEDELETE»**;
- **«FILEDIRECTORY»**;
- **«ADDITIONALSERVICE»**;
- **«GETDATAEXCHANGEATTRIBUTES»**;
- **«EXCHANGEDATA»**;

- **«DEFINEACCESSCONTROLLIST»**;
- **«GETACCESSCONTROLLISTATTRIBUTES»**;
- **«REPORTACCESSCONTROLLEDOBJECTS»**;
- **«DELETEACCESSCONTROLLIST»**;
- **«CHANGEACCESSCONTROL»**;
- **«RECONFIGUREPROGRAMINVOCATION»**.

При выборе типа службы «ADDITIONALSERVICE» появится поле **«Дополнительный тип сервиса»**, в котором доступны следующие типы дополнительного сервиса:

- **«VMDSTOP»**;
- **«VMDRESET»**;
- **«SELECT»**;
- **«ALTERPI»**;
- **«INITIATEUCLOAD»**;
- **«UCLOAD»**;
- **«UCUPLOAD»**;
- **«STARTUC»**;
- **«STOPUC»**;
- **«CREATEUC»**;
- **«ADDTOUC»**;
- **«REMOVEFROMUC»**;
- **«GETUCATTRIBUTES»**;
- **«LOADUCFROMFILE»**;
- **«STOREUCTOFILE»**;
- **«DELETEUC»**;
- **«DEFINEECL»**;
- **«DELETEECL»**;
- **«ADDECLREFERENCE»**;
- **«REMOVEECLREFERENCE»**;
- **«GETECLATTRIBUTES»**;
- **«REPORTECLSTATUS»**;

- **«ALTERECLMONITORING»**.

При выборе типа службы «READ» появятся поля:

- **«Item ID запроса чтения»**;
- **«Domain ID запроса чтения»**;
- **«Адрес запроса чтения»**.

При выборе типа службы «WRITE» появятся поля **«Item ID запроса чтения»** и **«Domain ID запроса чтения»**.

5.5.3.7.1 Пример создания правила СОВ

Необходимо создать пользовательское правило (см. Раздел 5.5.1) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «MMS»;
- **«Использовать шаблон»** – «MMS»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «MMS»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»
- **«Тип сообщения»** – «CONFIRMED_REQUEST»;
- **«Тип службы»** – «WRITE».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.7.2 Проверка созданного правила СОВ

Для проверки срабатывания пользовательского правила на основе шаблона протокола MMS на ПК **«Server»** должен быть установлен эмулятор протокола MMS, а на ПК **«Client»** – ПО «IEDExplorer».

Порядок проверки срабатывания пользовательских правил:

1. Запустить «IEDExplorer» и выполнить подключение к ПК **«Server»** (см. Рисунок 88).

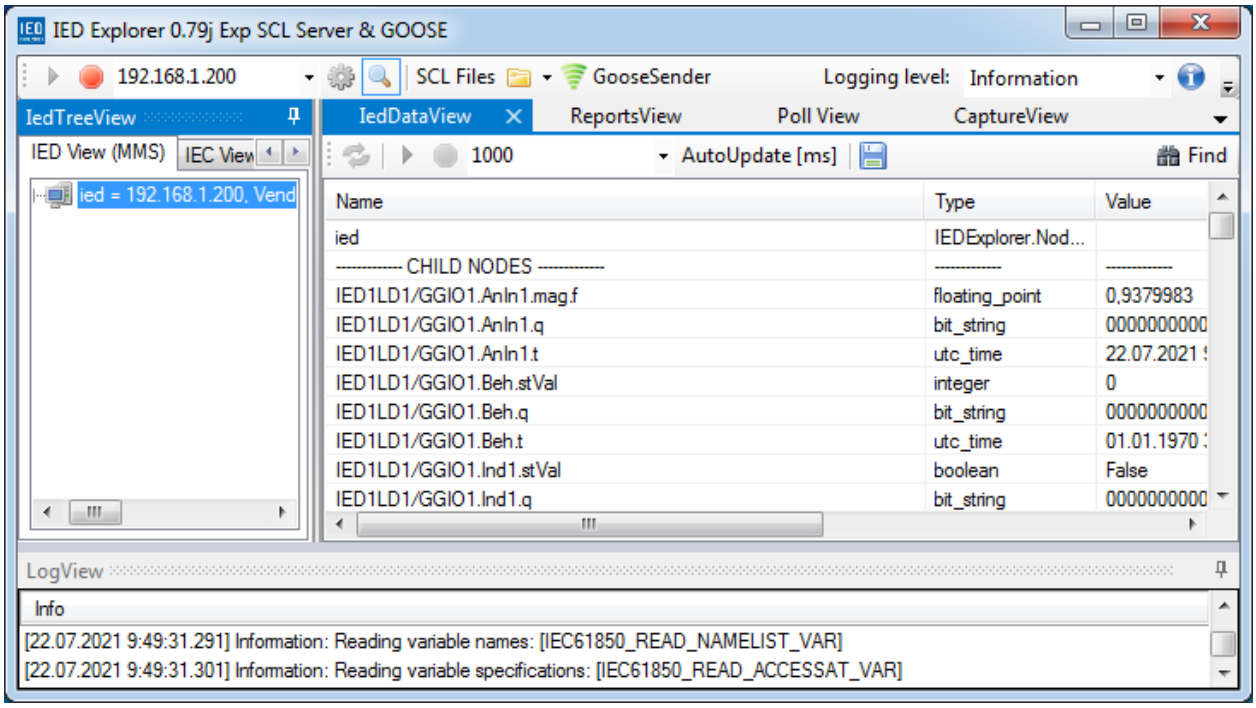

Рисунок 88 – Подключение к ПК «Server» в ПО «IEDExplorer»

2. Выбрать файл по пути «IED1LD1/MMDC1/FC SV/Watt/SubMag/DA f», нажать **правой кнопкой мыши**, выбрать **«Write data»**, в поле **«New Value»** ввести значение «1» и нажать **кнопку «OK»** (см. Рисунок 89) для сохранения нового значения.

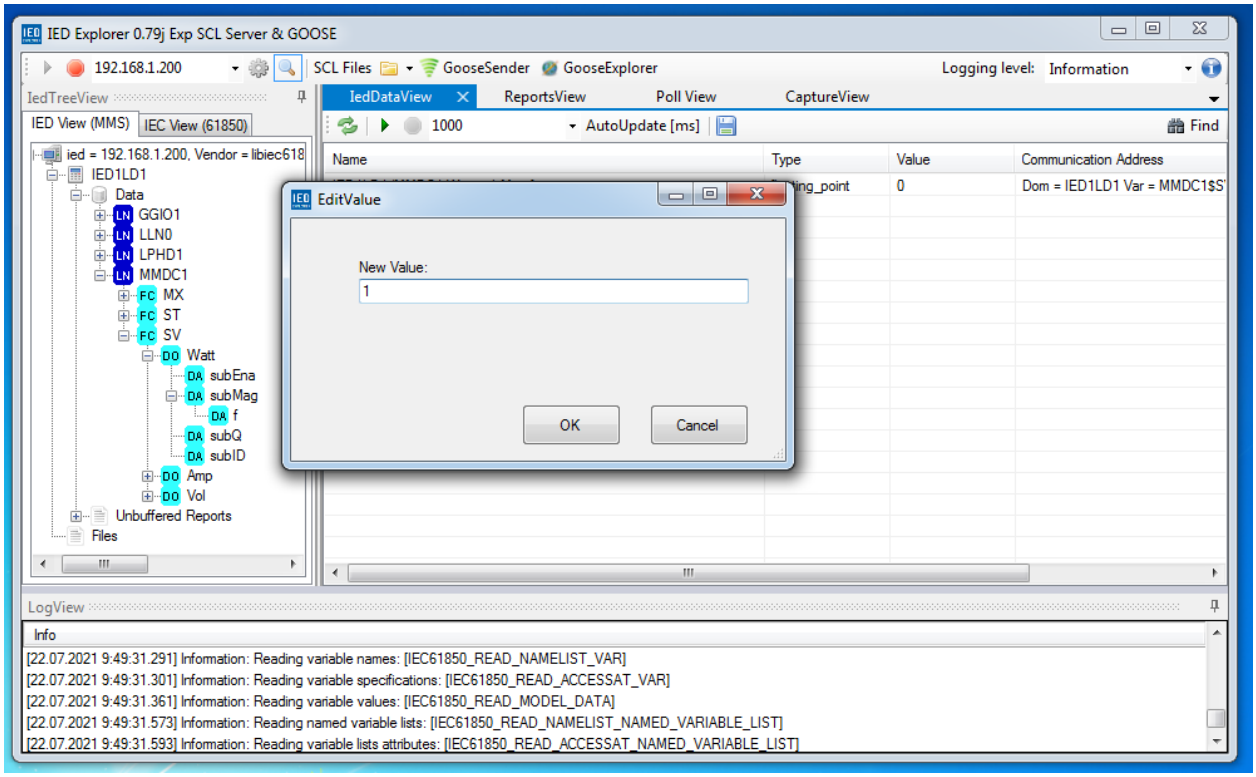

Рисунок 89 – Запись значения

3. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений» - «Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:

   - «MMS» (см. Рисунок 90).

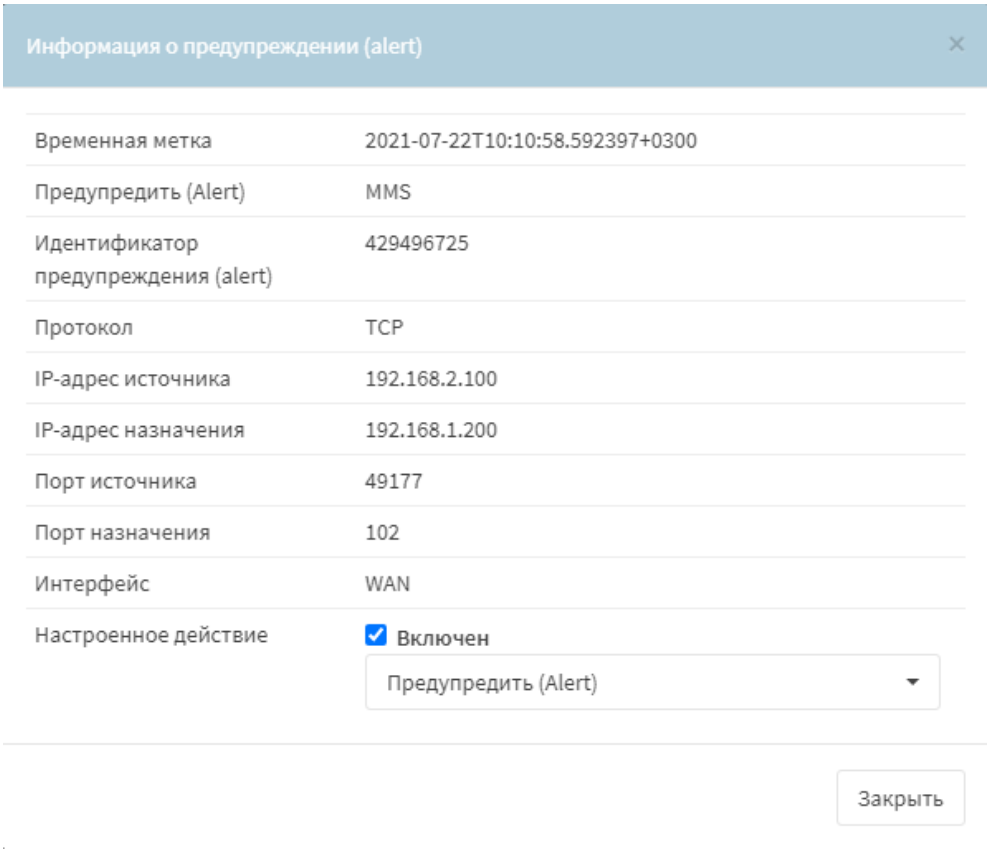

Рисунок 90 – Детальная информация, протокол MMS

5.5.3.8 Шаблон протокола GOOSE

При создании пользовательского правила на основе шаблона промышленного протокола GOOSE необходимо задать параметры протокола, выбрав в поле **«Фильтровать на основе протокола»** опцию «Указать дополнительные параметры».

При выборе опции «Указать дополнительные параметры» появятся поля, значения которых должны содержать не более 150 символов:

- **«APPID»**;
- **«Dataset»**;
- **«GoCBRef»**;
- **«GoID»**;
- **«Дельта секунд»**;

- **«Дельта наносекунд»**;
- **«Предустановленная дата и время»**;
- **«Предустановленные наносекунды»**.

ARMA IF пропускает пакеты промышленного протокола GOOSE только в режиме сетевого моста, который необходимо настроить перед проверкой (см. Раздел 16.1).

5.5.3.8.1 Пример создания правила СОВ

Необходимо создать пользовательское правило (см. Раздел 5.5.1) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «DREADED CANADIAN GOOSE»;
- **«Использовать шаблон»** – «GOOSE»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «DREADED CANADIAN GOOSE»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»
- **«Dataset»** – «[5:]».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.8.2 Проверка созданного правила СОВ

Для проверки срабатывания пользовательского правила на основе шаблона протокола GOOSE на ПК **«Server»** и **«Client»** должно быть установлено ПО «IED Explorer».

Порядок проверки срабатывания пользовательских правил:

1. На ПК **«Client»** запустить ПО «IED Explorer» и выполнить подключение к ПК **«Server»**.
2. Нажать **кнопку «GooseExplorer»**, в выпадающем списке выбрать используемую сетевую карту и нажать **кнопку «** **»** (см. Рисунок 91).

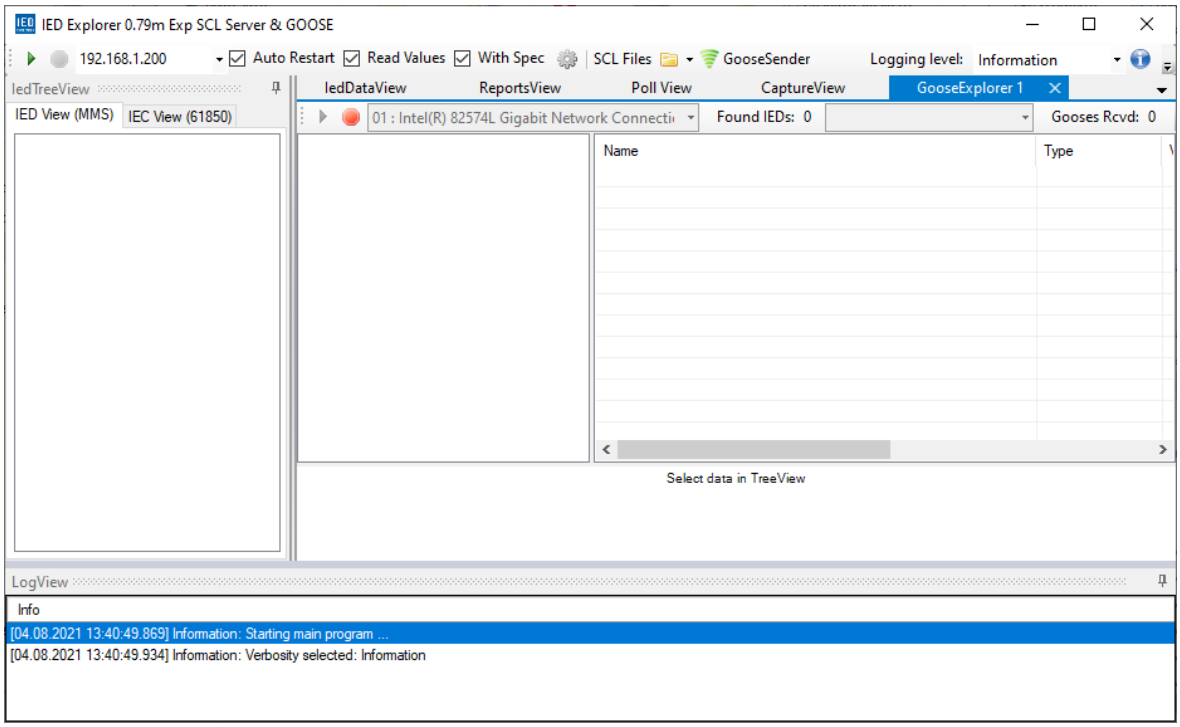

Рисунок 91 – Настройка ПО «IED Explorer» на ПК «Client»

3. На ПК **«Server»** запустить ПО «IED Explorer» и нажать **кнопку «GooseSender»**, в выпадающем списке выбрать используемую сетевую карту и нажать **кнопку «** **»**.

4. Нажать **кнопку «** **»**, в поле **«AppID»** поставить значение «5» и нажать **кнопку «Send 1x»** (см. Рисунок 92).

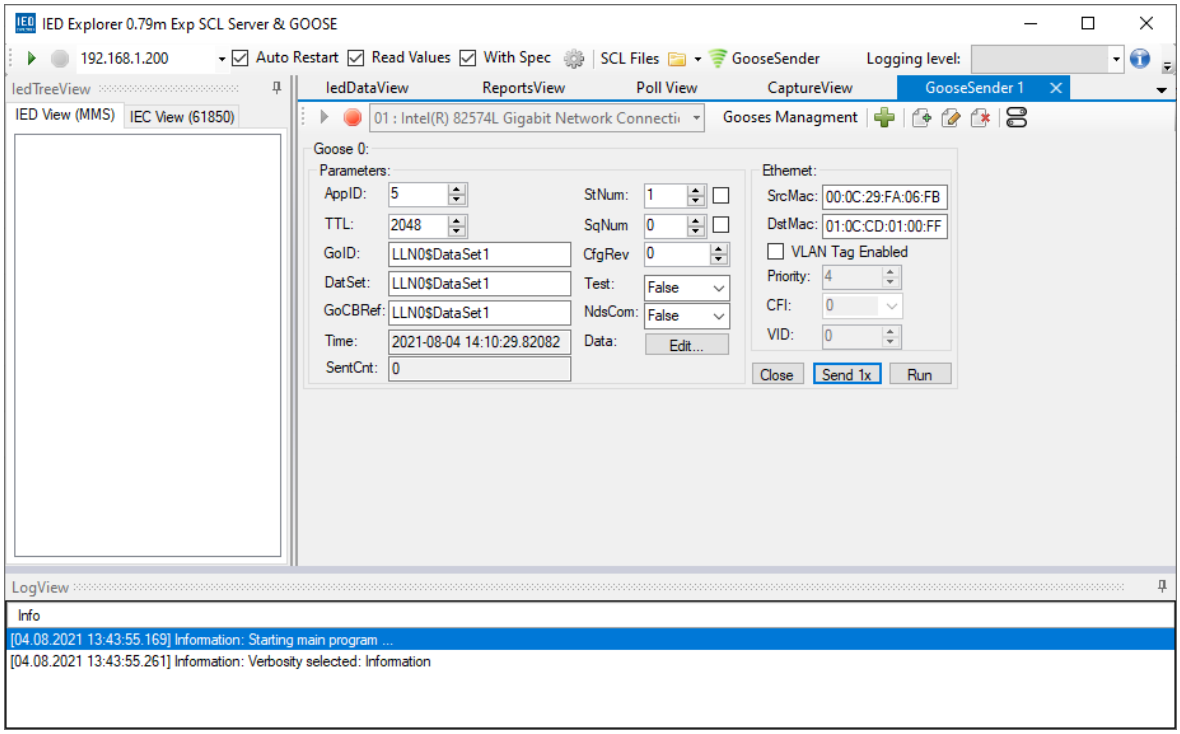

Рисунок 92 – Настройка ПО «IED Explorer» на ПК «Server»

5. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений» - «Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:
    - «DREADED CANADIAN GOOSE» (см. Рисунок 93).

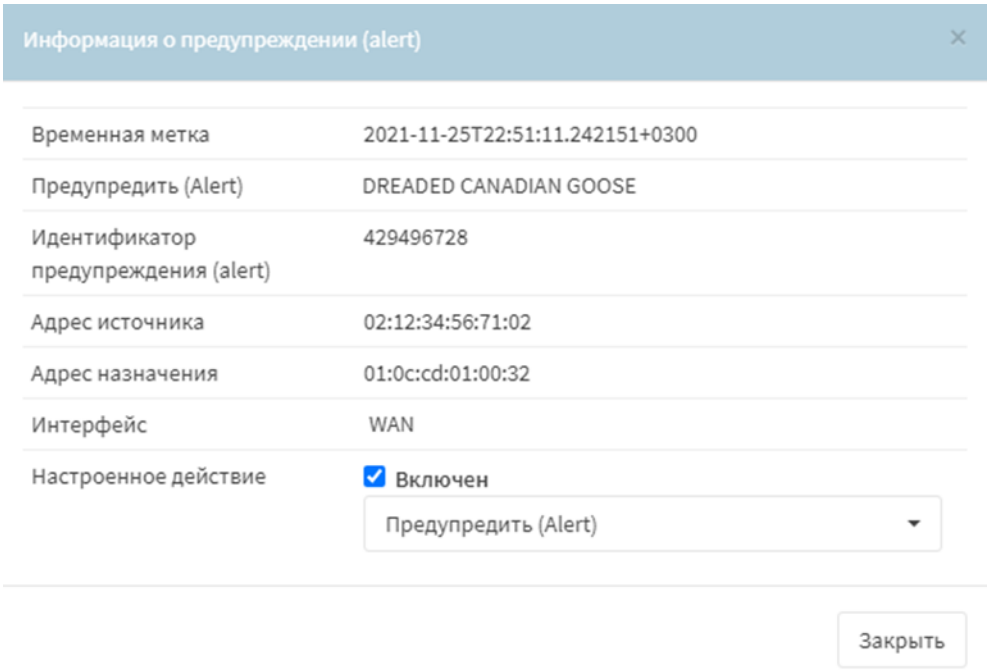

Рисунок 93 – Детальная информация. GOOSE

5.5.3.9 Шаблон протокола KRUG

При создании пользовательского правила на основе шаблона промышленного протокола KRUG необходимо задать параметры протокола, выбрав в поле **«Фильтровать на основе протокола»** опцию «Указать дополнительные параметры».

При выборе опции «Указать дополнительные параметры» появятся следующие поля:

- **«COMMAND»** – используется для передачи номера команды запроса от станции оператора, возможно указать число или диапазон чисел от «0» до «255»;
- **«CMD»** – используется для передачи номера команды запроса от станции инжиниринга, за исключением значения «23» – номера команды от станции оператора на запрос протокола событий, возможно указать число или диапазон чисел от «0» до «255»;
- **«PORT»** – используется для передачи номера устройства, для которого послан пакет, возможно указать число или диапазон чисел от «-32768» до «32767»;

- **«ACCESS»** – используется для передачи атрибута файла в запросах станции инжиниринга при работе с файловой системой, возможно указать число или диапазон чисел от «-32768» до «32767»;
- **«MODE»** – используется для передачи кода «тип переменной» в запросах/ответах от станции оператора, возможно указать число или диапазон чисел от «-32768» до «32767»;
- **«ERRCODE»** – используется для передачи кода ошибки в запросах/ответах от станции оператора, возможно указать число или диапазон чисел от «-32768» до «32767».

6 ОБНАРУЖЕНИЕ УСТРОЙСТВ

Обнаружение устройств в **ARMA IF** выполняется с помощью сервиса «ARPwatch», отслеживающим появление в сети новых устройств, подмену IP/MAC-адресов и обнаруживает атаки на сетевом уровне – «ARP-spoofing».

6.1 Общие настройки

Для настройки сервиса необходимо перейти в подраздел настроек обнаружения устройств (**«Сеть»** - **«Обнаружение устройств»** - **«Общие настройки»**), включить сервис и указать прослушиваемые интерфейсы (см. Рисунок 94).

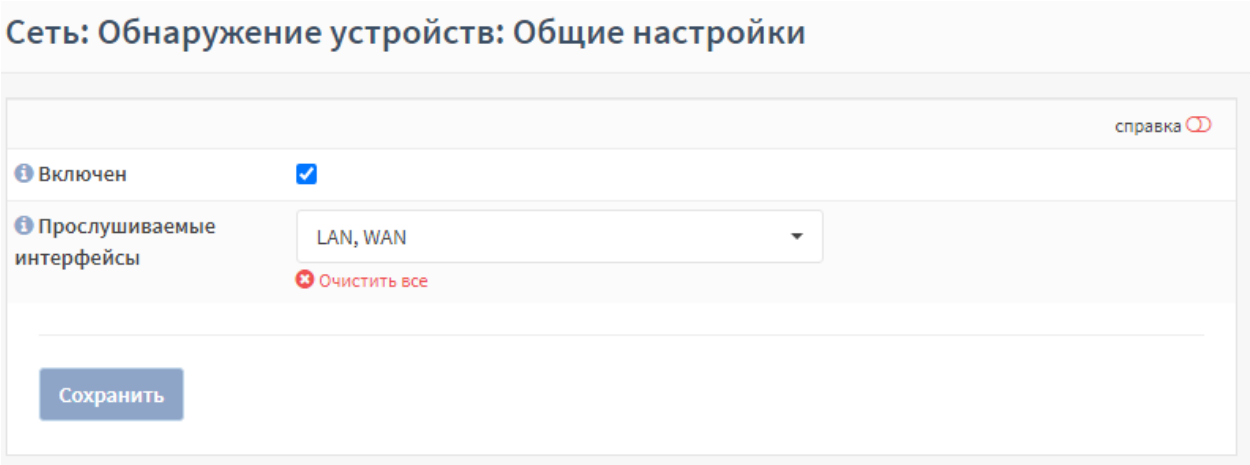

Рисунок 94 – Настройка сервиса «ARPwatch»

Запуск сервиса будет отображен в журнале syslog (**«Система»** - **«Журналы»** - **«Syslog»**) (см. Рисунок 96).

6.2 Список устройств

Информация об обнаруженных устройствах отображается в подразделе обнаруженных хостов (**«Сеть»** - **«Обнаружение устройств»** - **«Хосты»**) (см. Рисунок 95).

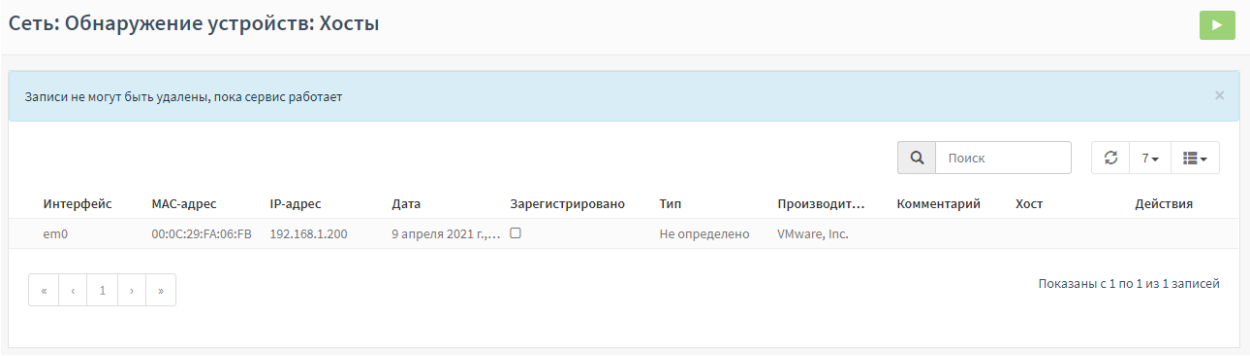

Рисунок 95 – Список подключенных устройств

Дополнительно записи об обнаружении устройств отображаются в журнале syslog (**«Система»** - **«Журналы»** - **«Syslog»**) и в журнале событий безопасности

(**«Система»** - **«Журналы»** - **«Журнал событий безопасности»**) (см. Рисунок 96 и Рисунок 97).

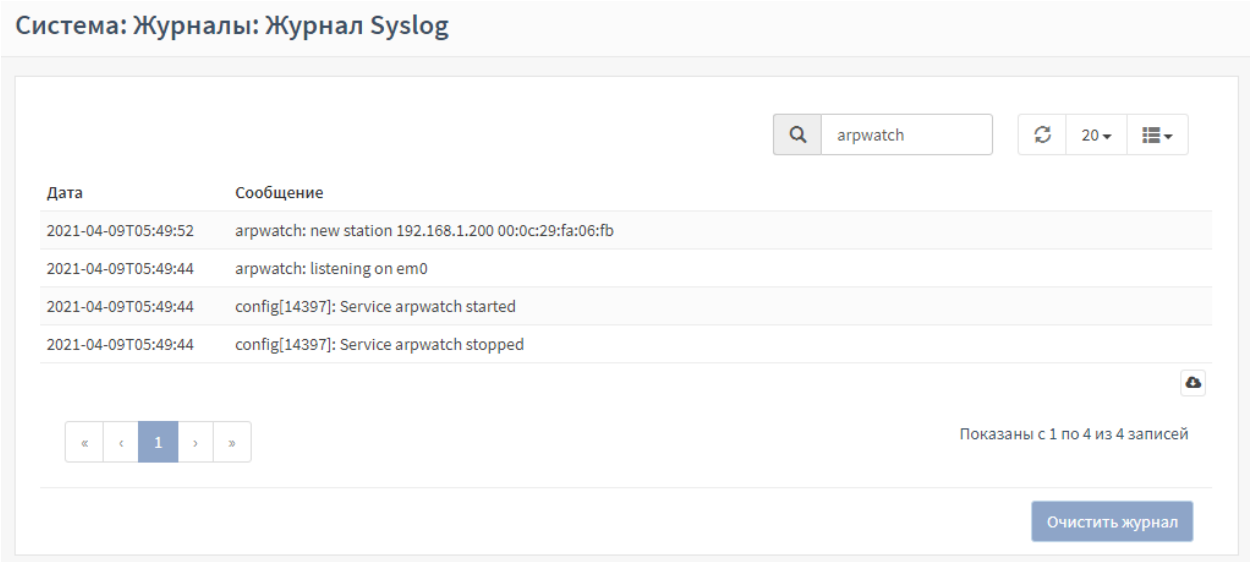

Рисунок 96 – Сообщения от сервиса «ARPwatch» в журнале syslog

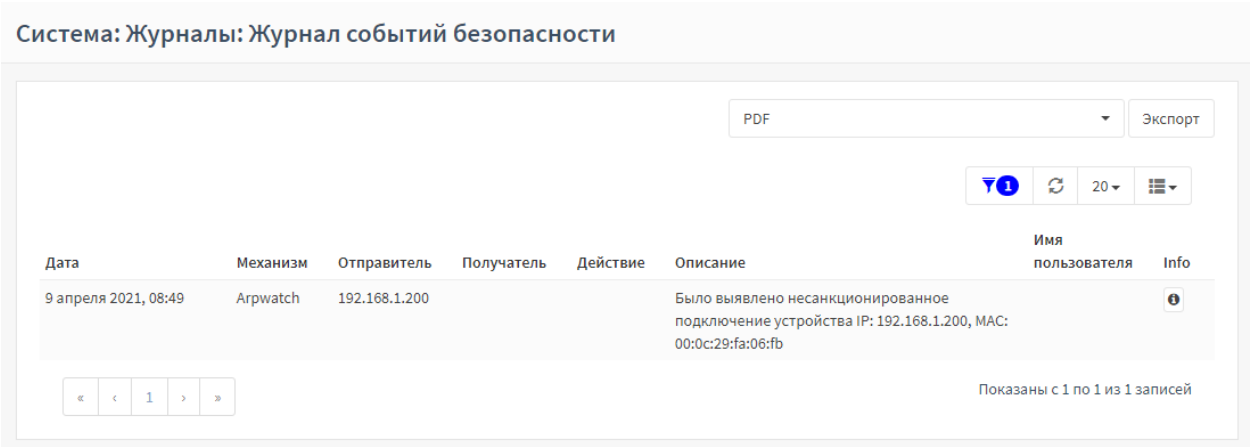

Рисунок 97 – Сообщения от сервиса «ARPwatch» в журнале событий безопасности

7 SNMP

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

В зависимости от выбранных опций мониторинг может выполняться для:

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

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

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

7.1 SNMP v.1,2

Настройка SNMP v.1,2 подразумевает аутентификацию на основе единой текстовой строки «Community String» – своеобразного пароля. Удаленная пользовательская программа SNMP и агент SNMP должны использовать одно и то же значение Community Strings.

7.1.1 Настройка SNMP v.1,2

Для настройки удаленного мониторинга по протоколам SNMP v.1,2 необходимо выполнить следующие действия:

1. Перейти в подраздел общих настроек SNMP (**«Система»** - **«Настройки»** - **«SNMP»** - **«Общие настройки»**) и установить флажок в параметре **«Включить»**.
2. Задать значение в параметре **«Общая строка SNMP»** и нажать **кнопку «Сохранить»** (см. Рисунок 98).

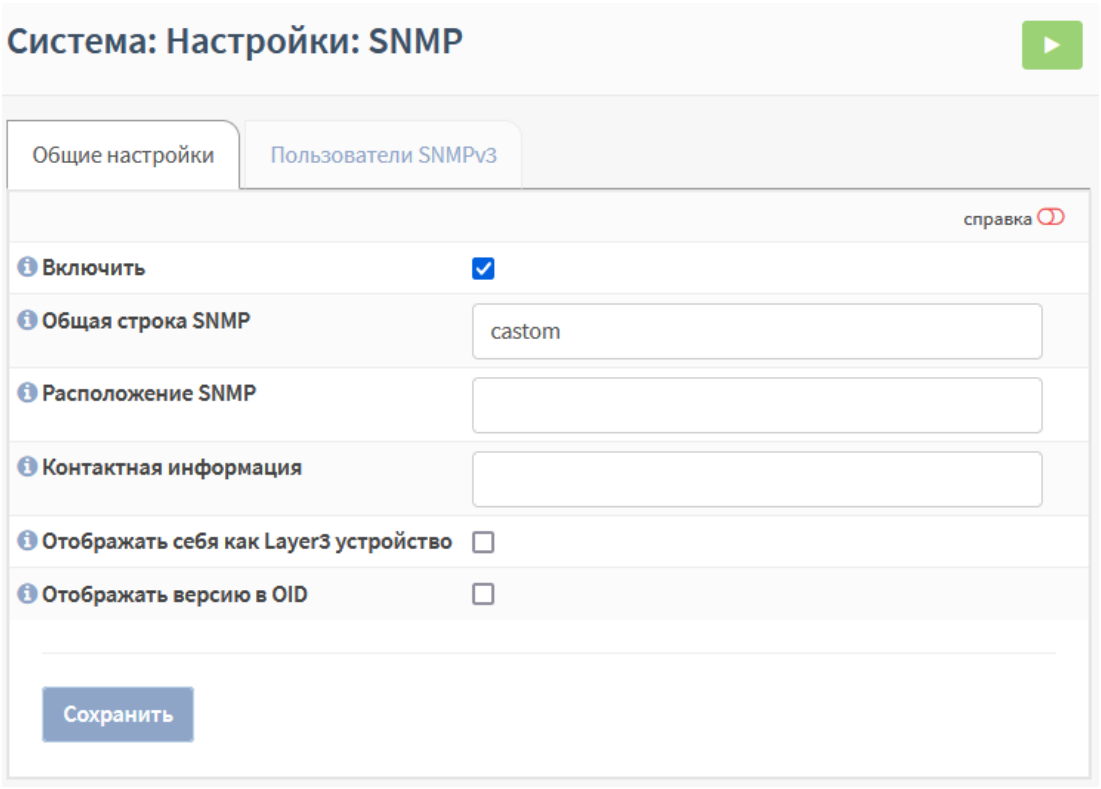

Рисунок 98 – Настройка SNMP v.1,2

Дополнительные параметры SNMP v.1,2

В качестве дополнительной информации возможно указать расположение **ARMA IF** и контактную информацию в полях **«Расположение SNMP»** и **«Контактная информация»** соответственно.

В случае установки флажка в параметре **«Отображать себя как Layer3 устройство»** устройство будет позиционировать себя, как устройство в сети на уровне L3, то есть устройство с IP-адресами на сетевом уровне модели OSI. По умолчанию **ARMA IF** работает в сети на уровне L2, то есть как устройство с MAC-адресом.

В случае установки флажка в параметре **«Отображать версию в OID»** будет передаваться OID устройства для идентификации поставщика данного устройства. Используется в случае, если по-другому получить информацию об установленной системе и других характеристиках устройства не получается через протокол SNMP.

7.1.2 Проверка работы SNMP v.1,2

Для проверки работы SNMP будет использоваться схема стенда, представленная на рисунке (см. Рисунок 99). На ПК **«Admin»** установлено ПО мониторинга «PowerSNMP Free Manager».

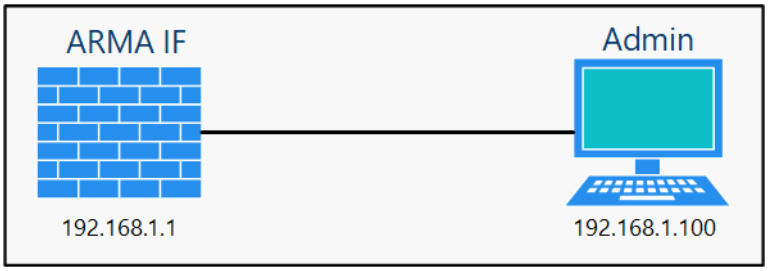

Рисунок 99 – Схема стенда для проверки SNMP

Для проверки работы SNMP v.1,2 необходимо выполнить следующие действия:

1. В ПО «PowerSNMP Free Manager» нажать **правой кнопкой мыши** на строку **«SNMP Agents»** и выбрать **«Add Agent»**.
2. В нижней части открывшегося окна нажать **кнопку «Add Agent»**, указать IP-адрес **ARMA IF**, в **«Community»** значение, указанное в настройках ранее (см. Раздел 7.1.1), выбрать версию протокола «1» или «2» и нажать **«OK»** (см. Рисунок 100).

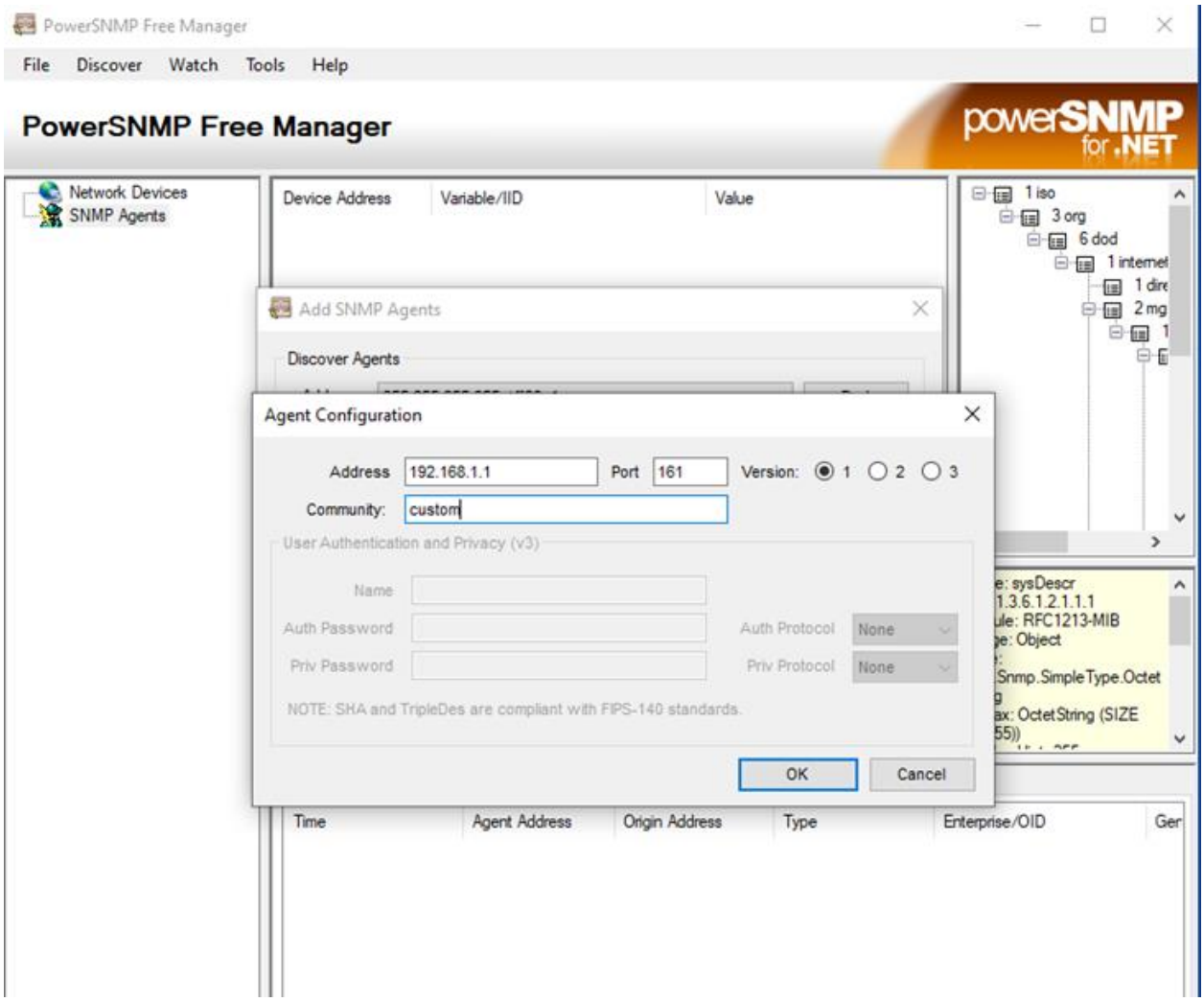

Рисунок 100 – Добавление SNMP агента, SNMP v.1,2

3. В правой области окна в дереве доступных данных выбрать поле **«1 sysDescr»**, нажать **правой кнопкой мыши** по IP-адресу **ARMA IF** и выбрать **«Query...»**. Результатом будет получение информации о значениях параметров **ARMA IF** (см. Рисунок 101).

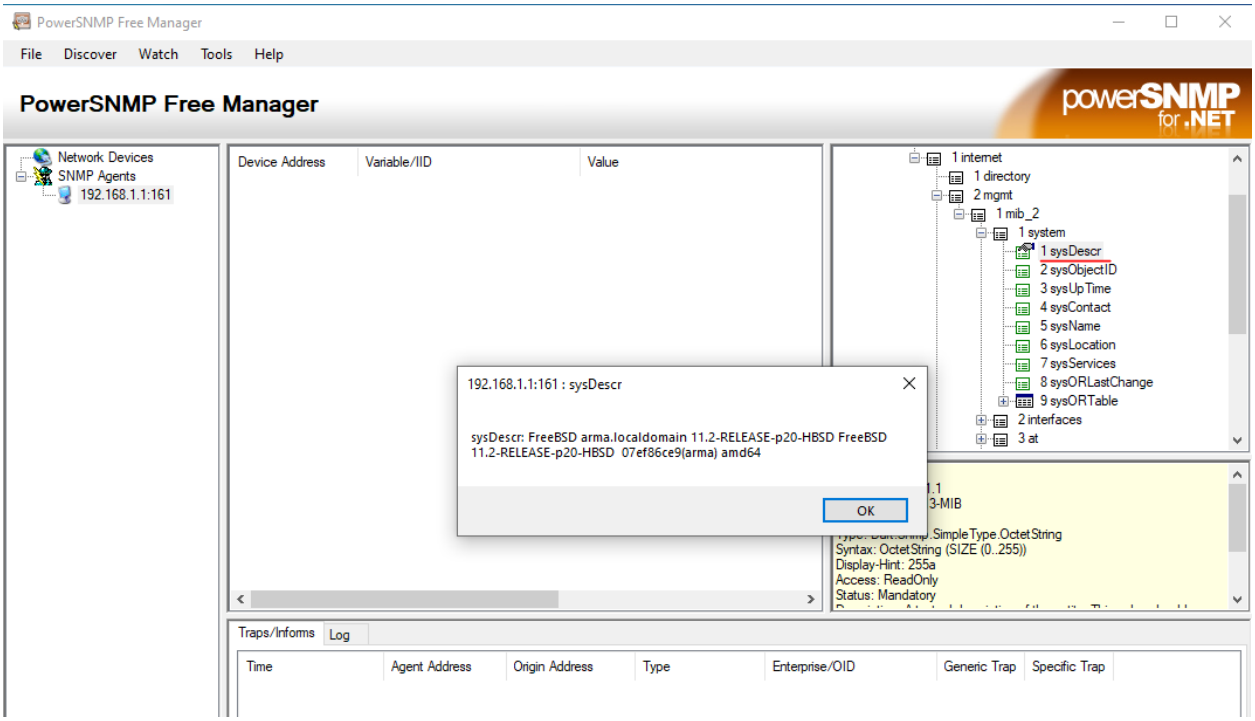

*Рисунок 101 – Информация о значениях параметров **ARMA IF***

7.2 SNMP v.3

Настройка SNMP v.3 подразумевает аутентификацию на основе имени пользователя и пароля, а также шифрование трафика.

7.2.1 Настройка SNMP v.3

Для настройки удаленного мониторинга по протоколу SNMP v.3 необходимо выполнить следующие действия:

1. Перейти в подраздел общих настроек SNMP (**«Система»** - **«Настройки»** - **«SNMP»** - **«Общие настройки»**) и установить флажок в параметре **«Включить»**.

2. Перейти во вкладку **«Пользователи SNMP v.3»** и нажать **кнопку «** **»**.

3. В открывшейся форме (см. Рисунок 102) заполнить поля **«Имя пользователя»**, **«Пароль»**, **«Ключ шифрования»** и нажать **кнопку «Сохранить»**. Для возможности редактирования дерева MIB, созданным пользователем, необходимо установить флажок для параметра **«Разрешить запись»**. Параметры **«Алгоритм хеша»** и **«Тип шифрования»** меняются при необходимости.

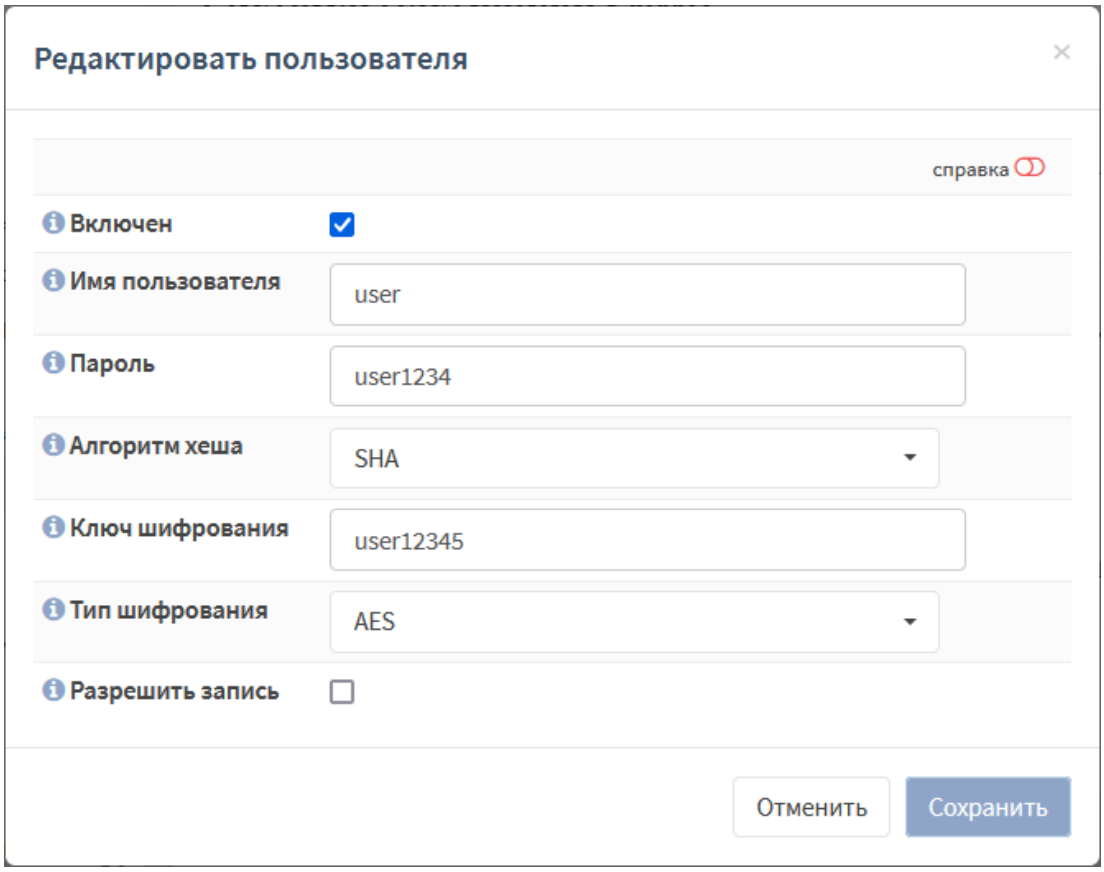

Рисунок 102 – Добавление пользователя SNMP v.3

!Важно Пароль и ключ шифрования должен содержать от 8 до 64 символов. Допустимые символы:

- 0-9a-zA-Z._-!$%/()+#=

7.2.2 Проверка работы SNMP v.3

Для проверки работы SNMP будет использоваться схема стенда, представленная на рисунке (см. Рисунок 99). На ПК **«Admin»** установлено ПО мониторинга «PowerSNMP Free Manager».

Для проверки работы SNMP v.3 необходимо выполнить следующие действия:

1. В ПО «PowerSNMP Free Manager» нажать **правой кнопкой мыши** на строку **«SNMP Agents»** и выбрать **«Add Agent»**.
2. В нижней части открывшегося окна нажать **кнопку «Add Agent»**, указать IP-адрес **ARMA IF**, указать данные для аутентификации, заданные в настройках ранее (см. Раздел 7.2.1), выбрать версию протокола «3» и нажать **«OK»** (см. Рисунок 103).

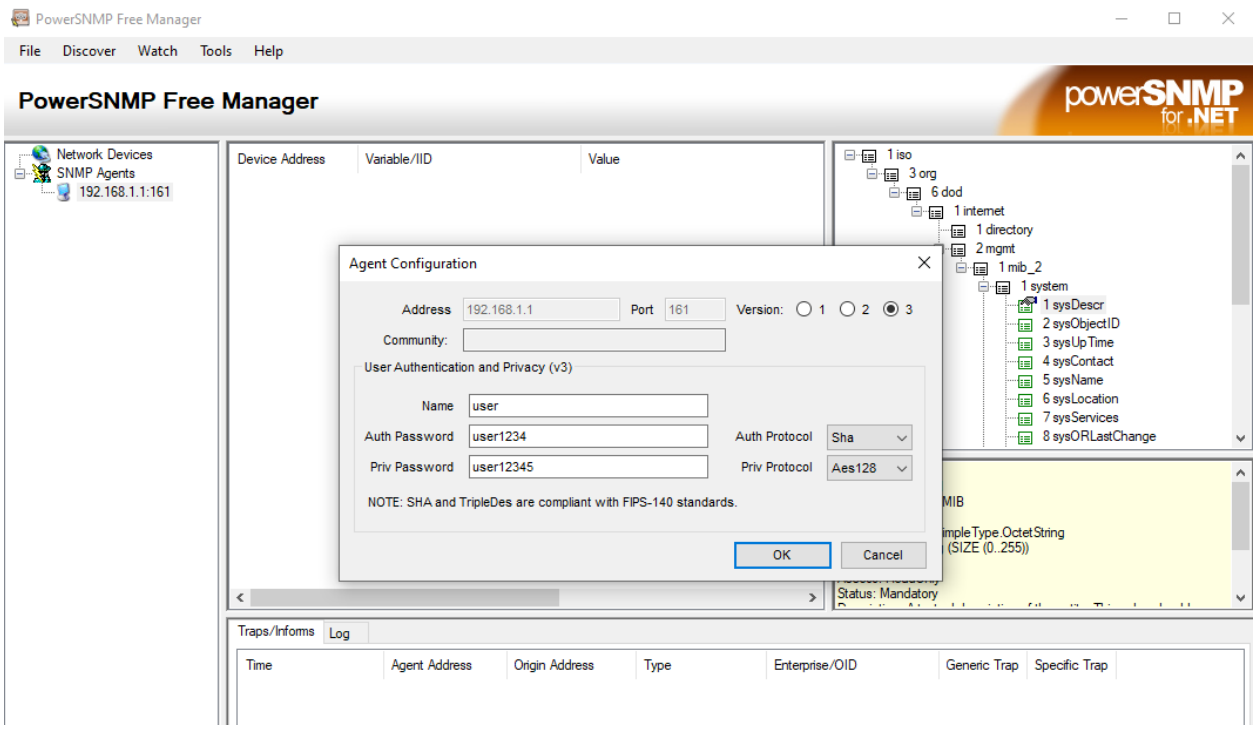

Рисунок 103 – Добавление SNMP агента (SNMP v.3)

3. В правой области окна в дереве доступных данных выбрать поле **«1 sysDescr»**, нажать **правой кнопкой мыши** по IP-адресу **ARMA IF** и выбрать **«Query…»**. Результатом будет получение информации о значениях параметров **ARMA IF**.

8 СЕРВИС SYSLOG

Syslog – это стандарт отправки и регистрации сообщений о происходящих в системе событиях, используемый для удобства администрирования и обеспечения ИБ.

ARMA IF позволяет отправлять события безопасности модулей МЭ, СОВ, контроля уровня приложений, портала авторизации пользователей, а также системные события на внешний syslog-сервер или в SIEM-системы, а также в единый центр управления **ARMA MC**. Взаимодействие с **ARMA MC** возможно только при включенном протоколе HTPPS на **ARMA IF**.

8.1 Настройка экспорта событий syslog

Для настройки экспорта событий необходимо выполнить следующие действия:

1. Перейти в настройки экспорта событий системы (**«Система»** - **«Настройки»** - **«Экспорт событий»**) и, во вкладке **«Получатели»,** нажать **кнопку «** **»**.
2. В открывшейся форме (см. Рисунок 104) установить флажок для параметра **«Включен»**.

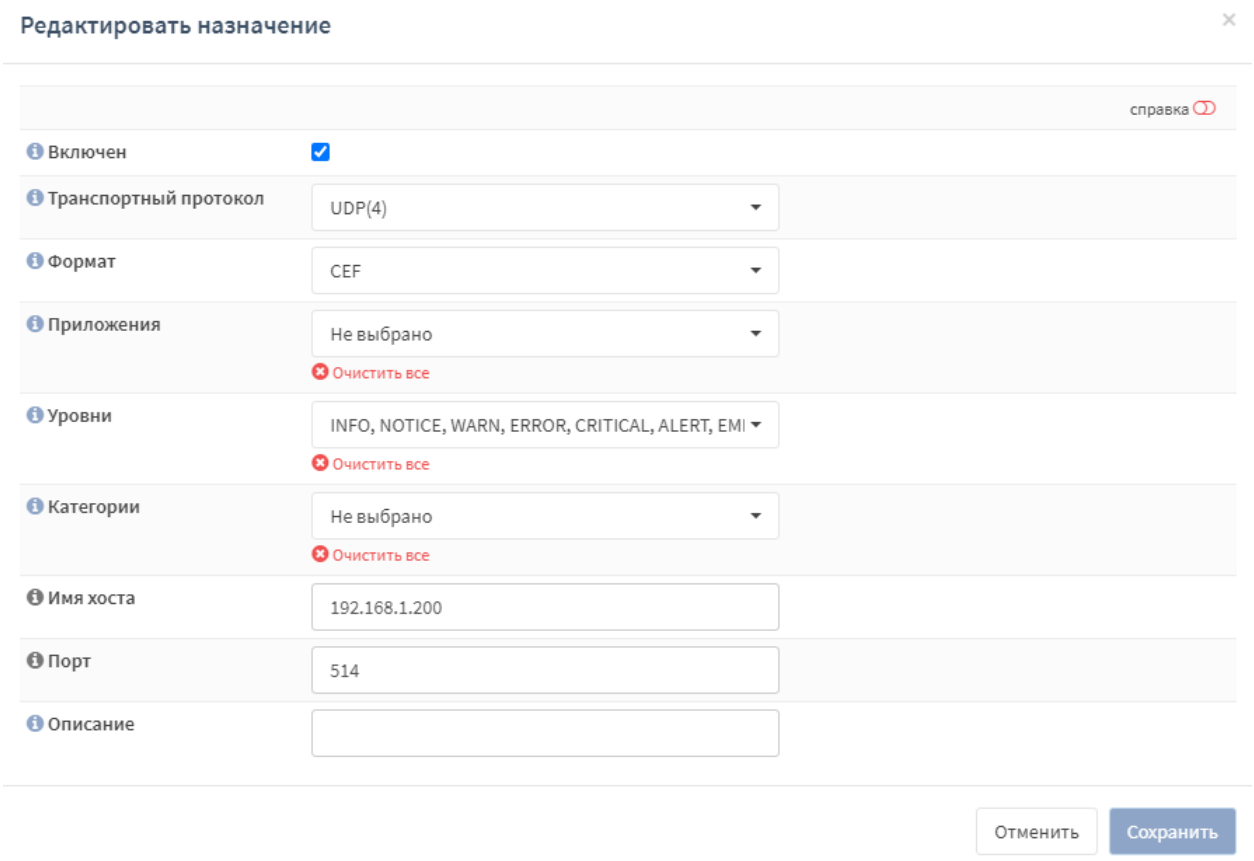

Рисунок 104 – Добавление получателя внешнего syslog-сервера

3. Выбрать значения параметров:
   - **«Формат»**;

- **«Транспортный протокол»**;
- **«Приложения»**;
- **«Уровни»**;
- **«Категории»**.

В параметрах **«Приложения»**, **«Уровни»** и **«Категории»** значение «Не выбрано» означает выбор всех значений.

4. Задать доменное имя и порт удаленного syslog-сервера в параметрах **«Имя хоста»** и **«Порт»** соответственно. Номер порта рекомендуется изменять только в тех случаях, когда отправка сообщений от **ARMA IF** будет происходить через порт, заданный в настройках удаленного syslog-сервера и отличный от стандартного 514.
5. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

8.2 Проверка экспорта событий syslog

Для проверки работы экспорта событий необходимо выполнить подключение к syslog-серверу и удостовериться в наличии событий от **ARMA IF**. В качестве syslog-сервера возможно использовать стороннее ПО, например, «Visual Syslog», в примере ниже будет описано подключение к продукту **ARMA MC**.

Настройка экспорта событий в единый центр управления **ARMA MC** описана в руководстве пользователя по эксплуатации **ARMA MC**. События от **ARMA IF** отображаются в журнале событий **ARMA MC** (**«Журналы»** - **«События»**) (см. Рисунок 105).

В **ARMA IF** просмотр информации о переданных сообщениях осуществляется во вкладке **«Статические данные»** подраздела настройки экспорта событий (**«Система»** - **«Настройки»** - **«Экспорт событий»**) (см. Рисунок 106).

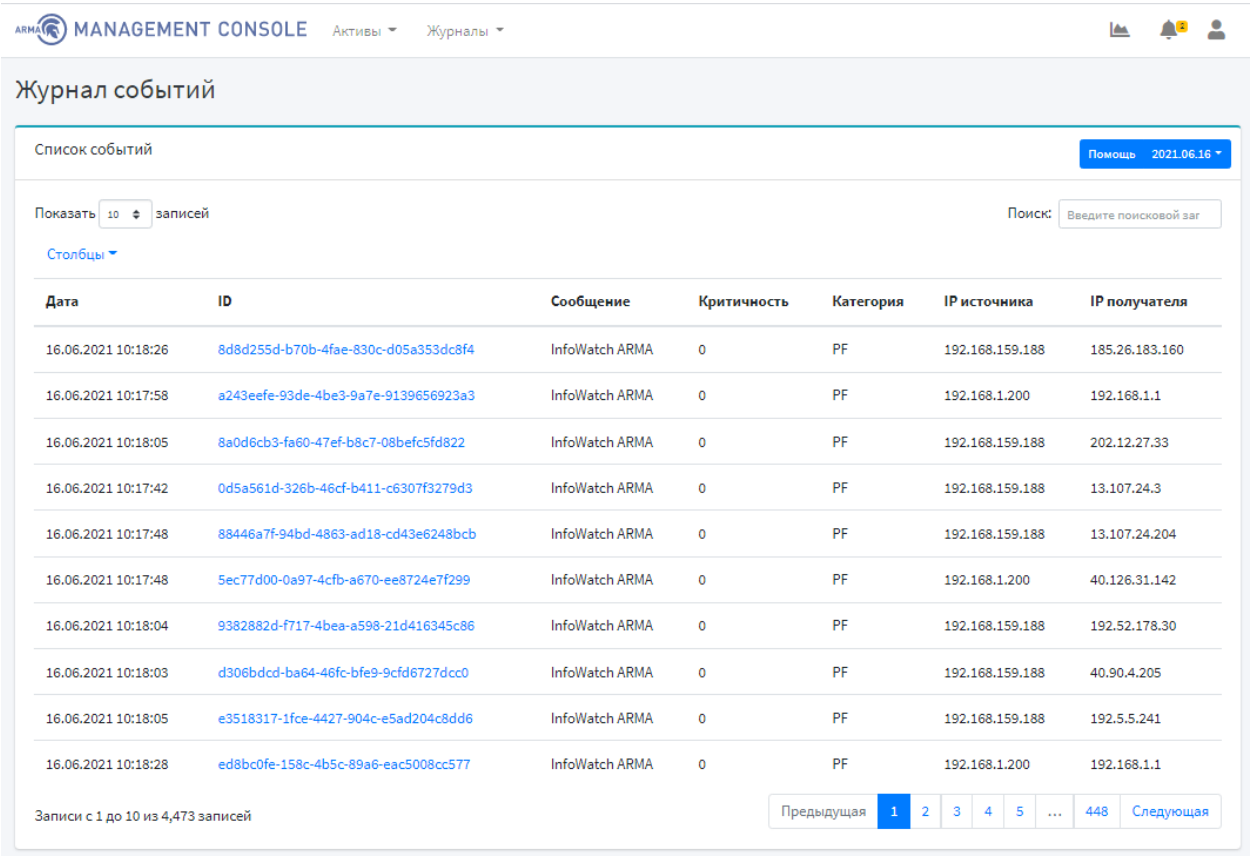

Рисунок 105 – Журнал событий ARMA Management Console

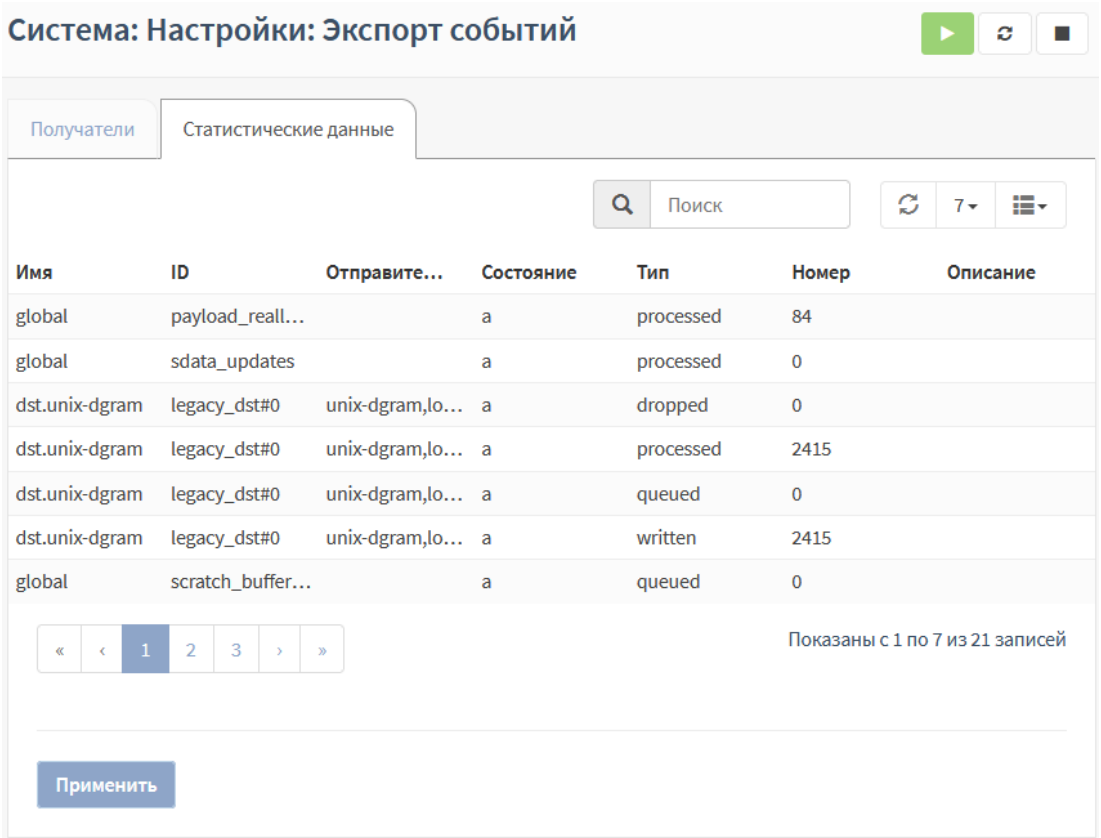

Рисунок 106 – Система: Настройки: Экспорт событий: Статистические данные

9 SSH-СЕРВЕР

Сервер SSH обеспечивает безопасный удаленный доступ к управлению функциями локального, консольного интерфейса **ARMA IF**. По умолчанию используется порт 22.

Для подключения по протоколу SSH к **ARMA IF** возможно использовать различные SSH-клиенты, например:

- «OpenSSH» для UNIX-подобных ОС;
- «PuTTY» или «SecureCRT» для ОС Windows и Linux.

Для включения доступа по протоколу SSH необходимо перейти в подраздел настроек администрирования системы (**«Система»** - **«Настройки»** - **«Администрирование»**), в блоке настроек SSH установить флажок для параметра **«Включить безопасный shell»** (см. Рисунок 107), при необходимости задать параметры доступа (см. Раздел 9.1) и нажать **кнопку «Сохранить»** внизу страницы.

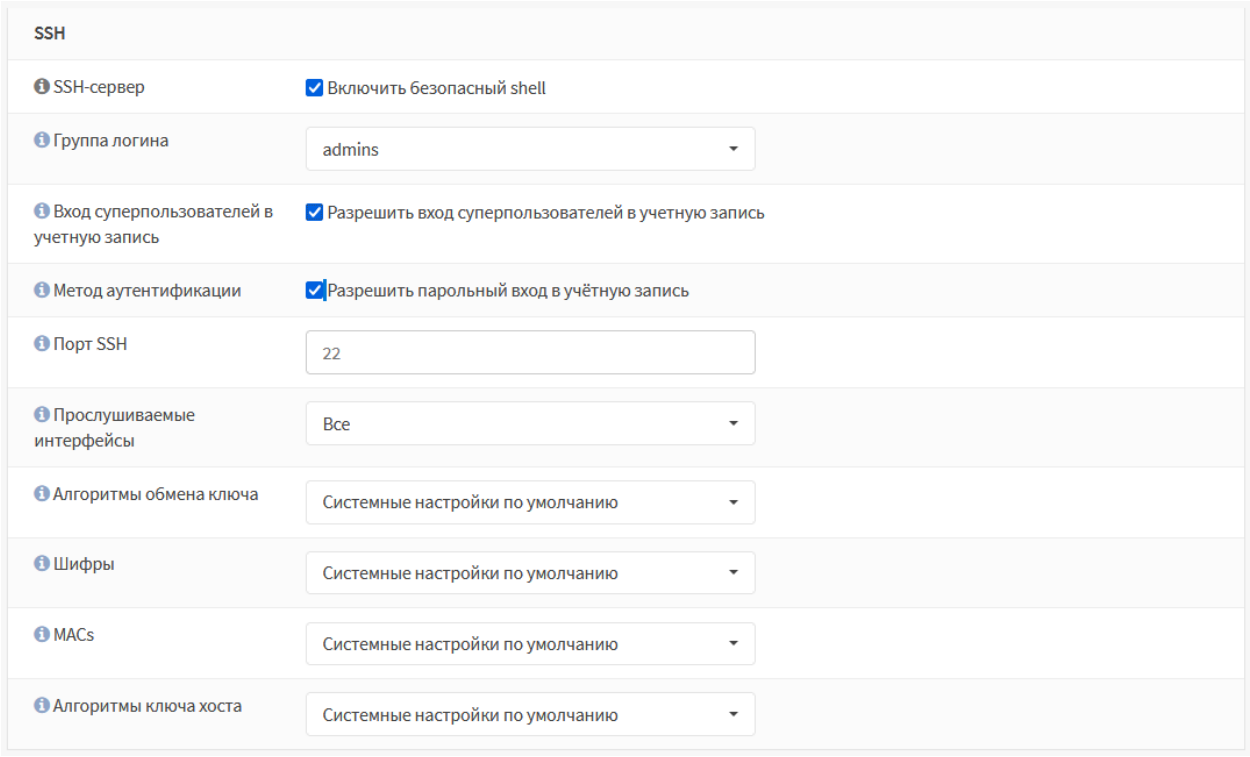

Рисунок 107 – Включение SSH-сервера

!Важно Для возможности доступа должно быть создано разрешающее правило МЭ (см. Раздел 1.1.1) для заданного порта.

9.1 Параметры доступа SSH

В параметре **«Группа логина»** указывается группа пользователей, члены которой будут иметь доступ по протоколу SSH. Предоставление прав доступа по SSH отдельному пользователю описано в разделе 21.1 настоящего документа.

При включенном значении «Разрешить вход суперпользователей в учетную запись» параметра **«Вход суперпользователей в учетную запись»** будет разрешен доступ с УЗ «root», рекомендуется не включать данное значение в целях безопасности.

При включенном значении «Разрешите парольный вход в учетную запись» для параметра **«Метод аутентификации»** будет задан метод аутентификации по паролю. При выключенном значении «Разрешите парольный вход в учетную запись» будет задан метод аутентификации по авторизированным ключам для каждого отдельного пользователя, которому предоставлен доступ по протоколу SSH. Генерация ключей в таком случае будет выполняться сторонним ПО.

Например, в случае использования для подключения ПО «PuTTY», генерация ключей возможно выполнить с помощью ПО «PuTTYgen», по умолчанию устанавливаемым вместе с ПО «PuTTY». При генерации ключей будет создана пара ключей:

- **«Public key, открытый ключ»** – хранится в памяти приложения;
- **«Private key, закрытый ключ»** – необходимо указать в настройках определенного пользователя **ARMA IF** в поле параметра **«Авторизованные ключи»** формы редактирования УЗ (**«Система»** - **«Доступ»** - **«Пользователи»**) (см. Раздел 21.1).

В параметре **«Прослушиваемые интерфейсы»** рекомендуется оставлять только внутренние интерфейсы.

Дополнительные параметры шифрования:

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

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

Настройка SSH-сервера считается успешной, в случае доступа к консольному интерфейсу **ARMA IF** после подключения (см. Рисунок 108).

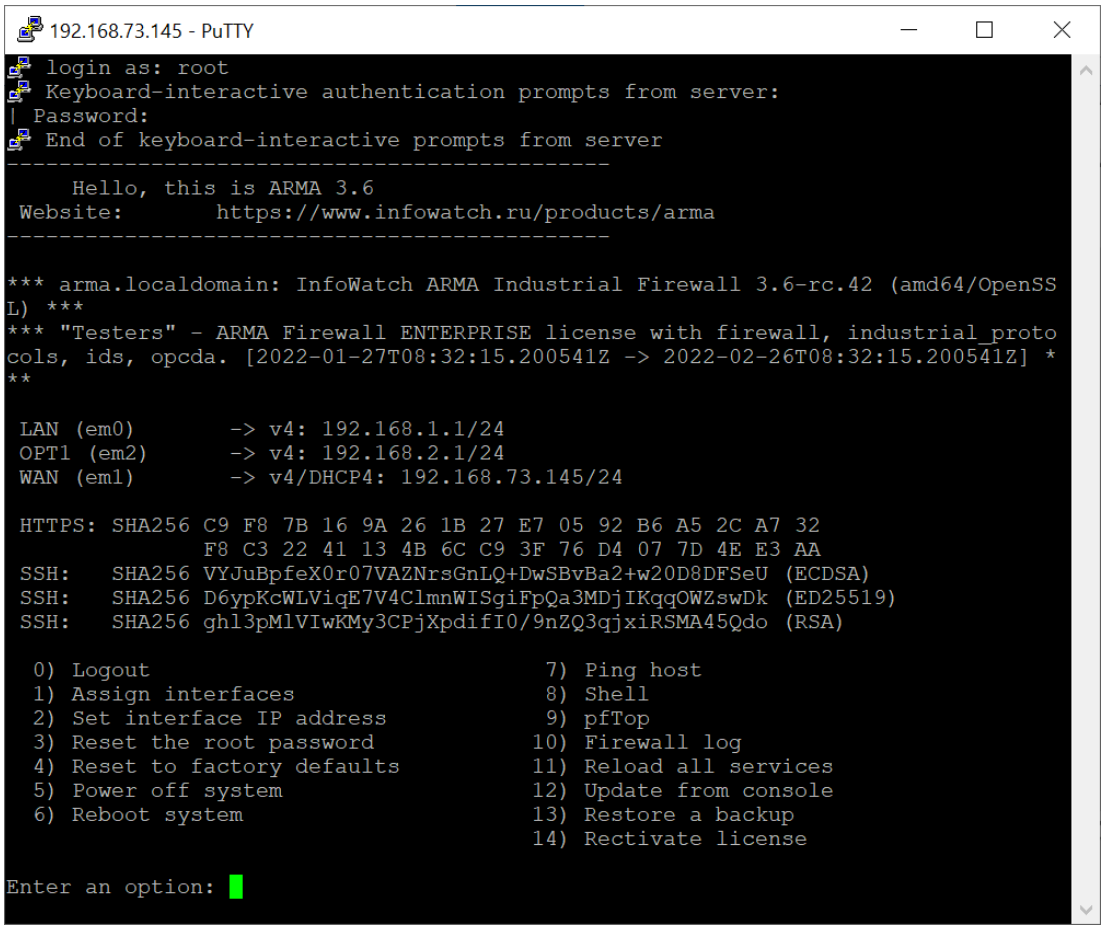

Рисунок 108 – Доступ к консольному интерфейсу по протоколу SSH

10 СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Статическая маршрутизация – это запись маршрутизации, настроенная вручную, без применения протоколов маршрутизации. После установки статического маршрута пакет для заданного назначения будет перенаправлен на путь, указанный ранее. Данный тип маршрутизации применяется при взаимодействии сети с одной или двумя другими сетями.

Статические маршруты используются в случае, когда узлы или сети доступны через маршрутизатор, отличный от шлюза по умолчанию. Маршрутизаторы, через которые осуществляется доступ к другим сетям, предварительно необходимо добавить в качестве шлюзов.

10.1 Настройка шлюзов

Для добавления и настройки шлюза необходимо перейти в подраздел настройки единичных шлюзов (**«Система»** - **«Шлюзы»** - **«Единичный»**), нажать **кнопку «+Добавить»**, в открывшейся форме (см. Рисунок 109) задать параметры шлюза, нажать **кнопку «Сохранить»** и нажать **кнопку «Применить изменения»**.

Параметры **«Имя»**, **«Интерфейс»**, **«Семейство адресов»** и **«IP-адрес»** являются необходимыми для заполнения.

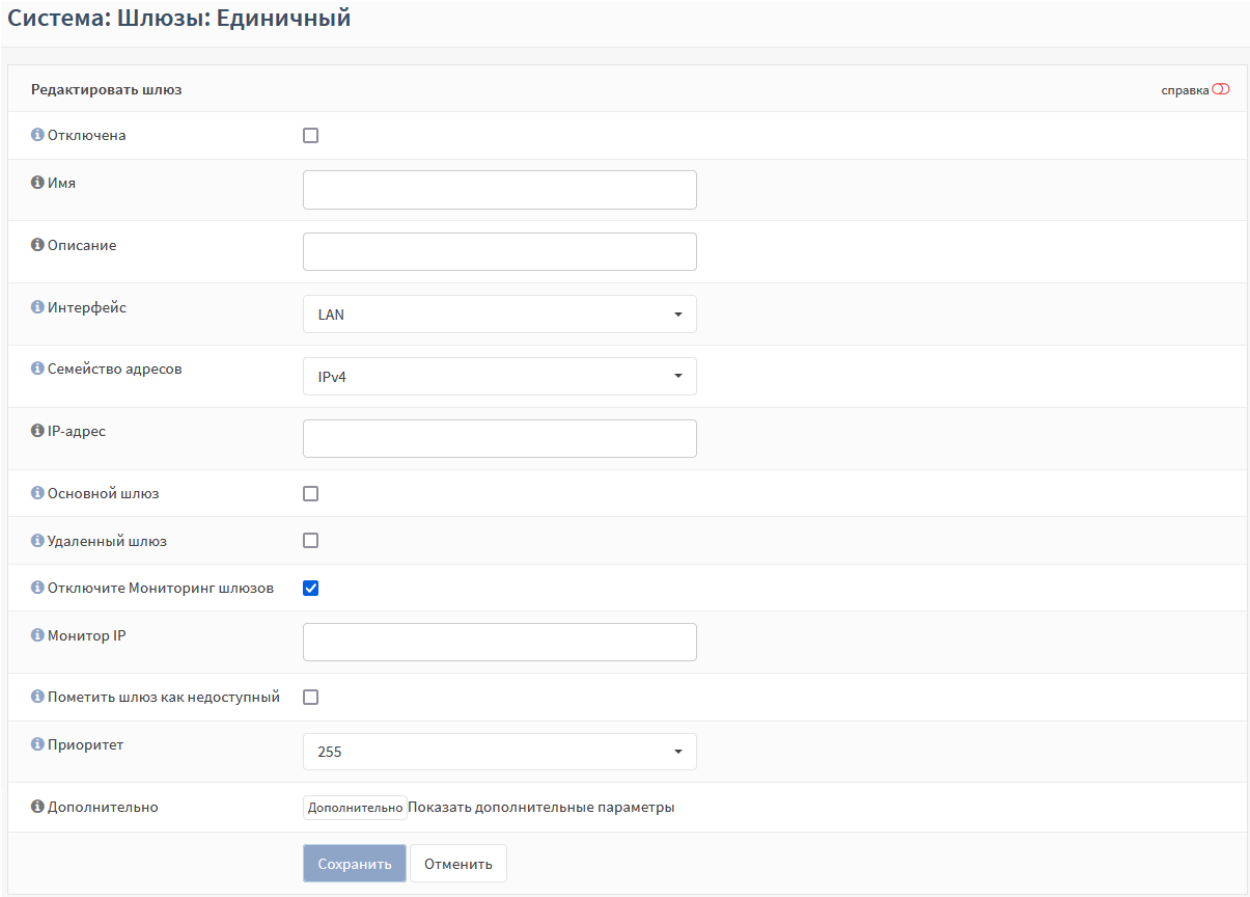

Рисунок 109 – Настройки шлюза

Для указания шлюза по умолчанию необходимо установить флажок для параметра **«Основной шлюз»**.

Для разрешения существовать шлюзу за пределами подсети интерфейса необходимо установив флажок для параметра **«Удаленный шлюз»**.

По умолчанию демон мониторинга шлюза периодически проверяет связь с каждым шлюзом, чтобы отслеживать задержку и потерю пакетов для трафика на отслеживаемый IP-адрес. Эти данные используются для информации о состоянии шлюза, а также для построения графика RRD.

Для отключения мониторинга необходимо установить флажок в **«Отключить мониторинг шлюзов»**. Мониторинг используется для отслеживания задержки и потери пакетов трафика для отслеживаемого IP-адреса. Данные используются для получения статуса состояния шлюза и построения графика RRD.

В случае необходимости настройки Multi-WAN – нескольких WAN, доступ к расширенным параметрам возможно получить нажав **кнопку «Дополнительно»** (см. Рисунок 110).

!Важно В большинстве случаев эти параметры не подлежат изменению.

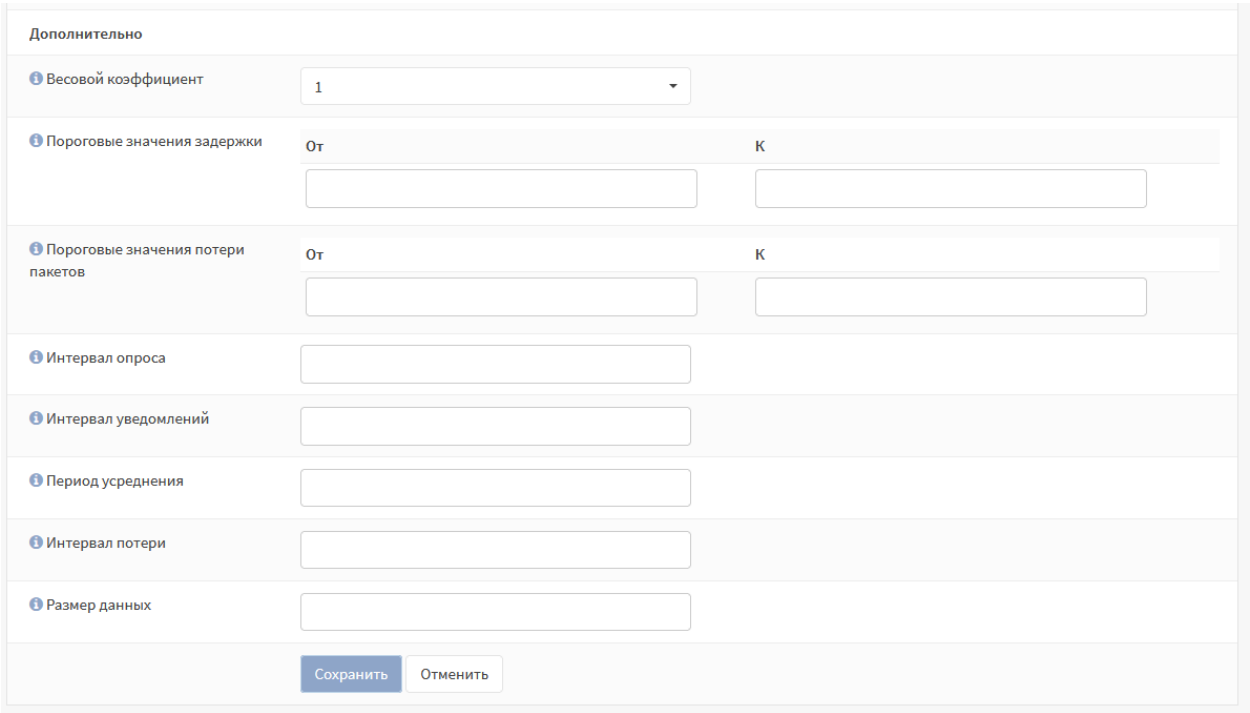

Рисунок 110 – Расширенные параметры настройки шлюза

Для обеспечения балансировки нагрузки, аварийного переключения или маршрутизации, основанной на правилах, в **ARMA IF** предусмотрена возможность добавления группы шлюзов.

Для добавления и настройки группы шлюзов необходимо перейти в подраздел настройки группы шлюзов (**«Система»** - **«Шлюзы»** - **«Группы»**), нажать **кнопку**

«+Добавить», в открывшейся форме (см. Рисунок 111) задать параметры группы шлюзов и нажать **кнопку «Сохранить»**.

Параметры **«Имя группы»** и **«Приоритет шлюзов»** являются необходимыми для заполнения

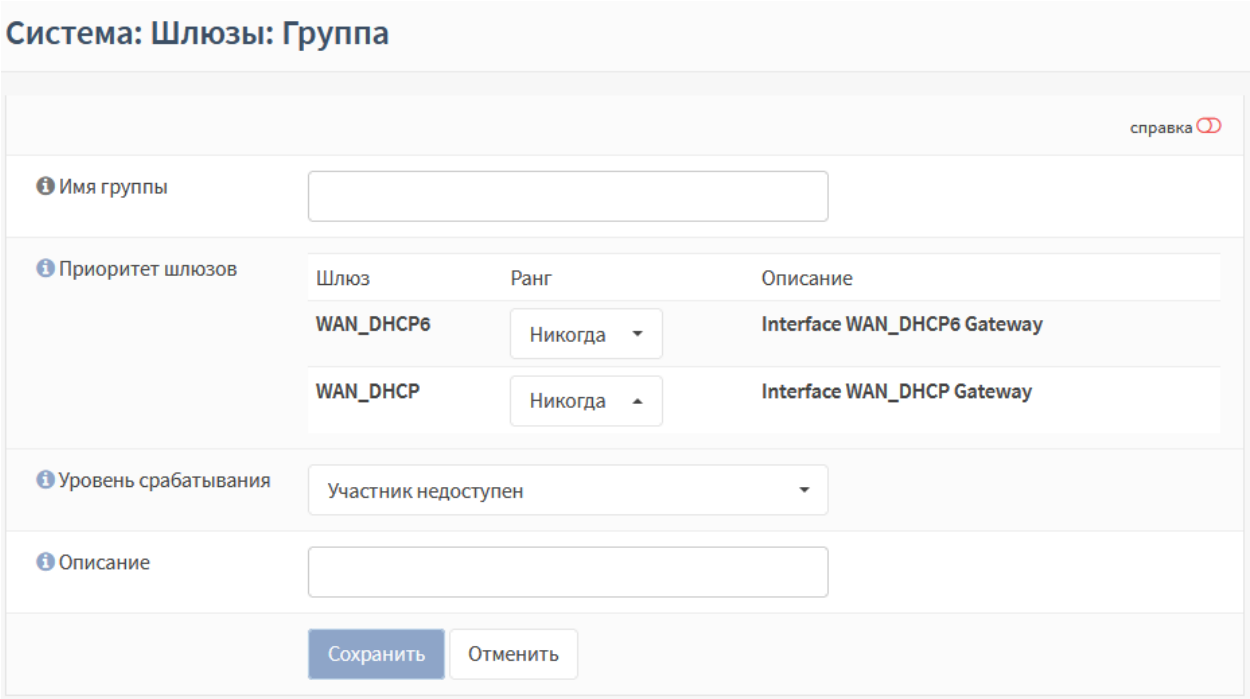

Рисунок 111 – Добавление группы шлюзов

В блоке **«Приоритет шлюзов»** необходимо выбрать шлюзы, входящие в создаваемую группу, и определить для них уровень приоритета в столбце **«Ранг»**: от «1» до «5». Для исключения шлюза из создаваемой группы необходимо выбрать значение уровня приоритета «Никогда».

!Важно Более низкие значения имеют более высокий приоритет. Например, шлюзы уровня **«Ранг 1»** используются перед шлюзами уровня **«Ранг 2»** и т.д.

Параметр **«Уровень срабатывания»** отвечает за то, как **ARMA IF** будет управлять записями группы шлюзов при возникновении определенных событий. Доступны следующие уровни:

- **«Участник недоступен»** – помечает шлюз как неработающий только тогда, когда он полностью отключен, превышая один или оба более высоких пороговых значения, настроенных для шлюза;
- **«Потеря пакетов»** – помечает шлюз как неработающий, когда потеря пакетов превышает нижний порог оповещения;
- **«Высокая задержка»** – помечает шлюз как неработающий, когда задержка превышает нижний порог оповещения;

- **«Потеря пакетов или высокая задержка»** – помечает шлюз как неработающий для любого типа предупреждений.

10.2 Настройка статических маршрутов

Конфигурация статического маршрута осуществляется в подразделе настройки маршрутизации (**«Система»** - **«Маршруты»** - **«Конфигурация»**).

Для добавления маршрута необходимо нажать **кнопку «+»**, указать адрес сети конечной точки маршрута и шлюз (см. Рисунок 112), при необходимости добавить описание маршрута, нажать **кнопку «Сохранить»** и нажать **кнопку «Применить»**.

Адрес сети задаётся в формате CIDR:

- [адрес сети]/[маска сети], например, «192.168.1.0/24»

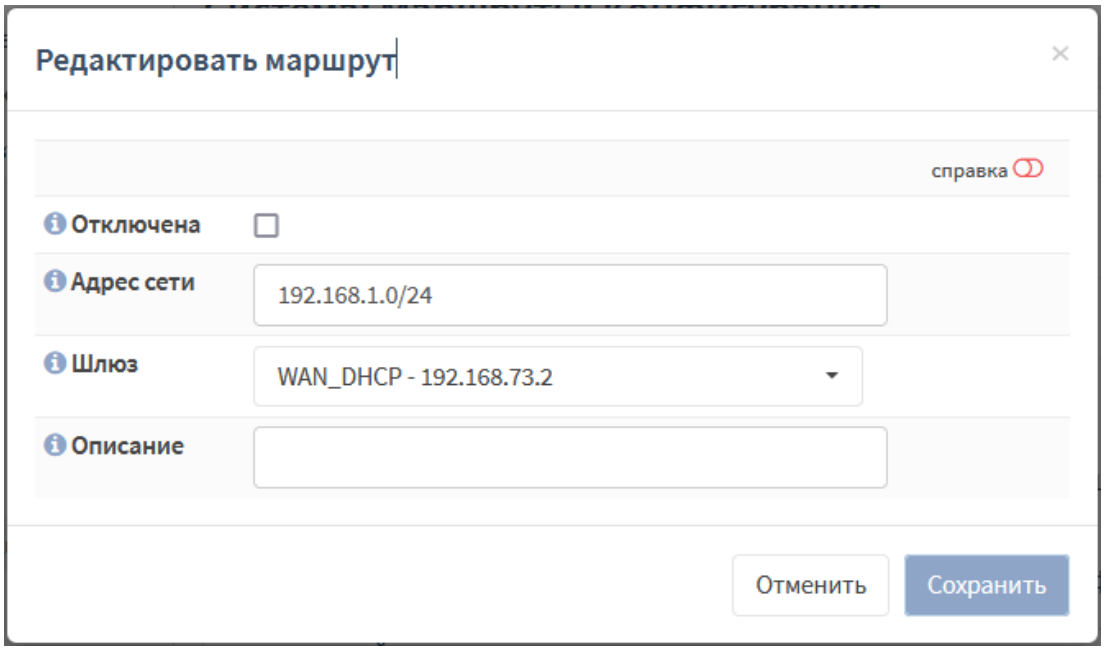

Рисунок 112 – Настройка конфигурации статического маршрута

10.2.1 Пример реализации статического маршрута

В качестве примера работы статического маршрута будет использоваться схема стенда, представленная на рисунке (см. Рисунок 113). Необходимо добиться прохождения трафика от ПК **«Server»** до ПК **«Client»**. На каждом **ARMA IF** предварительно должно быть создано правило МЭ (см. Раздел 1.1.1) для интерфейса **«[WAN]»**, разрешающее прохождение трафика по протоколу ICMP.

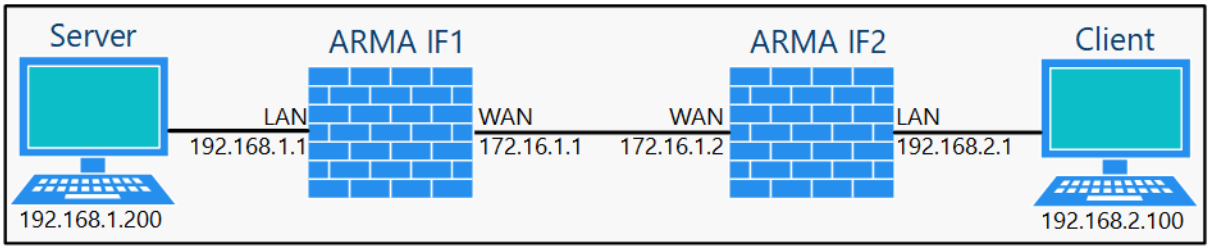

Рисунок 113 – Схема стенда для настройки статического маршрута

Для реализации прохождения трафика необходимо выполнить следующие действия:

1. Добавить на каждом **ARMA IF** единичный шлюз.
2. Добавить на каждом **ARMA IF** статические маршруты.

Для каждого **ARMA IF** необходимо добавить единичный шлюз (см. Раздел 10.1) с параметрами, указанными в таблице (см. Таблица 20).

Таблица 20

Значения параметров единичных шлюзов

Параметр	ARMA IF1	ARMA IF2
Имя	GW_AIF1	GW_AIF2
Интерфейс	WAN	WAN
Семейство адресов	IPv4	IPv4
IP-адрес	172.16.1.2	172.16.1.1

Для связи сетей «192.168.1.0/24» и «192.168.2.0/24» необходимо добавить статические маршруты (см. Раздел 10.2) с параметрами, указанными в таблице (см. Таблица 21).

Таблица 21

Значения параметров статических маршрутов

Параметр	ARMA IF1	ARMA IF2
Адрес сети	192.168.2.0/24	192.168.1.0/24
Шлюз	GW_AIF1 - 172.16.1.2	GW_AIF2 - 172.16.1.1

Для проверки работы статического маршрута необходимо на ПК **«Server»** запустить командную строку и выполнить команду трассировки до ПК **«Client»**. Успешным результатом выполнения команды является отображение маршрута трафика (см. Рисунок 114).

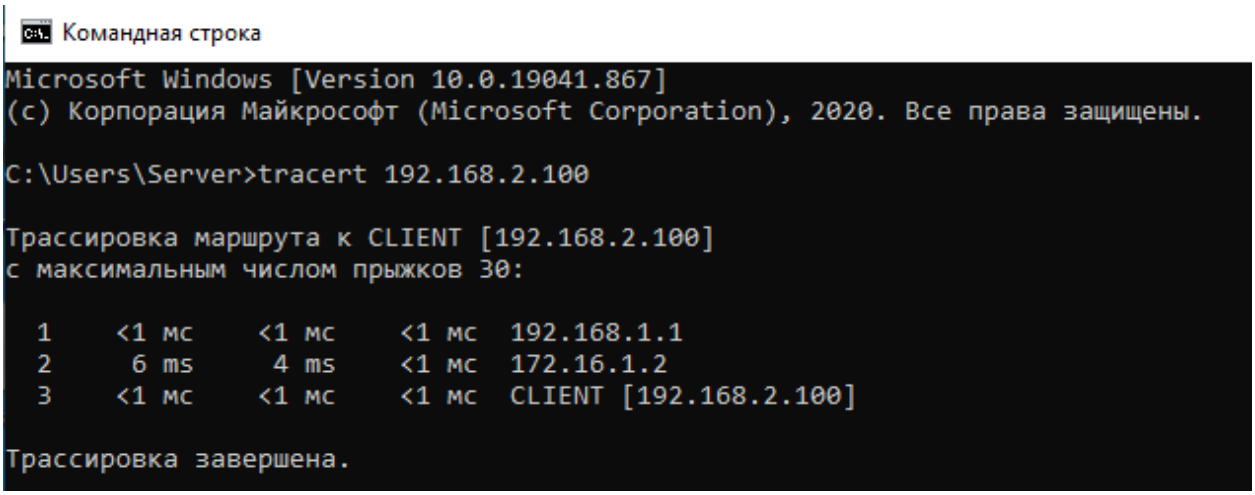

Рисунок 114 – Трассировка маршрута

11 ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ

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

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

11.1 RIP

Данный протокол применяется в небольших компьютерных сетях и позволяет маршрутизаторам динамически обновлять маршрутную информацию, получая ее от соседних маршрутизаторов.

11.1.1 Настройка динамической маршрутизации RIP

В качестве примера приведена настройка динамической маршрутизации на трех **ARMA IF** согласно схеме стенда, представленного на рисунке (см. Рисунок 115).

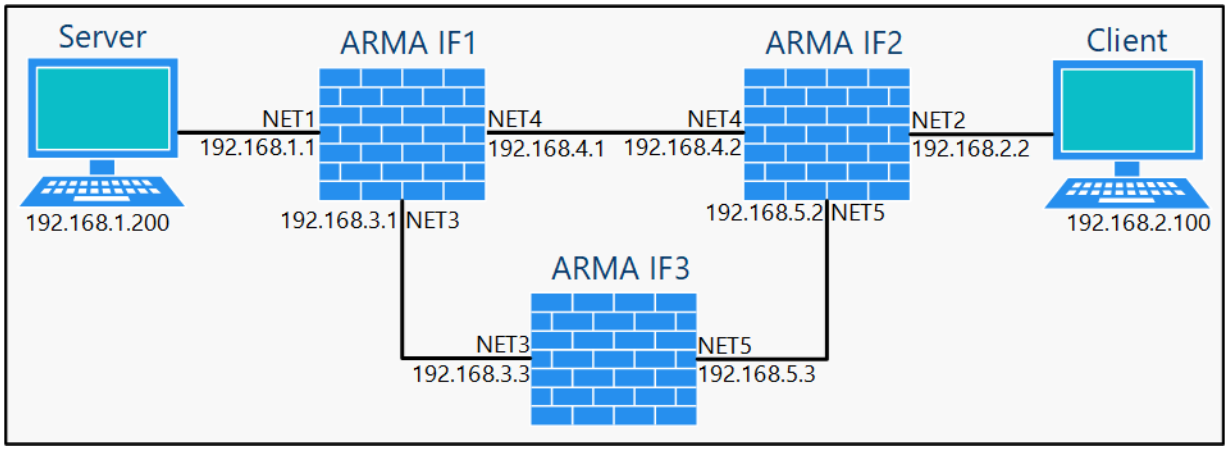

Рисунок 115 – Схема стенда для настройки динамической маршрутизации

Перечень интерфейсов со значениями IP-адресов для каждого **ARMA IF** приведен в таблице (см. Таблица 22).

Таблица 22
Перечень интерфейсов

Интерфейс	ARMA IF1	ARMA IF2	ARMA IF3
NET1	192.168.1.1/24	-	-
NET2	-	192.168.2.2/24	-
NET3	192.168.3.1/24	-	192.168.3.3/24
NET4	192.168.4.1/24	192.168.4.2/24	-

Интерфейс	ARMA IF1	ARMA IF2	ARMA IF3
NET5	-	192.168.5.2/24	192.168.5.3/24

На каждом **ARMA IF** предварительно необходимо создать разрешающее правило МЭ (см. Раздел 1.1.1) на интерфейсах **[NETx]**, где «x» – порядковый номер интерфейса, с параметрами, указанными в таблице (см. Таблица 23).

Таблица 23
Значения параметров правила для интерфейсов

Параметр	Значение
Действие	Разрешить (Pass)
Интерфейс	NETx, где «x» – порядковый номер интерфейса
Направление	Любой
Протокол	ICMP

Для настройки динамической маршрутизации по протоколу RIP необходимо выполнить следующие действия:

1. На каждом **ARMA IF** перейти в подраздел общих настроек маршрутизации (**«Маршрутизация»** - **«Общие настройки»**) установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок 116) для включения сервиса маршрутизации.

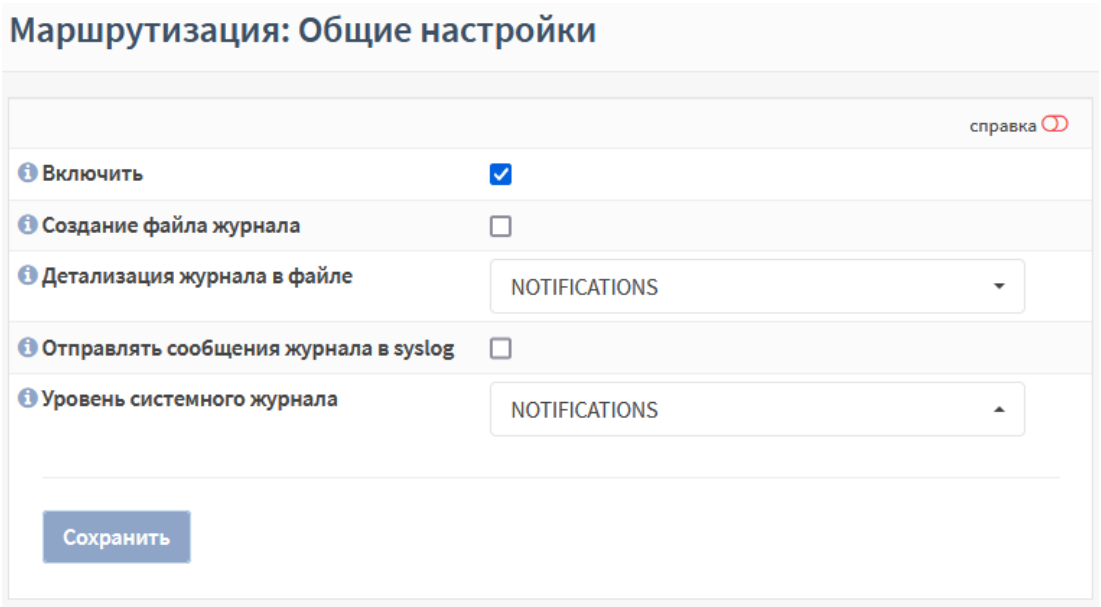

Рисунок 116 – Включение сервиса маршрутизации

2. На каждом **ARMA IF** перейти в подраздел настроек маршрутизации RIP (**«Маршрутизация»** - **«RIP»**), установить флажок для параметра

«Включить», указать параметры маршрутизации, представленные в таблице (см. Таблица 24), и нажать **кнопку «Сохранить»**.

Таблица 24

Параметры маршрутизации протокола RIP

Параметр	ARMA IF1	ARMA IF2	ARMA IF3
Версия	2	2	2
Пассивные интерфейсы	NET1	NET2	Не выбрано
Перераспределение маршрута	Подключенные маршруты (напрямую подключенная подсеть или хост)	Подключенные маршруты (напрямую подключенная подсеть или хост)	Подключенные маршруты (напрямую подключенная подсеть или хост)
Сети	192.168.3.0/24 192.168.4.0/24	192.168.4.0/24 192.168.5.0/24	192.168.3.0/24 192.168.5.0/24

11.1.2 Проверка работы динамической маршрутизации RIP

Для проверки динамической маршрутизации необходимо выполнить следующие действия:

1. На ПК **«Server»** запустить командную строку и выполнить команду трассировки до ПК **«Client»**, зафиксировать маршрут прохождения трафика (см. Рисунок 117).

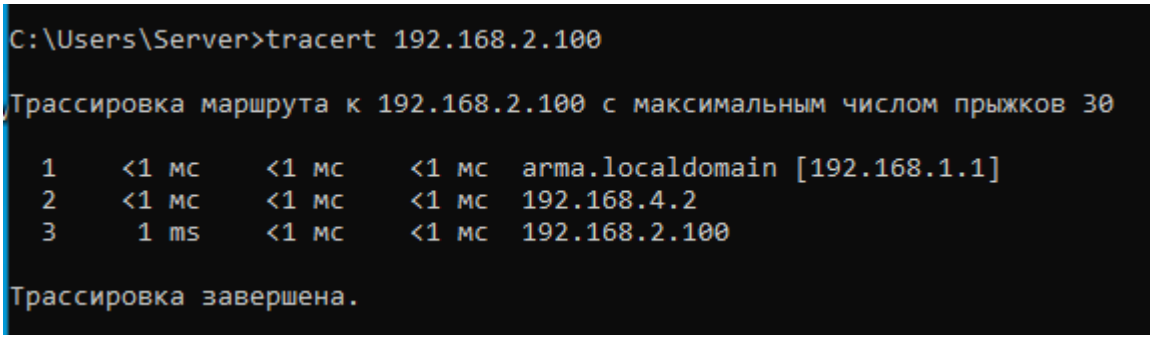

Рисунок 117 – Результат выполнения команды трассировки

2. Отключить сетевой интерфейс NET4 на **ARMA IF1** и **ARMA IF2** и дождаться перестроения маршрутов – до 5 минут.
3. На ПК **«Server»** запустить командную строку и выполнить команду трассировки до ПК **«Client»**, убедиться в смене маршрута (см. Рисунок 118).

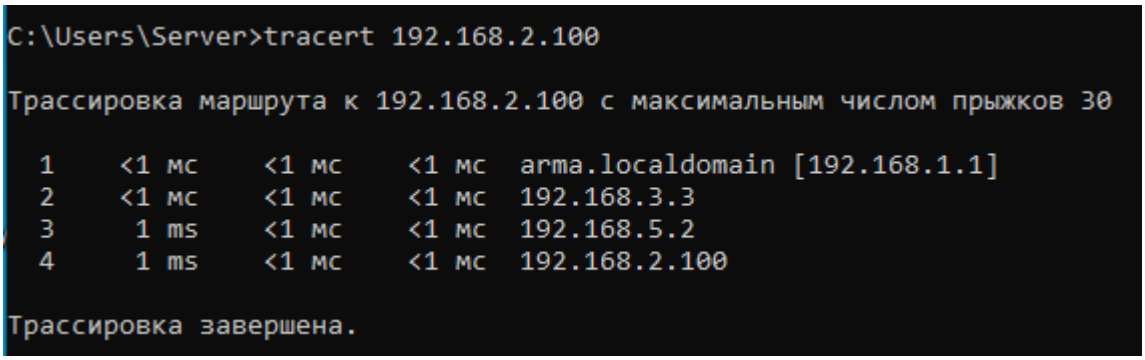

Рисунок 118 – Результат выполнения команды трассировки

11.2 OSPF

Данный протокол основан на технологии отслеживания состояния канала – «link-state technology» и использующий алгоритм поиска кратчайшего пути. OSPF представляет собой протокол внутреннего шлюза и распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

11.2.1 Настройка динамической маршрутизации OSPF

В качестве примера приведена настройка динамической маршрутизации на трех **ARMA IF** согласно схеме стенда, представленного на рисунке (см. Рисунок 115).

Перечень интерфейсов со значениями IP-адресов для каждого **ARMA IF** приведен в таблице (см. Таблица 22).

На каждом **ARMA IF** предварительно необходимо создать разрешающее правило МЭ (см. Раздел 1.1.1) на интерфейсах **[NETx]**, где «x» – порядковый номер интерфейса, с параметрами, указанными в таблице (см. Таблица 23)

Для настройки динамической маршрутизации по протоколу OSPF необходимо выполнить следующие действия:

1. На каждом **ARMA IF** перейти в подраздел общих настроек маршрутизации (**«Маршрутизация»** - **«Общие настройки»**) установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок 116) для включения сервиса маршрутизации.
2. На каждом **ARMA IF** перейти в подраздел настроек маршрутизации OSPF (**«Маршрутизация»** - **«OSPF»**), установить флажок для параметра **«Включить»**, указать параметры маршрутизации, представленные в таблице (см. Таблица 25), и нажать **кнопку «Сохранить»**.

Таблица 25
Параметры маршрутизации протокола OSPF

Параметр	ARMA IF1	ARMA IF2	ARMA IF3
Пассивные интерфейсы	NET1	NET2	Не выбрано

Параметр	ARMA IF1	ARMA IF2	ARMA IF3
Перераспределение маршрута	Подключенные маршруты (напрямую подключенная подсеть или хост)	Подключенные маршруты (напрямую подключенная подсеть или хост)	Подключенные маршруты (напрямую подключенная подсеть или хост)

3. На каждом **ARMA IF** перейти во вкладку **«Сети»** подраздела настроек маршрутизации OSPF (**«Маршрутизация»** - **«OSPF»**), нажать **кнопку «+»**, указать параметры сетей согласно таблице (см. Таблица 26) и нажать **кнопку «Сохранить»**. Действие выполнить для каждой сети в таблице.

Таблица 26
Параметры сетей для протокола OSPF

Параметр	Сеть	ARMA IF1	ARMA IF2	ARMA IF3
Адрес сети	№1	192.168.3.0	192.168.4.0	192.168.3.0
	№2	192.168.4.0	192.168.5.0	192.168.5.0
Область	№1	0.0.0.0	0.0.0.0	0.0.0.0
	№2	0.0.0.0	0.0.0.0	0.0.0.0

11.2.2 Проверка работы динамической маршрутизации OSPF

Для проверки динамической маршрутизации необходимо выполнить следующие действия:

1. На ПК **«Server»** запустить командную строку и выполнить команду трассировки до ПК **«Client»**, зафиксировать маршрут прохождения трафика (см. Рисунок 119).

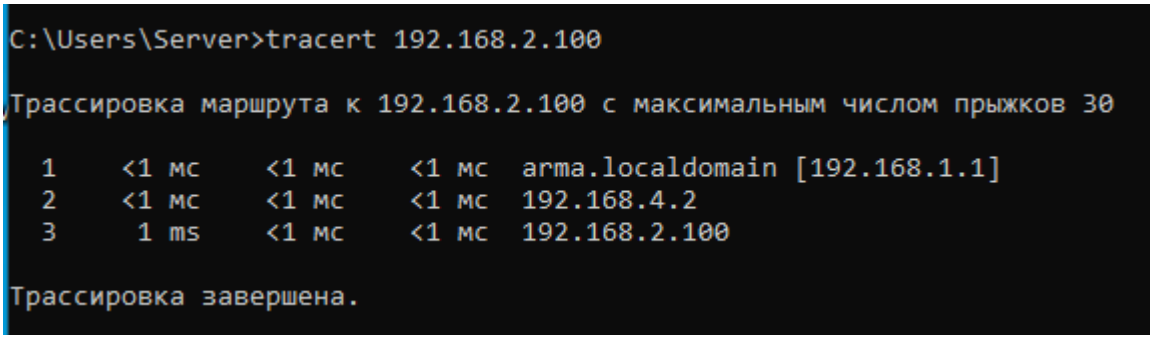

Рисунок 119 – Результат выполнения команды трассировки

2. Отключить сетевой интерфейс NET4 на **ARMA IF1** и **ARMA IF2** и дождаться перестроения маршрутов – до 5 минут.

3. На ПК **«Server»** запустить командную строку и выполнить команду трассировки до ПК **«Client»**, убедиться в смене маршрута (см. Рисунок 120).

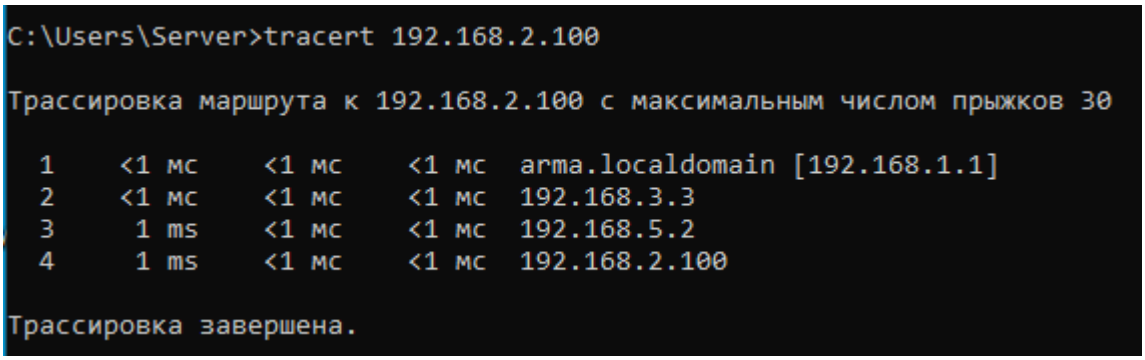

Рисунок 120 – Результат выполнения команды трассировки

12 DHCP-СЕРВЕР

DHCP-сервер используется для автоматического предоставления клиентам IP-адреса и других параметров, необходимых для работы в сети TCP/IP. DHCP-сервер доступен как для клиентов IPv4, так и для IPv6, представленных в подразделах **«DHCPv4»** и **«DHCPv6»** раздела **«Службы»** соответственно.

12.1 DHCPv4

Подраздел содержит настройки DHCP-сервера для клиентов IPv4.

В качестве примера использования DHCP-сервера будет рассмотрено назначение IP-адресов хостам во внутренней подсети интерфейса «LAN» из следующего диапазона:

- «192.168.1.100 – 192.168.1.199».

Результатом работы настроенного DHCP-сервера является назначение IP-адресов хостам, находящимся в подсети интерфейса «LAN». Выданные IP-адреса представлены в подразделе аренды адресов (**«Службы»** - **«DHCPv4»** - **«Аренда адресов»**).

12.1.1 Настройка по имени интерфейса

Перечень параметров и процесс их настройки является идентичным для всех интерфейсов («LAN», «WAN», «OPT1» и т.д.).

Для того, чтобы настроить DHCP-сервер, необходимо перейти в подраздел параметров DHCP-сервера настраиваемого интерфейса (**«Службы»** - **«DHCPv4»** - **«[LAN]»**), установить флажок **«Включить DHCP-сервер на LAN интерфейсе»**, задать параметры для работы в сети TCP/IP и нажать **кнопку «Сохранить»** внизу страницы.

Основные параметры (подсеть, маска подсети и доступный диапазон) будут заданы автоматически, на основании настроек интерфейса (см. Рисунок 121).

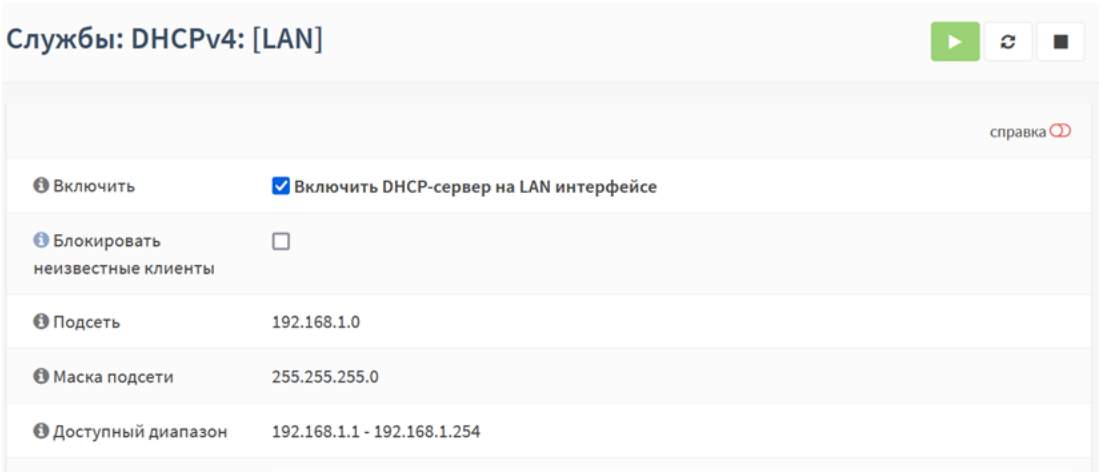

Рисунок 121 – Основные параметры DHCP

12.1.1.1 Диапазон IP-адресов

Основной диапазон возможно скорректировать указав значения в полях параметра **«Диапазон»** (см. Рисунок 122).

Важно! В случае, если поля параметра **«Диапазон»** будут пустыми, выдача адресов не произойдёт.

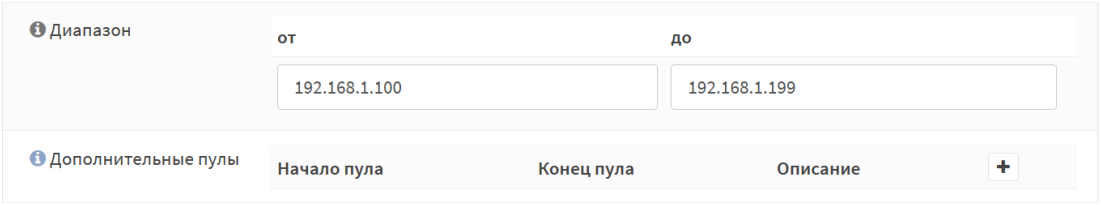

Рисунок 122 – Значение диапазона адресов

Так же существует возможность указать дополнительные диапазоны с заданными параметрами. Для этого необходимо нажать **кнопку «+»** в параметре **«Дополнительные пулы»** (см. Рисунок 122) и, указав требуемые настройки в открывшемся интерфейсе, нажать **кнопку «Сохранить»**.

12.1.1.2 Параметры для работы в сети TCP/IP

В случае, когда требуется изменить дополнительные параметры работы в сети TCP/IP, необходимо выполнить одно или несколько из доступных действий:

1. Указать новые значения в соответствующих полях:
    - **«WINS-серверы»**;
    - **«DNS-серверы»**;
    - **«Шлюз»**;
    - **«Имя домена;**
    - **«Список поиска доменов»**;
    - **«Время аренды по умолчанию (секунд)»**;
    - **«Максимальное время аренды (секунды)»**;
    - **«MTU интерфейса»**.
    - **«IP-адрес участника для аварийного переключения»**;
    - **«Разделение аварийного переключения»**.
2. Установить флажок в чек-боксах:
    - **«Статический ARP – Включить статические записи ARP»**;
    - **«Изменить формат даты – Изменить отображение времени аренды DHCP с UTC на местное время»**.

3. Раскрыть дополнительные значения параметра для последующей настройки, нажав **кнопку «Дополнительно»** напротив параметра:
    - **«Динамический DNS»**;
    - **«Контроль доступа по MAC-адресам»**;
    - **«NTP-серверы»**;
    - **«TFTP-сервер»**;
    - **«LDAP URI»**;
    - **«Включить загрузку по сети»**;
    - **«WPAD»**;
    - **«Включить OMAPI»**;
    - **«Дополнительные параметры»**.

12.1.1.3 Статическая маршрутизация

Для закрепления связки **«IP-адрес – хост»** на основании MAC-адреса используется статическая маршрутизация.

Для сопоставления выделяемого IP-адреса заданному хосту необходимо нажать **кнопку «+»** в блоке **«Статическая маршрутизация через DHCP для этого интерфейса»** (см. Рисунок 123).

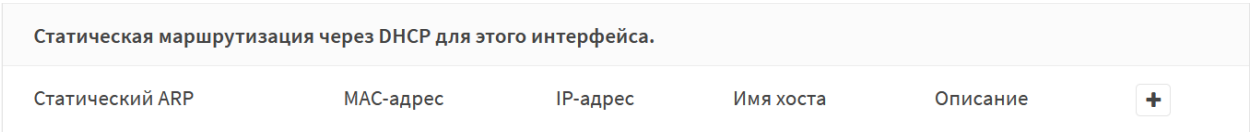

Рисунок 123 – Статическая маршрутизация через DHCP для этого интерфейса

В открывшемся интерфейсе (см. Рисунок 124) указать MAC-адрес хоста, за которым будет закреплен IP-адрес, непосредственно сам IP-адрес и нажать **кнопку «Сохранить»** внизу страницы. Дополнительные параметры вводятся при необходимости.

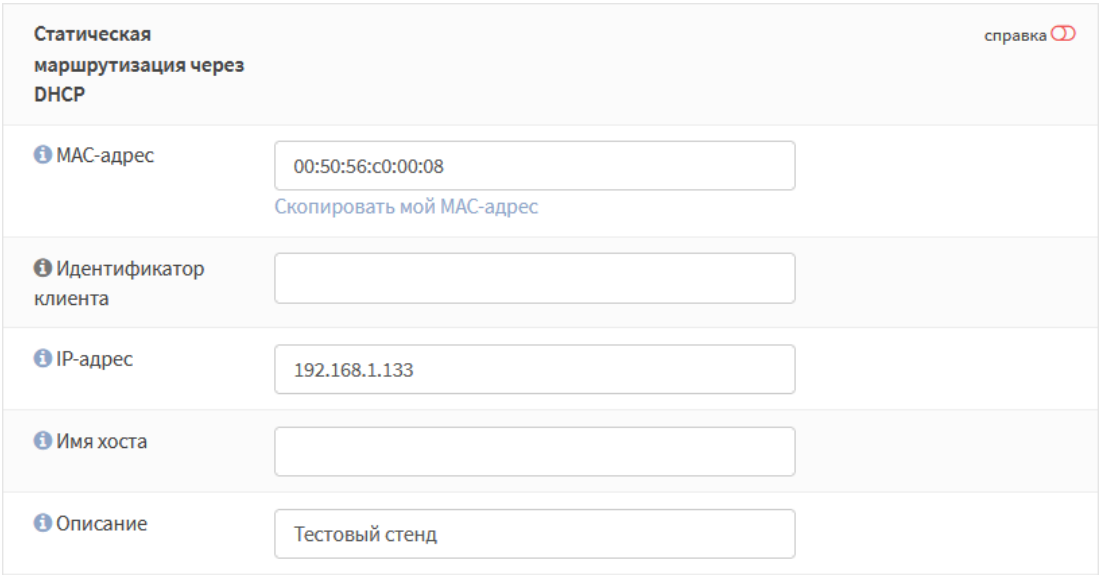

Рисунок 124 – Сопоставление MAC-адреса и IP-адреса

12.1.2 Ретрансляция

DHCP-ретрансляция – это пересылка полученных DHCP-запросов на другой сервер. Настройки ретрансляции доступны только при выключенном DHCP-сервере.

Для настройки DHCP-ретрансляции необходимо задать интерфейсы ретрансляции и адреса внешних DHCP-серверов в подразделе конфигурации DHCP-ретрансляции (**«Службы»** - **«DHCPv4»** - **«Ретрансляция»**), установить флажок **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок 125).

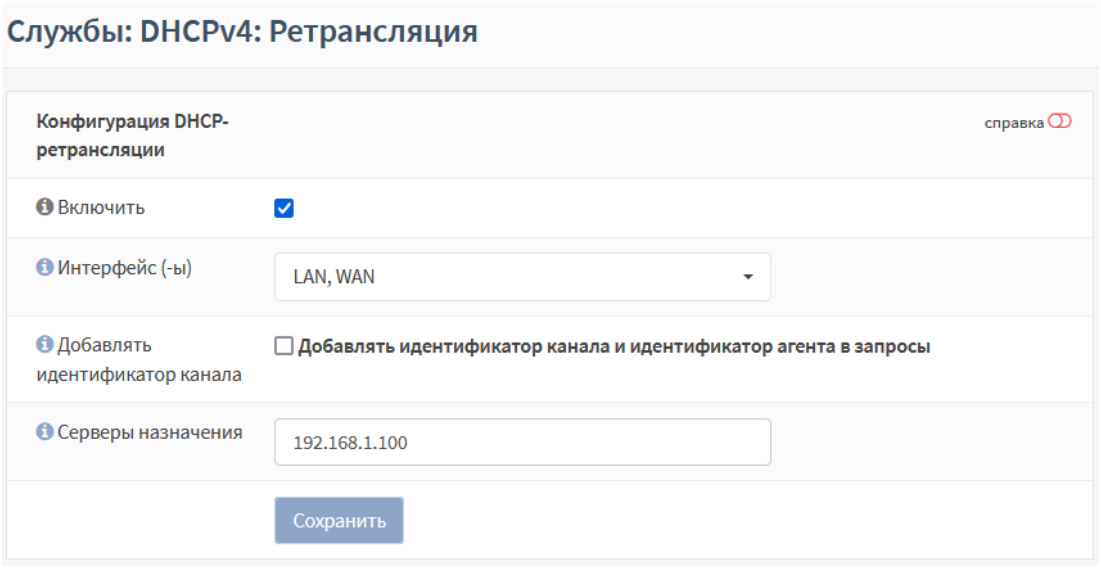

Рисунок 125 – Настройка ретрансляции DHCP

12.1.3 Аренда адресов

В подразделе назначенных адресов (**«Службы»** - **«DHCPv4»** - **«Аренда адресов»**) отображается перечень арендованных адресов (см. Рисунок 126). Наличие записей свидетельствует о правильно настроенном DHCP-сервере.

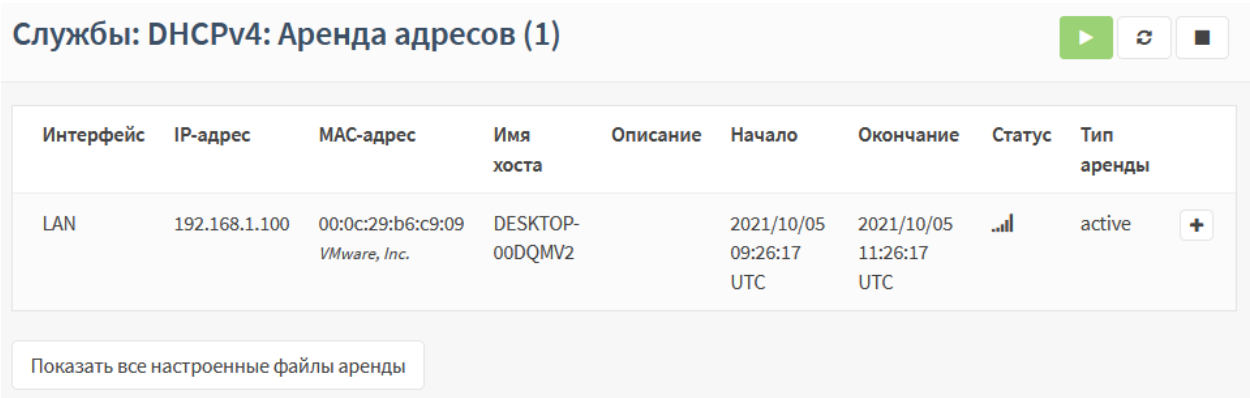

Рисунок 126 – Активные арендованные адреса

При нажатии **кнопки «+»** напротив выбранного адреса – откроется форма статической маршрутизации для закрепления связки **«IP-адрес – хост»** (см. Рисунок 124).

При нажатии **кнопки «Показать все настроенные файлы аренды»** будут отображены хосты с истекшим сроком аренды (см. Рисунок 127).

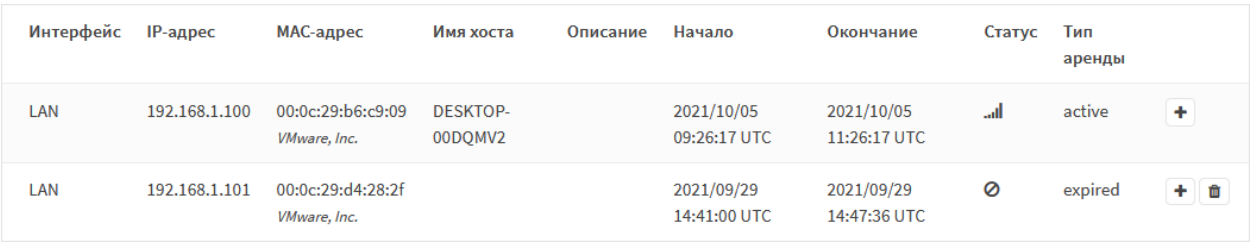

Рисунок 127 – Все настроенные файлы аренды

12.2 DHCPv6

Подраздел содержит настройки DHCP-сервера для клиентов IPv6. По умолчанию для DHCPv6-сервера доступны только подразделы **«Ретрансляция»** и **«Аренда адресов»**.

Для того, чтобы был доступен подраздел с настройками для каждого интерфейса («LAN», «WAN», «OPT1» и т.д.), необходимо произвести настройку протокола IPv6 для соответствующего интерфейса в разделе **«Интерфейсы»**.

Распространённым сценарием использования DHCPv6-сервера является назначение IPv6-адресов хостам во внутренней подсети интерфейса «LAN».

Далее будут приведены шаги настройки DHCPv6-сервера со следующими параметрами:

- Интерфейс «LAN»;
- Подсеть – «0010:0000:0000:0000:0000:0000:0000:0000», сокращённо – «10::»;
- Длина префикса –«64».

12.2.1 Настройка по имени интерфейса

Процесс настройки DHCP-сервера для IPv6 аналогичен настройке для IPv4.

Необходимо перейти в подраздел параметров DHCP-сервера настраиваемого интерфейса (**«Службы»** - **«DHCPv6»** - **«[LAN]»**), установить флажок **«Включить DHCPv6-сервер на LAN интерфейсе»**, задать параметры для работы в сети TCP/IP и нажать **кнопку «Сохранить»** внизу страницы.

Основные параметры (подсеть, маска подсети и доступный диапазон) будут заданы автоматически, основываясь на настройках интерфейса (см. Рисунок 128).

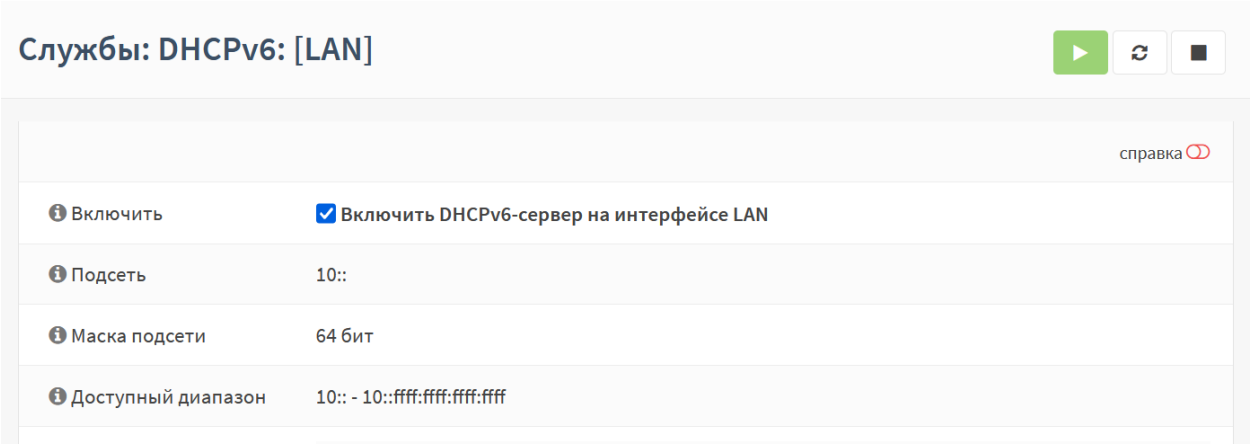

Рисунок 128 – Основные настройки DHCPv6

12.2.1.1 Диапазон IP-адресов

Настройки диапазона задаются в параметрах **«Диапазон»** и **«Диапазон делегируемых префиксов»** (см. Рисунок 129).

Важно! В случае, если поля параметра **«Диапазон»** будут пустыми, выдача адресов не произойдёт.

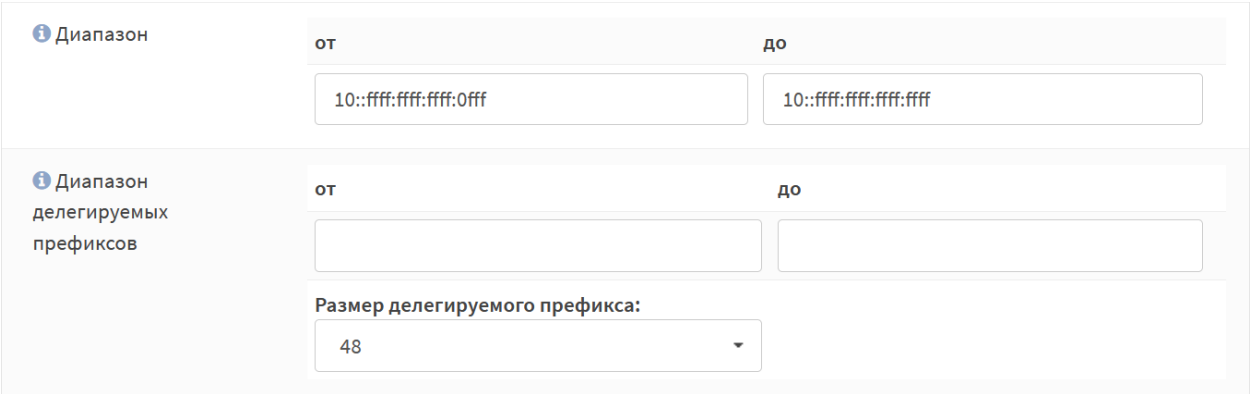

Рисунок 129 – Дополнительные настройки диапазона адресов

12.2.1.2 Параметры для работы в сети TCP/IP

В случае, когда требуется изменить дополнительные параметры работы в сети TCP/IP, необходимо выполнить одно или несколько доступных действий:

1. Указать новые значения в соответствующих полях:
    - **«DNS-серверы»**;
    - **«Список поиска доменов»**;
    - **«Время аренды по умолчанию (секунды)»**;
    - **«Максимальное время аренды (секунды)»**.
2. Установить флажок в чек-боксе:
    - **«Изменить формат даты – Изменить отображение времени аренды DHCPv6 с UTC на местное время»**.
3. Раскрыть дополнительные значения параметра для последующей настройки, нажав **кнопку «Дополнительно»** напротив параметра:
    - **«Динамический DNS»**;
    - **«NTP-серверы»**;
    - **«Включить загрузку по сети»**;
    - **«Дополнительные параметры BOOTP/DHCP»**.

12.2.1.3 Статическая маршрутизация

Для закрепления связки **«IPv6-адрес – хостами»** на основании идентификатора участников DHCP (DUID) используется статическая маршрутизация.

Для сопоставления выделяемого IP-адреса заданному хосту необходимо нажать **кнопку «+»** в параметре **«Статическая маршрутизация через DHCPv6 для этого интерфейса»** (см. Рисунок 130).

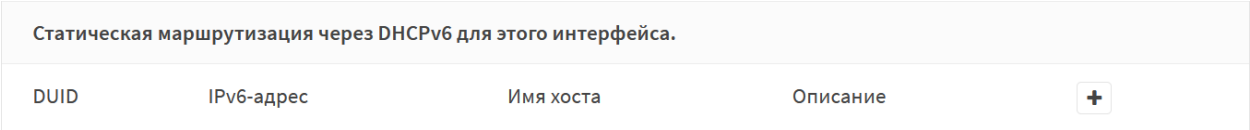

Рисунок 130 – Статическая маршрутизация через DHCPv6 для этого интерфейса

В открывшемся интерфейсе (см. Рисунок 131) указать DUID, за которым будет закреплён IPv6-адрес, непосредственно сам IPv6-адрес и нажать **кнопку «Сохранить»** внизу страницы. Дополнительные параметры вводятся при необходимости.

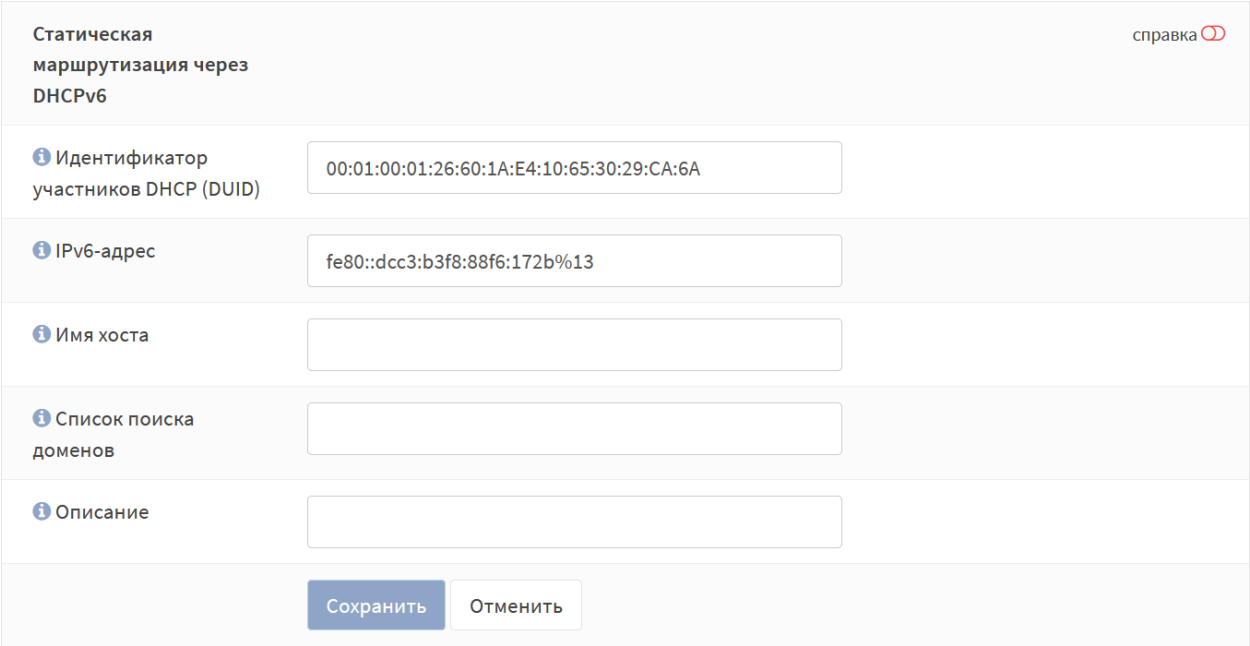

Рисунок 131 – Сопоставление DUID и IPv6-адреса

12.2.2 Ретрансляция

Настройки ретрансляции доступны только при выключенном DHCPv6-сервере.

Для настройки DHCPv6-ретрансляции необходимо задать интерфейсы ретрансляции и адреса внешних DHCPv6-серверов в подразделе конфигурации DHCP-ретрансляции (**«Службы»** - **«DHCPv6»** - **«Ретрансляция»**), установить флажок **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок 132). При необходимости установить флажок в параметре **«Добавлять идентификатор канала»**.

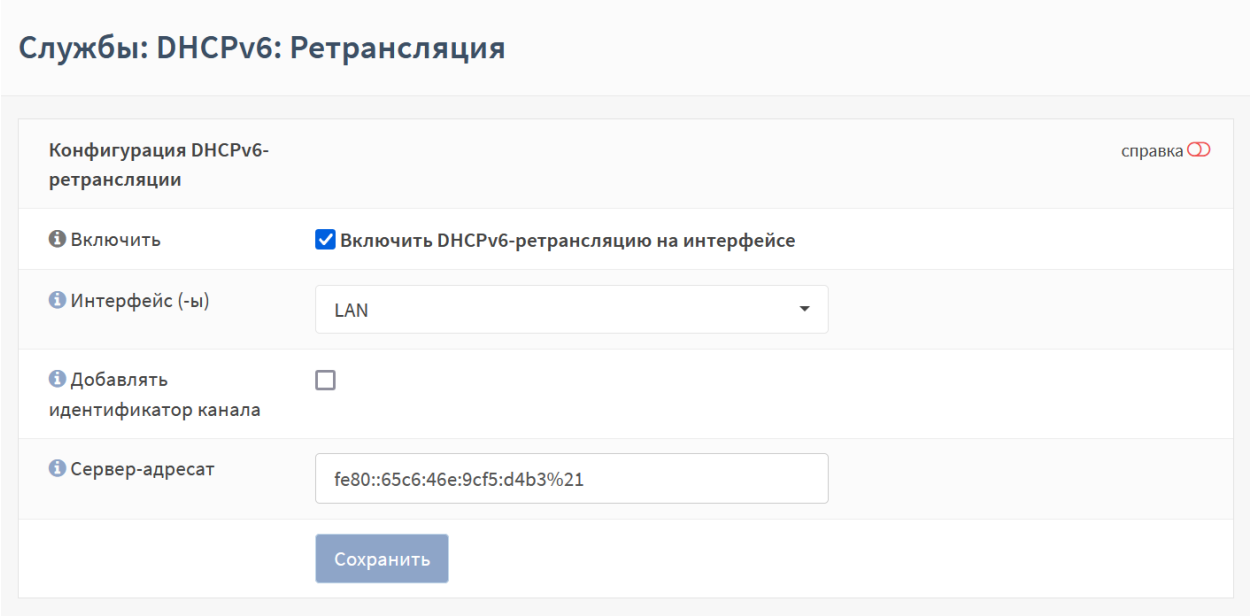

Рисунок 132 – Настройка ретрансляции DHCPv6

12.2.3 Аренда адресов

В подразделе назначенных адресов (**«Службы»** - **«DHCPv6»** - **«Аренда адресов»**) отображается перечень арендованных адресов IPv6 (см. Рисунок 133).

Наличие записей свидетельствует о правильно настроенном DHCPv6-сервере.

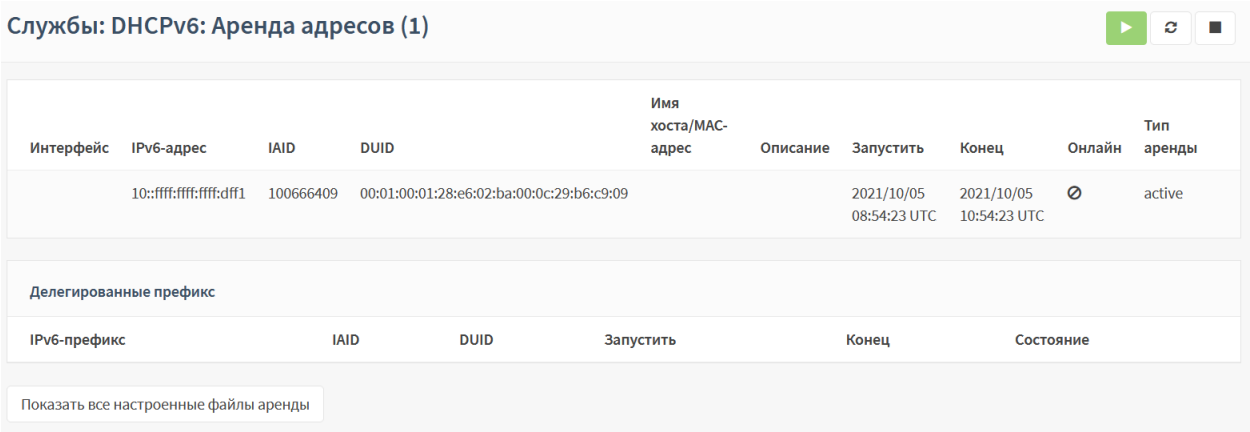

Рисунок 133 – Активные арендованные адреса IPv6

При нажатии кнопки **«Показать все настроенные файлы аренды»** будут отображены хосты с истекшим сроком аренды.

13 СЛУЖБА NTP

Служба NTP – это демон сетевого протокола времени, позволяющий устанавливать и поддерживать системное время, синхронизированное с серверами точного времени.

13.1 Настройка синхронизации времени по протоколу NTP

Первоначальная настройка синхронизации времени производится в мастере первоначальной настройки **ARMA IF** (см. Раздел 22).

Для изменения настроек синхронизации времени по протоколу NTP необходимо выполнить следующие действия:

1. Перейти в подраздел общих настроек NTP (**«Службы»** - **«Сетевое время»** - **«Общие настройки»**) (см. Рисунок 134).
2. Выбрать интерфейс для использования NTP в параметре **«Интерфейс (-ы)»**. По умолчанию прослушиваются все настроенные интерфейсы.
3. В блоке настроек **«Серверы времени»** из списка серверов выбрать предпочитаемые серверы времени или отключить нежелательные. По умолчанию задано четыре сервера. Для добавления сервера необходимо нажать **кнопку «+»** и указать его параметры, а для удаления нажать **кнопку «−»** напротив записи.
4. Нажать **кнопку «Сохранить»**.

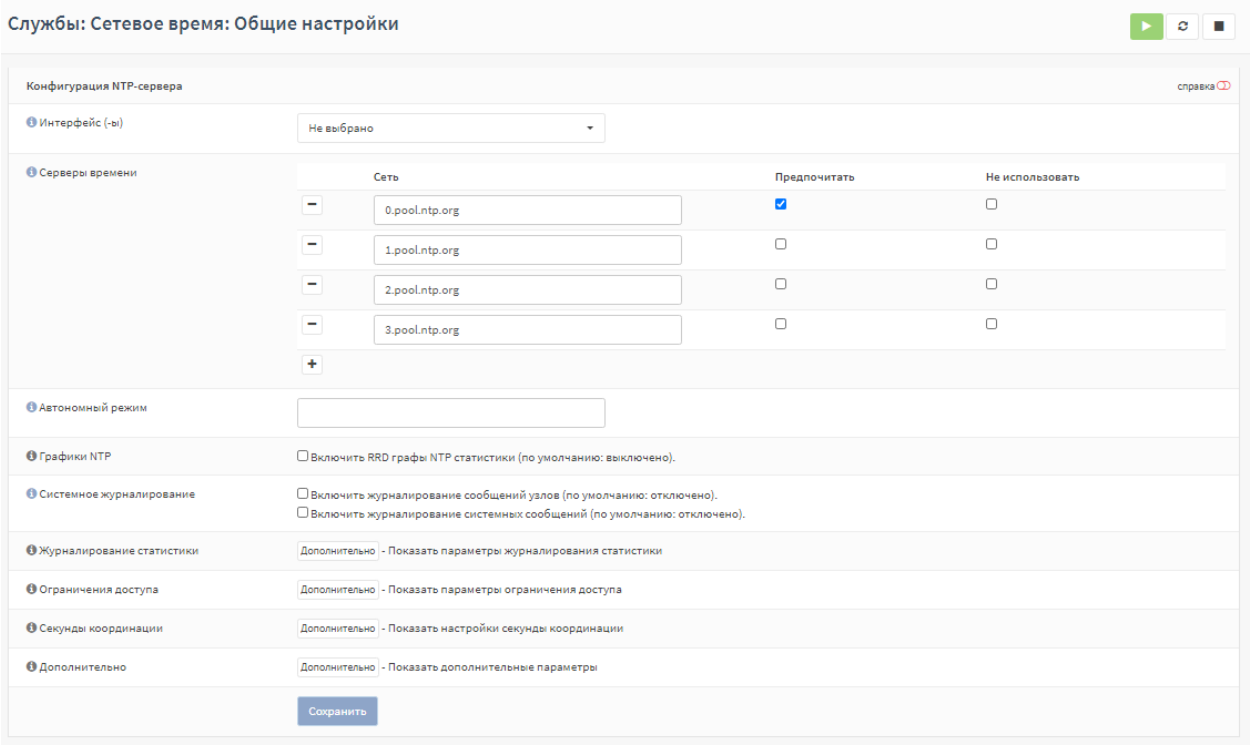

Рисунок 134 – Настройка конфигурации NTP-сервера

При необходимости существует возможность настроить следующие параметры:

- **«Автономный режим»** – позволяет использовать системные часы при недоступности других вариантов;
- **«Графики NTP»** – включает RRD-графы NTP статистики;
- **«Системное журналирование»** – включает дополнительные сообщения NTP в системный журнал;
- **«Журналирование статистики»** – создает сохраняемые ежедневные журналы;
- **«Ограничения доступа»** – настраивает опции контроля доступа к NTP из WAN;
- **«Секунды координации»** – позволяет анонсировать демону NTP последующее добавление или вычитание секунды координации;
- **«Дополнительно»** – позволяет указать дополнительные параметры конфигурации.

Дополнительно существует возможность синхронизировать время по подключаемому GPS-приёмнику. Для этого необходимо задать настройки приемника в соответствующем подразделе (**«Службы»** - **«Сетевое время»** - **«GPS-приемник»**).

14 СЕТЕВЫЕ ИНТЕРФЕЙСЫ

ARMA IF поддерживает множество типов интерфейсов используя как сетевые интерфейсы, так и различные сетевые протоколы. По умолчанию интерфейс «LAN» назначается сетевому интерфейсу «em0», а интерфейс «WAN» сетевому интерфейсу «em1». Для следующих по счёту сетевых интерфейсов по умолчанию применяется обозначение «OPT» – «OPT1» для «em2», «OPT2» для «em3» и так далее. Возможны другие варианты создаваемых интерфейсов, например:

- **«bridge»** – для сетевого моста (см. Раздел 16);
- **«LAGG»** – для LAGG-интерфейса (см. Раздел 15);
- **«VLAN»** – для интерфейса VLAN (см. Раздел 17).

Назначение интерфейсов, изменение существующих и создание новых виртуальных интерфейсов осуществляется в разделе **«Интерфейсы»**.

14.1 Назначение портов

Все определенные и обнаруженные на текущий момент интерфейсы перечислены в подразделе назначения портов (**«Интерфейсы»** - **«Назначение портов»**) или в списке интерфейсов, доступных для назначения (см. Рисунок 135).

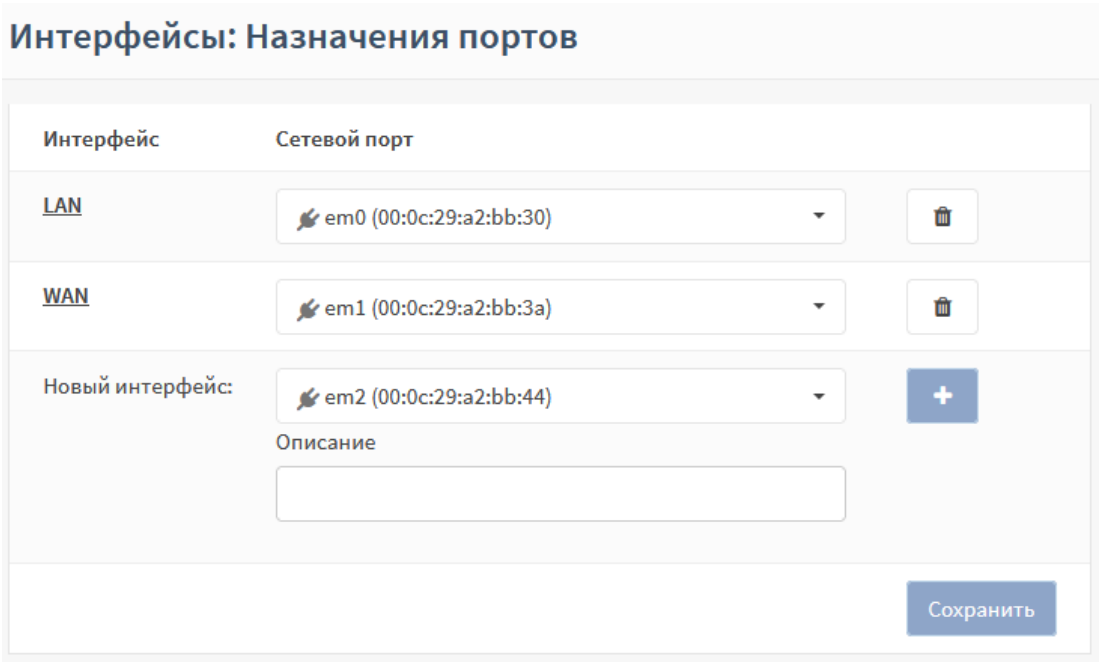

Рисунок 135 – Назначение портов

Для добавления интерфейса необходимо нажать **кнопку «+»** напротив обнаруженного интерфейса, а затем **кнопку «Сохранить»**. Если не указать имя создаваемого интерфейса в поле параметра **«Описание»**, то будет задано имя по умолчанию.

Для переназначения портов необходимо выбрать интерфейс и, в выпадающем списке сетевых портов, выбрать другой порт, затем нажать **кнопку «Сохранить»**. Сетевые порты имеют следующие индикаторы (см. Рисунок 136):

- **зелёный** – сетевое подключение установлено;
- **красный** – сетевое подключение отсутствует.

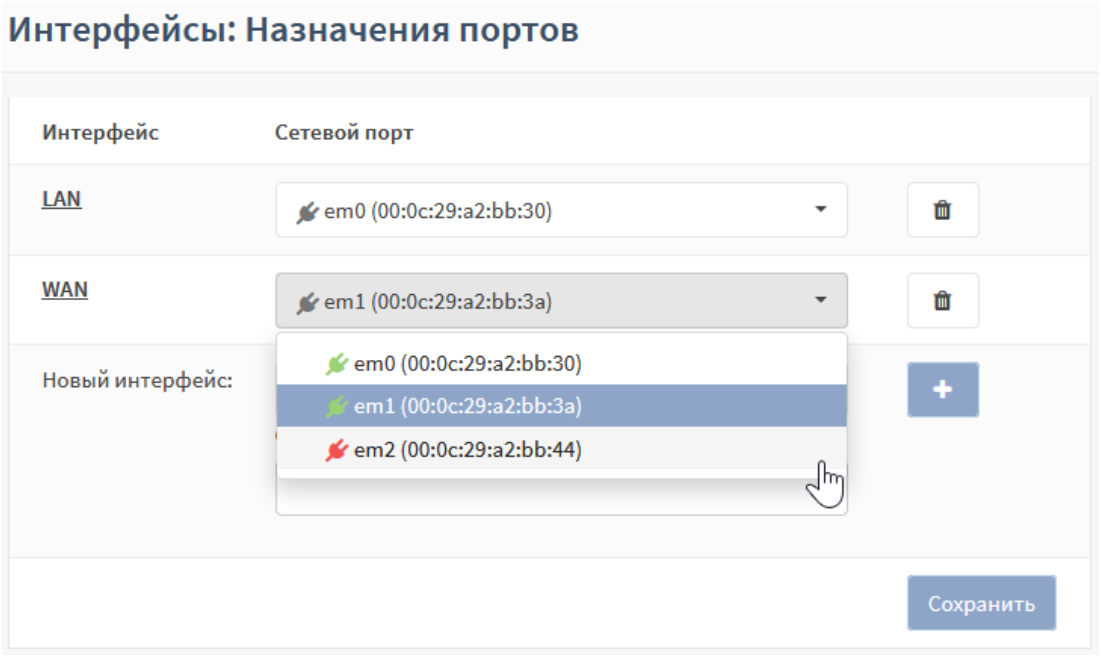

Рисунок 136 – Переназначение портов

14.2 Настройка сетевых интерфейсов

Для перехода в подраздел настроек конкретного сетевого интерфейса существуют два способа:

- нажать **левой кнопкой мыши** на имя необходимого интерфейса в подразделе назначения портов (**«Интерфейсы»** - **«Назначение портов»**) (см. Рисунок 135);
- выбрать необходимый интерфейс в списке раздела **«Интерфейсы»**.

При конфигурировании нового интерфейса или изменении существующего необходимо задать/изменить настройки в следующих блоков:

- **«Базовая конфигурация»**;
- **«Общая конфигурация»**;
- **«Контроль доступа устройств»**.

14.2.1 Блок «Базовая конфигурация»

В данном блоке (см. Рисунок 137) присутствуют следующие параметры:

- **«Включить»** – включает и выключает интерфейс;

- **«Блокировать»** – защищает от случайного удаление интерфейса;
- **«Устройство»** – отображает имя сетевого интерфейса;
- **«Описание»** – отображает имя интерфейса в **ARMA IF**;

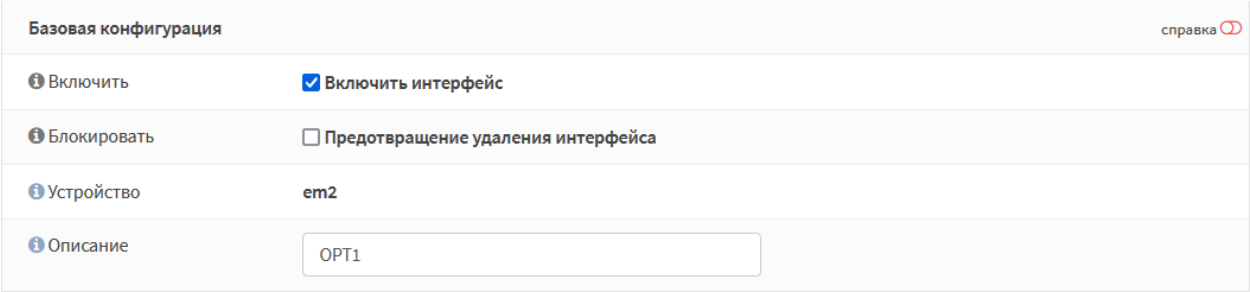

Рисунок 137 – Настройка сетевого интерфейса. Базовая конфигурация

14.2.2 Блок «Общая конфигурация»

В данном блоке (см. Рисунок 138) присутствуют следующие параметры:

- **«Блокировать частные сети»** – блокирует трафик с IP-адресов, зарезервированных для частных сетей: 10/8, 172.16/12, 192.168/16; адреса обратной связи: 127/8, адреса NAT: 100.64/10.
- **«Блокировать bogon сети»** – блокирует трафик с IP-адресов, которые не должны встречаться в таблицах маршрутизации в сети интернет или в качестве адреса отправителя получаемых пакетов;
- **«Тип конфигурации IPv4»** – задает настройки конфигурации IPv4 (см. Раздел 14.2.2.1);
- **«Тип конфигурации IPv6»** – задает настройки конфигурации IPv6;
- **«MAC-адрес»** – имитирует заданный MAC-адрес для интерфейса;
- **«Максимальный размер кадра»** – задает максимальный размер кадра для сетевой карты;
- **«Максимальный размер сегмента»** – задает максимальный размер сегмента для TCP соединений;
- **«Скорость и двусторонний режим передачи данных»** – задает скорость и режим передачи для сетевой карты;
- **«Политика динамического шлюза»** – позволяет создавать динамические шлюзы без прямых адресов.

!Важно Параметры **«MAC-адрес»**, **«Максимальный размер кадра»**, **«Максимальный размер сегмента»**, **«Скорость и двусторонний режим передачи данных»**, **«Политика динамического шлюза»** стоит изменять только в случае необходимости, так как некорректные значения могут повлиять на работоспособность интерфейса.

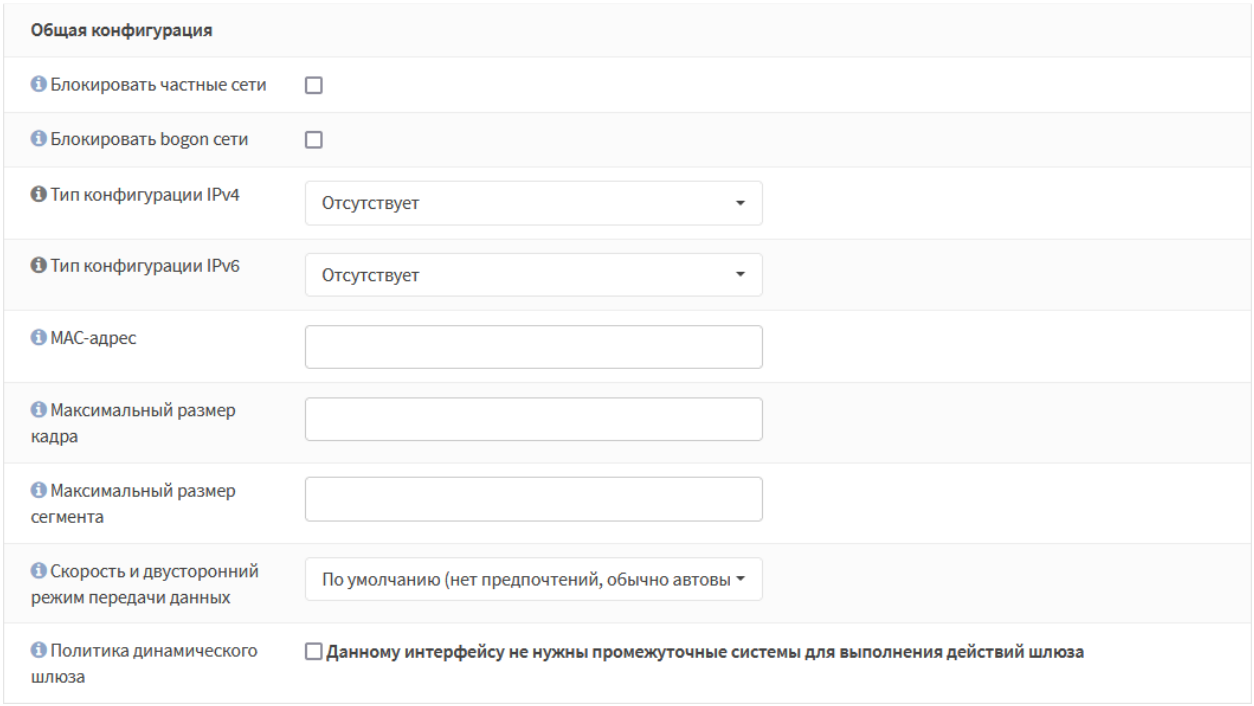

Рисунок 138 – Настройка сетевого интерфейса. Общая конфигурация

14.2.2.1 Конфигурация IPv4

Параметр **«Тип конфигурации IPv4»** включает в себя следующие значения:

- **«Отсутствует»** – конфигурация не задана;
- **«Статический IPv4»** – ручное указание настроек IPv4;
- **«DHCP»** – автоматическая настройка IPv4 посредством DHCP;
- **«PPTP»** – конфигурации IPv4 по протоколу туннелирования PPTP;
- **«L2TP»** – конфигурации IPv4 по протоколу туннелирования L2TP.

При выборе значения «Статический IPv4» появится дополнительный блок настроек (см. Рисунок 139), в котором указываются IP-адрес и маска подсети, а также, при необходимости, задаются параметры публичного IP-адреса шлюза после нажатия **кнопки «+»**.

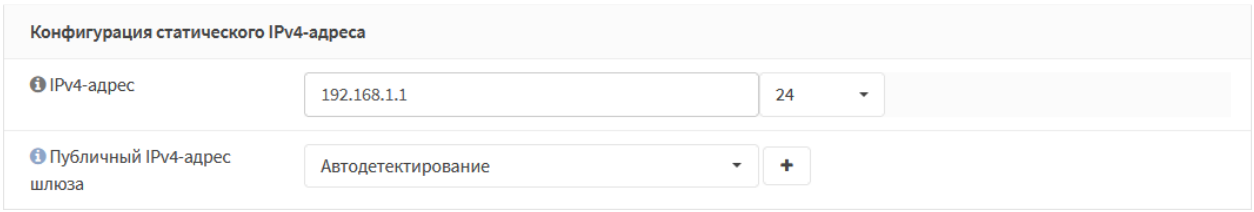

Рисунок 139 – Конфигурация статического IPv4-адреса

При выборе значения «DHCP» **ARMA IF** выполнит автоматическую настройку интерфейса посредством DHCP. При этом появится дополнительный блок настроек (см. Рисунок 140) для настройки конфигурации DHCP–клиента.

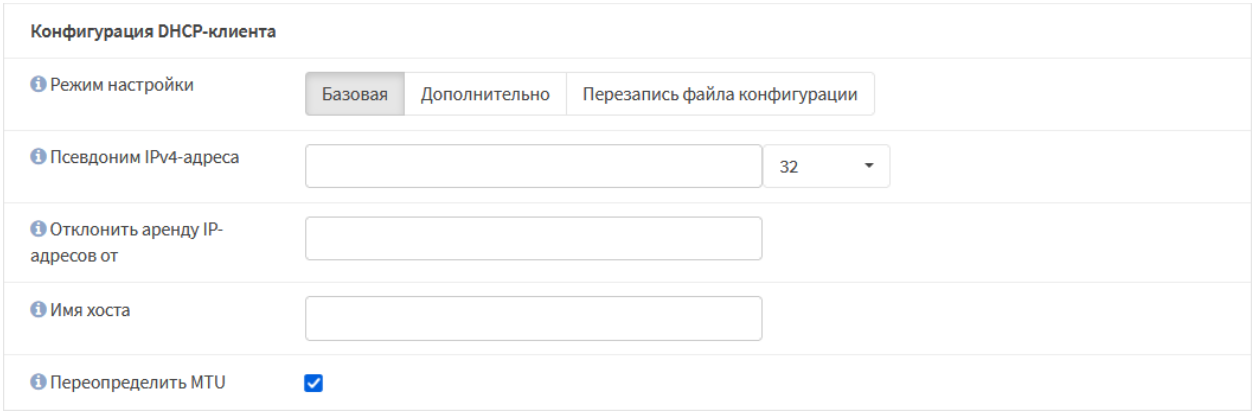

Рисунок 140 – Конфигурация DHCP-клиента

Полученный по DHCP IP-адрес будет отображаться в виджете **«Интерфейсы»** раздела **«Инструменты»** (см. Раздел 27.1).

При выборе значения «PPTP»/«L2TP» появится дополнительный блок конфигурации IPv4 по протоколам туннелирования (см. Рисунок 141).

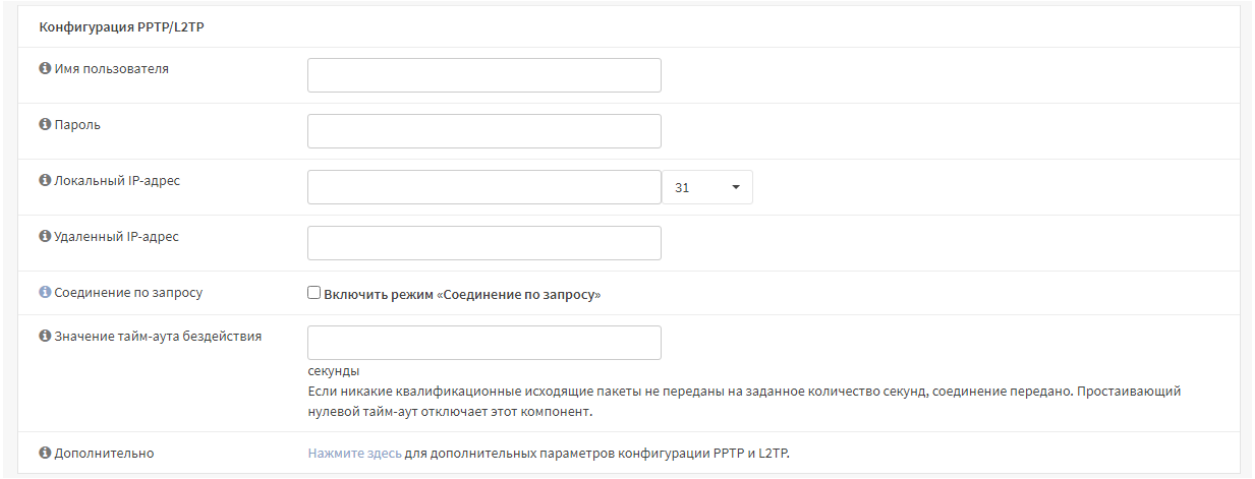

Рисунок 141 – Настройка сетевого интерфейса. Конфигурация PPTP/L2TP

Важно! При настройке конфигурации IPv4 адресное пространство различных интерфейсов не должно совпадать. При необходимости использовать для **ARMA IF** более одного IP-адреса из одной подсети необходимо воспользоваться подразделом настроек виртуальных адресов (**«Межсетевой экран»** - **«Виртуальные IP-адреса»** - **«Настройки»**).

14.2.2.2 Конфигурация IPv6

Параметр **«Тип конфигурации IPv6»** включает в себя следующие значения:

- **«Отсутствует»** – конфигурация не задана;
- **«Статический IPv6»** – ручное указание настроек IPv6;
- **«DHCPv6»** – автоматическая настройка IPv6 посредством DHCPv6;
- **«SLAAC»** – автоматическая настройка IPv6 посредством SLAAC;

- **«Туннель 6RD»** – автоматическая настройка IPv6 по протоколу 6RD;
- **«Туннель 6to4»** – автоматическая настройка IPv6 по протоколу 6to4;
- **«Отслеживать состояние интерфейсов»** – отслеживание настроек IPv6.

При выборе значения «Статический IPv6» появится дополнительный блок настроек (см. Рисунок 142), в котором указываются IP-адрес и маска подсети, а также, при необходимости, задаются параметры публичного IP-адреса шлюза после нажатия **кнопки «+»** и возможность использовать IPv4-подключение.

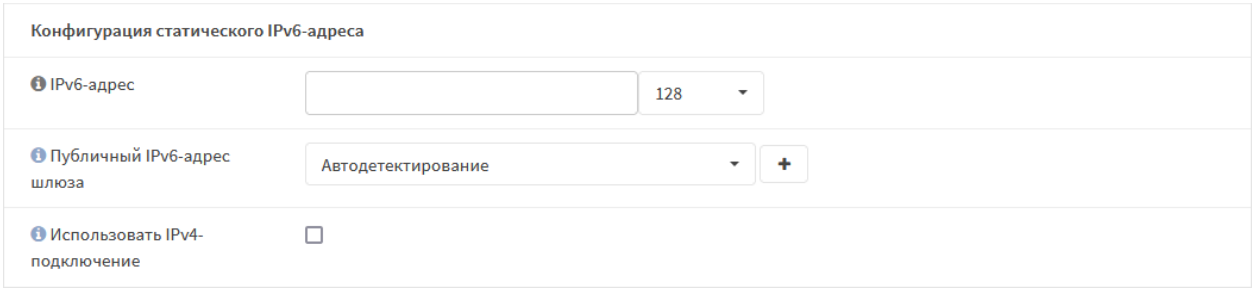

Рисунок 142 – Конфигурация статического IPv6-адреса

При выборе значения «DHCPv6» **ARMA IF** выполнит автоматическую настройку интерфейса посредством DHCP. При этом появится дополнительный блок настроек (см. Рисунок 143) для настройки конфигурации DHCP–клиента.

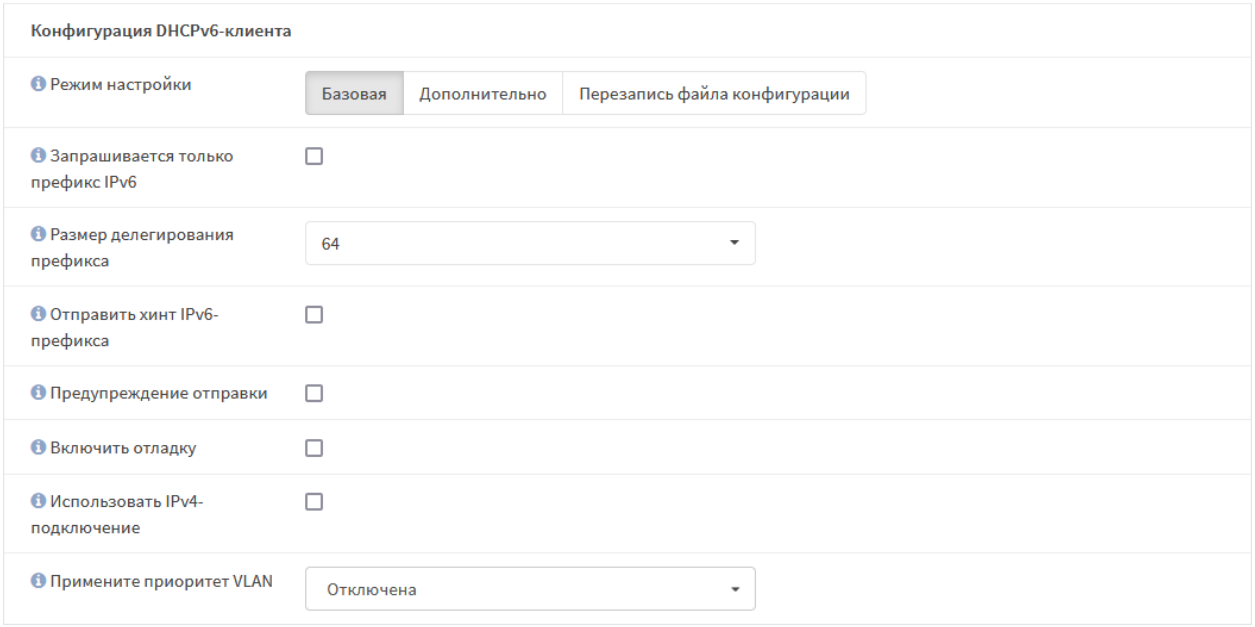

Рисунок 143 – Конфигурация DHCPv6-клиента

При выборе значения «SLAAC» **ARMA IF** выполнит автоматическую настройку интерфейса посредством SLAAC без помощи DHCPv6-сервера. При этом появится дополнительный блок настроек (см. Рисунок 144) для настройки конфигурации DHCP–клиента.

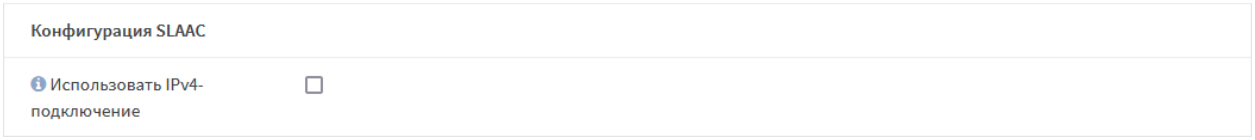

Рисунок 144 – Конфигурация SLAAC

При выборе значения «Туннель 6RD» **ARMA IF** выполнит автоматическую настройку интерфейса по протоколу 6RD. При этом появится дополнительный блок настроек (см. Рисунок 145) для настройки конфигурации протокола 6RD.

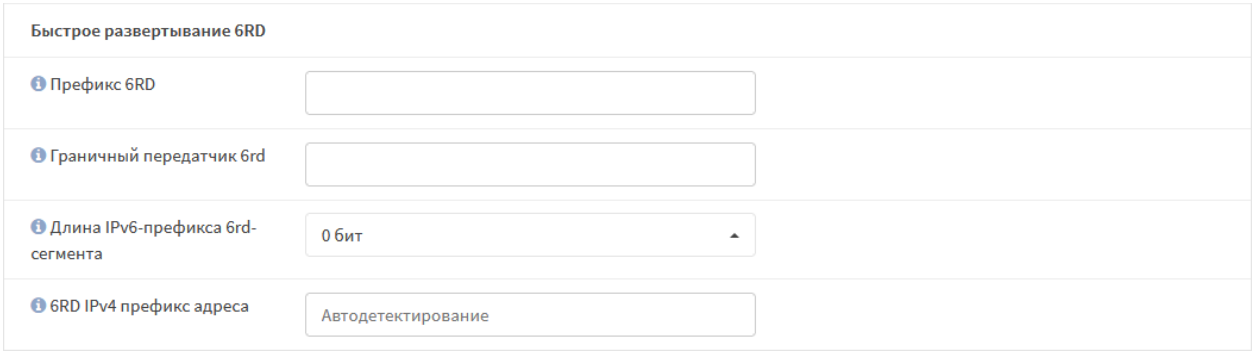

Рисунок 145 – Конфигурация протокола 6RD

При выборе значения «Туннель 6to4» **ARMA IF** выполнит автоматическую настройку интерфейса по протоколу 6to4.

Важно! При настройке конфигурации IPv6 адресное пространство различных интерфейсов не должно совпадать.

14.2.3 Блок «Контроль доступа устройств»

В данном блоке (см. Рисунок 146) возможно задать параметры контроля доступа устройств:

- **«Отключена»** – контроль доступа отключен;
- **«Белый список»** – доступ к настраиваемому интерфейсу имеют только указанные хосты;
- **«Черный список»** – доступ к настраиваемому интерфейсу имеют все, кроме указанных хостов.

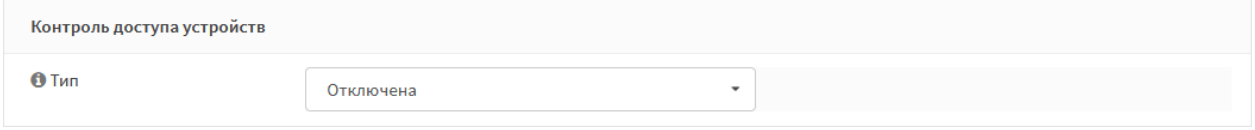

Рисунок 146 – Настройка сетевого интерфейса. Контроль доступа устройств

При выборе значений «Белый список» или «Черный список» будет доступен параметр **«Список устройств»** с полем ввода значений MAC-адресов в виде списка, разделённых знаком запятой.

14.3 Расширенные настройки

Для всех интерфейсов доступны расширенные настройки в подразделе настроек интерфейсов (**«Интерфейсы»** - **«Настройки»**) (см. Рисунок 147).

Расширенные настройки требуются для использования определенных сценариев, например, при включении СОВ. В большинстве случаев настройки рекомендуется оставлять по умолчанию.

В случае выбора в параметре **«Фильтрация аппаратного обеспечения VLAN»** значения «Отключить фильтрацию аппаратного обеспечения внешних VLAN» появится дополнительное поле с выбором интерфейса, на котором будет отключена фильтрация. Отключение фильтрации для выбранного интерфейса позволяет успешно проходить тегированному трафику VLAN'ов, созданных вне **ARMA IF**, при включенной IPS.

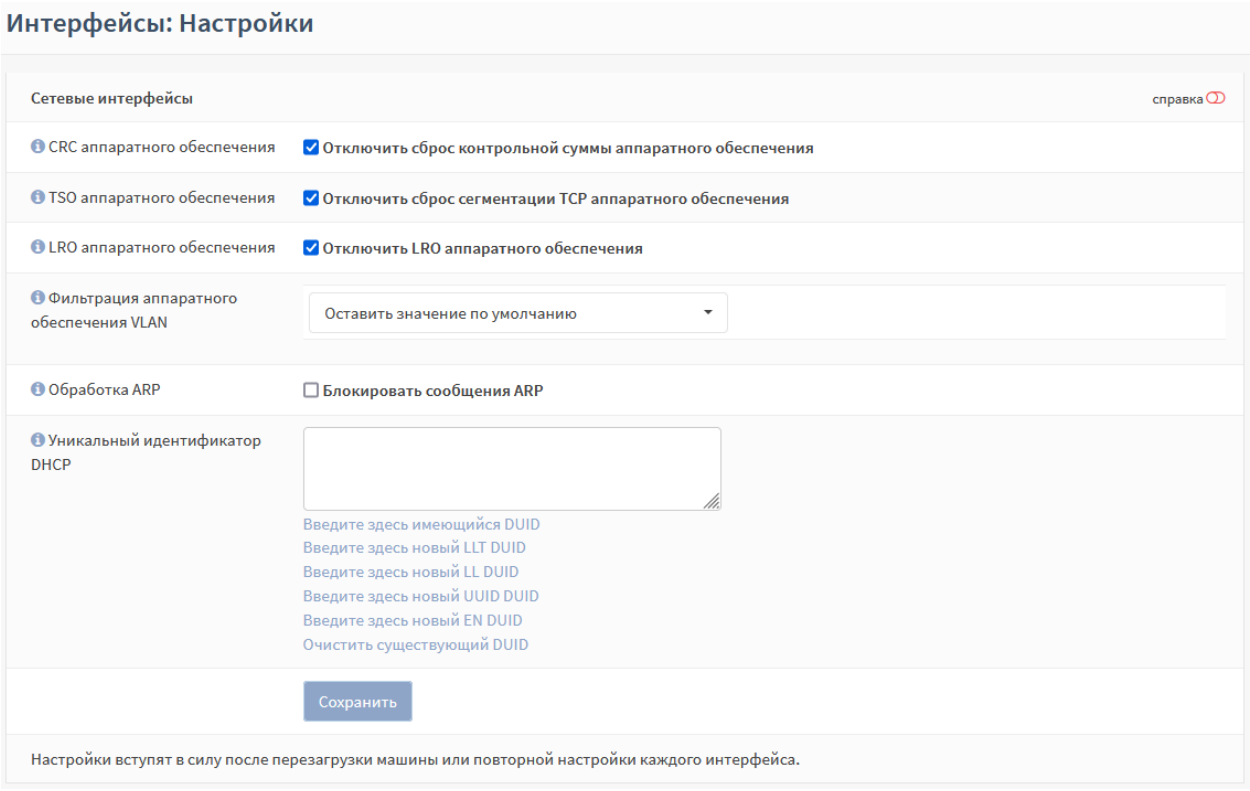

Рисунок 147 – Настройки интерфейсов

15 LAGG

Для повышения отказоустойчивости и пропускной способности интерфейсов используется функция агрегации каналов LAGG. Функция объединяет несколько физических интерфейсов в один логический интерфейс.

Создание LAGG-интерфейса возможно только из несконфигурированных интерфейсов.

Тестовый стенд имеет следующие параметры:

1. **ARMA IF** установлен на ВМ гипервизора VMware.
2. ВМ имеет три сетевых адаптера (см. Рисунок 148).
3. Первый и второй сетевые адаптеры подключены к виртуальной сети **«VMnet0»** в режиме **«Сетевой мост»** с сетевым адаптером гипервизора.
4. Третий сетевой адаптер используется для конфигурирования и доступа в Интернет **ARMA IF**.
5. Настройки сетевого адаптера гипервизора:
   - **Сеть** – 192.168.1.1/24.
   - **IP-адрес** – назначается DHCP.
6. Сетевые адаптеры в **ARMA IF** «em0» и «em1» не сконфигурированы.

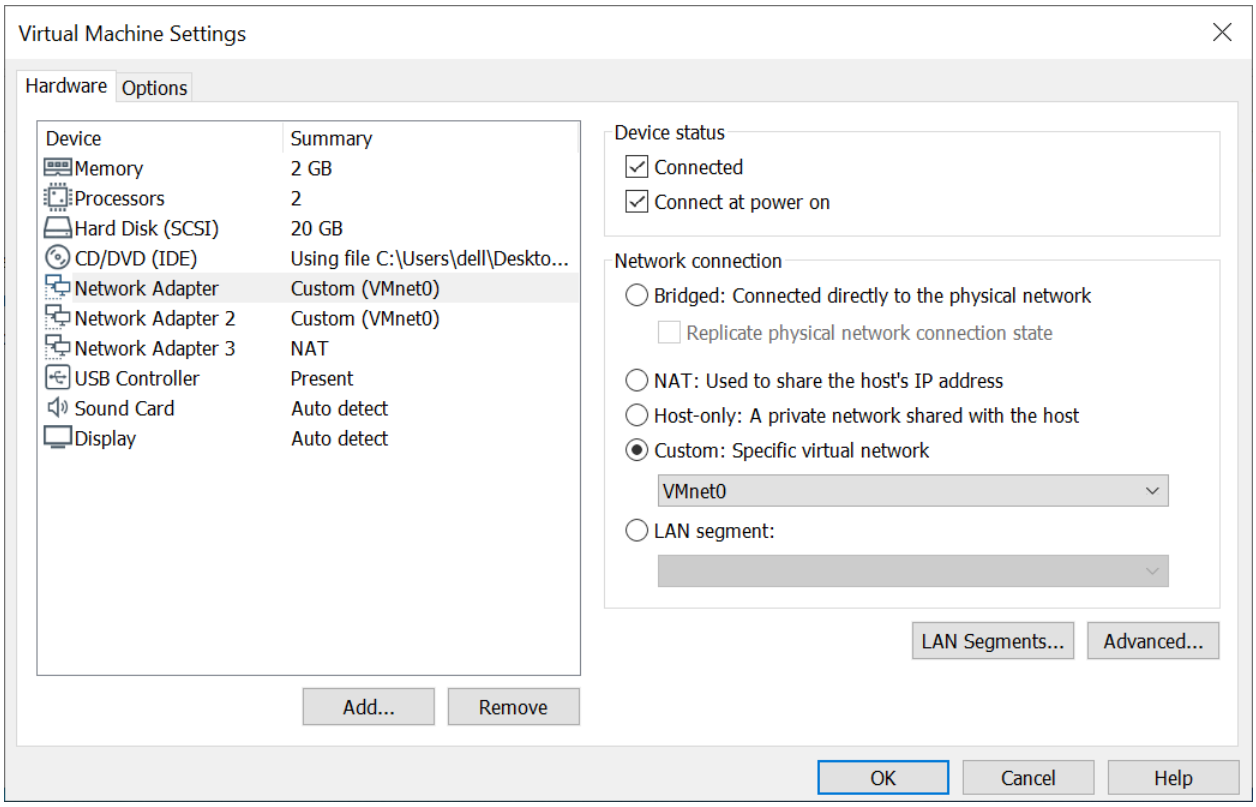

Рисунок 148 – Параметры виртуальной машины

15.1 Создание LAGG-интерфейса

Для создания LAGG-интерфейса необходимо выполнить следующие действия:

1. Перейти в подраздел настройки LAGG (**«Интерфейсы»** - **«Другие типы»** - **«LAGG»**).
2. В подразделе (см. Рисунок 149) нажать **кнопку «+Добавить»**.

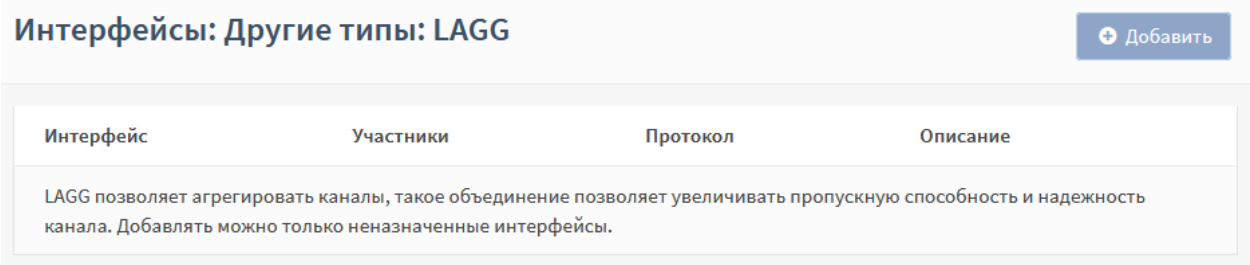

Рисунок 149 – Подраздел LAGG

3. В открывшейся форме (см. Рисунок 150) указать значения параметров:
   - **«Родительский интерфейс»** – «em0» и «em1»;
   - **«Протокол LAG»** – «FAILOVER», в данном режиме трафик проходит только через главный порт, указанный в интерфейсе первым. Если главный порт недоступен, используется следующий активный порт.
   - **«Описание»** – «Дублирование сетевых интерфейсов».

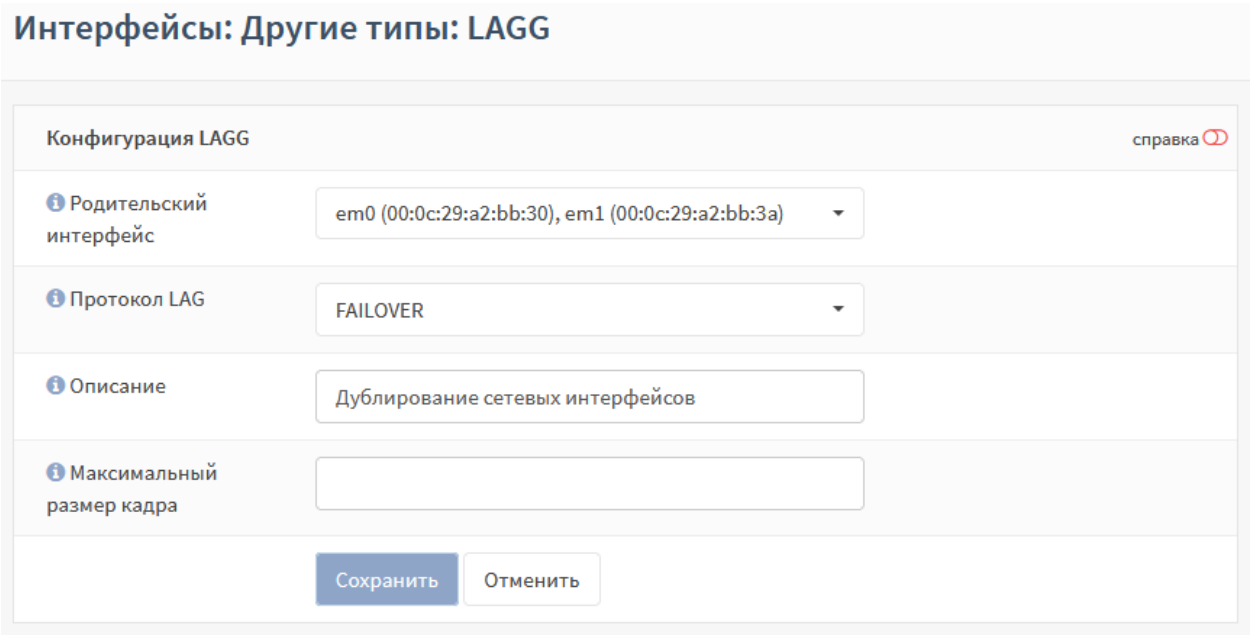

Рисунок 150 – Конфигурация LAGG

4. Нажать **кнопку «Сохранить»**.
5. В результате созданный LAGG-интерфейс будет отображен в списке (см. Рисунок 151).

Рисунок 151 – Список созданных интерфейсов

!Важно По умолчанию прием трафика осуществляется только через активный в данный момент интерфейс. Для того, чтобы прием трафика осуществлялся всеми членами LAGG-интерфейса, необходимо добавить параметр **«net.link.lagg.failover_rx_all»**. Без добавления данного параметра переключение между интерфейсами будет происходить некорректно.

Для добавления параметра необходимо выполнить следующие действия:

1. Перейти в подраздел параметров **ARMA IF** (**«Система»** - **«Настройки»** - **«Параметры»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать:
   - **«Параметр»** – «net.link.lagg.failover_rx_all»;
   - **«Значение»** – «1».

15.2 Настройка LAGG-интерфейса

Настройка сетевых интерфейсов осуществляется в подразделах интерфейса **«Назначение портов»** (см. Раздел 14.1) и **«[имя интерфейса]»** (см. Раздел 14.2).

Для настройки созданного LAGG-интерфейса необходимо выполнить следующие действия:

1. Перейти в подраздел назначения портов (**«Интерфейсы»** - **«Назначения портов»**).
2. Добавить новый интерфейс нажав **кнопку «+»** и выбрав в списке сетевых портов «lagg0 (Агрегация сетевых интерфейсов)».
3. Нажать **кнопку «Сохранить»**.
4. Перейти в созданный интерфейс (**«Интерфейсы»** - **«[OPT2]»**).
5. Установить флажок **«Включить интерфейс»** и выбрать значение параметра **«Тип конфигурации IPv4»** – **«DHCP»**.

6. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.
7. Результат настройки интерфейса **«[OPT2]»** будет отображен в подразделе общей информации об интерфейсах (**«Интерфейсы»** - **«Обзор»**) (см. Рисунок 152).

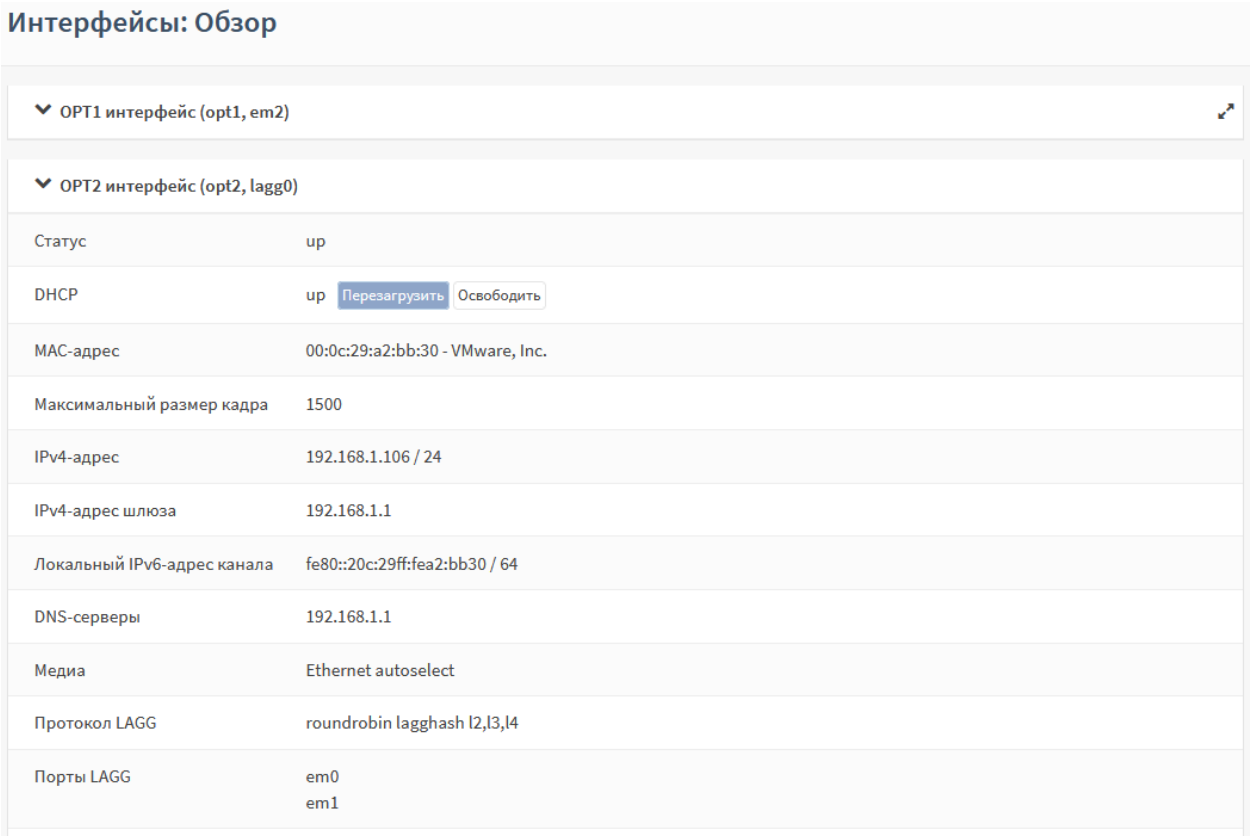

Рисунок 152 – Настроенный интерфейс

15.3 Проверка работы LAGG-интерфейса

Для проверки работы LAGG-интерфейса будет использоваться функция ping **ARMA IF** (**«Интерфейсы»** - **«Диагностика»** - **«Ping»**) (см. Рисунок 153).

Рисунок 153 – Функция «Ping»

Порядок проверки работы LAGG-интерфейса:

1. В форме функции **«Ping»** (см. Рисунок 153) задать следующие параметры:
   - **«Хост»** – «8.8.8.8»;
   - **«Протокол»** – «IPv4»;
   - **«IP-адрес источника»** – «OPT2»;
   - **«Количество»** – «3».
2. Нажать **кнопку «Ping»** – результат внизу страницы (см. Рисунок 154) свидетельствует о корректности настройки LAGG-интерфейса.

```
# /sbin/ping -S '192.168.1.200' -c '3' '8.8.8.8'
PING 8.8.8.8 (8.8.8.8) from 192.168.1.200: 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=46.217 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=47.309 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=53.642 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 46.217/49.056/53.642/3.273 ms
```

Рисунок 154 – Результат работы утилиты «Ping»

3. В интерфейсе гипервизора отключить один из сетевых интерфейсов, входящих в LAGG-интерфейс (см. Рисунок 155).

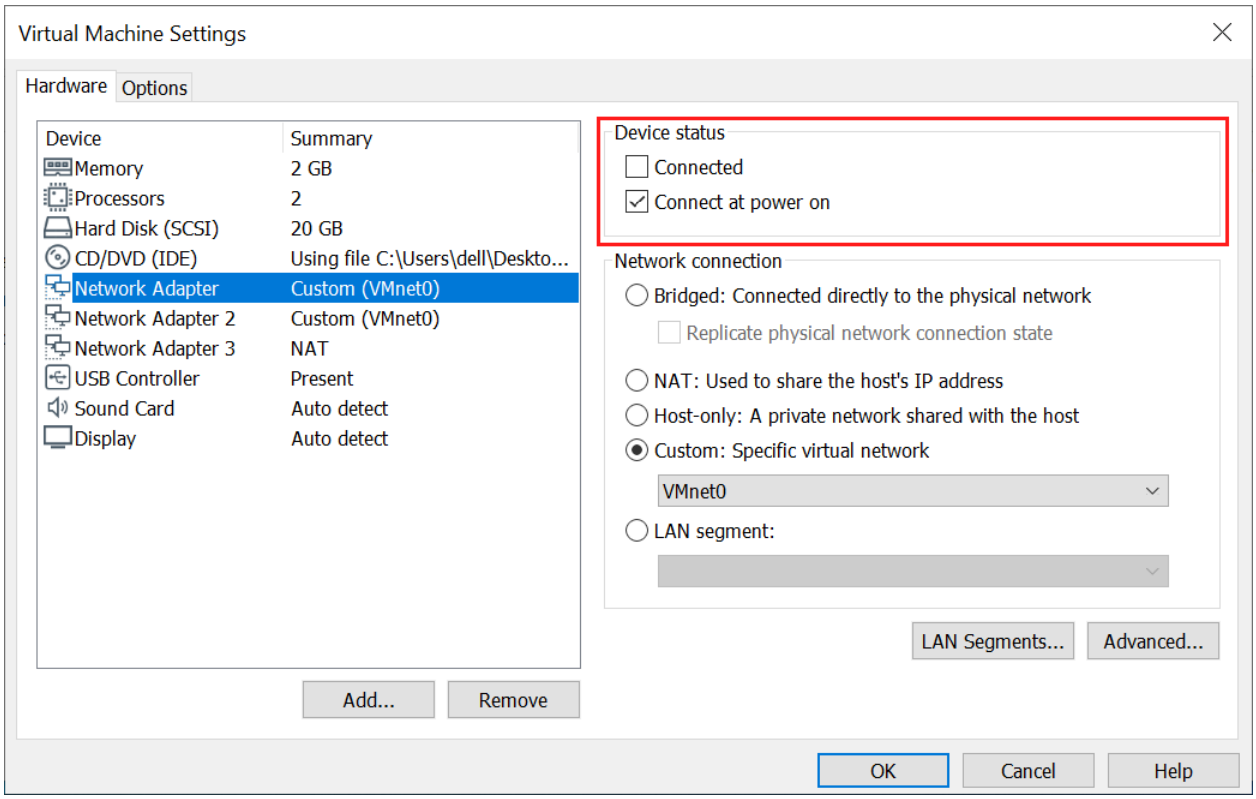

Рисунок 155 – Выключение сетевого интерфейса

4. Повторно нажать **кнопку «Ping»** – результат внизу страницы (см. Рисунок 156) свидетельствует о корректности работы LAGG-интерфейса в случае отключения одного из физических интерфейсов, входящих в его состав.

```
# /sbin/ping -S '192.168.1.200' -c '3' '8.8.8.8'
PING 8.8.8.8 (8.8.8.8) from 192.168.1.200: 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=46.217 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=47.309 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=53.642 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 46.217/49.056/53.642/3.273 ms
```

Рисунок 156 – Результат работы утилиты «Ping»

16 СЕТЕВОЙ МОСТ

Сетевой мост – это объединение различных сегментов сети передачи данных в единую сеть.

В **ARMA IF** добавление и настройка сетевых мостов производится в подразделе интерфейсов (**«Интерфейсы»** - **«Другие типы»** - **«Сетевые мосты»**). При создании сетевого моста в веб-интерфейсе **ARMA IF** создается новый сетевой интерфейс в ОС с именем «bridge» и порядковым номером, начиная с «0».

16.1 Пример настройки сетевого моста

Перед настройкой и включением сетевого моста необходимо изменить значения системных параметров:

- **«net.link.bridge.pfil_bridge»** – установить значение «1»;
- **«net.link.bridge.pfil_member»** – установить значение «0».

Для изменения параметров необходимо выполнить следующие действия:

1. Перейти в подраздел параметров **ARMA IF** (**«Система»** - **«Настройки»** - **«Параметры»**).
2. Нажать **кнопку «** **»** напротив изменяемого параметра и задать значение в поле **«Значение»**.
3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.

16.1.1 Создание сетевого моста

Для настройки и проверки работоспособности сетевого моста используется схема стенда, представленная на рисунке (см. Рисунок 157).

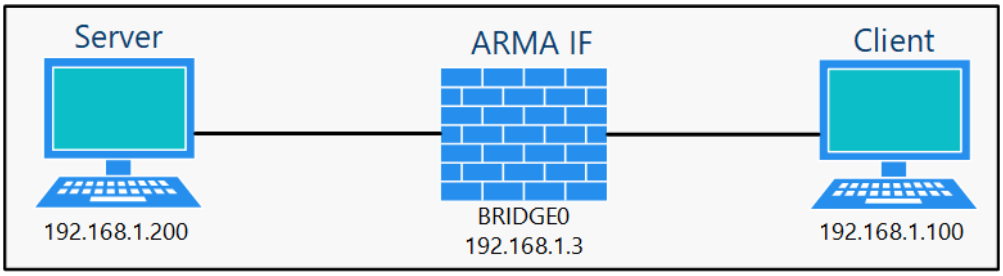

Рисунок 157 – Схема стенда для настройки сетевого моста

Для добавления сетевого моста необходимо выполнить следующие действия:

1. Перейти в подраздел настройки сетевых мостов (**«Интерфейсы»** - **«Другие типы»** - **«Сетевой мост»**) и нажать **кнопку «+Добавить»**.

2. В поле параметра **«Интерфейсы-участники»** указать интерфейсы, соединяемые с помощью моста – «LAN» и «WAN», а затем нажать **кнопку «Сохранить»** (см. Рисунок 158).

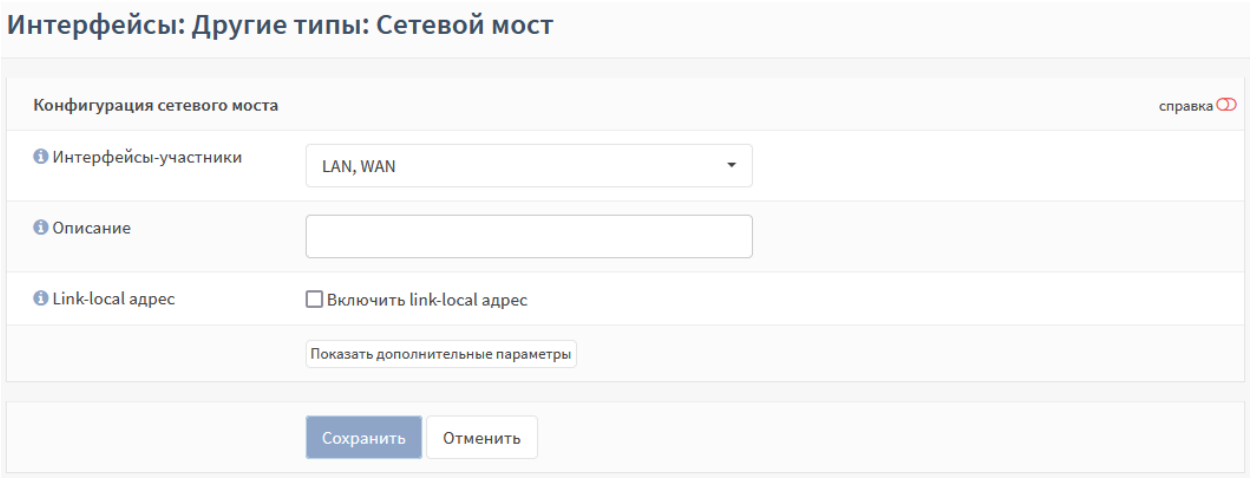

Рисунок 158 – Добавление сетевого моста

3. Добавленный сетевой мост будет отображен в общей таблице (см. Рисунок 159).

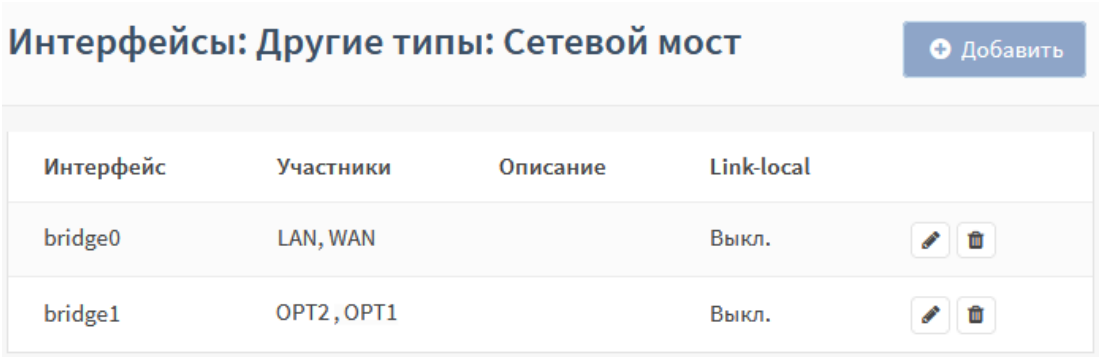

Рисунок 159 – Перечень созданных сетевых мостов

4. Перейти в подраздел назначения портов (**«Интерфейсы»** - **«Назначение портов»**), выбрать значение «bridge0» в параметре **«Новый интерфейс»**, ввести «BRIDGE0» в поле параметра **«Описание»** и нажать **кнопку «+»** для создания интерфейса (см. Раздел 14.1).

5. Перейти в настройки созданного сетевого интерфейса (**«Интерфейсы»** - **«[BRIDGE0]»**) и задать настройки согласно таблице (см. Таблица 27).

Таблица 27
Параметры интерфейса

Параметр	Значение
Включить	Значение установлено
Тип конфигурации IPv4	Статический IPv4

Параметр	Значение
Тип конфигурации IPv6	Отсутствует
IPv4-адрес	192.168.1.3/24

6. Нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

!Важно После настройки сетевого моста правила МЭ необходимо создавать для интерфейса сетевого моста. Правила МЭ для интерфейсов-участников сетевого моста будут игнорироваться.

16.1.2 Проверка настроенного сетевого моста

Перед проверкой настроенного моста необходимо добавить правило МЭ (см. Раздел 1.1.1) для интерфейса **«[BRIDGE0]»**, разрешающее прохождение трафика по протоколу ICMP.

Для проверки работоспособности необходимо выполнить следующие действия:

1. Перейти в настройки DHCP-сервера интерфейса «LAN» (**«Службы»** - **«DHCPv4»** -**«[LAN]»**) и выключить DHCP-сервер убрав флажок с параметра **«Включить DHCP-сервер на LAN интерфейсе»**, а затем нажав **кнопку «Сохранить»**.
2. На ПК **«Client»** открыть браузер, выполнить подключение к веб-интерфейсу **ARMA IF** по адресу сетевого интерфейса «BRIDGE0» – «https://192.168.1.3» и произвести аутентификацию в веб-интерфейсе.
3. Перейти в подраздел настроек LAN интерфейса (**«Интерфейсы»** - **«[LAN]»**), в поле **«Тип конфигурации IPv4»** выбрать **«Отсутствует»**, нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**. В подразделе настроек WAN (**«Интерфейсы»** - **«[WAN]»**) интерфейса повторить те же действия.
4. Перезагрузить **ARMA IF**. С ПК **«Client»** выполнить команду «ping» ПК **«Server»**. При правильной настройке сетевого моста команда выполнится успешно (см. Рисунок 160).

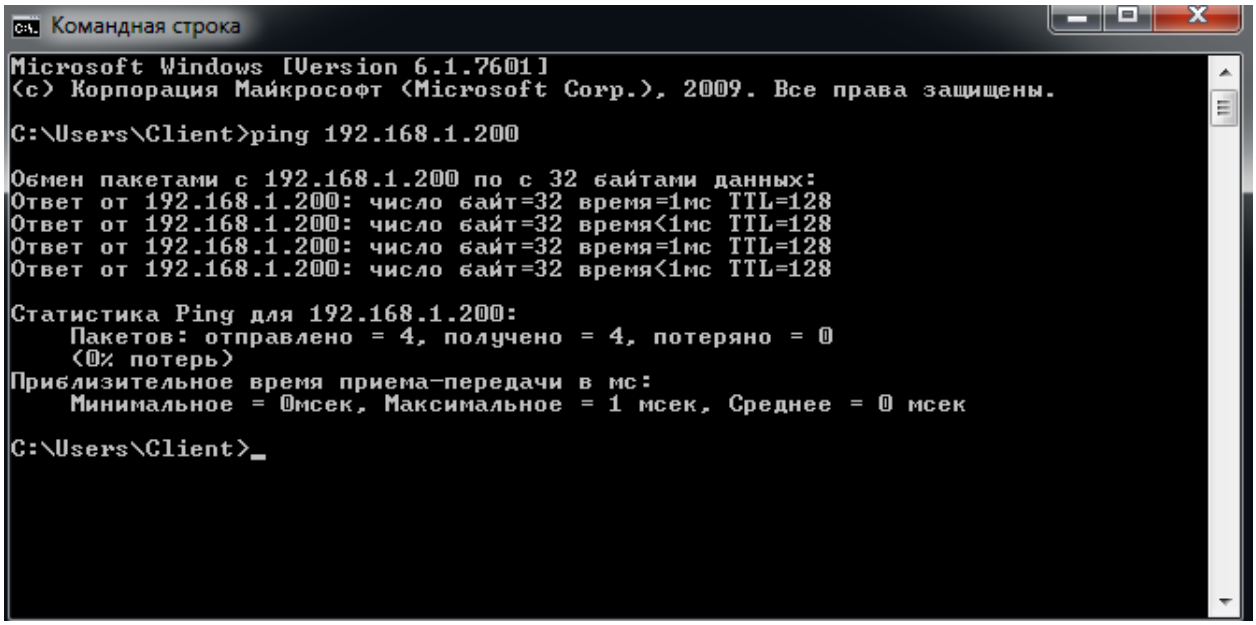

Рисунок 160 – Успешное выполнение команды ping

При добавлении сетевого моста, нажав **кнопку «Показать дополнительные параметры»** (см. Рисунок 158), будут доступны расширенные настройки, которые описаны в разделах 16.2 и 16.3 настоящего руководства.

16.2 Настройка RSTP/STP

Функция RSTP/STP предназначена для устранения петель (бесконечных повторов передачи трафика) в топологии сети. Протокол автоматически блокирует соединения, являющимися в данный момент для коммутаторов избыточными.

Для протокола RSTP/STP основными параметрами являются:

- **«Приоритет»** – используется для определения корневого коммутатора. Коммутатор с наименьшим значением параметра назначается корневым в топологии сети.
- **«Стоимость»** – используется для определения корневого порта коммутатора. Порт с наименьшим значением параметра назначается корневым. По умолчанию стоимость увеличивается с уменьшением скорости передачи порта.

Для проверки работоспособности протокола будет использоваться стенд с виртуальными машинами, представленный на рисунке (см. Рисунок 161).

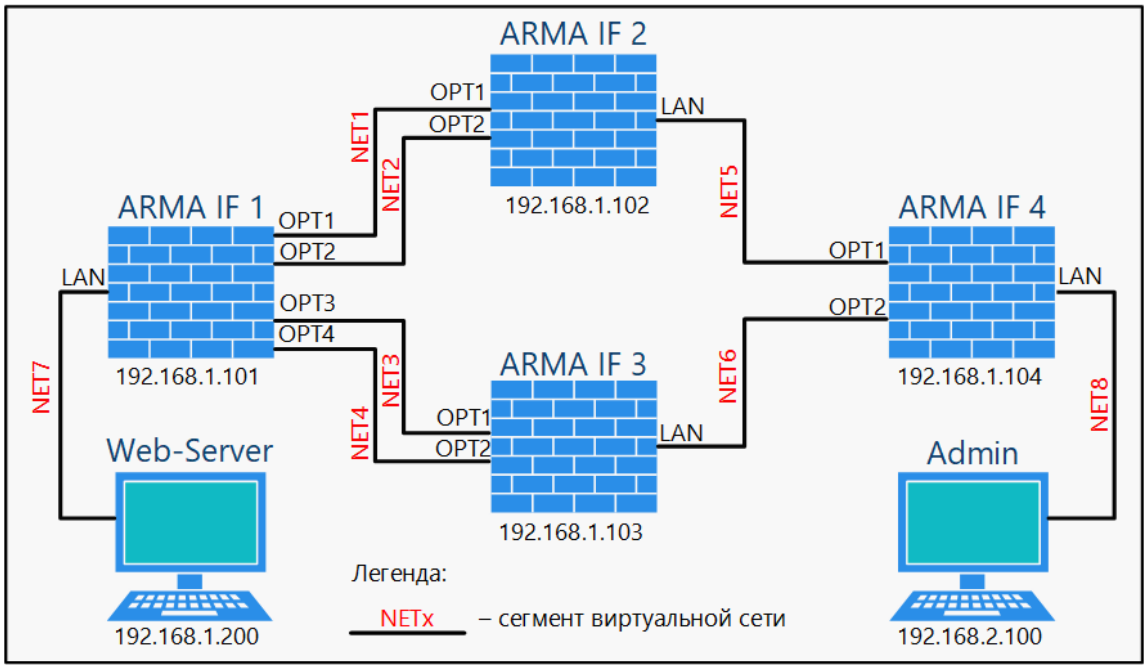

Рисунок 161 – Стенд для проверки RSTP

Порты **«WAN»** каждой ВМ с **ARMA IF** подключены к гипервизору для возможности управления через веб-интерфейс. На ВМ **«Web-Server»** запущено приложение веб-сервера.

Для настройки протокола RSTP/STP необходимо выполнить следующие действия:

1. На каждой ВМ с **ARMA IF** включить необходимые интерфейсы.
2. На каждой ВМ с **ARMA IF** объединить включенные интерфейсы в сетевой мост с указанием параметров RSTP/STP.
3. Задать созданным сетевым мостам IP-адреса в соответствии со схемой стенда (см. Рисунок 161).

Для проверки работоспособности протокола RSTP/STP будет использоваться утилита **«Wireshark»**, запущенная на ВМ **«Web-Server»**.

16.2.1 Включение интерфейсов

Для включения интерфейса требуется выполнить следующие действия:

1. Перейти в подраздел назначения портов (**«Интерфейсы»** - **«Назначения портов»**) создать новый интерфейс (см. Раздел 14.1). Имя интерфейса выбирается в соответствии со схемой стенда (см. Рисунок 161).
2. Перейти в раздел интерфейсов (**«Интерфейсы»**), выбрать созданный интерфейс, установить флажок **«Включить»** и, не изменяя другие параметры, нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»** (см. Раздел 14.2).

3. Повторить пункты 1-2 для каждого интерфейса каждой ВМ **ARMA IF**, указанных на схеме стенда (см. Рисунок 161).

16.2.2 Объединение интерфейсов в сетевой мост

Для настройки параметров RSTP/STP будут использоваться значения, указанные в таблице (см. Таблица 28).

Таблица 28
Параметры RSTP/STP

Параметр	ARMA IF 1	ARMA IF 2	ARMA IF 3	ARMA IF 4
Протокол	RSTP	RSTP	RSTP	RSTP
STP-интерфейсы	BRIDGE0	BRIDGE0	BRIDGE0	BRIDGE0
	LAN	LAN	LAN	LAN
	OPT1	OPT1	OPT1	OPT1
	OPT2			
	OPT3	OPT2	OPT2	OPT2
	OPT4			
Приоритет	4096	8192	12288	16384

Для объединения интерфейсов необходимо выполнить следующие действия:

1. Перейти в подраздел настройки сетевых мостов (**«Интерфейсы»** - **«Другие типы»** - **«Сетевой мост»**) и создать сетевой мост (см. Раздел 16.1.1) указав в качестве интерфейсов-участников интерфейсы ВМ **ARMA IF** в соответствии со схемой стенда (см. Рисунок 161). Для каждой ВМ **ARMA IF** указываются все перечисленные на схеме интерфейсы.
2. Нажать **кнопку «Показать дополнительные параметры»** и, в открывшейся форме (см. Рисунок 162), в блоке **«Протокол основного дерева (RSTP/STP)»**, установить флажок **«Включить»**, затем указать параметры RSTP/STP в соответствии с таблицей (см. Таблица 28) и нажать **кнопку «Сохранить»**.

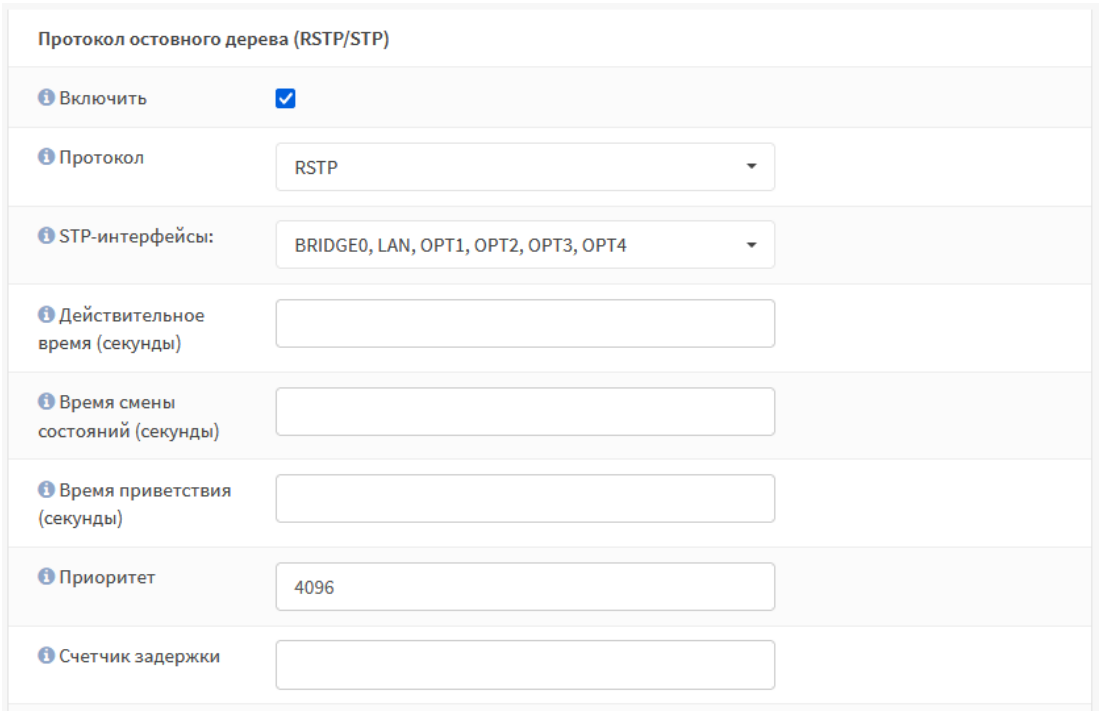

Рисунок 162 – Включение протокола RSTP/STP

3. Для сетевого моста ВМ **«ARMA IF1»** дополнительно указать значения в полях каждого интерфейса для параметра **«Приоритет»** (см. Рисунок 163):
   - **«LAN»** – 112.
   - **«OPT1»** – 96.
   - **«OPT2»** – 80.
   - **«OPT3»** – 48.
   - **«OPT4»** – 64.

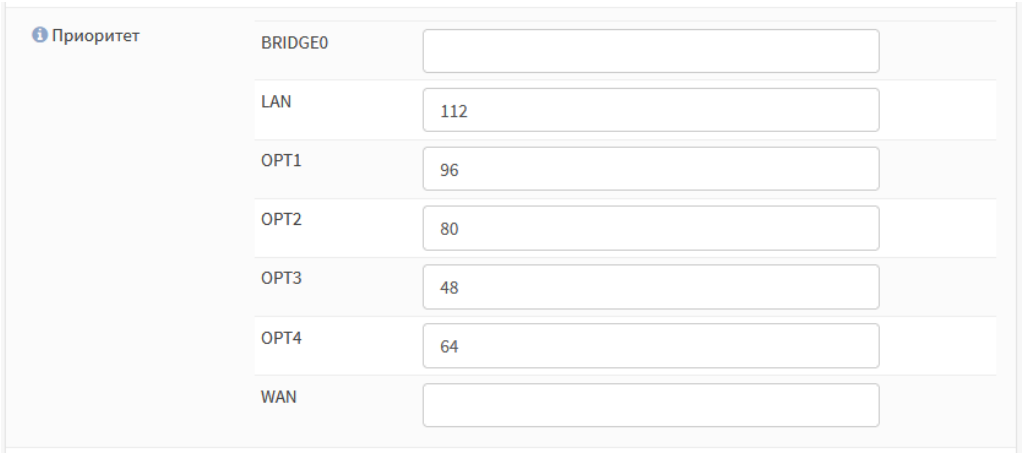

Рисунок 163 – Указание приоритета для сетевых интерфейсов

4. Для сетевого моста ВМ **«ARMA IF4»** дополнительно указать значения в полях каждого интерфейса для параметра **«Приоритет»**:
   - **«OPT1»** – 16.

- **«OPT2»** – 32.

16.2.3 Настройка сетевого моста

Созданные сетевые мосты необходимо настроить аналогично алгоритму, указанному в разделе 16.1.1 настоящего руководства.

IP-адреса для настройки представлены на схеме стенда (см. Рисунок 161).

16.2.4 Проверка работы RSTP/STP

Для проверки работоспособности функции необходимо выполнить следующие действия:

1. На ВМ **«Admin»** запустить веб-браузер и перейти по адресу «192.168.1.200» (см. Рисунок 164) – это позволит проверить правильность настройки стенда.

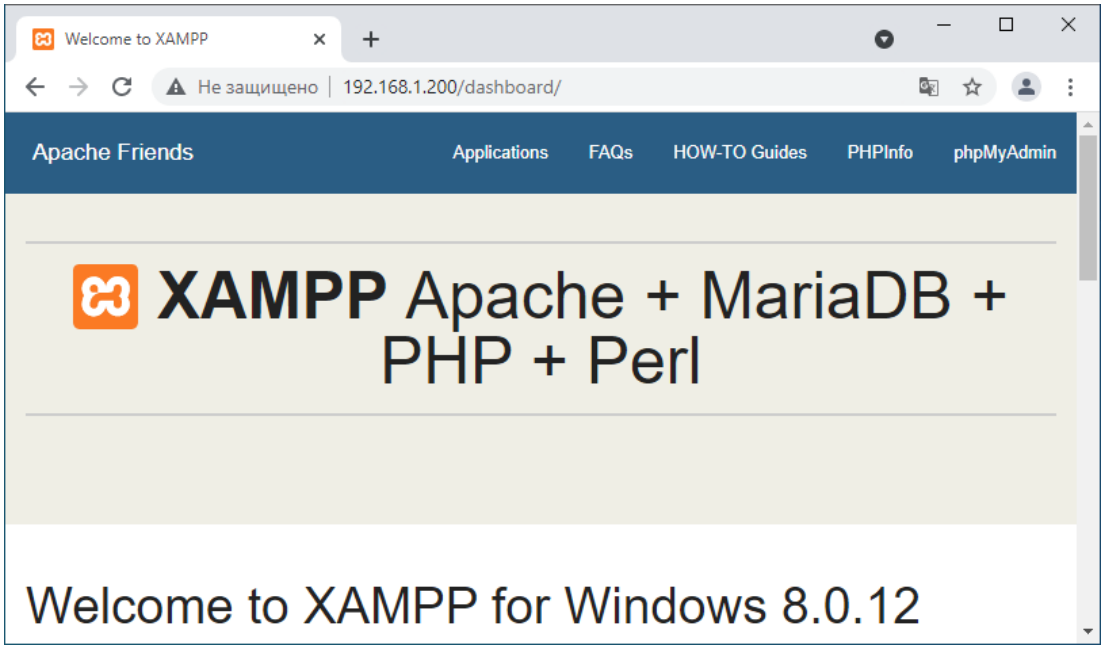

Рисунок 164 – Доступ к веб-серверу с ПК администратора

2. На ВМ **«Web-Server»** запустить программу «Wireshark» и выполнить захват трафика на сетевом интерфейсе (см. Рисунок 165). В списке захваченных пакетов будет присутствовать STP-трафик.

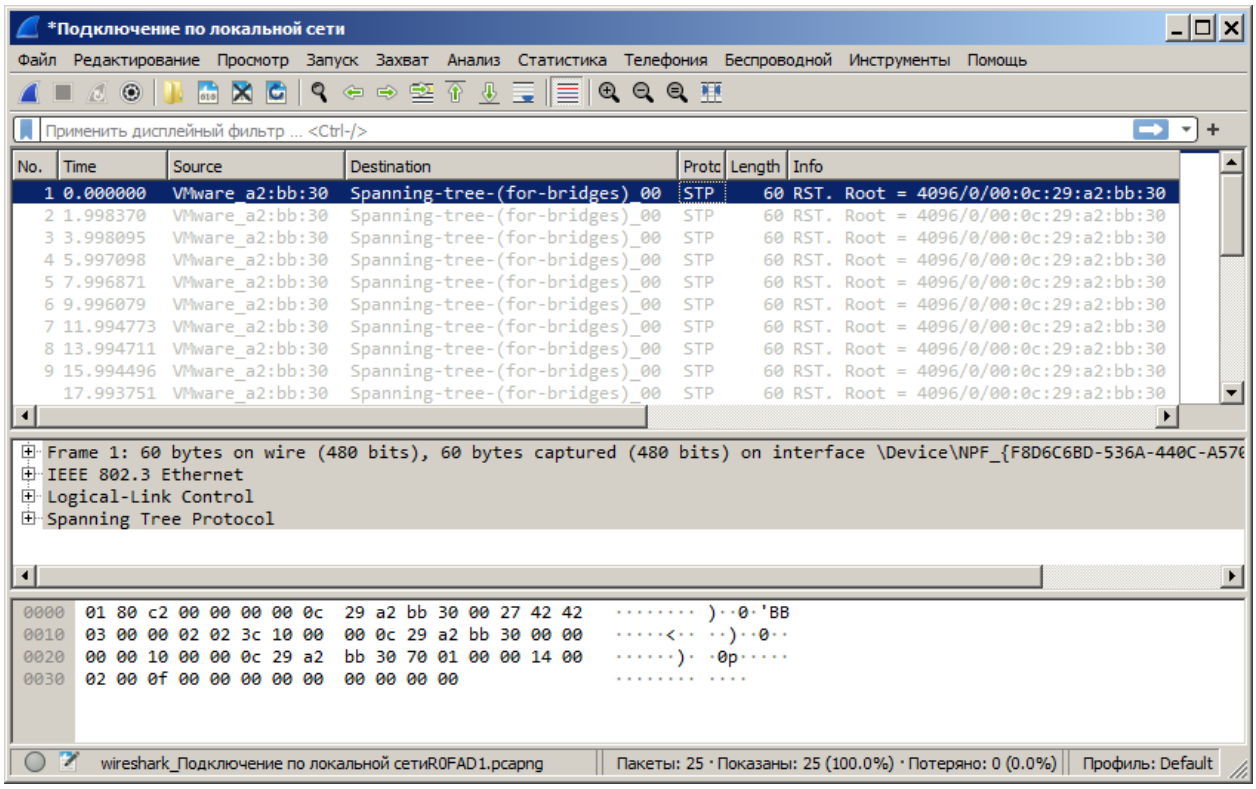

Рисунок 165 – Трафик с STP-пакетами

3. На ВМ **«ARMA IF1»** перейти в настройки сетевого моста (**«Интерфейсы»** - **«Другие типы»** - **«Сетевой мост»**), нажать **кнопку «Дополнительные настройки»** и отключить функцию RSTP/STP убрав соответствующий флажок.
4. На ВМ **«Web-Server»** запустить программу «Wireshark» и выполнить захват трафика на сетевом интерфейсе (см. Рисунок 166). В списке захваченных пакетов будет присутствовать постоянно растущий трафик широковещательной рассылки, указывающий на присутствие петли в топологии сети.

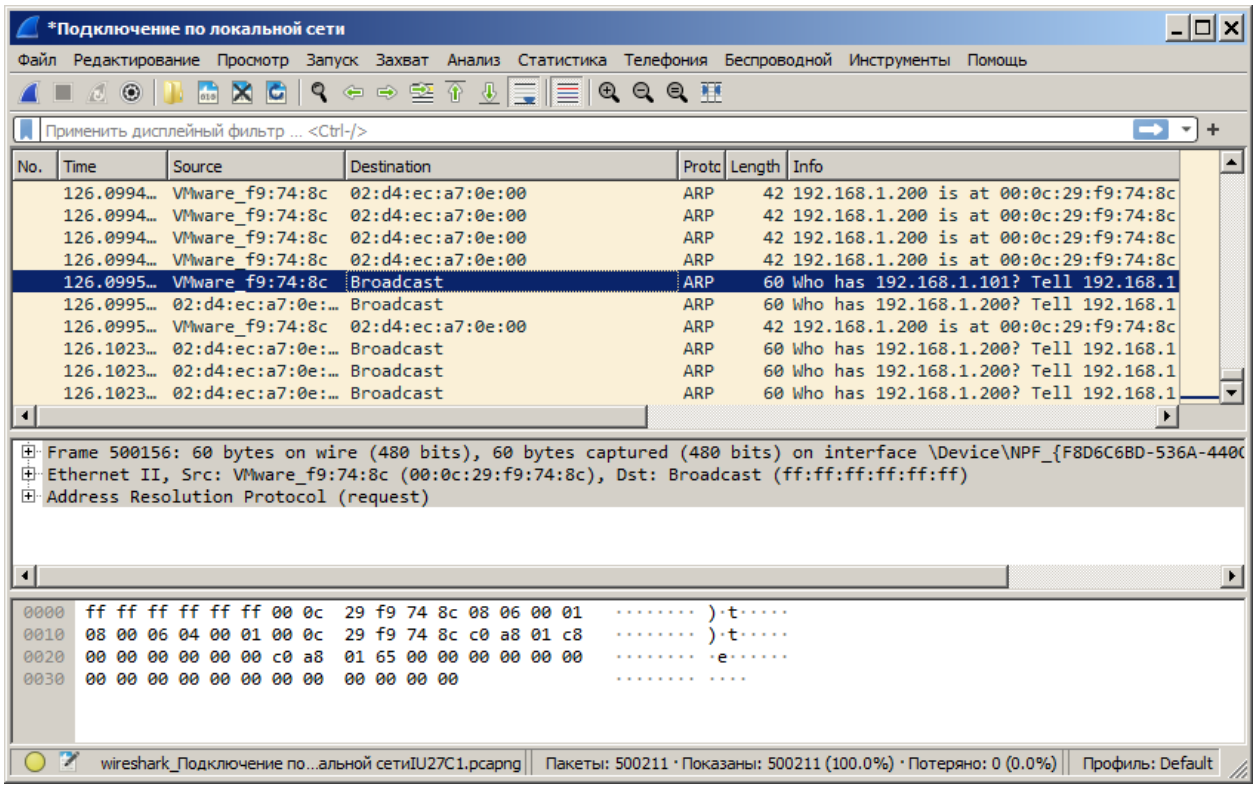

Рисунок 166 – Трафик широковещательной рассылки

16.3 Настройка SPAN

Функция SPAN предназначена для зеркалирования трафика, проходящего через сетевой мост. Функция используется для анализа трафика и должна поддерживаться принимающим устройством, например, коммутатором.

В качестве примера настройки зеркалирования трафика будет использоваться схема стенда, представленная на рисунке (см. Рисунок 167), со следующими параметрами:

- интерфейсы «OPT1» и «LAN» объединены в сетевой мост;
- интерфейс «OPT2» используется в качестве порта SPAN.

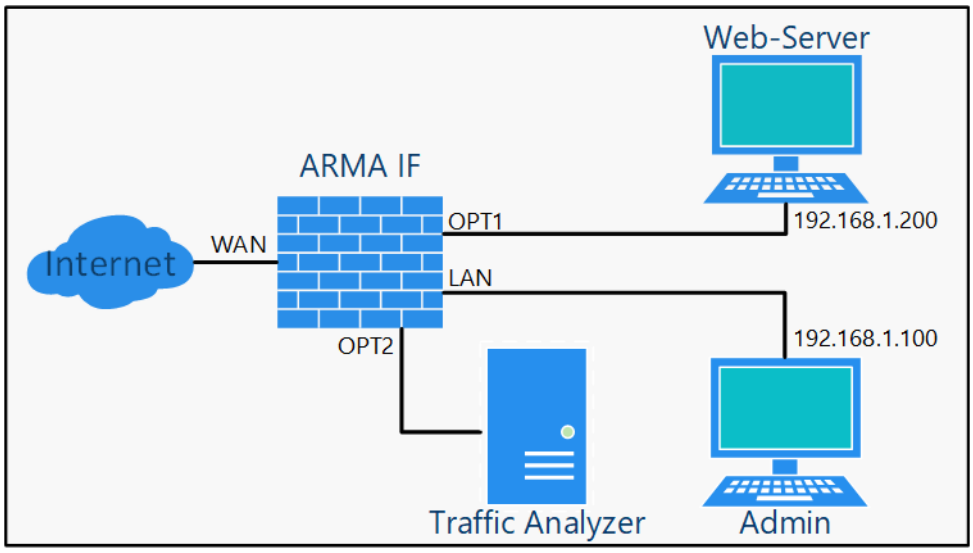

Рисунок 167 – Стенд для настройки зеркалирования трафика

Для настройки зеркалирования необходимо выполнить следующие действия:

1. Включить интерфейс «OPT2».
2. Объединить интерфейсы «OPT1» и «LAN» в сетевой мост с указанием порта SPAN.
3. Настроить созданный сетевой мост.

Для проверки наличия трафика на интерфейсе «OPT2» будет использоваться утилита «Wireshark», запущенная на ПК **«Traffic Analyser»**.

16.3.1 Включение интерфейса «OPT2»

Для включения интерфейса необходимо выполнить следующие действия:

1. Перейти в подраздел назначения портов (**«Интерфейсы»** - **«Назначения портов»**) и создать новый интерфейс с именем «OPT2» (см. Раздел 14.1).
2. В разделе интерфейсов (**«Интерфейсы»**) выбрать созданный интерфейс, установить флажок **«Включить»**, не изменяя другие параметры нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»** (см. Раздел 14.2).

16.3.2 Объединение интерфейсов «OPT1» и «LAN» в сетевой мост

Для объединения интерфейсов необходимо выполнить следующие действия:

1. Перейти в подраздел настройки сетевых мостов (**«Интерфейсы»** - **«Другие типы»** - **«Сетевой мост»**) и создать сетевой мост (см. Раздел 16.1.1), указав в качестве интерфейсов-участников порты «OPT1» и «LAN».
2. Нажать **кнопку «Показать дополнительные параметры»** и, в открывшейся форме, указать «OPT2» в параметре **«Порт SPAN»** (см. Рисунок 168), затем нажать **кнопку «Сохранить»**.

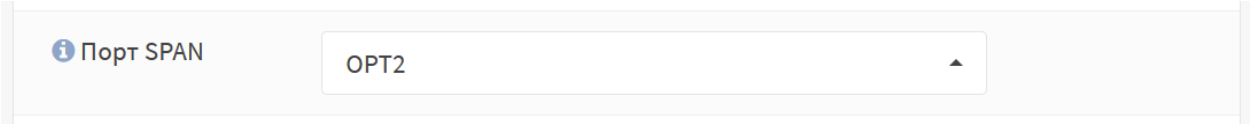

Рисунок 168 – Выбор порта SPAN

Для корректной работы режима SPAN необходимо изменить значения следующих параметров (**«Система»** - **«Настройки»** - **«Параметры»**):

- **«net.link.bridge.pfil_member»** – «0»;
- **«net.link.bridge.pfil_bridge»** – «0».

Данные значения параметров отключают фильтрацию со стороны **ARMA IF** для коммутируемых кадров.

Для изменения параметров необходимо выполнить следующие действия:

1. Перейти в подраздел параметров **ARMA IF** (**«Система»** - **«Настройки»** - **«Параметры»**).
2. Нажать **кнопку «** **»** напротив изменяемого параметра и задать значение в поле **«Значение»**.
3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.

16.3.3 Настройка сетевого моста

Созданный сетевой мост необходимо настроить аналогично алгоритму, указанному в разделе 16.1.1 настоящего руководства.

В результате настройки весь трафик, проходящий по созданному сетевому мосту, будет зеркалироваться на интерфейс «OPT2».

Настройка принимающего трафик устройства производится в соответствии с инструкцией к данному устройству и не описывается в данном документе.

16.3.4 Проверка зеркалирования трафика

Для проверки зеркалирования трафика необходимо выполнить следующие действия:

1. На ПК **«Admin»** запустить веб-браузер и перейти по адресу «192.168.1.200» (см. Рисунок 169).

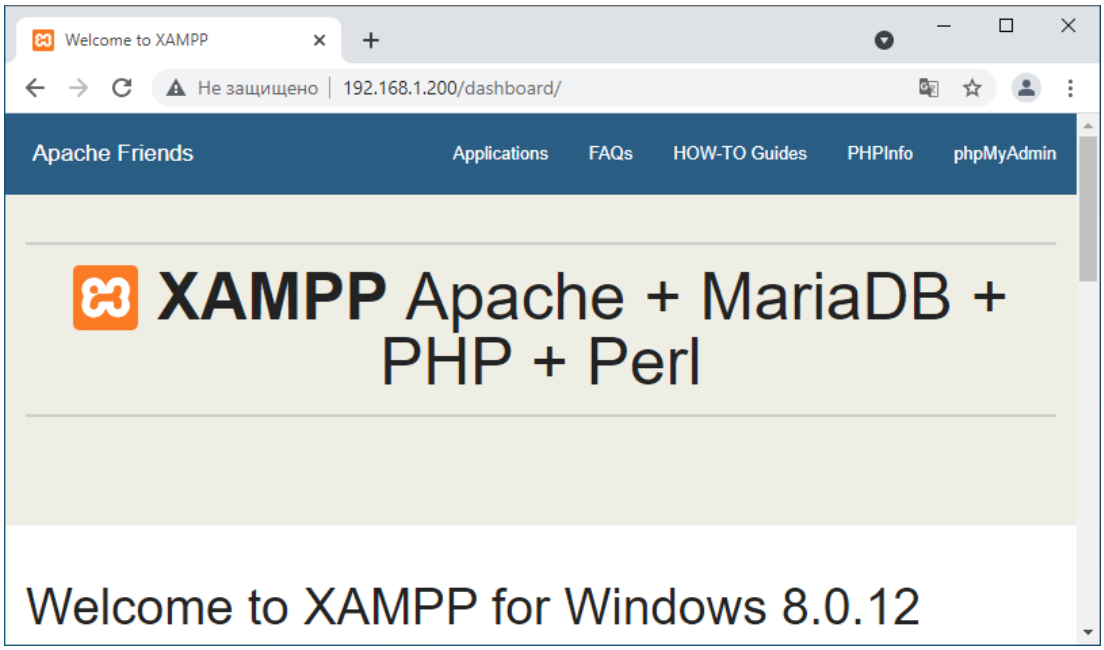

Рисунок 169 – Доступ к веб-серверу с ПК администратора

2. На ПК **«Traffic Analyzer»** запустить программу «Wireshark» и выполнить анализ трафика с фильтром по IP (см. Рисунок 170).

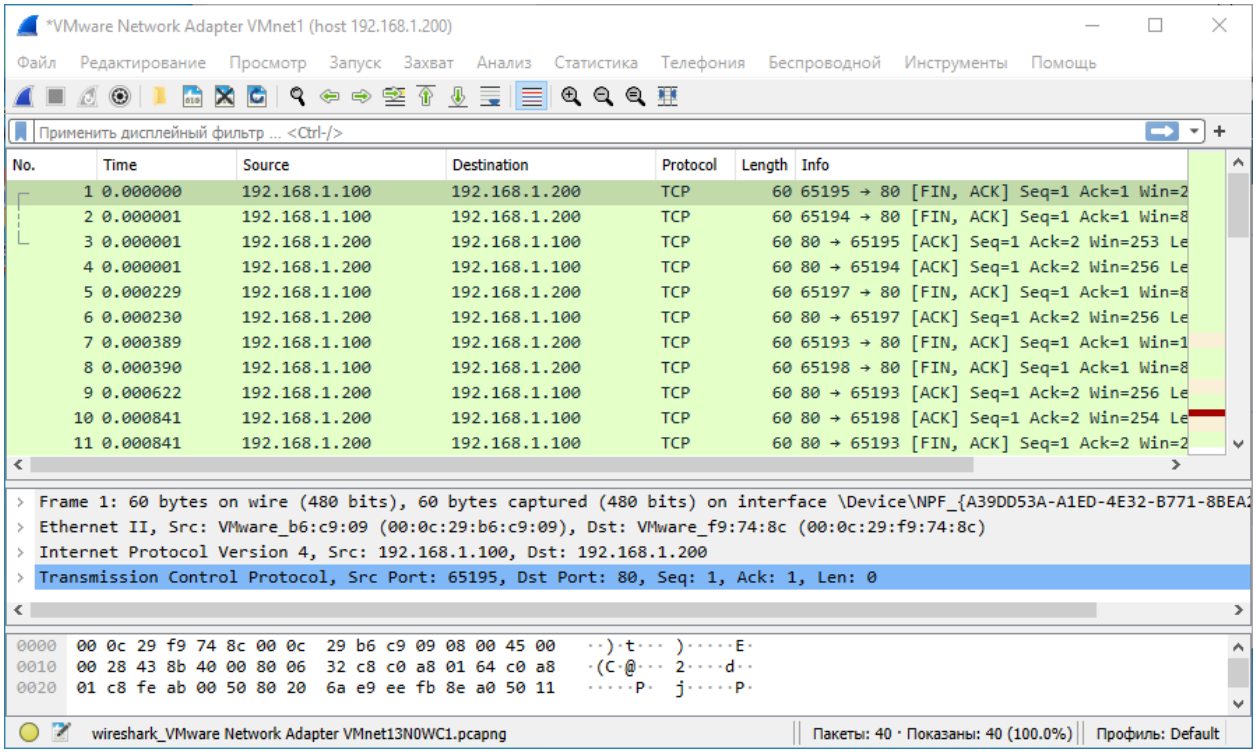

Рисунок 170 – Зеркалированный трафик на интерфейсе «OPT2»

17 VLAN

VLAN – это технология, позволяющая строить виртуальные сети с независимой от физических устройств топологией.

ARMA IF поддерживает технологию VLAN по стандарту IEEE 802.1Q.

!Важно При использовании технологии VLAN коммутатор также должен поддерживать стандарт IEEE 802.1Q и быть настроен соответствующим образом.

Для настройки и проверки работоспособности технологии VLAN используется схема стенда, представленная на рисунке (см. Рисунок 171).

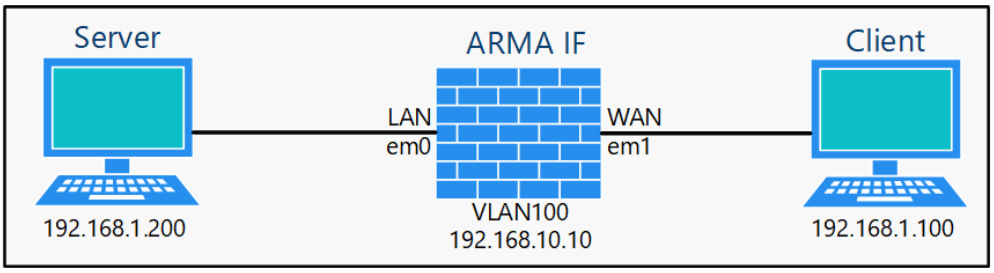

Рисунок 171 – Схема стенда для настройки VLAN

17.1 Создание VLAN

Для создания интерфейса VLAN необходимо выполнить следующие действия:

1. Перейти в подраздел настройки VLAN (**«Интерфейсы»** - **«Другие типы»** - **«VLAN»**) и нажать **кнопку «+Добавить»**.
2. В параметре **«Родительский интерфейс»** выбрать сетевой интерфейс «em1», установить значение уникального идентификатора равным «100» в поле параметра **«Тег VLAN»**, оставить по умолчанию значение параметра **«Приоритет VLAN»** и нажать **кнопку «Сохранить»** (см. Рисунок 172).

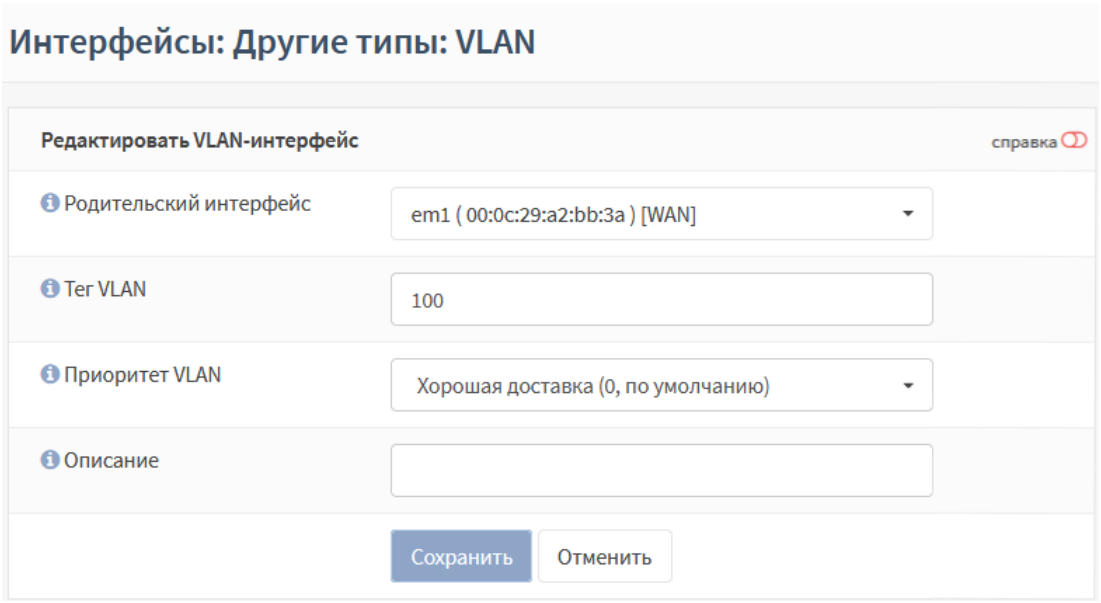

Рисунок 172 – Создание интерфейса VLAN

3. Перейти в подраздел назначения портов (**«Интерфейсы»** - **«Назначение портов»**), выбрать значение «виртуальная локальная сеть 100 на em1()» в параметре **«Новый интерфейс»**, ввести «VLAN100» в поле параметра **«Описание»** и нажать **кнопку «+»** для создания интерфейса (см. Раздел 14.1).
4. Перейти в настройки созданного сетевого интерфейса (**«Интерфейсы»** - **«VLAN100»**) и задать настройки согласно таблице (см. Таблица 29).

Таблица 29
Параметры интерфейса

Параметр	Значение
Включить	Значение установлено
Тип конфигурации IPv4	Статический IPv4
Тип конфигурации IPv6	Отсутствует
IPv4-адрес	192.168.10.10/24

5. Нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

17.2 Проверка работы созданного VLAN

Для проверки работоспособности настроенного интерфейса «VLAN100» необходимо выполнить следующие действия:

1. Перейти в подраздел диагностики захватом пакетов (**«Интерфейсы»** - **«Диагностика»** - **«Захват пакетов»**).
2. Изменить следующие параметры:

- **«Интерфейс»** – «WAN»;
- **«Смешанный режим»** – включен;
- **«Количество»** – «0», для отключения предела захваченных пакетов;

остальные параметры оставить без изменения и нажать **кнопку «Запустить»**.

3. На ПК **«Server»** выполнить команду «ping» до IP-адреса «192.168.10.100» – результат будет неуспешным.
4. Остановить захват пакетов, нажав **кнопку «Остановить»** в подразделе диагностики захватом пакетов (**«Интерфейсы»** - **«Диагностика»** - **«Захват пакетов»**) и скачать захваченные пакеты (см. Рисунок 173).
5. Скачать захваченные пакеты нажав **левой кнопкой мыши** на имя файла внизу подраздела (см. Рисунок 173) и следуя указаниям веб-браузера.

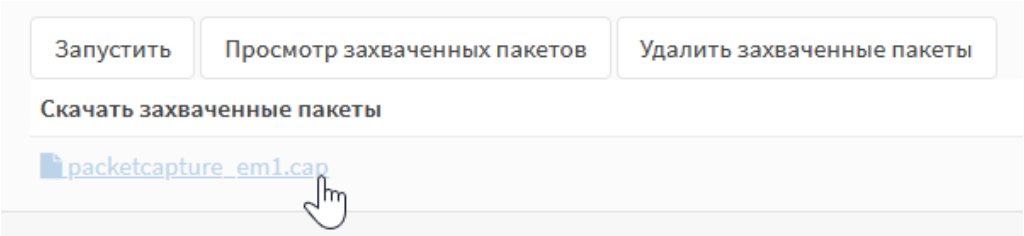

Рисунок 173 – Остановка захвата пакетов

6. В ПО «Wireshark» открыть скачанный файл, в поле фильтра ввести – «vlan» и нажать **клавишу «Enter»**. В списке захваченных пакетов будут присутствовать пакеты с полем «802.1Q Virtual LAN, ID: 100».

17.3 VXLAN

VXLAN – это технология сетевой виртуализации, позволяющая наложения виртуализированных сетей 2 уровня на сети 3 уровня согласно rfc7348.

Настроенные интерфейсы VXLAN отображены в подразделе настройки VXLAN (**«Интерфейсы»** - **«Другие типы»** - **«VXLAN»**) (см. Рисунок 174).

В подразделе доступны следующие команды:

- **кнопка «** **»** – открывает форму «Редактировать VxLan» (см. Рисунок 175) для создания нового VXLAN.
- **кнопка «** **»** – открывает форму «Редактировать VxLan» (см. Рисунок 175) для редактированного ранее созданного VXLAN.
- **кнопка «** **»** – удаляет ранее созданный VXLAN.
- **кнопка «** **»** – открывает форму «Редактировать VxLan» (см. Рисунок 175) для создания нового VXLAN путём копирования раннее созданного.

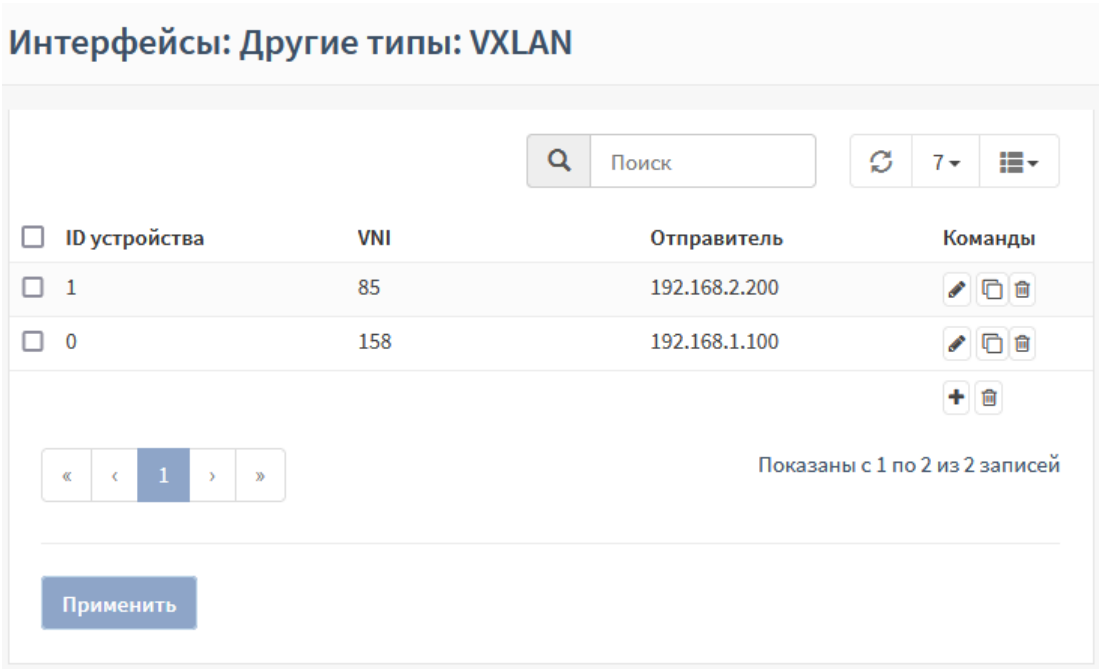

Рисунок 174 – Перечень VXLAN

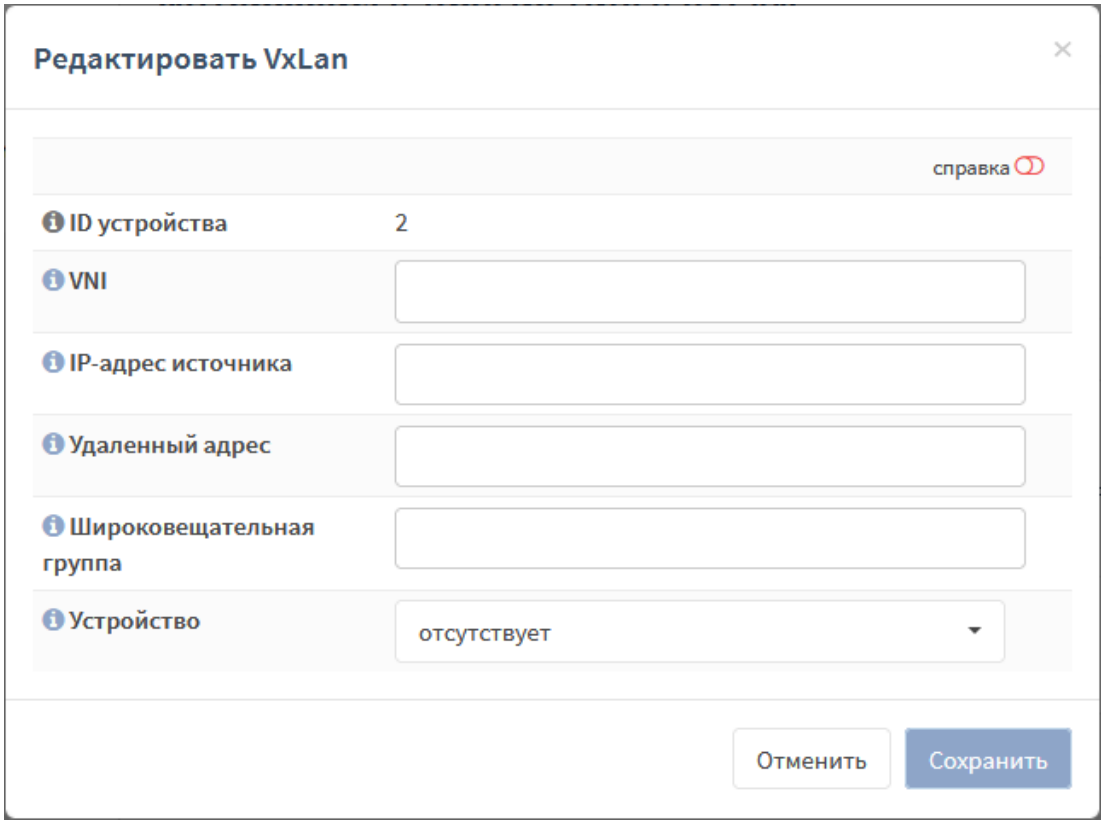

Рисунок 175 – Форма редактирования VXLAN

18 ПРОКСИ

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

В качестве примера настройки прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. Рисунок 176) со следующими параметрами прокси-сервера:

- интерфейс хостов локальной сети – «LAN», подсеть 192.168.1.0/24;
- работа в прозрачном режиме для HTTP и HTTPS;
- кэширование данных включено;
- работает без аутентификации;
- номер порта для HTTP – «3128», номера порта для HTTPS – «3129»;
- ограничение доступа к ресурсам настроено для сайта «mail.ru» и согласно внешнему списку доступа «Blacklists UT1»;
- используется встроенный в **ARMA IF** антивирус для проверки веб-трафика.

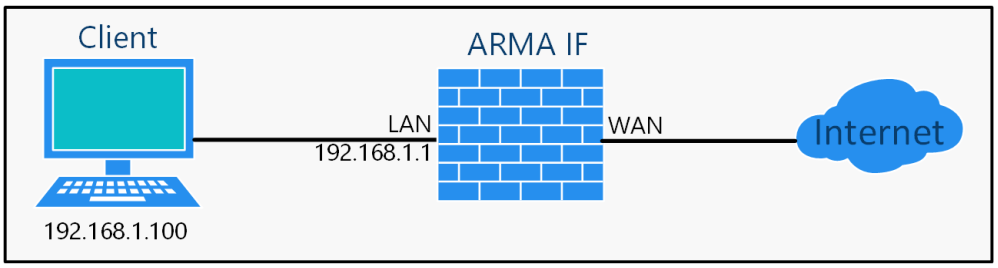

Рисунок 176 – Схема стенда для настройки прокси-сервера

До момента настройки прокси-сервера подключение на ПК **«Client»** к сети Интернет отсутствует (см. Рисунок 177).

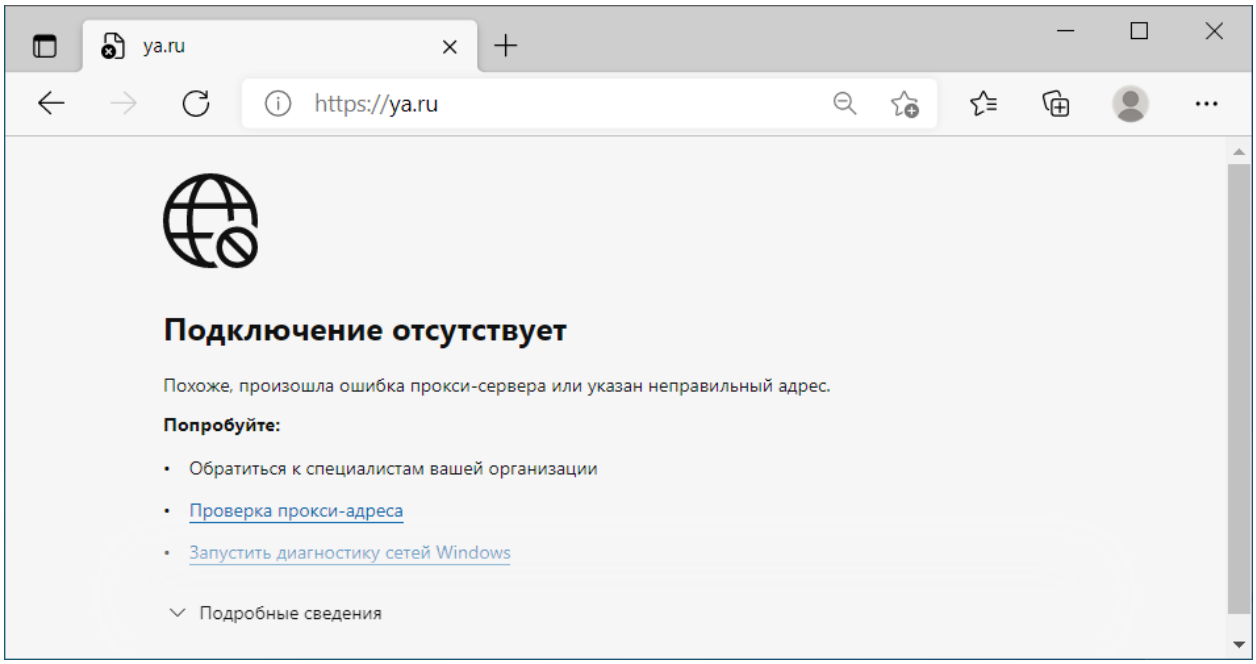

Рисунок 177 – Отсутствие подключения к сети Интернет

18.1 Настройка кэширующего прокси-сервера

Для настройки кэширующего прокси-сервера необходимо выполнить следующие шаги:

1. Создать доверенный центр сертификации.
2. Настроить прокси-сервер.
3. Создать правила NAT для прокси-сервера.

18.1.1 Создание доверенного центра сертификации

Для корректной работы прокси-сервера с HTTPS-трафиком необходимо создать доверенный центр сертификации и добавить данный центр клиентам прокси-сервера.

В примере доверенный центр сертификации создается с параметрами, приведёнными в таблице (см. Таблица 30).

Таблица 30
Значения параметров центра сертификации

Параметр	Значение
Описательное имя	ARMA CA
Метод	Создать внутренний центр сертификации
Длина ключа (биты)	2048
Digest алгоритм	SHA256

Параметр	Значение
Срок жизни (дней)	365
Код страны	RU (Russia)
Область	MO
Город	Москва
Организация	InfoWatch
Email адрес	admin@infowatch.ru
Простое имя	arma-ca

Параметры **«Описательное имя»**, **«Код страны»**, **«Область»**, **«Город»**, **«Организация»**, **«Email адрес»**, **«Простое имя»** указаны справочно.

Для создания доверенного центра сертификации необходимо выполнить следующие действия:

1. Перейти в подраздел полномочий (**«Система»** - **«Доверенные сертификаты»** - **«Полномочия»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать параметры из таблицы (см. Таблица 30).
4. Нажать **кнопку «Сохранить»**.

Для добавления доверенного центра сертификации клиентам прокси-сервера необходимо предварительно экспортировать сертификат созданного центра сертификации нажав **кнопку «Экспортировать сертификат CA»** (см. Рисунок 178) в подразделе полномочий (**«Система»** - **«Доверенные сертификаты»** - **«Полномочия»**).

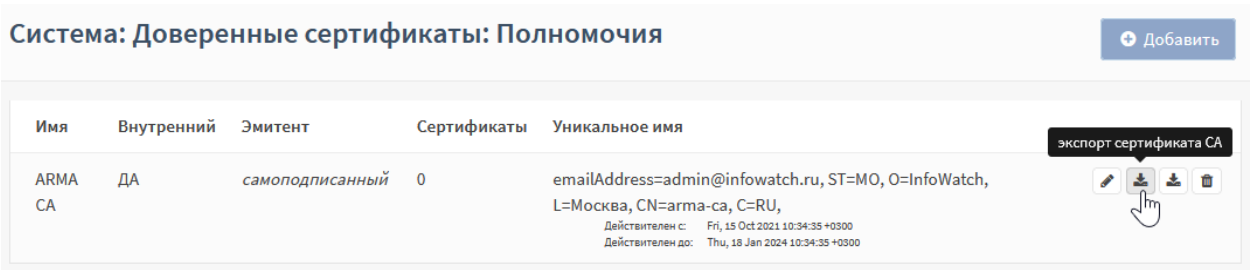

Рисунок 178 – Экспорт сертификата CA

Установка сертификата клиентам прокси-сервера предполагается произвольным способом в зависимости от используемого оборудования – через групповые политики, с помощью браузера и т.д.

18.1.2 Настройка прокси-сервера

Для настройки прокси-сервера необходимо выполнить следующие действия:

1. Перейти в подраздел администрирования прокси-сервера (**«Службы»** - **«Веб-прокси»** - **«Администрирование»**) и установить флажок в параметре **«Включить прокси»** на вкладке **«Основные настройки»** (см. Рисунок 179).

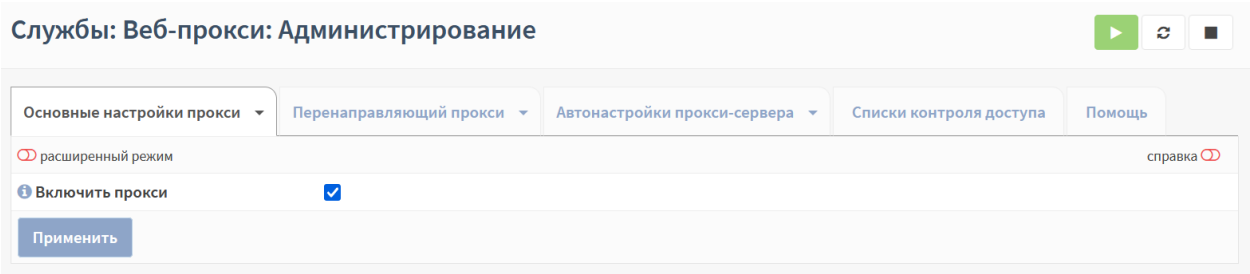

Рисунок 179 – Основные настройки прокси

2. Раскрыть вкладку **«Основные настройки прокси»** нажав **кнопку «** ▼ **»** и выбрать **«Настройки локального кэша»** (см. Рисунок 180).

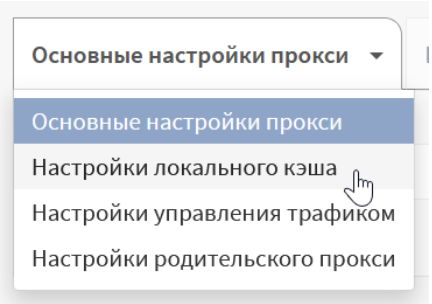

Рисунок 180 – Выбор настроек прокси-сервера

3. В открывшейся форме (см. Рисунок 181) установить флажок для параметра **«Включить локальный кэш»**.

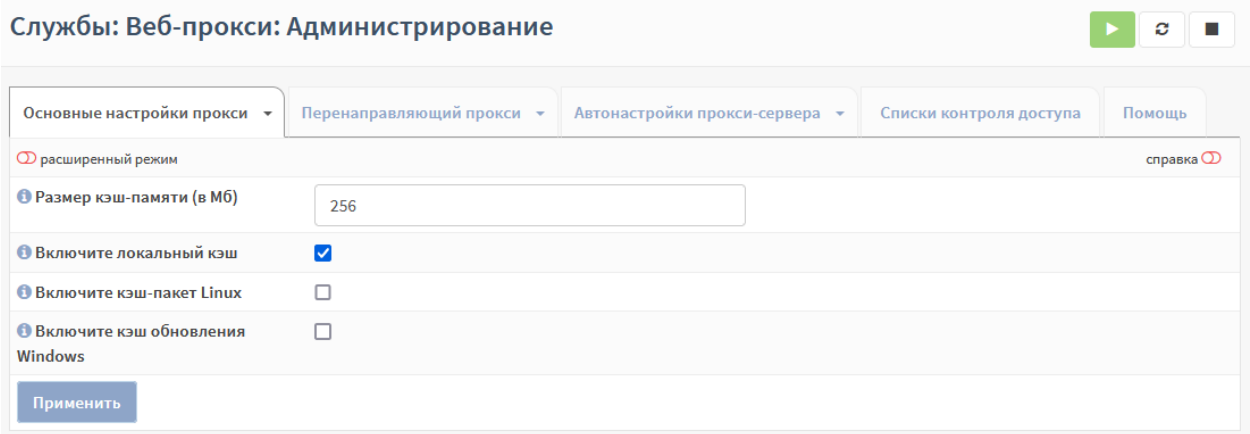

Рисунок 181 – Настройки локального кэша

4. Перейти во вкладку **«Перенаправляющий прокси»** (см. Рисунок 182).

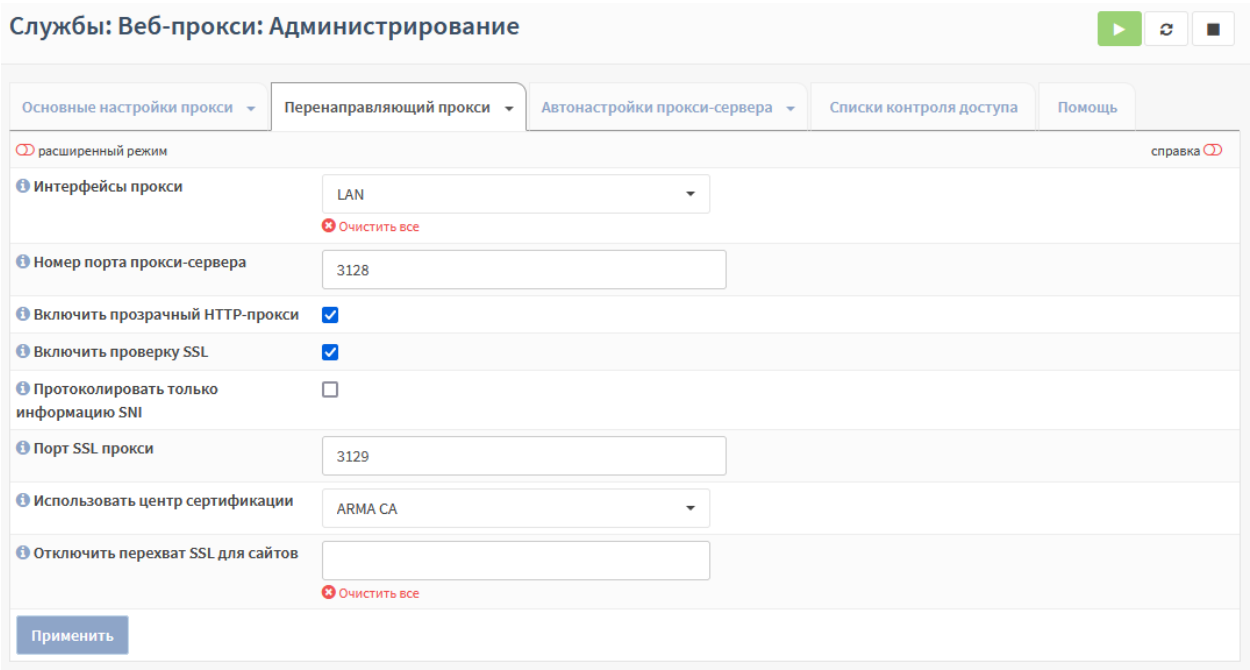

Рисунок 182 – Перенаправляющий прокси

5. Проверить значение параметра **«Интерфейс прокси»** – «LAN», выбрать значение «ARMA CA» в параметре **«Использовать центр сертификации»** и установить флажки для параметров:
   - **«Включить прозрачный HTTP-прокси»**;
   - **«Включить проверку SSL»**.
6. Нажать **кнопку «Применить»**.

18.1.3 Создание правил NAT для прокси-сервера

Для работы прозрачного режима HTTP-прокси и HTTPS-прокси необходимо добавить правила NAT.

Создание правил NAT описано в разделе 2.3.2.2 настоящего руководства.

Необходимо создать правила с параметрами, указанными в таблице (см. Таблица 31).

Таблица 31
Значения параметров правил NAT

Параметр	HTTP	HTTPS
Интерфейс	LAN	LAN
Протокол	TCP	TCP
Источник	LAN-сеть	LAN-сеть
Диапазон портов источника	Любой-Любой	Любой-Любой

Параметр	HTTP	HTTPS
Назначение	Любой	Любой
Диапазон портов назначения	HTTP-HTTP	HTTPS-HTTPS
Адрес перенаправления	127.0.0.1	127.0.0.1
Порт перенаправления	3128	3129
Описание	Трафик HTTP-прокси	Трафик HTTPS-прокси
Зеркальный NAT	Включить	Включить

После настройки NAT ПК **«Client»** имеет доступ к сети Интернет (см. Рисунок 183).

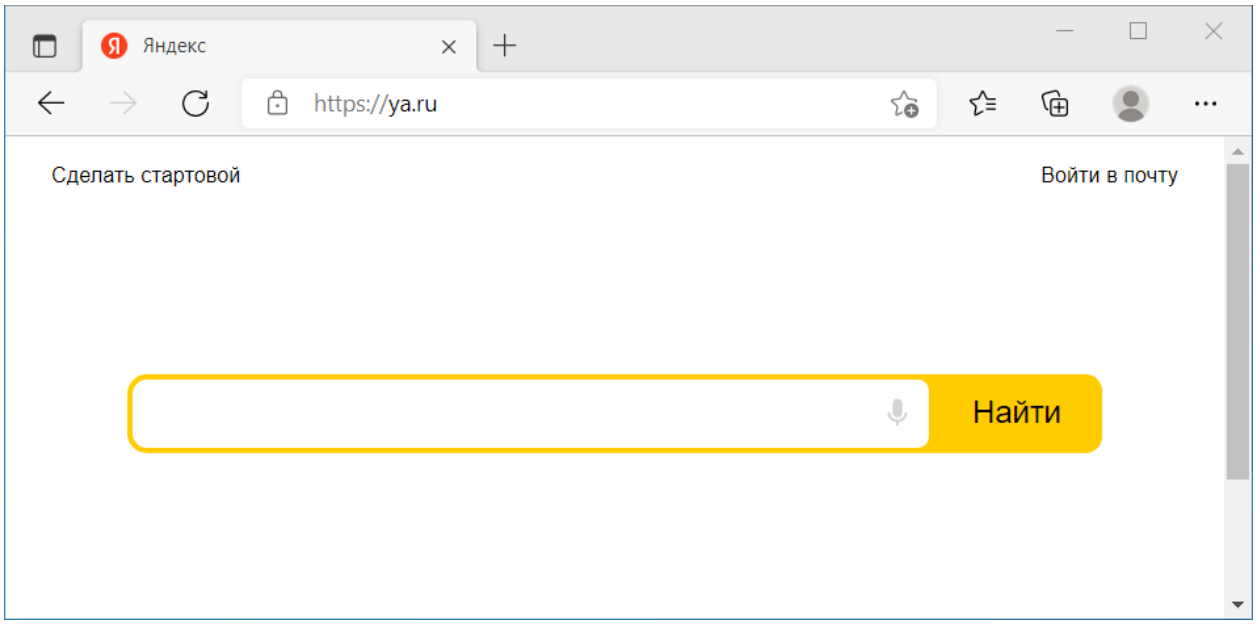

Рисунок 183 – Подключение к сети Интернет

Важно! В случае отключения прокси-сервера созданное правило NAT продолжит работать.

18.1.4 Создание правил запрета обхода трафика на МЭ

Для рассматриваемого примера настройка запрета обхода трафика не применяется.

В случае, когда прокси-сервер работает в режиме «**Непрозрачный прокси»**, для исключения доступа в сеть Интернет в обход прокси-сервера необходимо настроить правила блокировки HTTP и HTTPS трафика на МЭ.

Создание правил МЭ описано в разделе 1.1.1 настоящего руководства.

Необходимо создать правила для интерфейса «LAN» с параметрами, указанными в таблице (см. Таблица 32).

Таблица 32
Значения параметров правил блокировки

Параметр	HTTP	HTTPS
Действие	Блокировка	Блокировка
Интерфейс	LAN-сеть	LAN-сеть
Протокол	TCP	TCP
Источник	LAN	LAN
Диапазон портов назначения	HTTP	HTTPS
Описание	HTTP мимо прокси	HTTPS мимо прокси

Важно! В случае отключения прокси-сервера созданные правила МЭ продолжат работать.

18.2 Настройка веб-фильтрации

Данная функция предназначена для ограничения доступа к Интернет-ресурсам вредоносного или сомнительного содержания – фишинговые сайты, сайты с запрещённым контентом и т.д.

Для фильтрации трафика необходимо выполнить следующие действия:

1. Перейти во вкладку **«Перенаправляющий прокси»**.
2. Раскрыть вкладку **«Перенаправляющий прокси»** нажав **кнопку «** ▼ **»** и выбрать **«Список управления доступом»** (см. Рисунок 184).

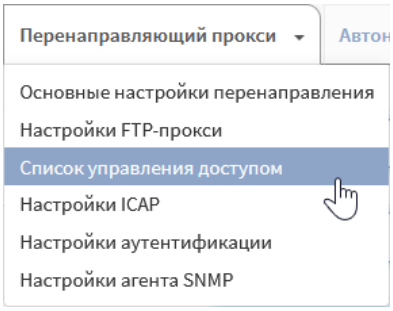

Рисунок 184 – Выбор настроек перенаправляющего прокси

3. В открывшейся форме (см. Рисунок 185), в поле параметра **«Черный список»** указать список сайтов, подлежащих блокировке. В примере используется сайт «mail.ru».

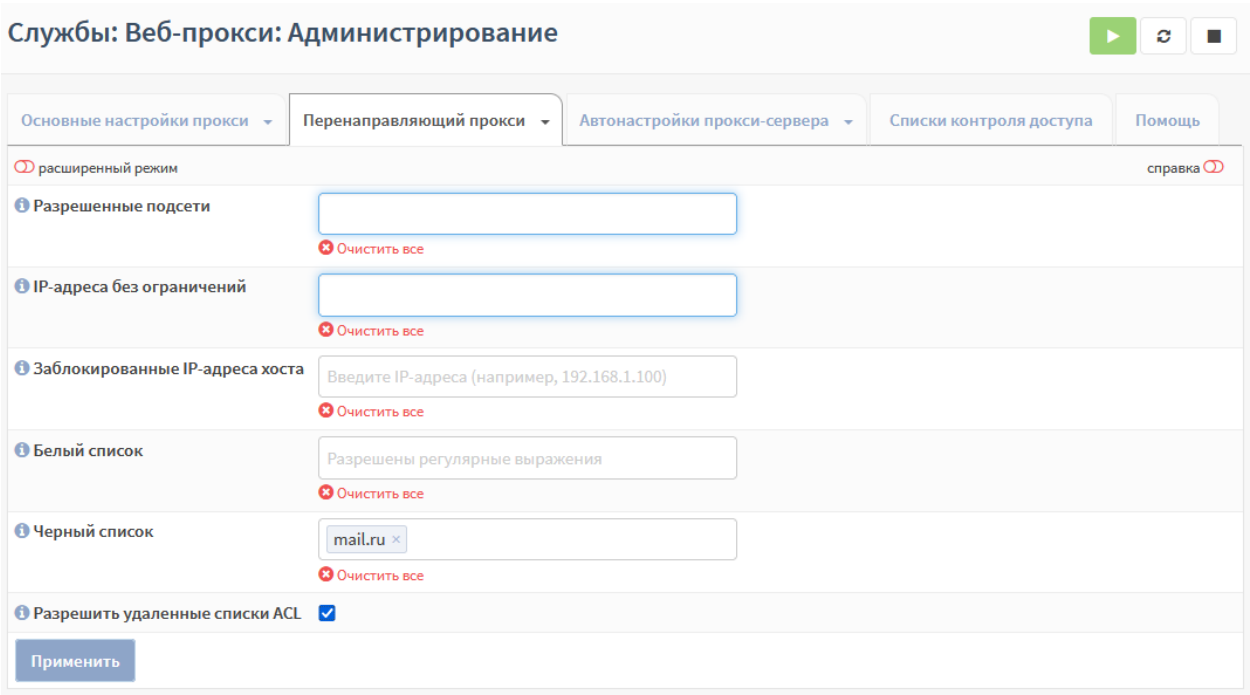

Рисунок 185 – Список управления доступом

4. С целью разрешения загрузки удалённых списков доступа установить флажок для параметра **«Разрешить удаленные списки ACL»**.
5. Перейти во вкладку **«Списки контроля доступа»** (см. Рисунок 186) и нажать **кнопку «+»** для добавления внешнего списка доступа.

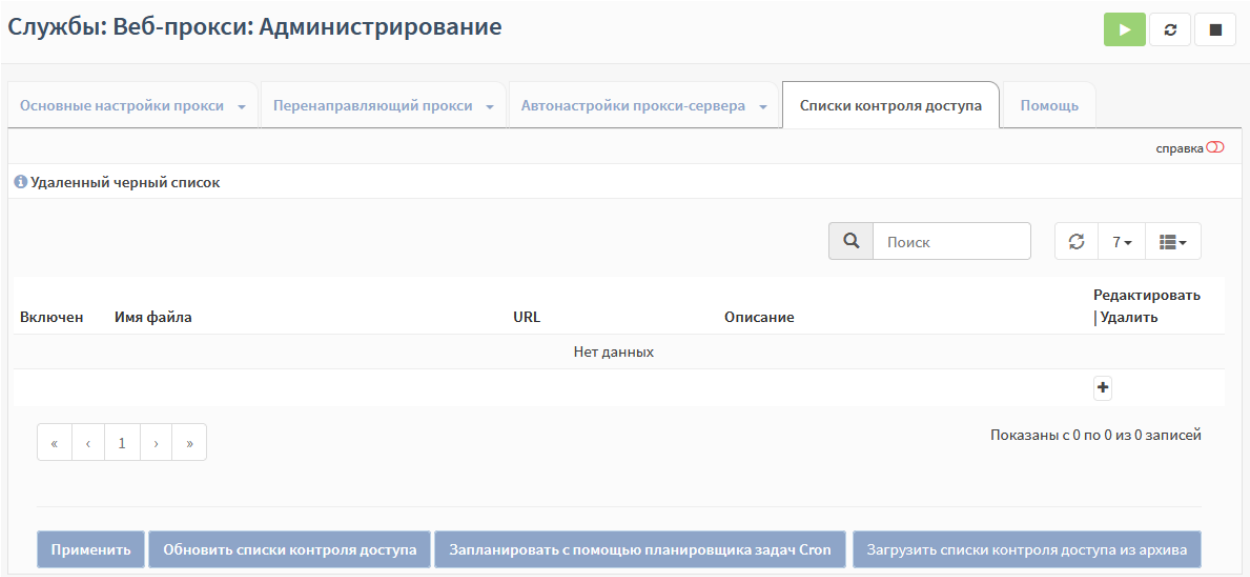

Рисунок 186 – Списки контроля доступа

6. В открывшейся форме (см. Рисунок 187) указать следующие параметры:
   - **«Имя файла»** – «UT1 web filter»;
   - **«URL»** – «ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz»;

- **«Описание»** – «Блокировка UT1 web filter».

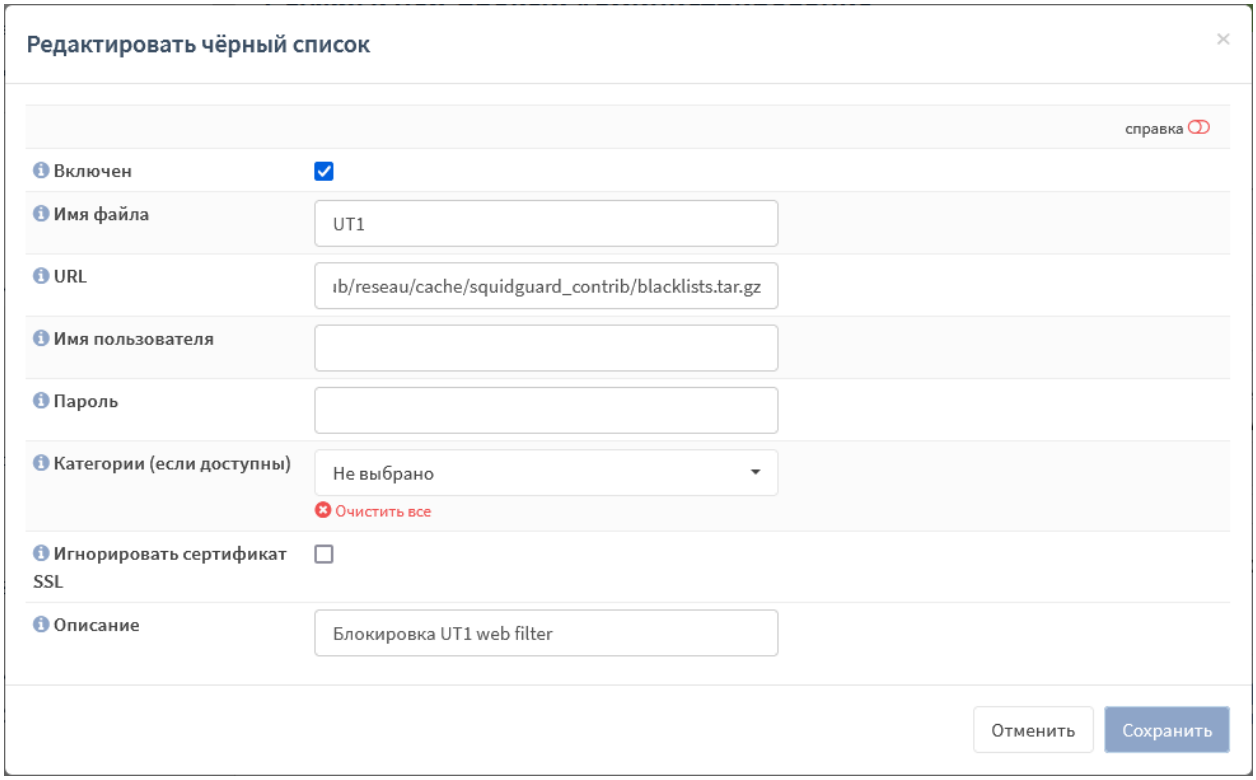

Рисунок 187 – Редактировать черный список

7. Нажать **кнопку «Обновить списки контроля доступа»**, а затем нажать **кнопку «Применить»**.

В результате настройки сайт «mail.ru» будет заблокирован как включённый в чёрный список **ARMA IF**, а сайт «pornhub.com» будет заблокирован как включенный во внешний чёрный список (см. Рисунок 188).

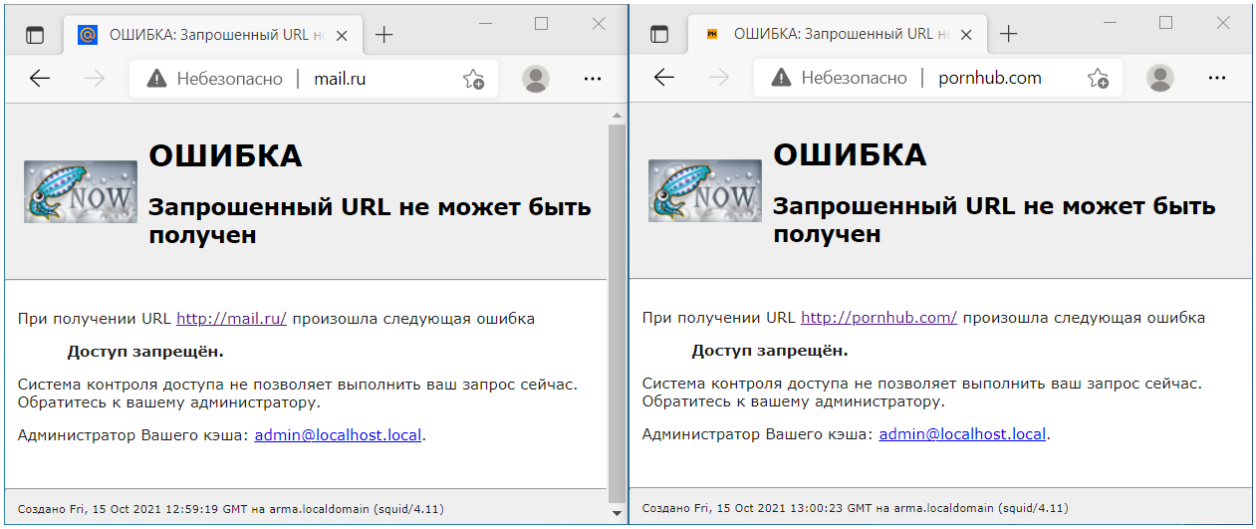

Рисунок 188 – Заблокированные сайты

18.3 ICAP

ICAP используется для настройки взаимодействия прокси-сервера с антивирусом, в том числе, расположенным на внешнем хосте. В примере для проверки веб-трафика используется встроенный в **ARMA IF** антивирус. Подробная настройка рассмотрена в разделе 24 настоящего руководства.

18.4 Дополнительные настройки

В рамках выполнения сценария настройки прокси-сервера не используются некоторые вкладки и параметры, представленные в подразделе администрирования прокси-сервера (**«Службы»** - **«Веб-прокси»** - **«Администрирование»**):

1. Вкладка **«Основные настройки»**:
    - **«Настройка управления трафиком»** – задаёт максимальные значения пропускной способности и размеров скачиваемых/загружаемых файлов;
    - **«Настройка родительского прокси»** – задаёт настройки родительского (вышестоящего) прокси-сервера.
2. Вкладка **«Перенаправляющий прокси»**:
    - **«Настройки FTP-прокси»** – задаёт настройки для FTP-трафика;
    - **«Настройки аутентификации»** – задаёт настройки аутентификации;
    - **«Настройки агента SNMP»** – задаёт настройки для мониторинга работоспособности прокси-сервера.
3. Вкладка **«Автонастройка прокси-сервера»** задаёт параметры автоматической конфигурации прокси-сервера для клиентских браузеров:
    - **«Правила»** – позволяет задать правила использования прокси-сервера;
    - **«Прокси-сервера»** – позволяет задать конфигурации прокси-сервера;
    - **«Шаблон совпадений»** – позволяет задать шаблоны соответствий для прокси-сервера.
4. Вкладка **«Помощь»** – позволяет сбросить настройки прокси-сервера с последующей перезагрузкой.

Для некоторых вкладок подраздела доступны дополнительные настройки параметров. Их отображение включается переключателем **«Расширенный режим»** в левой части формы (см. Рисунок 189).

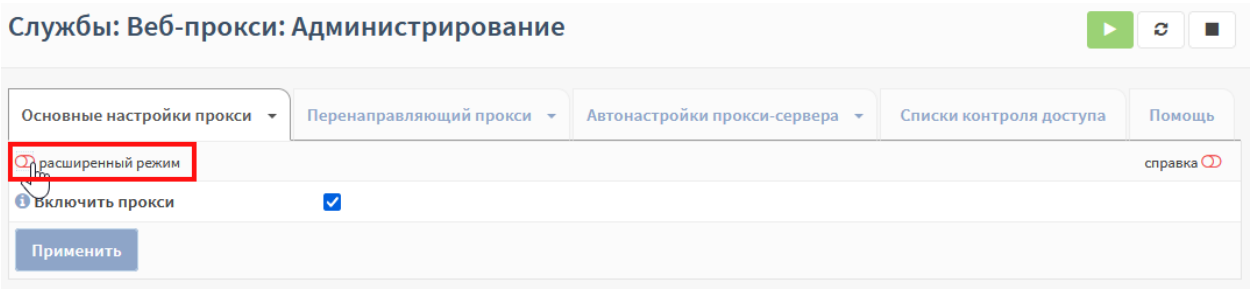

Рисунок 189 – Переключатель «Расширенный режим»

19 VPN

VPN – это обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети, например сети Интернет.

ARMA IF поддерживает работу двух технологий VPN:

- **OpenVPN**;
- **IPsec**.

19.1 OpenVPN

OpenVPN – это реализация технологии VPN, использующая SSL/TLS для защиты туннелируемого трафика. В работе OpenVPN используется механизм TUN/TAP, реализованный в виде загружаемого драйвера ядра.

ARMA IF поддерживает работу OpenVPN в режимах **«сеть - сеть»** и **«узел - сеть»**.

19.1.1 Настройка OpenVPN в режиме «сеть - сеть»

В качестве примера настройки OpenVPN в режиме **«сеть - сеть»** будет использоваться схема стенда, представленная на рисунке (см. Рисунок 190).

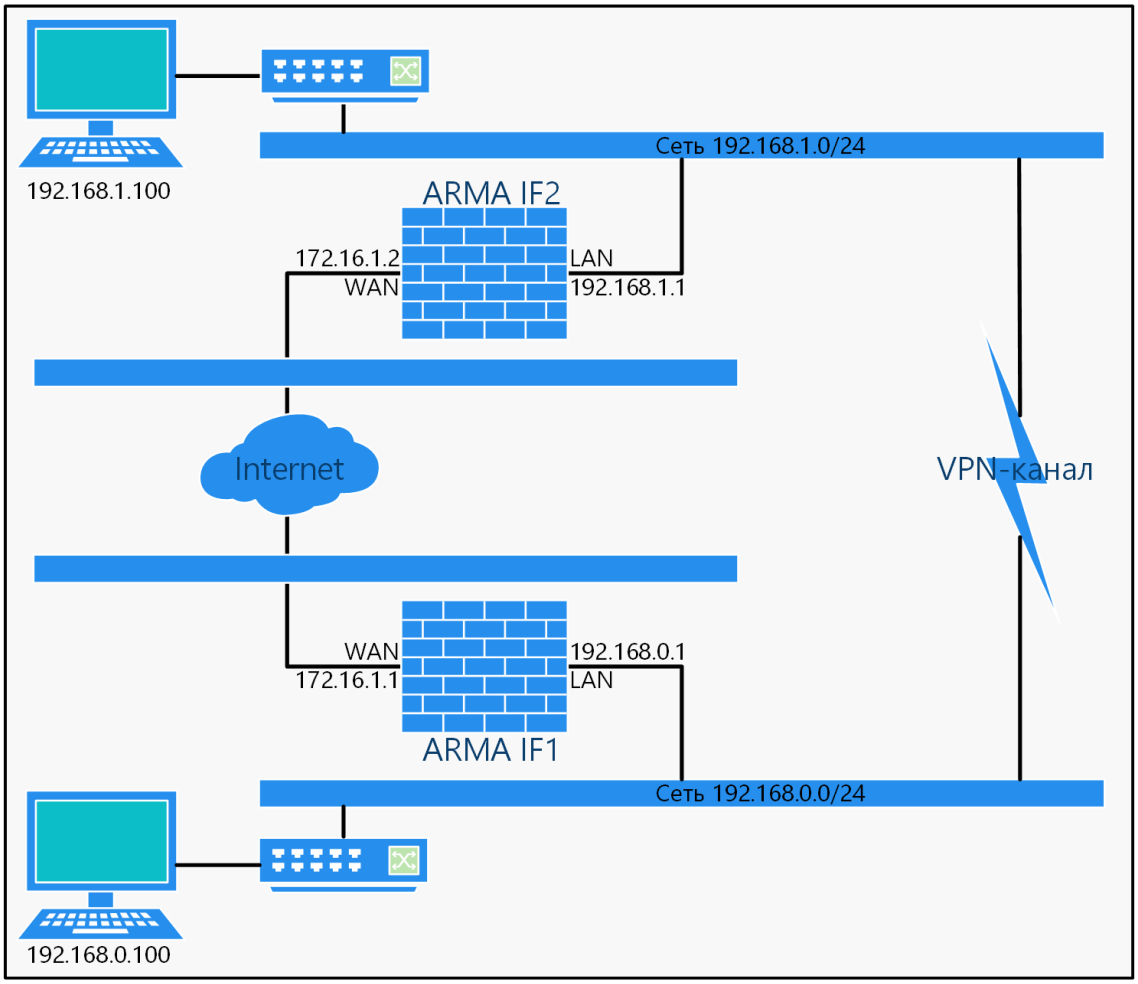

Рисунок 190 – Схема стенда для настройки OpenVPN в режиме «сеть - сеть»

Перед началом настройки необходимо создать правила МЭ (см. Раздел 1.1.1) для интерфейсов **«[WAN]»**, разрешающее трафик ICMP и убедиться в следующем:

- интерфейсы «WAN» каждого **ARMA IF** используют публичные IP-адреса доступные друг другу при команде «ping», в примере используются адреса «172.16.1.1» и «172.16.1.2»;
- сегмент интерфейса «LAN» каждого **ARMA IF** использует уникальную IP-сеть, в примере используются сети «192.168.0.0/24» и «192.168.1.0/24».

19.1.1.1 Настройка на ARMA IF1

Для настройки OpenVPN на **ARMA IF1** необходимо выполнить следующие действия:

1. Перейти в подраздел настройки серверов OpenVPN (**«VPN»** - **«OpenVPN»** - **«Серверы»**) и нажать **кнопку «+Добавить»** для добавления нового сервера.
2. В открывшейся форме указать параметры согласно таблице (см. Таблица 33) и нажать **кнопку «Сохранить»**. Настройки, не указанные в таблице оставить по умолчанию.

Таблица 33
Параметры OpenVPN ARMA IF1

Параметр	Значение параметра
Режим сервера	Пиринговая сеть (общий ключ)
Протокол	UDP
Режим работы устройства	tun
Интерфейс	WAN
Локальный порт	1194
Описание	OpenVPN peer 1
Совместно используемый ключ	Флажок установлен
Алгоритм шифрования	AES-256-CBC (256 bit key, 128 bit block)
Дайджест-алгоритм аутентификации	SHA512 (512-bit)
Аппаратные средства криптозащиты	Без аппаратного ускорения криптоалгоритмов
Туннельная сеть IPv4	10.10.0.0/24
Локальная сеть/сети IPv4	192.168.0.0/24
Удаленная сеть/сети IPv4	192.168.1.0/24

Параметр	Значение параметра
Сжатие	Включено с использованием адаптивного сжатия

19.1.1.2 Копирование ключа

После создания сервера необходимо в параметре **«Совместно использующийся Ключ»** будет отображен сгенерированный ключ (см. Рисунок 191).

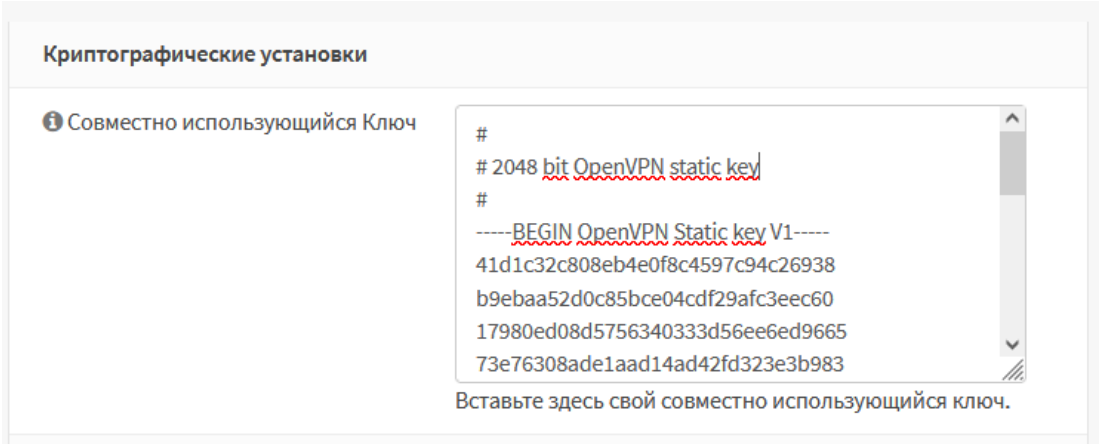

Рисунок 191 – Совместно используемый ключ OpenVPN

Для копирования ключа необходимо выполнить следующие действия:

1. Перейти в подраздел настройки серверов OpenVPN (**«VPN»** - **«OpenVPN»** - **«Серверы»**) и нажать **кнопку «** **»** напротив созданного сервера.
2. В открывшейся форме перейти в блок настроек **«Криптографические установки»** и скопировать в буфер обмена содержимое значения параметра **«Совместно использующийся Ключ»**.

19.1.1.3 Настройка на ARMA IF2

Для настройки OpenVPN на **ARMA IF2** необходимо выполнить следующие действия:

1. Перейти в подраздел настройки серверов OpenVPN (**«VPN»** - **«OpenVPN»** - **«Серверы»**) и нажать **кнопку «+Добавить»** для добавления нового сервера.
2. В открывшейся форме указать параметры согласно таблице (см. Таблица 34) и нажать **кнопку «Сохранить»**. Настройки, не указанные в таблице оставить по умолчанию.

Таблица 34
Параметры OpenVPN ARMA IF2

Параметр	Значение параметра
Режим сервера	Пиринговая сеть (общий ключ)

Параметр	Значение параметра
Протокол	UDP
Режим работы устройства	tun
Интерфейс	WAN
Адрес сервера	172.16.1.1
Порт сервера	1194
Описание	OpenVPN peer 2
Совместно используемый ключ	Флажок не установлен. Вставлено значение ранее скопированного ключа (см. Раздел 19.1.1.2)
Алгоритм шифрования	AES-256-CBC (256 bit key, 128 bit block)
Дайджест-алгоритм аутентификации	SHA512 (512-bit)
Аппаратные средства криптозащиты	Без аппаратного ускорения криптоалгоритмов
Туннельная сеть IPv4	10.10.0.0/24
Удаленная сеть/сети IPv4	192.168.0.0/24
Сжатие	Включено с использованием адаптивного сжатия

В результате настройки OpenVPN будет создан VPN-канал со следующими характеристиками:

- SSL/TLS используется;
- туннелируемый трафик инкапсулируется в UDP-пакеты;
- демон OpenVPN обрабатывает подключения только на IP-адрес, присвоенный WAN-адаптеру;
- сертификаты не используются;
- аутентификация по логину/паролю не используется;
- аутентификация TLS не используется;
- сжатие данных используется.

19.1.1.4 Создание правил МЭ

Для корректной работы VPN-туннеля необходимо настроить правила МЭ:

- на **ARMA IF1**, используемым в качестве сервера, правило для разрешения OpenVPN трафика;
- на **ARMA IF1** правило для разрешения трафика из IP-сети 192.168.1.0/24;
- на **ARMA IF2** правило для разрешения трафика из IP-сети 192.168.0.0/24.

Создание правил МЭ описано в разделе 1.1.1. настоящего руководства, необходимо создать правила с параметрами, указанными в таблице (см. Таблица 35), не указанные в таблице параметры следует оставить по умолчанию.

Таблица 35
Параметры создаваемых правил

Параметр	ARMA IF1 правило №1	ARMA IF1 правило №2	ARMA IF2
Интерфейс	[WAN]	[OpenVPN]	[OpenVPN]
Действие	Разрешить (Pass)	Разрешить (Pass)	Разрешить (Pass)
Быстрая проверка	Включено	Включено	Включено
Версии TCP/IP	IPv4	IPv4	IPv4
Протокол	UDP	Любой	Любой
Отправитель	Единственный хост или сеть, 172.16.1.2/32	192.168.1.0/24	192.168.0.0/24
Диапазон портов назначения	OpenVPN	Любой	любой
Описание	Allow VPN	Allow VPN Traffic	Allow VPN Traffic

После применения правил МЭ необходимо убедиться в работе канала, для этого на любом из **ARMA IF** перейти в подраздел статусов соединения OpenVPN (**«VPN»** - **«OpenVPN»** - **«Статус соединения»**), значение столбца **«Статус»** должно быть «up» (см. Рисунок 192).

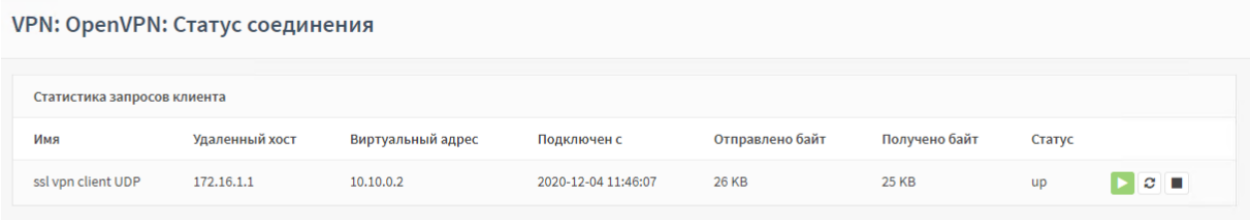

Рисунок 192 – Статус соединения OpenVPN

19.1.2 Настройка OpenVPN в режиме «клиент – сеть»

В качестве примера настройки OpenVPN в режиме **«клиент - сеть»** будет использоваться схема стенда, представленная на рисунке (см. Рисунок 193), авторизация пользователей осуществляется согласно локальной **БД ARMA IF**.

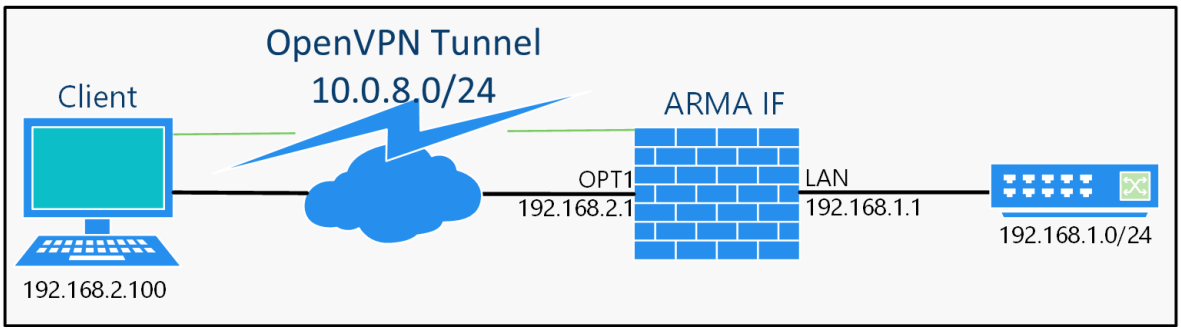

Рисунок 193 – Схема стенда для настройки OpenVPN в режиме «клиент - сеть»

Настройка будет производиться с помощью мастера настройки нового сервера.

19.1.2.1 Настройка сервера

Для настройки OpenVPN в режиме **«клиент - сеть»** необходимо выполнить следующие действия:

1. Перейти в подраздел настройки серверов OpenVPN (**«VPN»** - **«OpenVPN»** - **«Серверы»**) и нажать **кнопку «Использовать мастер для настройки нового сервера»** (см. Рисунок 194) для запуска мастера настройки сервера OpenVPN.

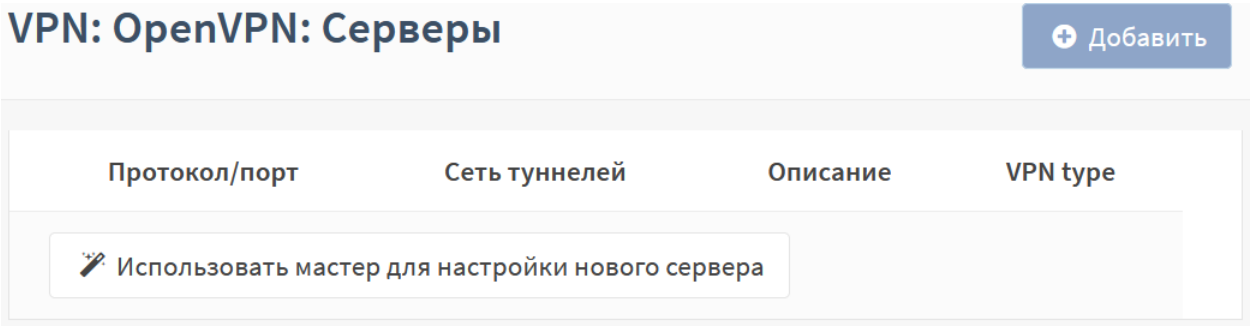

Рисунок 194 – Подраздел настройки серверов OpenVPN

2. Первый шаг мастера – **«Выбор типа аутентификации»**:
   - выбрать тип аутентификации сервера **«Локальный доступ пользователей»** и нажать **кнопку «Далее**. При этом для авторизации будут использоваться локальные пользователи и их пароли (см. Раздел 21).
3. Второй шаг мастера – **«Выбор центра сертификации»**:
   - в параметре **«Описательное имя»** ввести «arma-ovpn-ca»;

- в параметре **«Код страны»** ввести двухсимвольный ISO-код страны, в примере – «RU»;
- в параметре **«Штат или область»** ввести полное имя области, в примере – «Moscow»;
- в параметре **«Город»** ввести имя города, в примере – «Moscow»;
- в параметре **«Организация»** ввести наименование организации, в примере – «IWARMA»;
- в параметре **«Email»** ввести контактный адрес организации, в примере – «info@iwarma.ru»;
- остальные параметры оставить без изменения и нажать **кнопку «Добавить новый CA»**.

4. Третий шаг мастера – **«Добавить сертификат сервера»**:
   - нажать **кнопку «Добавить новый Сертификат»**;
   - в появившейся форме задать название сертификата в параметре **«Описательное имя»**, в примере – «arma-ovpn-cert», остальные параметры будут заполнены автоматически;
   - нажать **кнопку «Создать новый Сертификат»**.
5. Четвёртый шаг мастера – **«Настройка сервера»**:
   - в параметре **«Интерфейс»** выбрать «OPT1»;
   - в параметре **«Протокол»** выбрать «UDP»;
   - в параметре **«Туннельная сеть IPv4»** ввести «10.0.8.8/24»;
   - в параметре **«Локальная сеть IPv4»** ввести «192.168.1.0/24», необходимо обратить внимание на то, что сеть на подключаемых устройствах и целевая сеть не должны совпадать;
   - в параметре **«Сжатие»** выбрать «Включено с использованием адаптивного сжатия»;
   - в параметре **«DNS-сервер 1»** указать внешний DNS-сервер «8.8.8.8»;
   - остальные параметры оставить без изменения и нажать **кнопку «Далее»**.
6. Пятый шаг мастера – **«Конфигурация правила межсетевого экрана»**:
   - установить флажки для автоматического создания всех предложенных разрешающих правил МЭ и нажать **кнопку «Далее»**.

7. Заключительный шаг мастера – нажать **кнопку «Конец»** для завершения настройки OpenVPN.

8. Нажать **кнопку «**  **»** напротив созданного сервера , в октрывшейся форме в параметре **«Режим сервера»** выбрать значение «Удаленный доступ (аутентификация пользователя)» для доступа только по имени и паролю и ключу сервера и нажать **кнопку «Сохранить»**.

19.1.2.2 Настройка клиента

Для настройки клиента необходим конфигурационный файл OpenVPN.

Для создания конфигурационного файла необходимо выполнить следующие действия:

1. Перейти в подраздел экспорта настроек клиента (**«VPN»** - **«OpenVPN»** - **«Экспорт настроек клиента»**) (см. Рисунок 195).

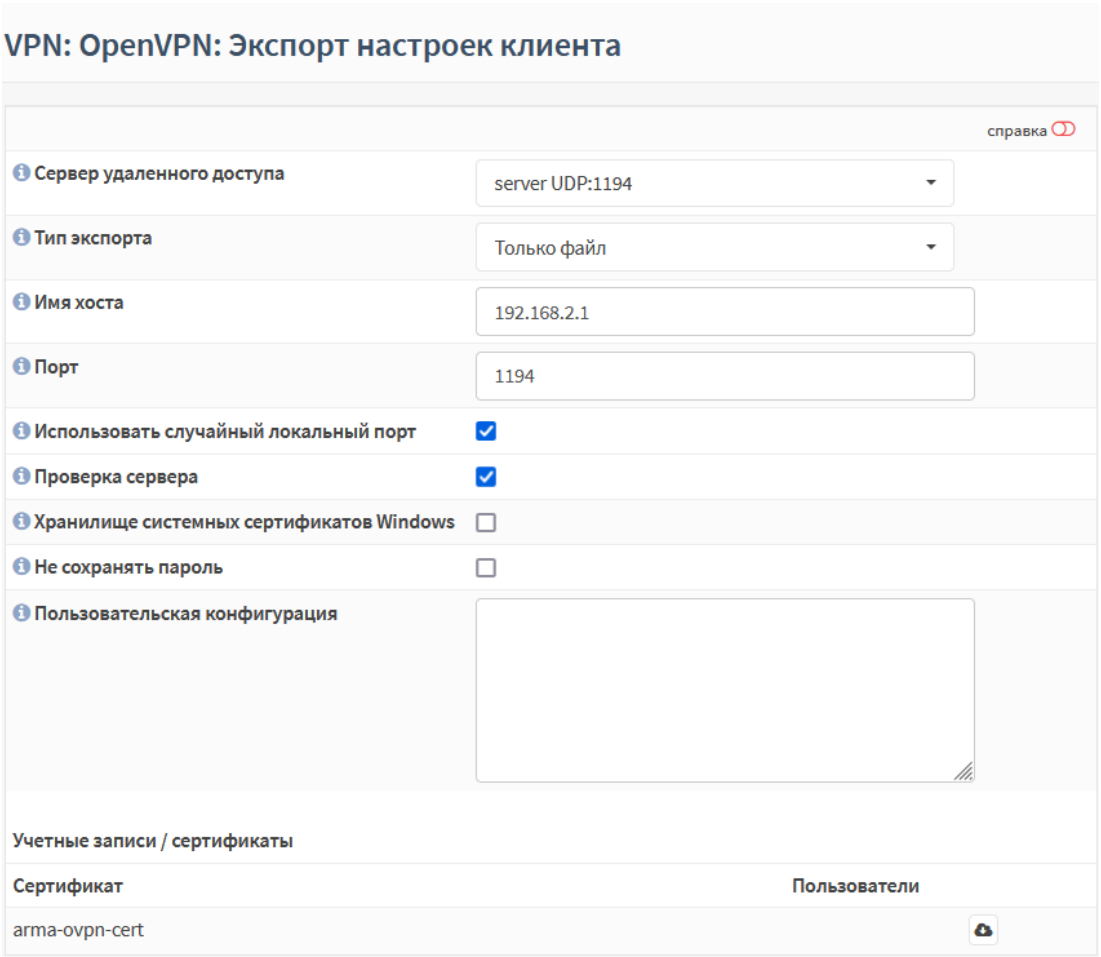

Рисунок 195 – Экспорт настроек клиента

2. Задать параметры для экспорта:
   - **«Сервер удаленного доступа»** – выбрать созданный сервер;
   - **«Тип экспорта»** – выбрать значение «Только файл»;

- **«Имя хоста»** – указать имя или IP-адрес сервера, в примере «192.168.2.1».

3. Остальные параметры оставить без изменения, нажать **кнопку «** **»** внизу страницы и сохранить конфигурационный файл следуя указаниям веб-браузера.

Экспортированный конфигурационный файл необходимо импортировать в клиентскую часть ПО «OpenVPN» на ПК **«Client»** и выполнить подключение к созданному серверу на **ARMA IF**.

19.2 IPsec

IPsec – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.

ARMA IF поддерживает работу IPsec в режимах «сеть - сеть» и «узел - сеть».

19.2.1 Настройка IPsec в режиме «узел» - «сеть»

В качестве примера настройки IPsec в режиме **«узел - сеть»**, используется схема стенда, представленная на рисунке (см. Рисунок 196).

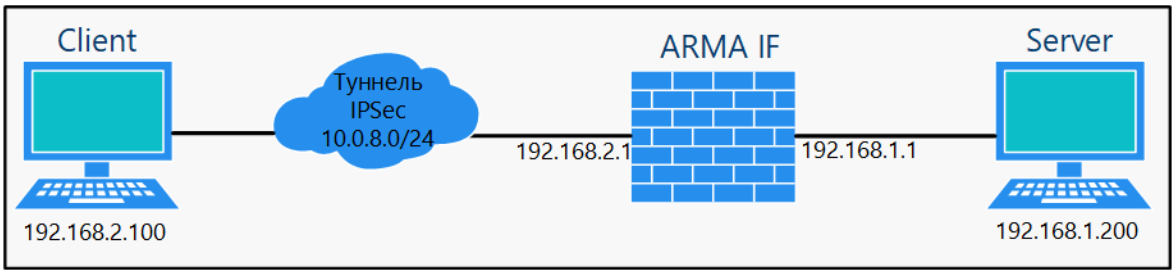

Рисунок 196 – Схема стенда для настройки IPsec в режиме «узел» - «сеть»

Для настройки IPsec в режиме **«узел - сеть»** необходимо выполнить следующие шаги:

1. Создать внутренний центр сертификации.
2. Создать внутренний сертификат.
3. Настроить мобильный клиент и туннель IPsec.
4. Добавить ключ IPsec.
5. Импортировать сертификат клиенту.
6. Настроить новое сетевое подключение.

19.2.1.1 Шаг 1. Создание внутреннего центра сертификации

В примере доверенный центр сертификации создается с параметрами, приведёнными в таблице (см. Таблица 36), не указанные параметры необходимо оставить по умолчанию.

Таблица 36
Значения параметров центра сертификации

Параметр	Значение
Описательное имя	ARMA CAF
Метод	Создать внутренний центр сертификации
Длина ключа (биты)	2048
Digest алгоритм	SHA256
Срок жизни (дней)	365
Код страны	RU (Russia)
Область	MO
Город	Москва
Организация	IWARMA
Email адрес	info@infowatch.ru
Простое имя	internal-ca

Параметры **«Описательное имя»**, **«Код страны»**, **«Область»**, **«Город»**, **«Организация»**, **«Email адрес»**, **«Простое имя»** указаны справочно.

Для создания доверенного центра сертификации необходимо выполнить следующие действия:

1. Перейти в подраздел полномочий (**«Система»** - **«Доверенные сертификаты»** - **«Полномочия»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать параметры из таблицы (см. Таблица 36).
4. Нажать **кнопку «Сохранить»**.

Сертификат созданного центра сертификации необходимо экспортировать нажав **кнопку «Экспортировать сертификат CA»** (см. Рисунок 197) в подразделе полномочий (**«Система»** - **«Доверенные сертификаты»** - **«Полномочия»**).

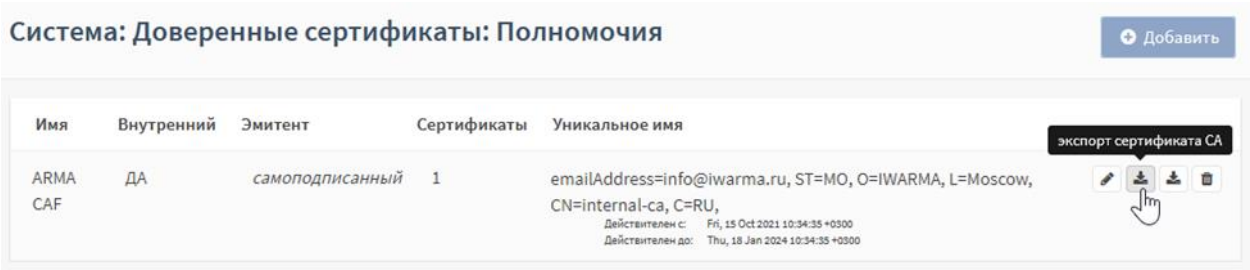

Рисунок 197 – Экспорт сертификата CA

19.2.1.2 Шаг 2. Создать внутренний сертификат

В примере внутренний сертификат создается с параметрами, приведёнными в таблице (см. Таблица 36), не указанные параметры необходимо оставить по умолчанию.

Таблица 37
Значения параметров сертификата

Параметр	Значение
Метод	Создать внутренний сертификат
Описательное имя	IKEv2 cert
Центр сертификации	ARMA CAF
Тип	Сертификат сервера
Время существования (дни)	365
Код страны	RU (Russia)
Область	MO
Город	Moscow
Организация	IWARMA
Email адрес	info@infowatch.ru
Стандартное имя	192.168.2.1

Параметры **«Описательное имя»**, **«Код страны»**, **«Область»**, **«Город»**, **«Организация»**, **«Email адрес»**, **«Стандартное имя»** указаны справочно.

Для создания внутреннего сертификата необходимо выполнить следующие действия:

1. Перейти в подраздел сертификатов (**«Система»** - **«Доверенные сертификаты»** - **«Полномочия»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать параметры из таблицы (см. Таблица 37).
4. Нажать **кнопку «Сохранить»**.

19.2.1.3 Шаг 3. Настройка мобильного клиента и туннеля IPsec

Для поддержки мобильных клиентов IPsec необходимо выполнить следующие действия:

1. Перейти в подраздел настроек мобильных клиентов IPsec (**«VPN»** - **«IPsec»** - **«Мобильные клиенты»**) (см. Рисунок 198).

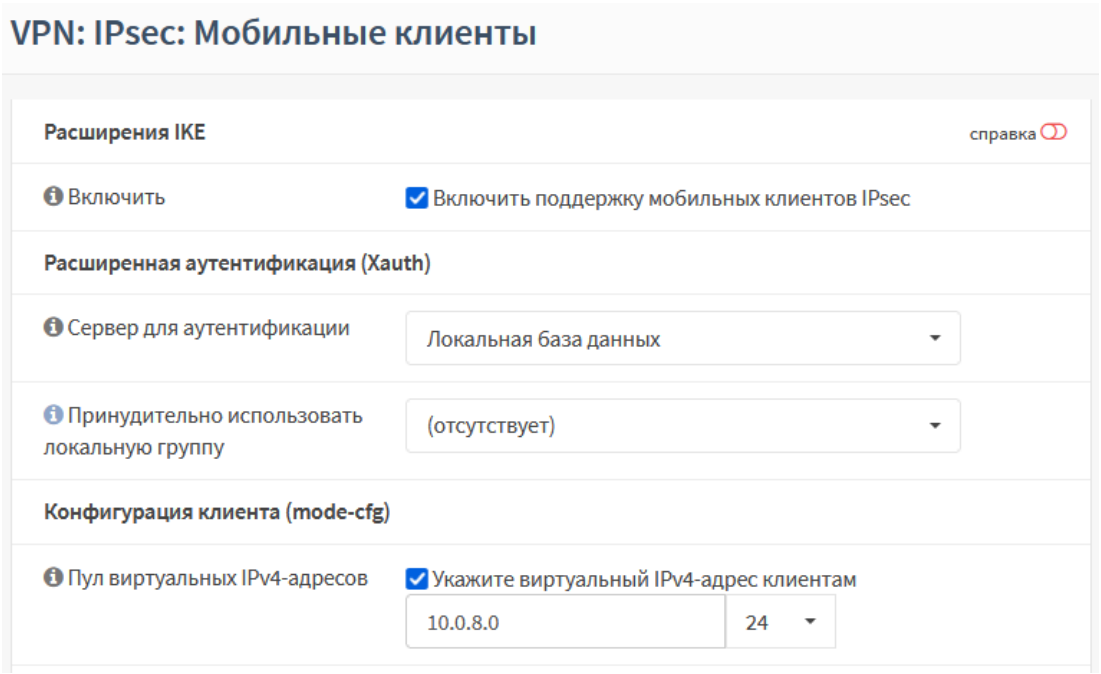

Рисунок 198 – Настройка мобильного клиента IPsec

2. Указать следующие настройки:
   - **«Включить»** – флажок установлен;
   - **«Сервер для аутентификации»** – выбрать «Локальная база данных»;
   - **«Пул виртуальных IPv4-адресов»** – флажок установлен и указано значение «10.0.8.0/24».
3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**. Появится предупреждение о необходимости создания фазы 1 (см. Рисунок 199).

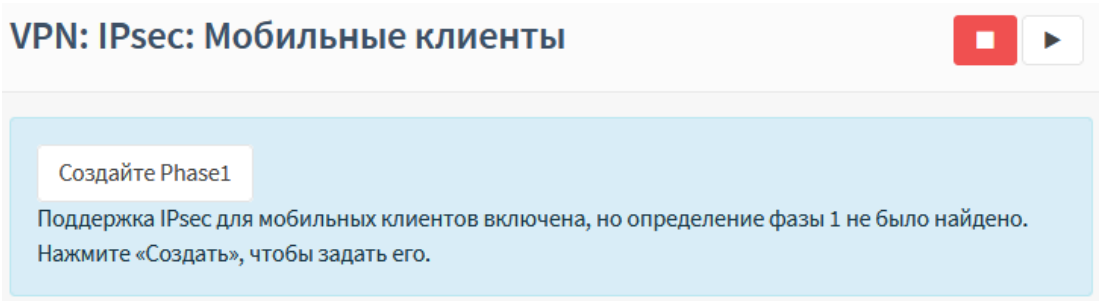

Рисунок 199 – Предупреждение о необходимости создания фазы 1

4. Нажать **кнопку «Создайте Phase1»** и указать следующие настройки в открывшейся форме (см. Рисунок 200):
   - **«Метод аутентификации»** – выбрать «EAP-MSCHAPV2»;
   - **«Мой идентификатор»** – выбрать «Уникальное имя» и указать «192.168.2.1»;
   - **«Алгоритм шифрования»** – «AES, 256»;

- **«Группа ключей DH»** – «2 (1024 bits), 14 (2048 bits)».

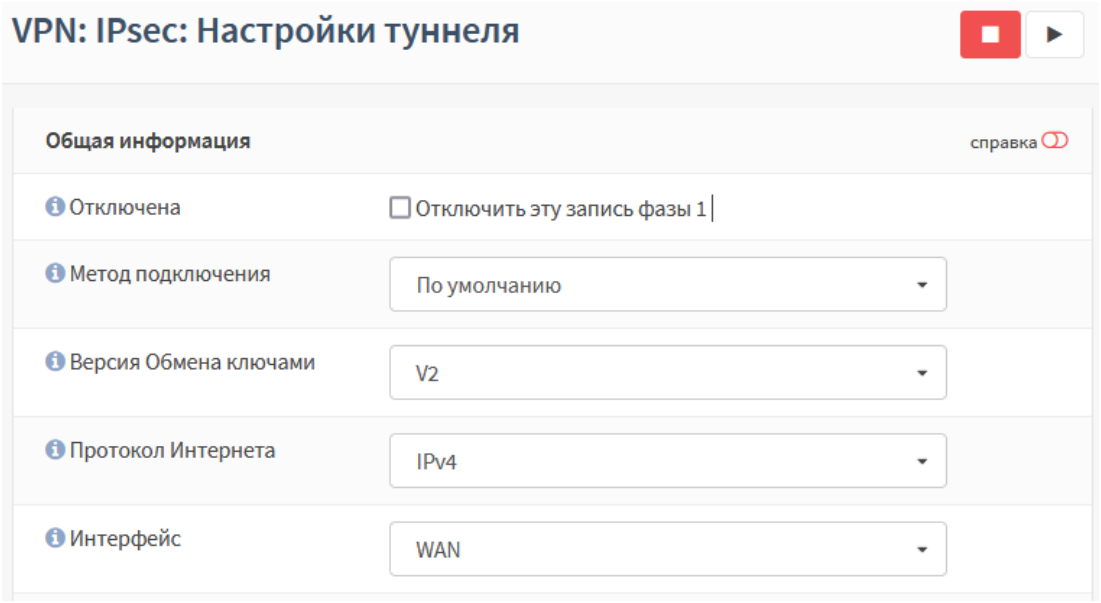

Рисунок 200 – Настройка фазы 1

5. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.
6. Для созданной записи нажать **кнопку «+»** (см. Рисунок 201) для добавления записи фазы 2.

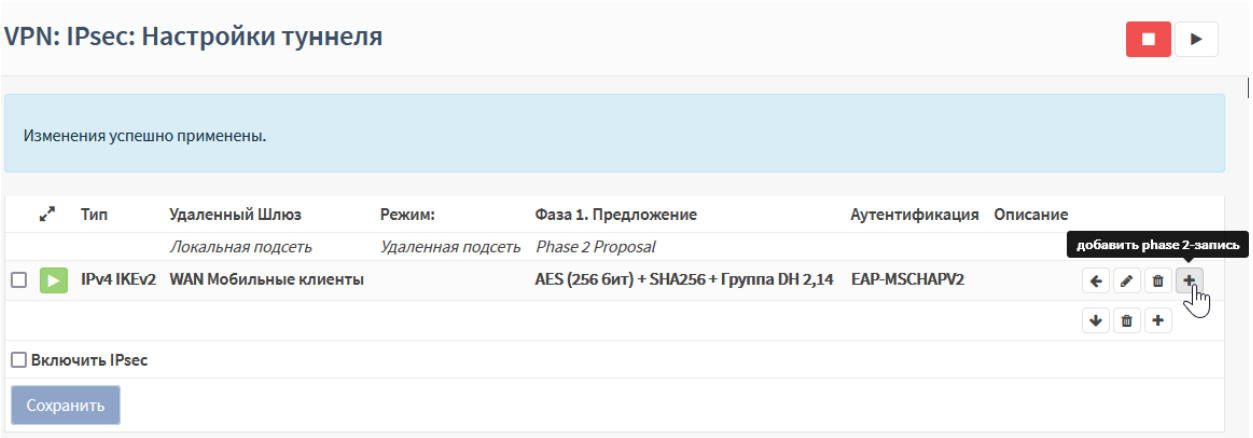

Рисунок 201 – Добавление записи фазы 2

7. Указать следующие настройки в открывшейся форме (см. Рисунок 202):
   - **«Алгоритмы шифрования»** – снять флажок со значений **«Blowfish»** и **«CAST128»**;
   - **«Алгоритмы хеша»** – выбрать «SHA1».

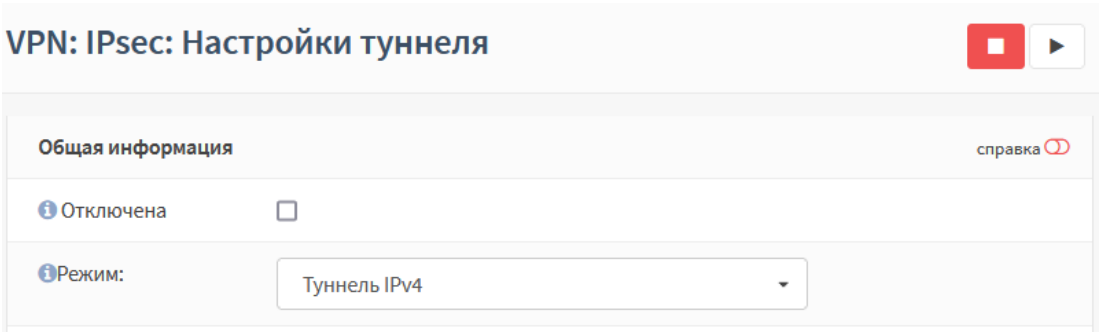

Рисунок 202 – Настройка фазы 2

8. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

19.2.1.4 Шаг 4. Добавление ключа IPsec

Для добавления ключа IPsec необходимо выполнить следующие действия:

1. Перейти в подраздел предварительно выданных ключей (**«VPN»** - **«IPsec»** - **«Предварительно выданные ключи»**) и нажать **кнопку «+Добавить»**.
2. Указать следующие настройки в открывшейся форме (см. Рисунок 203):
   - **«Идентификатор»** – ввести «User»;
   - **«Предварительно выданный ключ»** – ввести «123»;
   - **«Тип»** – выбрать «EAP».

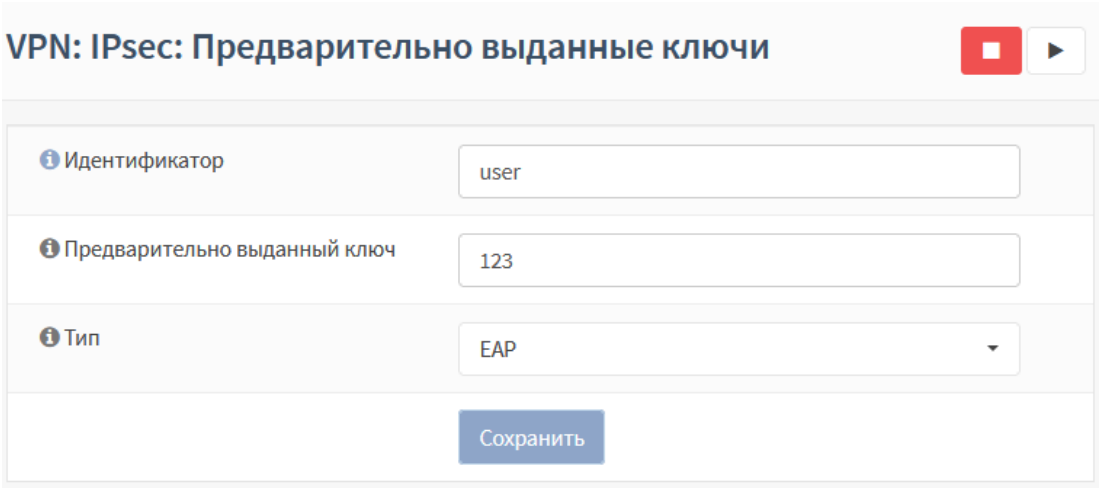

Рисунок 203 – Добавление ключа IPsec

3. Нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

19.2.1.5 Шаг 5. Импорт сертификата клиенту

Перед началом импорта необходимо создать оснастку для работы с сертификатами, в качестве примера будет использоваться ОС «Windows».

Порядок создания оснастки для работы с сертификатами на ПК **«Client»** необходимо выполнить следующие действия:

1. Нажать **комбинацию клавиш «Win+R»** и, в появившемся меню **«Выполнить»**, ввести «mmc» и нажать **клавишу «Enter»** для запуска консоли управления.
2. В меню **«Файл»** открывшейся консоли управления выбрать **«Добавить или удалить оснастку...»**.
3. В открывшейся форме добавления и удаления оснасток из столбца **«Доступные оснастки»** выбрать **«Сертификаты»** и нажать **«+Добавить»**.
4. На первом шаге открывшейся оснастки выбрать значение **«Учетной записи компьютера»** и нажать **кнопку «Далее»**, в следующем шаге выбрать значение **«Локальным компьютером»** и нажать **кнопку «Готово»**.
5. Нажать **кнопку «ОК»** в форме добавления и удаления оснасток (см. Рисунок 204).

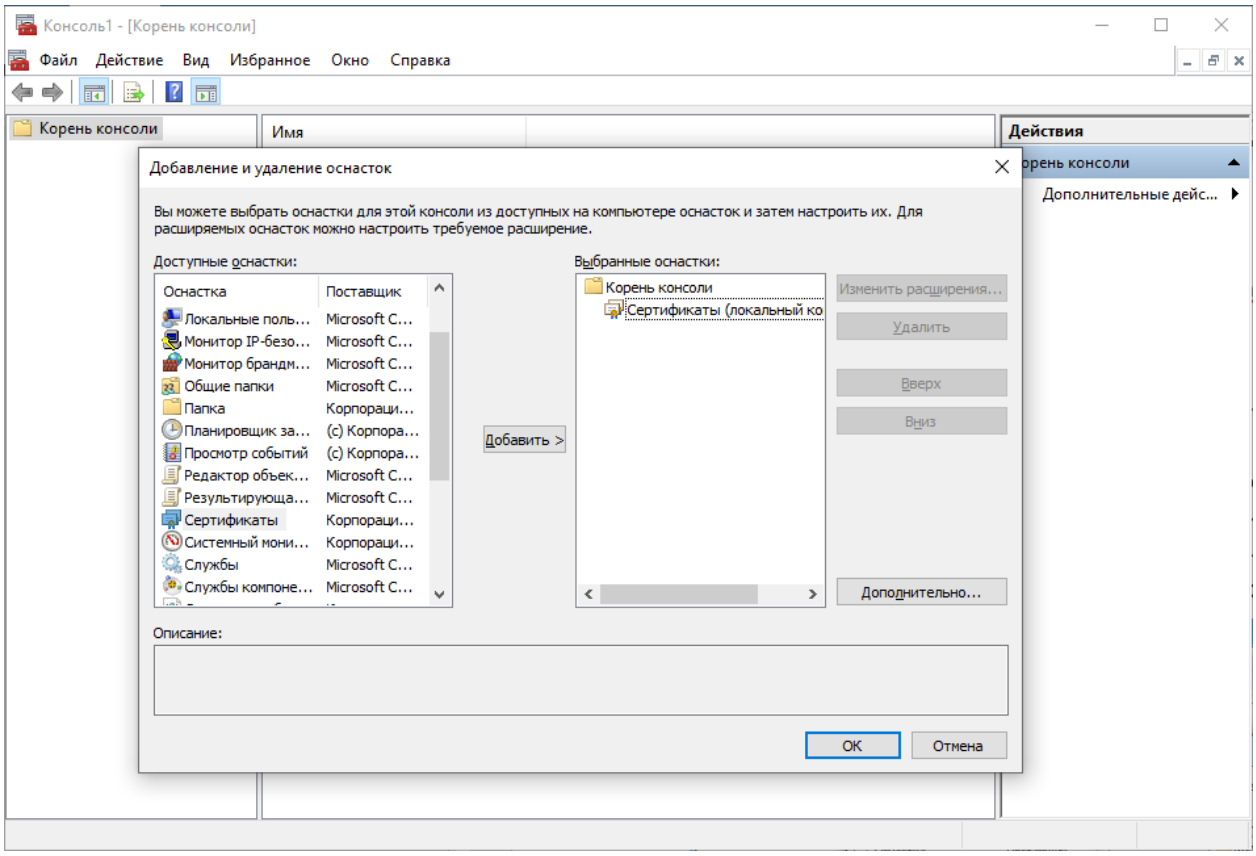

Рисунок 204 – Создание оснастки для работы с сертификатами на ПК «Client»

6. При необходимости сохранить консоль выбрать значение **«Сохранить»** или **«Сохранить как»** меню **«Файл»**. Рекомендуемое имя **«armacertmngr»**.

Для импорта сертификата, экспортированного на шаге 1 (см. Раздел 19.2.1.1), необходимо выполнить следующие действия:

1. В оснастке для работы с сертификатами перейти в иерархии по пути:

- **«Сертификаты (локальный компьютер)»** - **«Доверенные корневые центры сертификации»** - **«Сертификаты»**.

2. В меню **«Действие»** консоли управления выбрать **«Все задачи»**, а затем **«Импорт»**.
3. Следовать указаниям мастера импорта сертификатов выбрав сертификат, экспортированный на шаге 1 (см. Раздел 19.2.1.1).

19.2.1.6 Шаг 6. Настройка нового сетевого подключения.

В качестве примера настройки нового сетевого подключения будет использоваться создание и настройка подключения в ОС «Windows»

Для создания и настройки VPN подключения на ПК **«Client»** необходимо выполнить следующие действия:

1. Перейти в **«Панель управления»**, установить режим просмотра **«Мелкие значки»**, выбрать раздел **«Центр управления сетями и общим доступом»** и нажать **«Создание и настройка нового подключения или сети»**.
2. В открывшемся мастере выбрать **«Подключение к рабочему месту»** и нажать **кнопку «Далее»**.
3. На следующем шаге выбрать **«Использовать мое подключение к интернету (VPN)»**, а в следующем шаге задать настройки подключения (см. Рисунок 205):
   - **«Адрес в Интернете»** – ввести «192.168.2.1»;
   - **«Имя объекта назначения»** – ввести «VPN-подключение»;

   и нажать **кнопку «Создать»**.

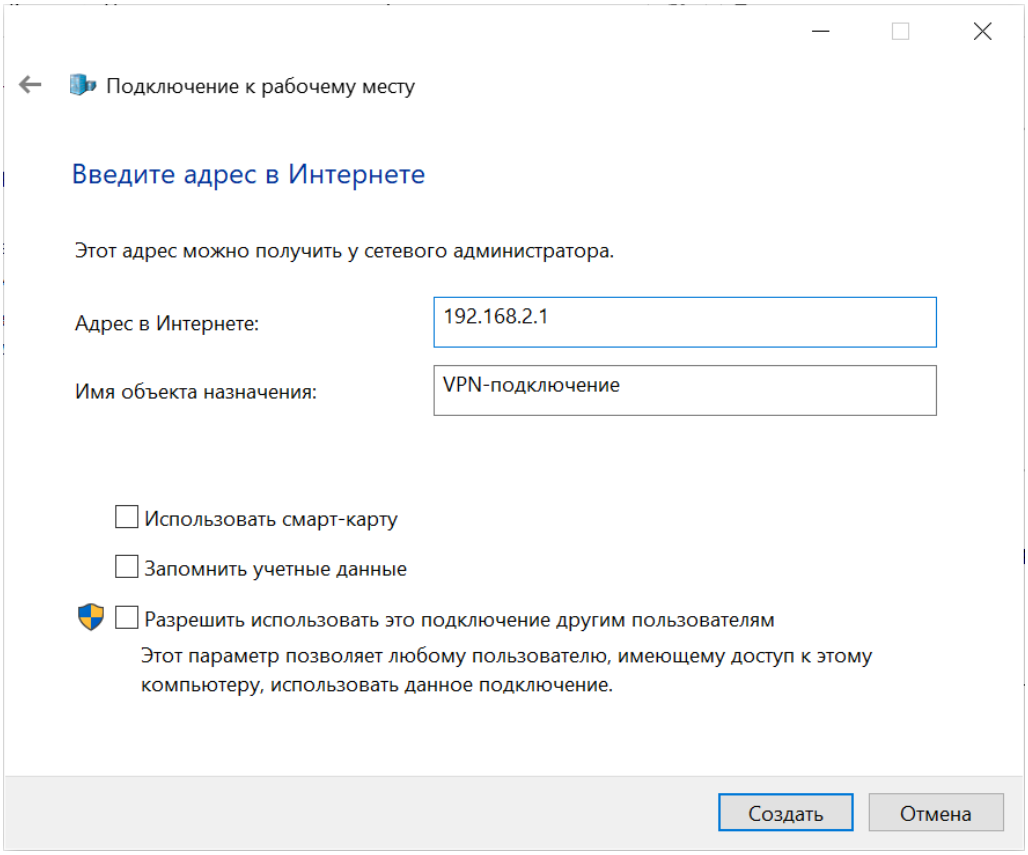

Рисунок 205 – Настройка нового сетевого подключения

4. Перейти в **«Панель управления»**, установить режим просмотра **«Мелкие значки»**, выбрать раздел **«Центр управления сетями и общим доступом»**.
5. Выбрать **«Изменение параметров адаптера»**, нажать **правой кнопкой мыши** на созданное ранее подключение **«VPN-подключение»** и выбрать **«Свойства»**.
6. Перейти во вкладку **«Безопасность»** (см. Рисунок 206) и указать следующие параметры:
   - **«Тип VPN»** – выбрать «IKEv2»;
   - **«Шифрование данных»** – выбрать «обязательное (отключиться, если нет шифрования)»;
   - **«Проверка подлинности»** – установить флажок и выбрать «Microsoft: защищённый пароль (EAP-MSCHAP v2) (шифрование включено)»;

   и нажать **кнопку «ОК»**.

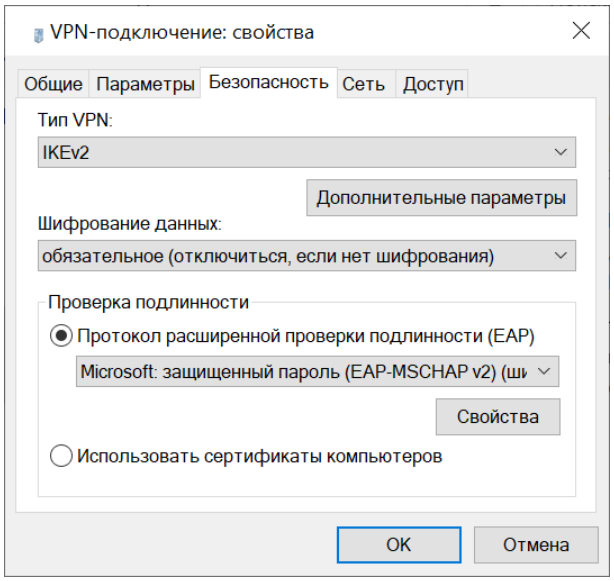

Рисунок 206 – Настройка параметров сетевого подключения

Для подключения VPN соединения необходимо **нажать правой кнопкой** мыши на созданное ранее подключение **«VPN-подключение»** и выбрать **«Подключить»**. Ввести аутентификационные данные, созданные на шаге 4 (см. Раздел 19.2.1.4) и нажать **кнопку «ОК»** для подключения.

19.2.1.7 Проверка подключения

Для проверки успешного подключения необходимо убедиться в соответствующих записях в следующих подразделах:

1. Статуса аренды адресов (**«VPN» - «IPsec» - «Статус аренды адресов»**) (см. Рисунок 207).

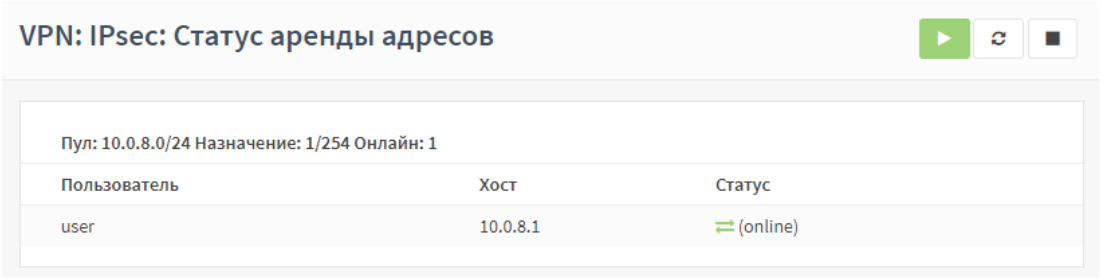

Рисунок 207 – «VPN» - «IPsec» - «Статус аренды адресов»

2. Базы данных безопасных ассоциаций **(«VPN» - «IPsec» - «База данных безопасных ассоциаций (SAD)»**) (см. Рисунок 208).

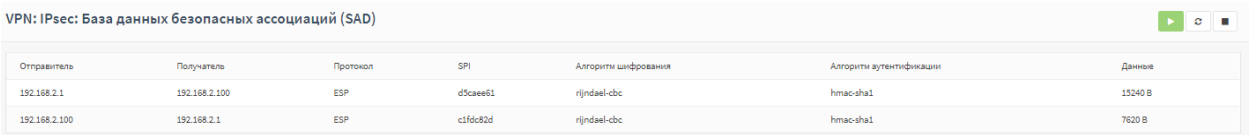

Рисунок 208 – «VPN» - «IPsec» - «База данных безопасных ассоциаций (SAD)»

3. Базы данных политик безопасности (**«VPN» - «IPsec» - «База данных политик безопасности (SPD)»**) (см. Рисунок 209).

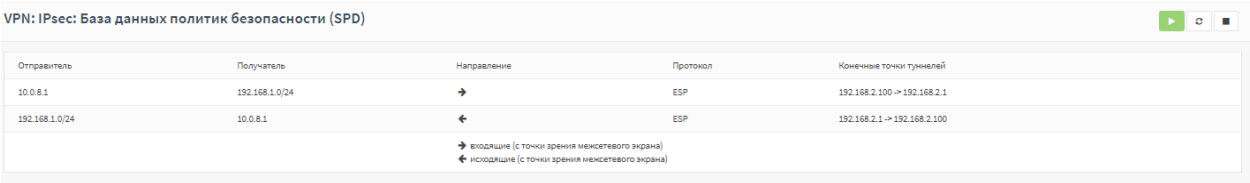

Рисунок 209 – «VPN» - «IPsec» - «База данных политик безопасности (SPD)»

19.2.2 Настройка IPsec в режиме «сеть» - «сеть»

В качестве примера настройки IPsec в режиме **«сеть - сеть»**, используется схема стенда, представленная на рисунке (см. Рисунок 210).

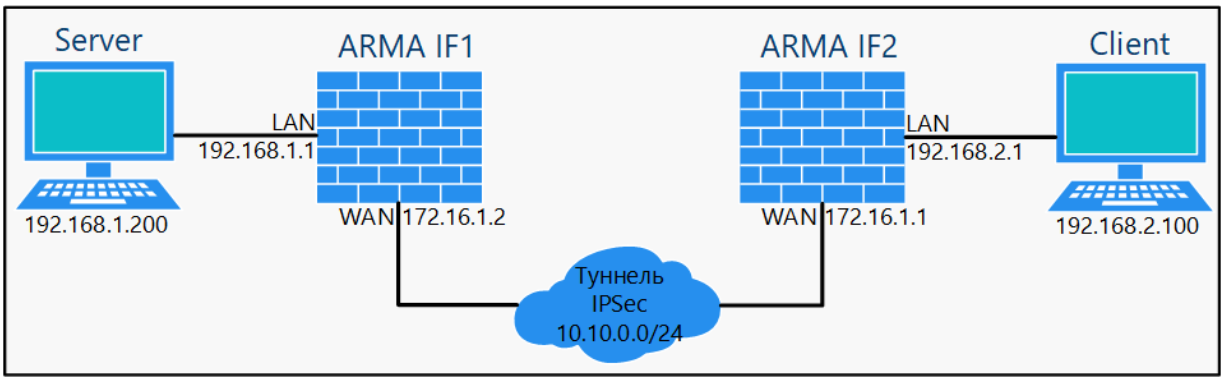

Рисунок 210 – Схема стенда для настройки IPsec в режиме «сеть» - «сеть»

Для настройки IPsec в режиме **«сеть - сеть»** необходимо выполнить следующие шаги:

1. Добавить ключ IPsec.
2. Настроить туннель IPsec на **ARMA IF1**.
3. Настроить туннель IPsec на **ARMA IF2**.

19.2.2.1 Шаг 1. Добавление ключа IPsec

Для добавления ключа IPsec необходимо выполнить следующие действия:

1. На ПК **«Server»** в веб-интерфейсе AIF 1 перейти в подраздел предварительно выданных ключей (**«VPN»** - **«IPsec»** - **«Предварительно выданные ключи»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок 211) указать следующие параметры:
   - **«Идентификатор»** – ввести «ANY»;
   - **«Предварительно выданный ключ»** – ввести «12345»;
   - **«Тип»** – выбрать «PSK».

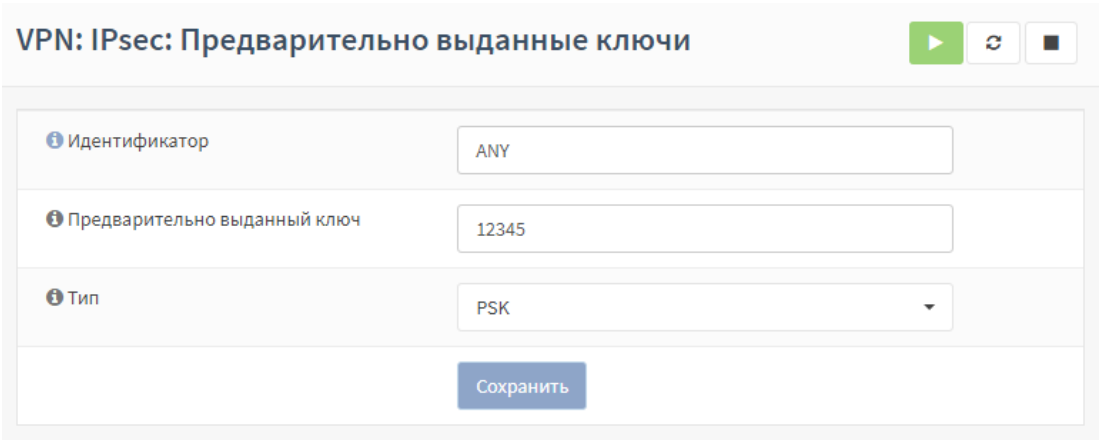

Рисунок 211 – Добавление ключа IPsec

3. Нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

Параметры созданного ключа необходимо будет указать при настройке туннеля IPsec на **ARMA IF1** и **ARMA IF2**.

19.2.2.2 Шаг 2. Настройка туннеля IPsec на ARMA IF1

Для настройки туннеля IPsec **ARMA IF1** необходимо выполнить следующие действия:

1. Перейти в подраздел настроек IPsec (**«VPN»** - **«IPsec»** - **«Настройки туннеля»**) и нажать **кнопку «+»** для создания фазы 1.
2. Указать следующие настройки в открывшейся форме (см. Рисунок 212):
   - **«Удалённый шлюз»** – указать «172.16.1.1»;
   - **«Описание»** – внести «peer1»;
   - **«Предварительно выданный ключ»** – указать «12345»;
   - **«Алгоритм шифрования»** – «AES, 256»;
   - **«Группа ключей DH»** – «14 (2048 bits)»;
   - **«Отключить MOBIKE»** – флажок установлен;
   - **«Обнаружение недоступных пиров»** – флажок установлен.

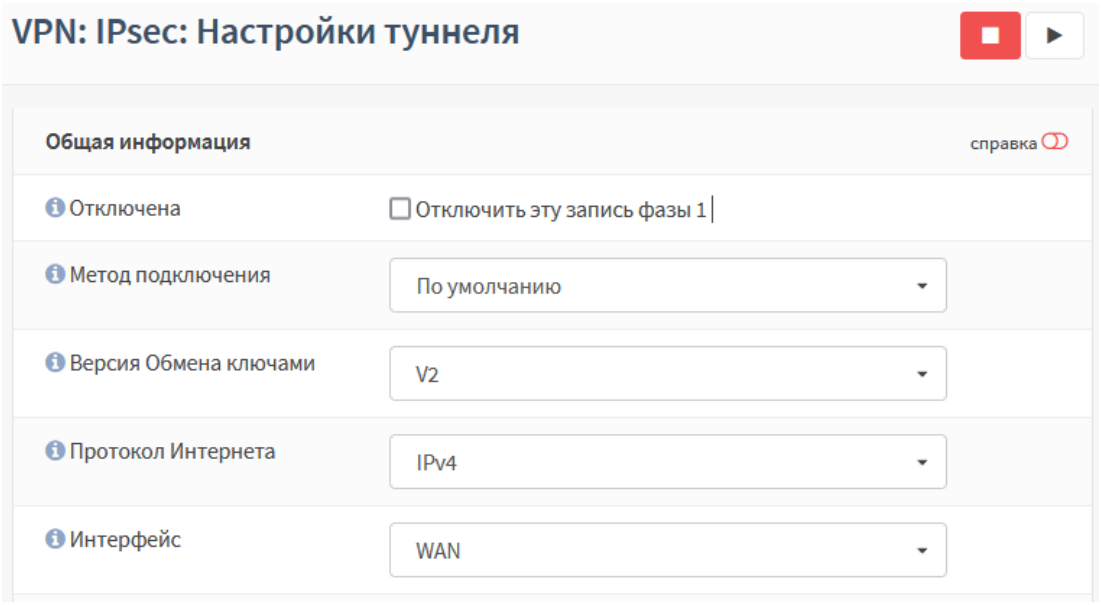

Рисунок 212 – Настройка фазы 1 на ARMA IF1

3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.
4. Для созданной записи нажать **кнопку «+»** (см. Рисунок 213) для добавления записи фазы 2.

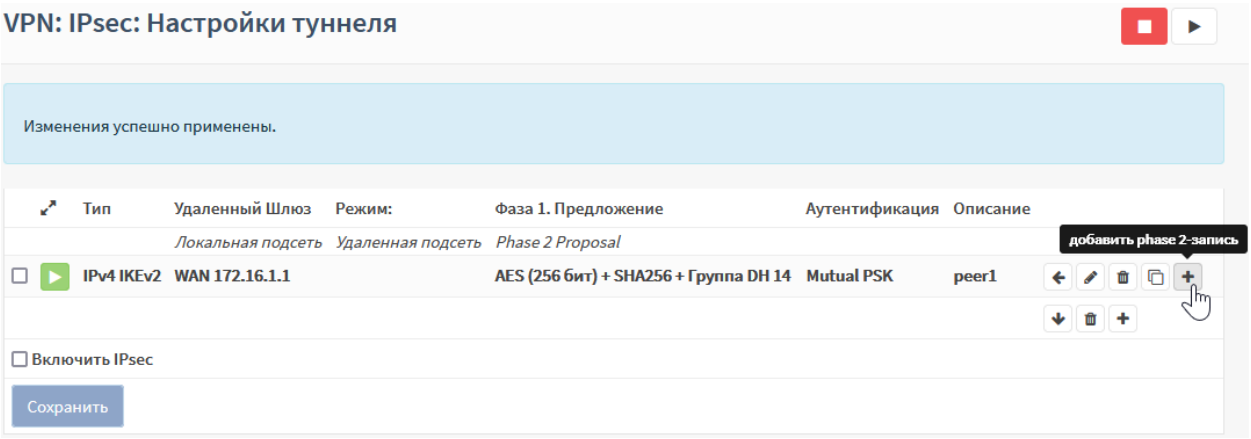

Рисунок 213 – Добавление записи фазы 2 на ARMA IF1

5. Указать следующие настройки в открывшейся форме (см. Рисунок 214):
   - **«Описание»** – указать «peer 1»;
   - **«Адрес»** (Удаленная сеть) – ввести «192.168.2.0/24»
   - **«Алгоритмы шифрования»** – установить флажок для значения **«aes256gcm16»**;
   - **«Алгоритмы хеша»** – выбрать «SHA1»;
   - **«Автоматически пингуйте хост»** – ввести «192.168.2.1».

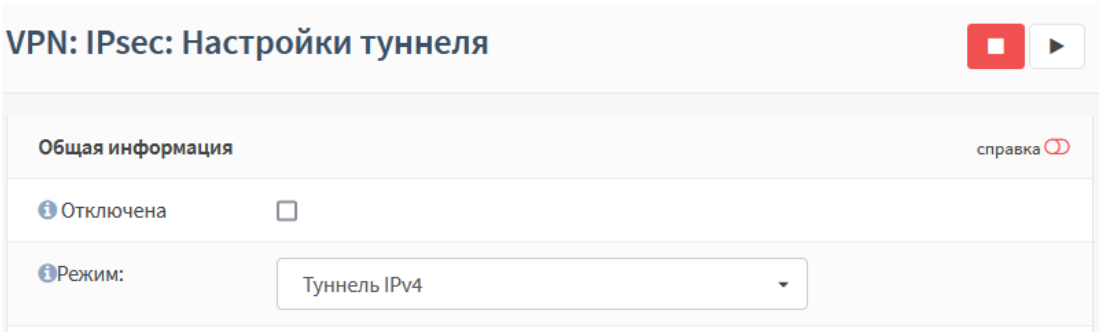

Рисунок 214 – Настройка фазы 2 на ARMA IF1

6. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.
7. Установить флажок для параметра **«Включить IPsec»** и нажать **кнопку «Сохранить»**.

Для разрешения прохождения трафика в LAN сеть необходимо создать разрешающее правило МЭ (см. Раздел 1.1.1) для интерфейса **«[IPsec]»**, выбрав в параметре **«Получатель»** LAN-сеть.

19.2.2.3 Шаг 3. Настройка туннеля IPsec на ARMA IF2

Для настройки туннеля IPsec **ARMA IF2** необходимо выполнить следующие действия:

1. Перейти в подраздел настроек IPsec (**«VPN»** - **«IPsec»** - **«Настройки туннеля»**) и нажать **кнопку «+»** для создания фазы 1.
2. Указать следующие настройки в открывшейся форме (см. Рисунок 212):
   - **«Удалённый шлюз»** – указать «172.16.1.2»;
   - **«Описание»** – внести «peer1»;
   - **«Предварительно выданный ключ»** – указать «12345»;
   - **«Алгоритм шифрования»** – «AES, 256»;
   - **«Группа ключей DH»** – «14 (2048 bits)»;
   - **«Отключить MOBIKE»** – флажок установлен;
   - **«Обнаружение недоступных пиров»** – флажок установлен.
3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.
4. Для созданной записи нажать **кнопку «+»** для добавления записи фазы 2.
5. Указать следующие настройки в открывшейся форме:
   - **«Описание»** – указать «peer 2»;

- **«Адрес»** (Удаленная сеть) – ввести «192.168.1.0/24»
- **«Алгоритмы шифрования»** – установить флажок для значения **«aes256gcm16»**;
- **«Алгоритмы хеша»** – выбрать «SHA1»;
- **«Автоматически пингуйте хост»** – ввести «192.168.1.1»

6. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.
7. Установить флажок для параметра **«Включить IPsec»** и нажать **кнопку «Сохранить»**.

Для разрешения прохождения трафика в LAN сеть необходимо создать разрешающее правило МЭ (см. Раздел 1.1.1) для интерфейса **«[IPsec]»**, выбрав в параметре **«Получатель»** LAN-сеть.

19.2.2.4 Проверка подключения

Для проверки работоспособности подключения необходимо на одном из **ARMA IF** перейти в подраздел статуса IPsec (**«VPN»** - **«IPsec»** - **«Информация о статусе»**) и убедиться в наличии активного соединения (см. Рисунок 215).

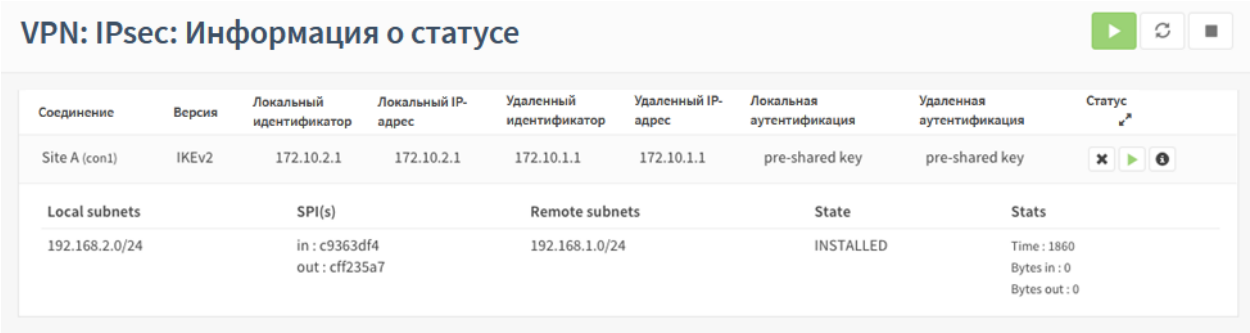

Рисунок 215 – Информация о статусе IPsec VPN

19.3 ГОСТ VPN

ГОСТ VPN – это реализация OpenVPN, с применением алгоритмов шифрования, соответствующих ГОСТ и криптографических средств, прошедших процедуру оценки соответствия в ФСБ России.

ARMA IF поддерживает работу ГОСТ VPN в режимах **«сеть - сеть»** и **«узел - сеть»**.

Перед настройкой режимов подключения необходимо выполнить установку лицензии ГОСТ VPN.

19.3.1 Установка или обновление лицензии ГОСТ VPN

Установка и обновление лицензии ГОСТ VPN производится через локальный консольный интерфейс. Для получения лицензии необходим доступ в Интернет.

Для установки или обновления лицензии необходимо выполнить следующие действия:

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

   и нажать **клавишу «Enter»** для смены кодировки и корректного отображения выводимой информации.
4. При первоначальном получении лицензии ввести команду:
   - «sudo -H /opt/cryptopack3/bin/mkseed -r /opt/cryptopack3/ssl/random_seed»

   и нажать **клавишу «Enter»** для запуска формирования файла инициализации программного ДСЧ. При обновлении лицензии запуск формирования файла инициализации программного ДСЧ не используется.
5. Последовательно нажимать на клавиатуре **клавиши**, соответствующие указанным в консоли символам (см. Рисунок 216). При правильном вводе будет произведена запись файла инициализации ДСЧ.

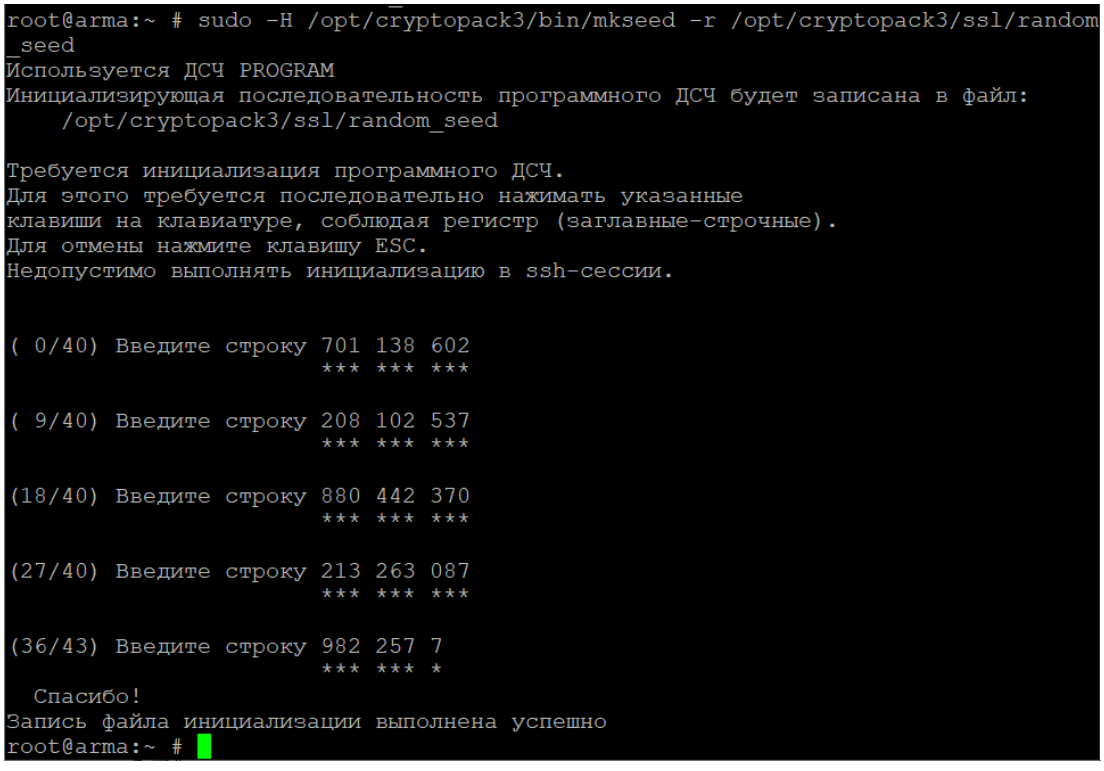

Рисунок 216 – Запись файла инициализации ДСЧ

6. Запустить процесс получения требуемой лицензии:

- для **серверной лицензии** ввести команду: «/opt/cryptopack3/bin/updater -n -k <Ключ продукта> -s http://licenses.cryptocom.ru/licgen2.php -l /opt/cryptopack3/ssl/cryptocom_server.lic»;
- для **клиентской лицензии** ввести команду: «/opt/cryptopack3/bin/updater -n -k <Ключ продукта> -s http://licenses.cryptocom.ru/licgen2.php -l /opt/cryptopack3/ssl/cryptocom_client.lic»

и нажать **клавишу «Enter»**.

7. В случае успешного получения лицензии будет выведено сообщение:
   - для **серверной лицензии**: «Получен файл лицензии. Лицензия успешно сохранена в файл "/opt/cryptopack3/ssl/cryptocom_server.lic"»;
   - для **клиентской лицензии**: «Получен файл лицензии. Лицензия успешно сохранена в файл "/opt/cryptopack3/ssl/cryptocom_ client.lic"».

!Важно Лицензия для ГОСТ VPN не входит в комплект поставки **ARMA IF** и приобретается отдельно.

19.3.2 Особенности создания подключений ГОСТ VPN

При активной лицензии ГОСТ VPN в веб-интерфейсе доступны следующие функции:

1. При запуске мастера настройки сервера OpenVPN перед первым шагом (см. Раздел 19.1.2.1) предлагается выбрать тип VPN (см. Рисунок 217).

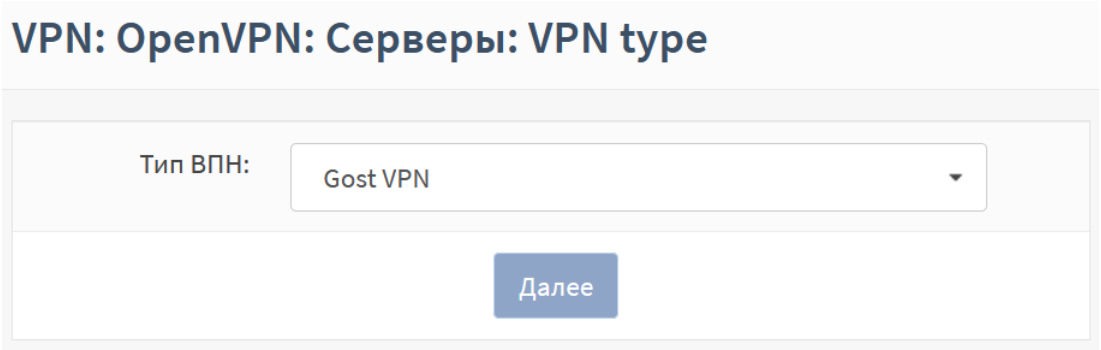

Рисунок 217 – Выбор типа VPN в мастере настроек OpenVPN сервера

   При выборе значения **«Gost VPN»** в последующих шагах мастера будут скрыты поля параметров, значения которых задаются в соответствии с ГОСТ VPN.

2. В открывшейся форме при нажатии **кнопки «+Добавить»** в разделе настройки серверов OpenVPN (**«VPN»** - **«OpenVPN»** - **«Серверы»**) будет доступен выбор тип VPN в выпадающем списке параметра **«Тип ВПН»** (см. Рисунок 218).

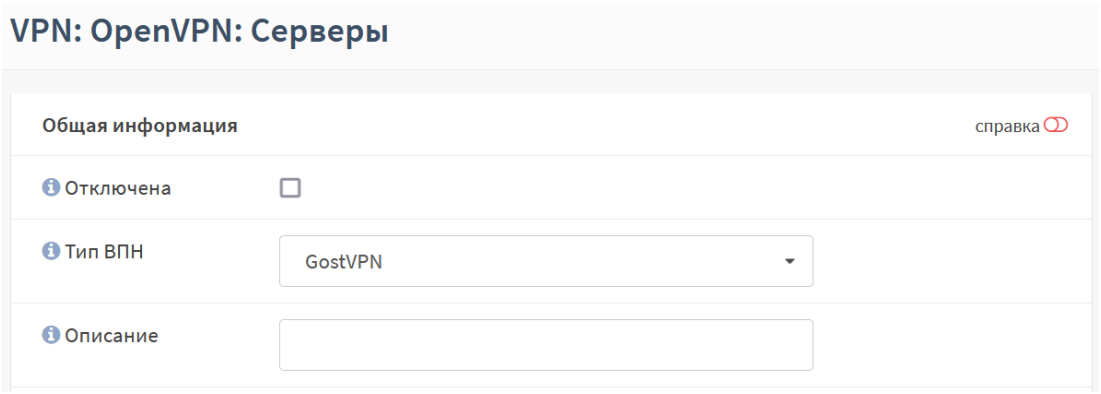

Рисунок 218 – Выбор типа VPN в форме добавления сервера OpenVPN

При выборе значения **«GostVPN»** будут скрыты поля параметров, значения которых задаются в соответствии с ГОСТ VPN.

3. В открывшейся форме при нажатии **кнопки «+Добавить»** в разделе настройки клиентов OpenVPN (**«VPN»** - **«OpenVPN»** - **«Клиенты»**) будет доступен выбор тип VPN в выпадающем списке параметра **«Тип ВПН»** (см. Рисунок 219).

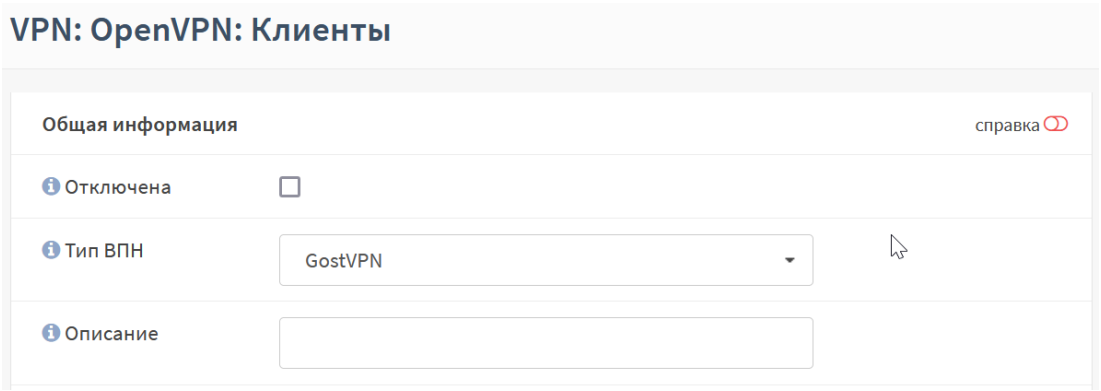

Рисунок 219 – Выбор типа VPN в форме добавления клиента OpenVPN

При выборе значения **«GostVPN»** в будут скрыты поля параметров, значения которых задаются в соответствии с ГОСТ VPN.

20 ПОРТАЛ АВТОРИЗАЦИИ

20.1 Настройка портала авторизации

Портал авторизации – это веб-страница авторизации, на которую принудительно перенаправляются пользователи, подключившиеся к выделенной сети, перед тем как получить доступ к веб-ресурсам. Принцип работы портала авторизации заключается в перехвате HTTP/HTTPS-сессии подключившегося к выделенной сети пользователя, и перенаправление их на веб-сервер авторизации.

В качестве примера будет рассмотрен следующий сценарий использования портала авторизации (см. Рисунок 220):

1. Гостевая сеть на интерфейсе **«OPT1»**.
2. Аутентификация на портале через локальную базу данных **ARMA IF**.
3. Доступ к веб-серверу имеют только пользователи из группы **«guests»**.
4. Для ПК **«Guest2»** отключена необходимость авторизации.

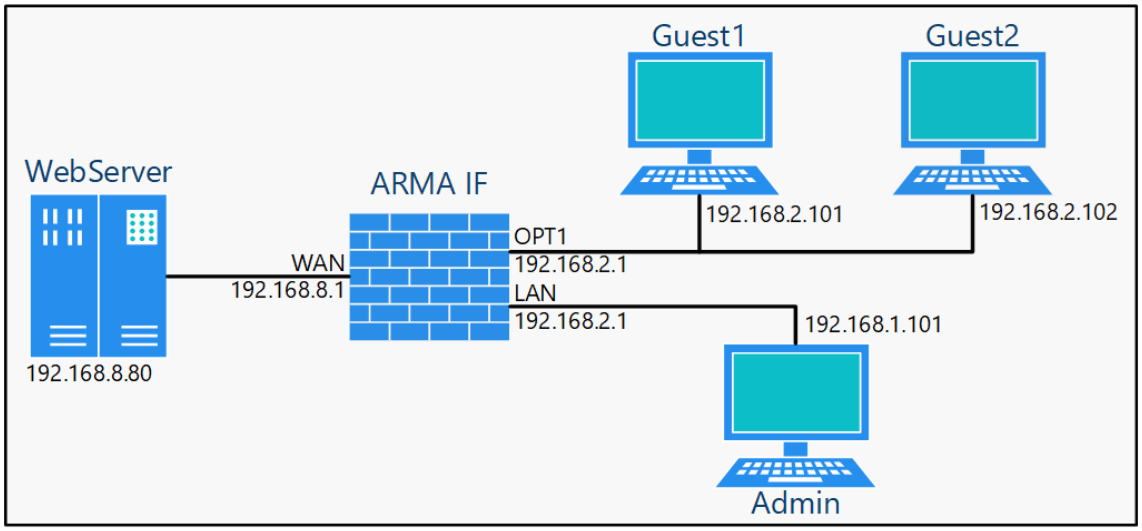

Рисунок 220 – ARMA IF в качестве портала авторизации для OPT1

Для настройки портала авторизации необходимо выполнить следующие действия:

1. Создать для интерфейса **«[OPT1]»** правила МЭ (см. Раздел 1.1.1):
   - разрешающее доступ к порталу авторизации (к порту 8000);
   - разрешающие доступ к веб-серверу.
2. Создать портал авторизации на выбранном интерфейсе.

Параметры правил представлены в таблице (см. Таблица 38).

Таблица 38
Параметры создаваемых правил

Параметр	Доступ к порталу авторизации	Доступ к веб-серверу по HTTP	Доступ к веб-серверу по HTTPS
Действие	Разрешить (Pass)	Разрешить (Pass)	Разрешить (Pass)
Интерфейс	OPT1	OPT1	OPT1
Протокол	TCP	TCP	TCP
Отправитель	OPT1 сеть	OPT1 сеть	OPT1 сеть
Получатель	Этот межсетевой экран	192.168.8.80	192.168.8.80
Диапазон портов назначения	Другое/8000	HTTP	HTTPS
Описание	Доступ к порталу авторизации	Разрешающее правило HTTP	Разрешающее правило HTTPS

20.1.1 Добавление портала авторизации

Для добавления портала авторизации на выбранном интерфейсе необходимо перейти в подраздел зон портала авторизации (**«Службы»** - **«Портал авторизации»** - **«Администрирование»**-вкладка **«Зоны»**), нажать **кнопку «+»**, заполнить поля в соответствии с таблицей (см. Таблица 39) и нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

Таблица 39
Добавление зоны авторизации

Параметр	Значение
Включено	Выбрано
Интерфейсы	OPT1
Аутентификация через	Локальная база данных
Значение тайм-аута бездействия	0
Значение тайм-аута сеанса	0
Множественный вход пользователя в систему	Не выбрано
Сертификат SSL	Отсутствует
Имя хоста	(оставить пустым)

Параметр	Значение
Разрешенные адреса	(оставить пустым)
Пользовательский шаблон	Интегрированный шаблон
Описание	Гостевой доступ

При создании или редактировании уже созданной зоны следует обратить внимание на данные параметры:

- **«Значение тайм-аута бездействия (в минутах)»** – в поле задаётся время, после которого клиенты будут отключены принудительно в случае бездействия.
- **«Значение тайм-аут сеанса (в минутах)»** – в поле задаётся время, после которого клиенты будут отключены принудительно.
- **«Множественный вход пользователя в систему»** – при включении данного параметра возможно выходить в сеть с одним логином с разных устройств одновременно.
- **«Прозрачный прокси (HTTP)»** – при включении данного параметра трафик будет перенаправлен на прозрачный прокси. Настройки прокси-сервера описаны в разделе 18 настоящего руководства.
- **«Прозрачный прокси (HTTPS)»** – параметр аналогичен предыдущему.

20.1.2 Работа портала авторизации

Для авторизации в портале авторизации необходимо на ПК **«Guest1»** открыть веб-браузер и ввести IP-адрес веб-сервера, «192.168.8.80». При успешной настройке портала авторизации появится форма входа (см. Рисунок 221).

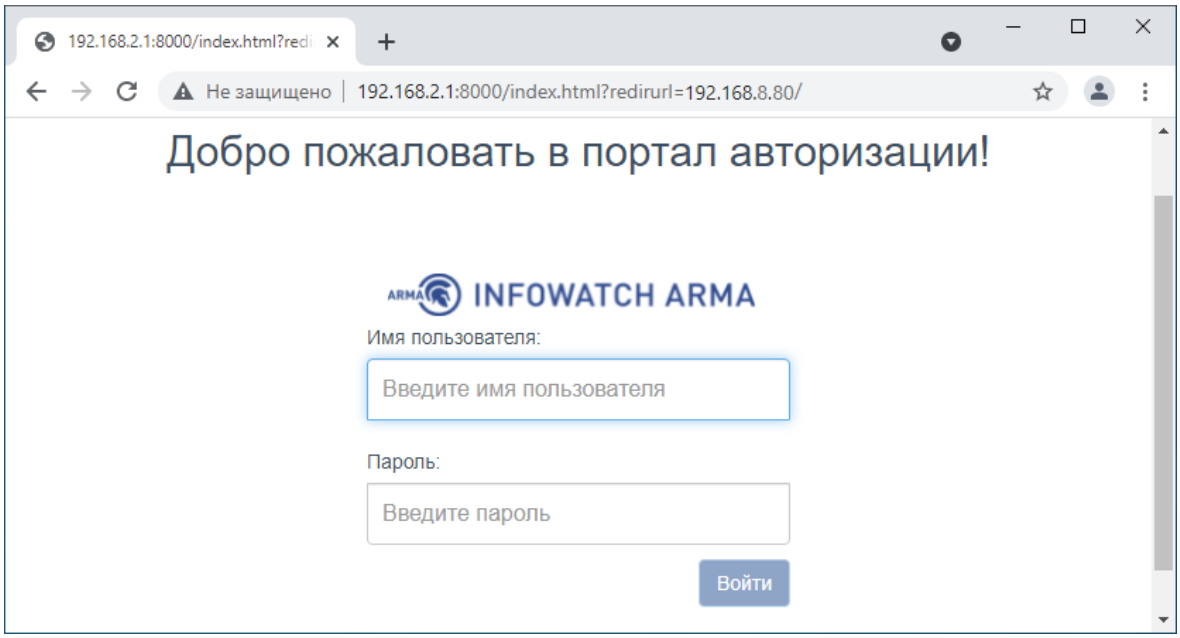

Рисунок 221 – Форма входа в портал авторизации

Необходимо ввести аутентификационные данные и нажать **кнопку «Вход»**. При успешной авторизации отобразится запрашиваемая страница (см. Рисунок 222).

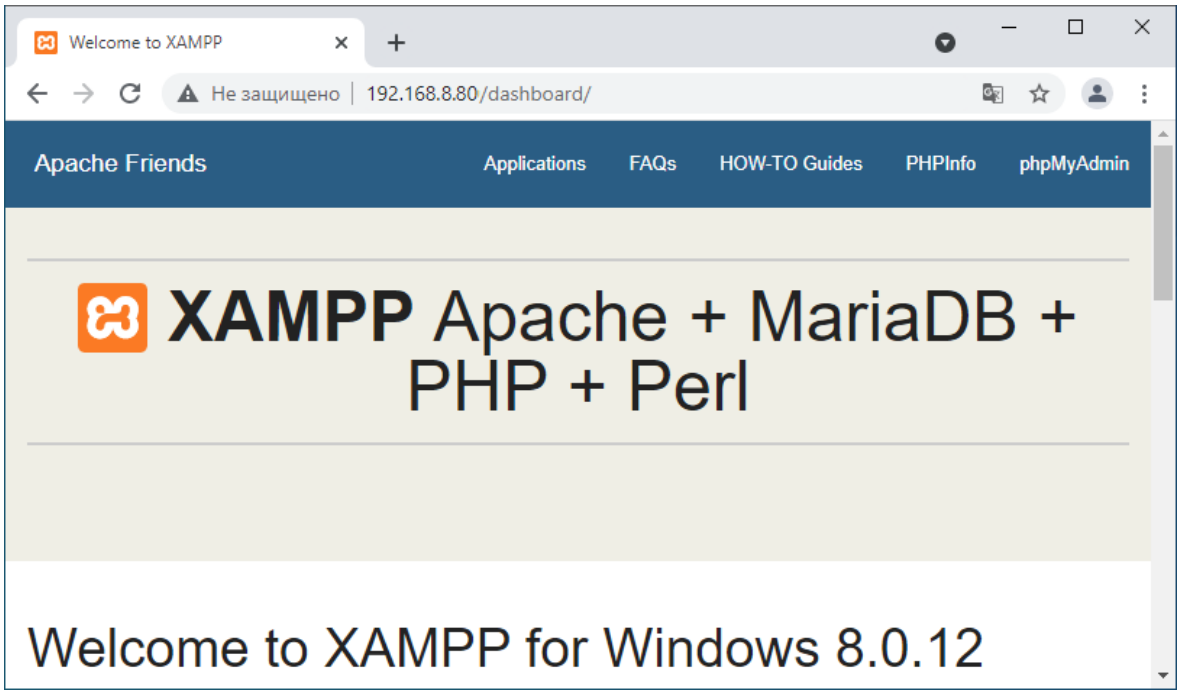

Рисунок 222 – Доступ к веб-серверу

Для выхода из Портала авторизации необходимо перейти на страницу «192.168.2.1:8000» и нажать **кнопку «Выйти»** (см. Рисунок 223).

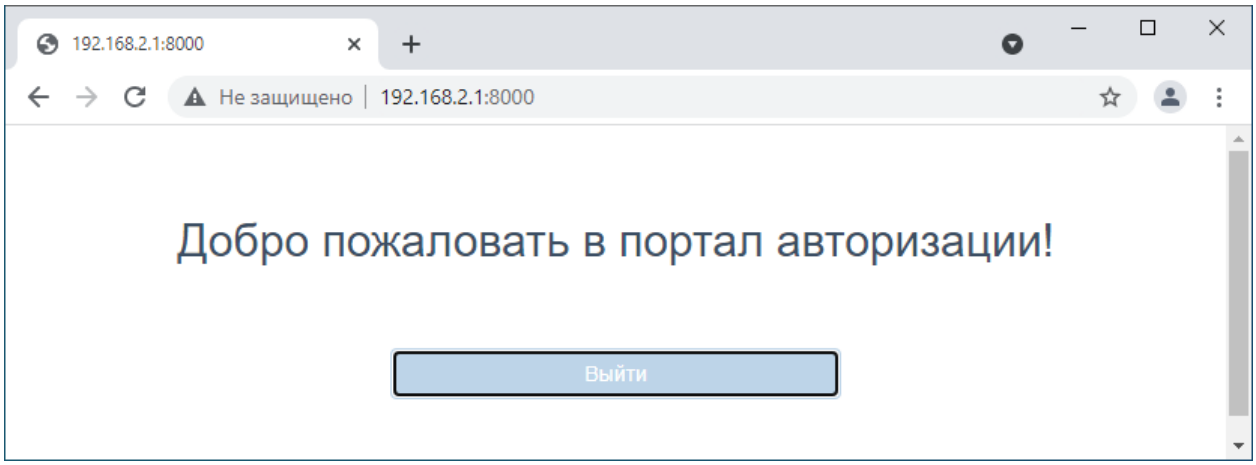

Рисунок 223 – Выход из Портала авторизации

20.2 Доступ пользователей к порталу авторизации

Доступ пользователей возможно корректировать следующими параметрами:

- **«Принудительно использовать локальную группу»**;
- **«Разрешенные адреса»**;
- **«Разрешенные MAC-адреса»**.

20.2.1 Параметр «Принудительно использовать локальную группу»

При создании или редактировании уже созданной зоны доступен параметр **«Принудительно использовать локальную группу»** (см. Рисунок 224).

Создание пользователей и групп пользователей для локальной БД описаны в разделе 21 настоящего руководства.

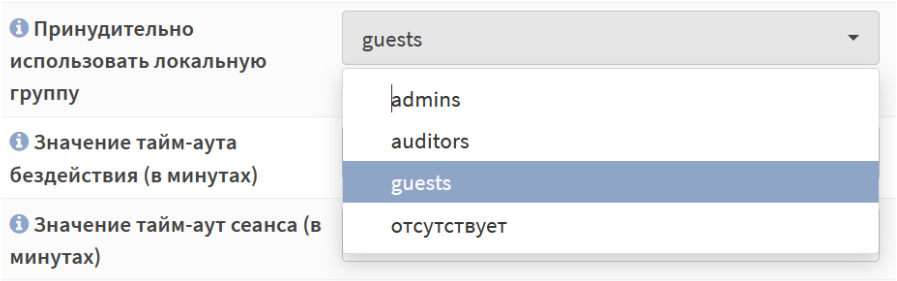

Рисунок 224 – Выбор группы для портала авторизации

В случае выбора группы доступ будет только у пользователей данной группы.

Согласно примеру, в данном параметре необходимо выбрать значение **«guests»** и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить»** для вступления изменений в силу.

В случае, если пользователь не состоит в выбранной группе, при аутентификации будет выведена ошибка (см. Рисунок 225).

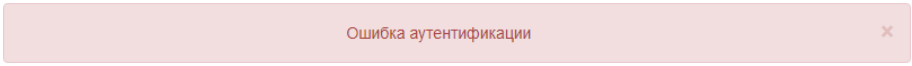

Рисунок 225 – Ошибка аутентификации

20.2.2 Параметр «Разрешенные адреса»

При создании или редактировании уже созданной зоны доступен параметр **«Разрешенные адреса»** (см. Рисунок 226).

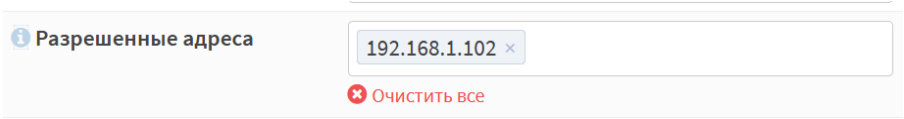

Рисунок 226 – Разрешенные адреса

Для всех IP-адресов или подсетей, указанных в поле данного параметра, доступ в сеть Интернет будет производиться без аутентификации на портале.

Согласно примеру, в данном параметре необходимо выбрать значение «192.168.2.102» и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить»** для вступления изменений в силу.

20.2.3 Параметр «Разрешенные MAC-адреса»

При создании или редактировании уже созданной зоны доступен параметр **«Разрешенные MAC-адреса»** (см. Рисунок 227). Данный параметр доступен только при взведении переключателя **«расширенный режим»** в верхней левой части формы.

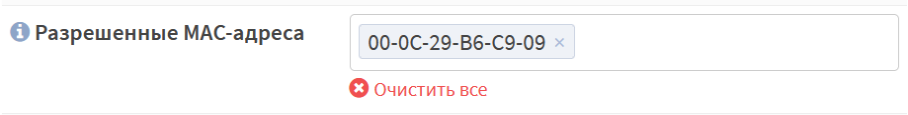

Рисунок 227 – Разрешенные MAC-адреса

Для всех MAC-адресов, указанных в поле данного параметра, доступ к веб-серверу будет производиться без аутентификации на портале.

21 УЧЕТНЫЕ ЗАПИСИ И ПРАВА ДОСТУПА

Пользовательские УЗ и их привилегии позволяют контролировать доступ к подразделам и службам **ARMA IF**.

21.1 Создание пользовательских учетных записей и их привилегий

Для создания пользовательской УЗ необходимо выполнить следующие действия:

1. Перейти в подраздел управления пользователями (**«Система»** - **«Доступ»** - **«Пользователи»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме заполнить обязательные параметры **«Имя пользователя»** и **«Пароль»** (см. Рисунок 228) и нажать **кнопку «Сохранить»**.

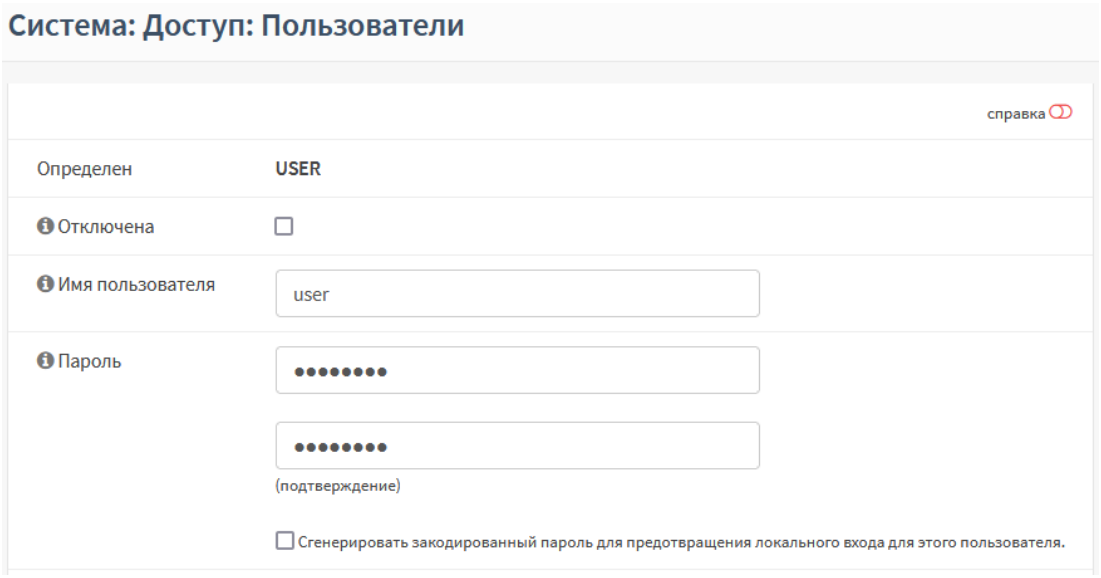

Рисунок 228 – Создание пользовательской УЗ

!Важно Значение параметра **«Имя пользователя»** не может быть:

- более 32 символов;
- начинаться с цифры;
- содержать символы, отличные от цифр **«0-9»**, **«A-Z»** верхнего и нижнего регистров и символов **«.-_»**.

21.1.1 Дополнительные параметры УЗ

Для более точной и полной информации о пользователе необходимо заполнить параметры **«Полное имя»**, **«Электронная почта»** и **«Комментарий»**.

Для создания временной пользовательской УЗ необходимо указать дату окончания срока действия в параметре **«Дата окончания срока действия»**. Пользователь будет иметь возможность авторизации по указанную дату включительно.

Флажок **«Сгенерировать закодированный пароль для предотвращения локального входа для этого пользователя»** параметра **«Пароль»** может используется, например, для создания УЗ с SSH-ключом, но без доступа к веб-интерфейсу.

Для изменения стартовой страницы необходимо задать значение параметра **«Предпочтительная целевая страница»**, например, «ui/integritycontrol». По умолчанию при авторизации в веб-интерфейсе **ARMA IF** пользователю отображается страница инструментальной панели – информационные виджеты (см. Раздел 27.1).

Для разрешения УЗ доступа к консольному интерфейсу **ARMA IF** необходимо установить флажок для параметра **«Доступ к консольному интерфейсу»**.

Для создания сертификата необходимо установить флажок для параметра **«Сертификат»**. Создание сертификатов используется **ARMA IF** для таких целей, как доступ к веб-интерфейсу через HTTPs, доступ к API, VPN, LDAP и т.д.

При настройке двухфакторной аутентификации в **ARMA IF** необходимо генерировать одноразовый пароль, установив флажок в **«Сгенерировать новый ключ (160 бит)»** параметра **«Выдача одноразовых паролей»**.

Для предоставления пользователю доступа к консольному интерфейсу **ARMA IF** по SSH (см. Раздел 9) необходимо ввести сгенерированный ранее открытый ключ в поле параметра **«Авторизованные ключи»**.

Для подключения к настройке мобильного IPsec необходимо задать предварительный общий ключ в поле параметра **«Предварительно выданные ключи IPsec»**.

21.1.2 Назначение привилегий пользовательской УЗ

Назначение привилегий пользовательской учетной записи возможно двумя способами:

- добавление пользователя в определенную группу с уже заданными привилегиями;
- выбор привилегий из списка, установкой флажка напротив соответствующей привилегии в блоке настроек **«Системные привилегии»** (см. Рисунок 229).

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

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

- **«Отменить выбор (видимые)»**.

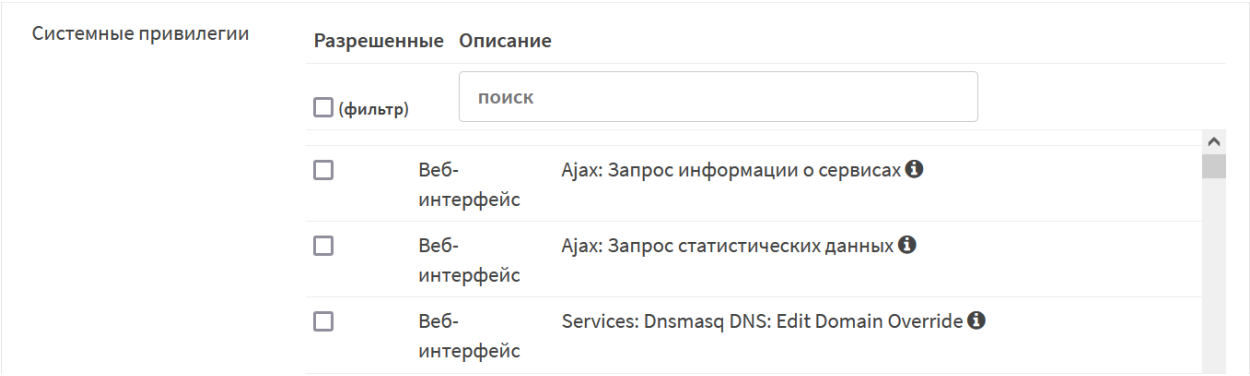

Рисунок 229 – Установка системных привилегий

21.2 Создание группы и добавление им привилегий

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

Для создания группы пользователей необходимо выполнить следующие действия:

1. Перейти в подраздел управления группами пользователей (**«Система»** - **«Доступ»** - **«Группы»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме заполнить обязательный параметр **«Имя группы»** (см. Рисунок 230) и нажать **кнопку «Сохранить»**.

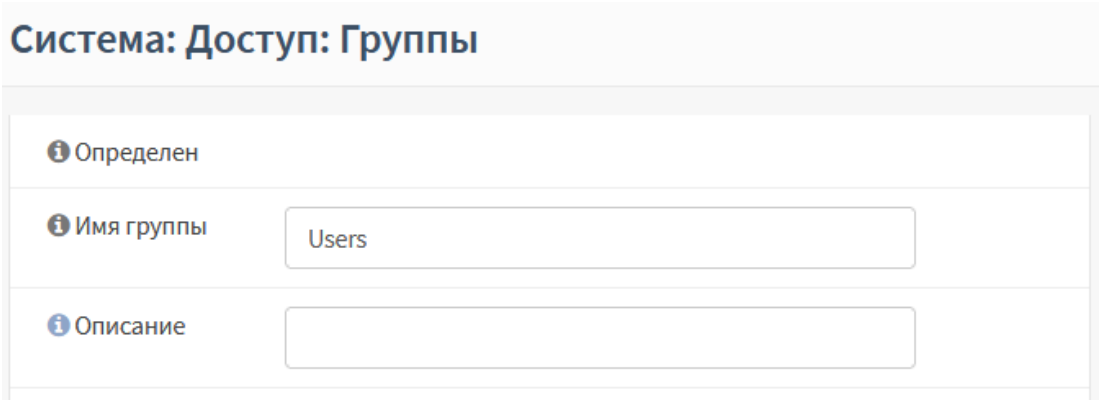

Рисунок 230 – Создание группы пользователей

21.2.1 Дополнительные параметры групп

Для удобства использования групп необходимо добавить описание группы в поле параметра **«Описание»**.

Для добавления пользователей в создаваемую группу необходимо в блоке настроек **«Участники группы»** перенести имена пользователей из левой части в правую нажав **кнопку «»** (см. Рисунок 231).

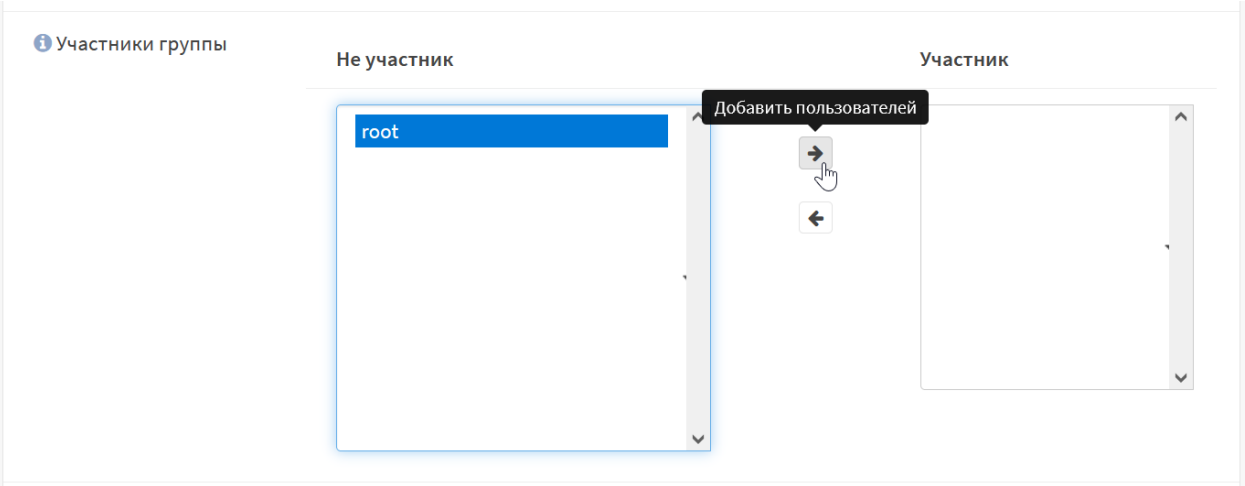

Рисунок 231 – Добавление участников в группу

21.2.2 Назначение привилегий группе

Для назначения привилегий группе пользователей необходимо выбрать привилегии из списка, установив флажок напротив соответствующей привилегии в блоке настроек **«Системные привилегии»** аналогично назначению привилегий пользовательской УЗ (см. Раздел 21.1.2).

21.3 Настройка парольной политики

Парольная политика – это набор правил при создании пароля, позволяющих повысить безопасность доступа к **ARMA IF**.

Для включения и настройки парольной политики необходимо выполнить следующие действия:

1. Перейти в подраздел редактирования серверов авторизации (**«Система»** - **«Доступ»** - **«Серверы»**) и нажать **кнопку «** **»** напротив строки «Локальная база данных» для входа в режим редактирования.
2. В открывшейся форме установить флажок для параметра **«Включить ограничения политики паролей»**.
3. При необходимости задать значение в появившихся параметрах (см. Рисунок 232):
    - **«Срок действия»** – количество дней, в течение которых пароль остается действительным;
    - **«Длина»** – минимальная длина пароля;
    - **«Сложность»** – соответствие пароля требованиям сложности: пароль должен содержать цифры, прописные буквы, строчные буквы, специальные символы.

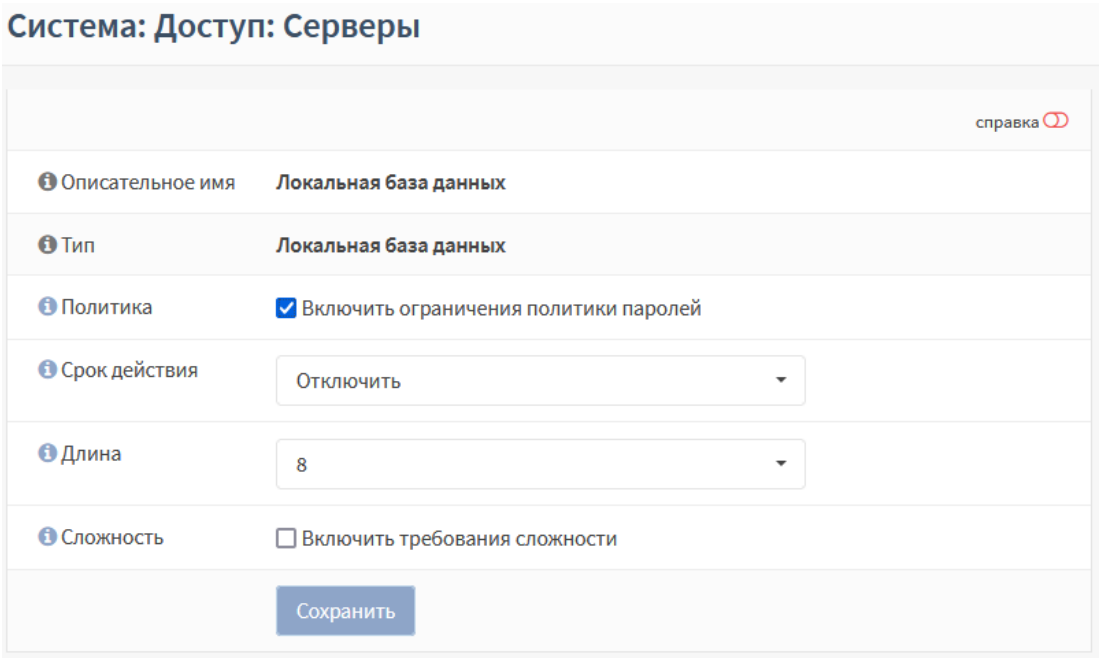

Рисунок 232 – Настройка парольной политики

4. Нажать **кнопку «Сохранить»**

После внесенных изменений при входе в систему с УЗ, пароль которой не отвечает установленным требованиям, будет предложено изменить пароль.

21.4 Аутентификация

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

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

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

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

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

21.4.1 Ваучер-сервер

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

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

Для создания и настройки ваучер-сервера необходимо выполнить следующие действия:

1. Перейти в подраздел редактирования серверов авторизации (**«Система»** - **«Доступ»** - **«Серверы»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок 233), в параметре **«Тип»**, выбрать «Ваучер».
3. При необходимости установить флажок для параметра **«Использовать простые пароли (менее безопасные)»** и задать значения для параметров:
   - **«Описательное имя»**;
   - **«Длина имени пользователя»**;
   - **«Длина пароля»**.

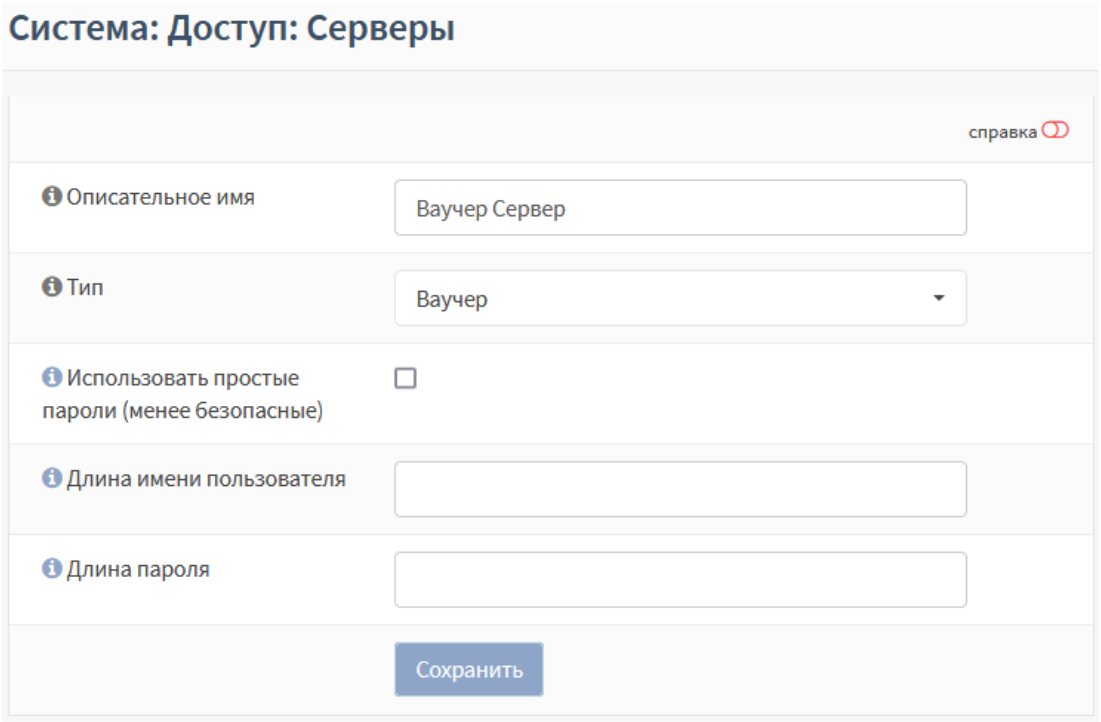

Рисунок 233 – Создание ваучер сервера

4. Нажать **кнопку «Сохранить»**.

21.4.1.1 Использование ваучер-сервера для авторизации

Для использования ваучер-сервера на созданном портале авторизации необходимо выполнить следующие действия:

1. Перейти в подраздел зон портала авторизации (**«Службы»** - **«Портал авторизации»** - **«Администрирование»** - **«Зоны»**).
2. Нажать **кнопку «** **»** напротив созданной зоны и, в открывшейся форме, в параметре **«Аутентификация через»**, выбрать созданный ваучер сервер (см. Рисунок 234) и нажать **кнопку «Сохранить»**.

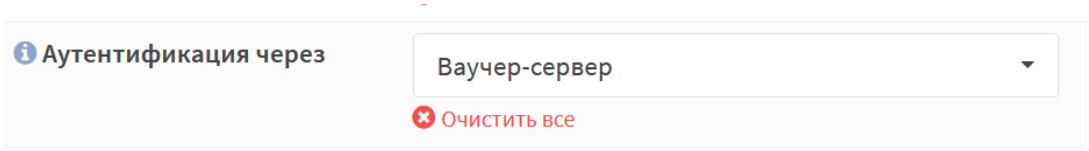

Рисунок 234 – Выбор метода аутентификации

3. Перейти в подраздел управления ваучерами (**«Службы»** - **«Портал авторизации»** - **«Ваучеры»**) и нажать **кнопку «Создать ваучеры»**.
4. При необходимости в открывшейся форме задать значения для параметров:
   - **«Достоверность»**;
   - **«Истекает после»**;
   - **«Количество ваучеров»**;
   - **«Имя группы»**;

   и нажать **кнопку «Сгенерировать»**.
5. Созданный ваучер в формате «.CSV» будет предложено скачать средствами используемого веб-браузера. Скаченный ваучер позволяет успешно аутентифицироваться через портал авторизации.

21.4.2 Двухфакторная аутентификация

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

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

Для настройки двухфакторной аутентификации необходимо выполнить следующие шаги:

1. Добавить сервер аутентификации.
2. Добавить или настроить пользовательские УЗ.

3. Активировать одноразовый пароль.
4. Проверить токен.

21.4.2.1 Шаг 1 – Добавление сервера аутентификации

Для добавления сервера двухфакторной аутентификации необходимо выполнить следующие действия:

1. Перейти в подраздел редактирования серверов авторизации (**«Система»** - **«Доступ»** - **«Серверы»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме задать настройки в соответствии с таблицей (см. Таблица 40). Значения параметров в таблице приведены справочно.

Таблица 40
Настройки сервера аутентификации

Параметр	Значение
Описательное имя	Сервер TOTP
Тип	Локальный + Синхронизированный по времени одноразовый пароль

3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**.

Дополнительные параметры:

- **«Длина токена»** – может быть изменен при необходимости;
- **«Интервал времени»** – может быть изменен при необходимости;
- **«Разрешенный период регистрации»** – используется для генерации нескольких различных токенов для разных периодов времени и сравнения их с токеном по передаваемому паролю;
- **«Обратный порядок токена»** – используется для установки требования пароля перед токеном.

21.4.2.2 Шаг 2 – Добавление или настройка пользовательской учетной записи

Для добавления пользовательской УЗ необходимо выполнить следующие действия:

1. Перейти в подраздел управления пользователями (**«Система»** - **«Доступ»** - **«Пользователи»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме заполнить обязательные параметры **«Имя пользователя»** и **«Пароль»**, установить флажок в значении **«Сгенерировать**

новый ключ (160 бит)» параметра **«Выдача одноразовых паролей»** и нажать **кнопку «Сохранить»**.

21.4.2.3 Шаг 3 – Активация одноразового пароля

Для активации нового одноразового пароля необходимо выполнить следующие действия:

1. Нажать **кнопку «** **»** напротив созданной на шаге 2 (см. Раздел 21.4.2.2) УЗ.
2. Нажать **кнопку «Нажмите, чтобы показать»** в параметре **«OTP QR код»** (см. Рисунок 235).

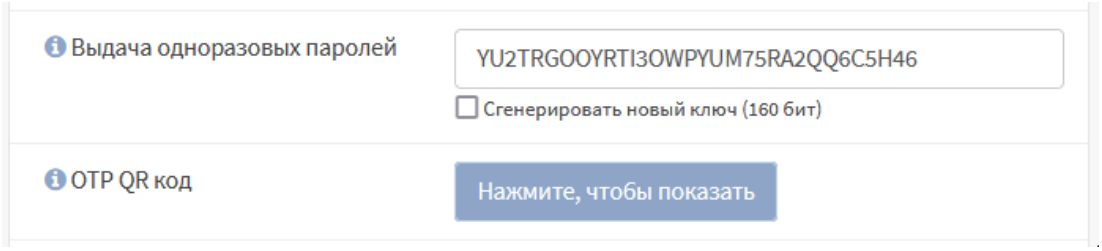

Рисунок 235 – Активация одноразового пароля

3. Появившийся QR-код или содержимое значения параметра **«Выдача одноразовых паролей»** необходимо передать владельцу пользовательской УЗ.
4. Владельцу УЗ на мобильном устройстве открыть определенное администратором приложение, например, FreeOTP для ОС Android, и отсканировать полученный QR-код или ввести полученный одноразовый пароль. Подтвердить правильность сканирования QR-кода или ввода одноразового пароля и дождаться получения токена в приложении.

21.4.2.4 Шаг 4 – Проверка токена

Для тестирования аутентификации пользователя необходимо выполнить следующие действия:

1. Перейти в подраздел средств проверки (**«Система»** - **«Доступ»** - **«Средство проверки»**).
2. В параметре **«Сервер аутентификации»** выбрать созданный на шаге 1 (см. Раздел 21.4.2.1) сервер, в параметрах **«Имя пользователя»** и **«Пароль»** ввести данные УЗ, созданной на шаге 2 (см. Раздел 21.4.2.2), в параметре **«Токен»** указать токен из шага 3 (см. Раздел 21.4.2.3) и нажать **кнопку «Проверка»**.
3. В случае правильной настройки сервера появится уведомление об успешной проверке (см. Рисунок 239). В случае указания некорректных данных появится уведомление об ошибке (см. Рисунок 240).

21.4.3 LDAP

LDAP – протокол прикладного уровня для доступа к службе каталогов, использующий TCP/IP и позволяющий производить операции аутентификации, поиска и сравнения, а также операции добавления, изменения или удаления записей.

В качестве примера настройки LDAP будет описана настройка работы **ARMA IF** с MS Active Directory согласно схеме стенда, представленной на рисунке (см. Рисунок 236).

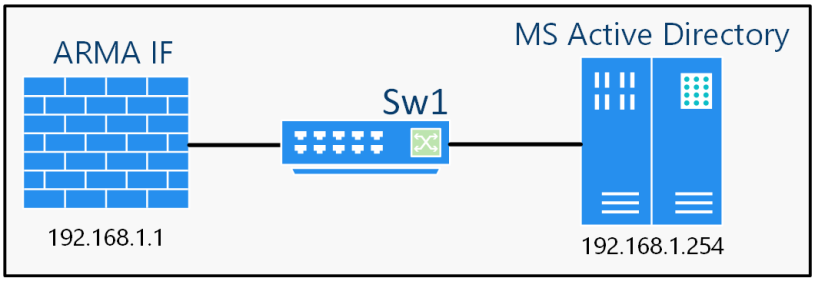

Рисунок 236 – Подключение внешнего сервера LDAP

Перед началом настройки внешнего LDAP-сервера необходимо убедиться в наличии сетевого доступа к серверу Active Directory.

При использовании учётных записей LDAP-сервера для доступа к веб-интерфейсу **ARMA IF** необходимо определить привилегии УЗ, путем импорта пользовательских УЗ из LDAP-сервера.

Для настройки внешнего сервера LDAP необходимо выполнить следующие шаги:

1. Добавить внешний сервер LDAP.
2. Протестировать соединение.
3. Обновить настройки доступа к системе.
4. Импортировать пользовательские УЗ.

21.4.3.1 Шаг 1 – Добавление сервера LDAP

Для добавления сервера LDAP необходимо выполнить следующие действия:

1. Перейти в подраздел редактирования серверов авторизации (**«Система»** - **«Доступ»** - **«Серверы»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме задать настройки в соответствии с таблицей (см. Таблица 41). Значения параметров в таблице приведены справочно и зависят от настроек внешнего сервера Active Directory.

Таблица 41
Настройки LDAP сервера

Параметр	Значение
Описательное имя	LDAP server
Тип	LDAP
Имя хоста или IP-адрес	192.168.1.254
Привязать параметры доступа	Указать Имя пользователя и пароль
Область поиска	Целое поддерево
Базовый DN:	DC=opc,DC=local
Контейнеры для аутентификации	Нажать **кнопку «Выбрать»** и выбрать из доступного списка (см. Рисунок 237).
Начальный шаблон	Microsoft AD
Чтение свойств	Установить флажок

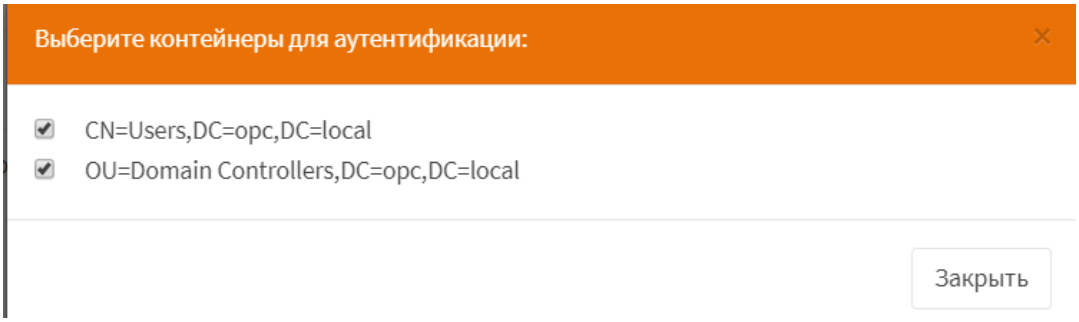

Рисунок 237 – Контейнеры для аутентификации

3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**.

Дополнительные параметры:

- **«Расширенный запрос»** – может быть использован для выбора пользователей, которые являются членами определенной группы;
- **«Синхронизировать группы»** – рекомендуется использовать только при необходимости;
- **«Ограничение групп»** – рекомендуется использовать только при необходимости.

21.4.3.2 Шаг 2 – Тест соединения

Для проверки правильности настройки сервера необходимо выполнить следующие действия:

1. Перейти в подраздел средств проверки (**«Система»** - **«Доступ»** - **«Средство проверки»**) (см. Рисунок 238).

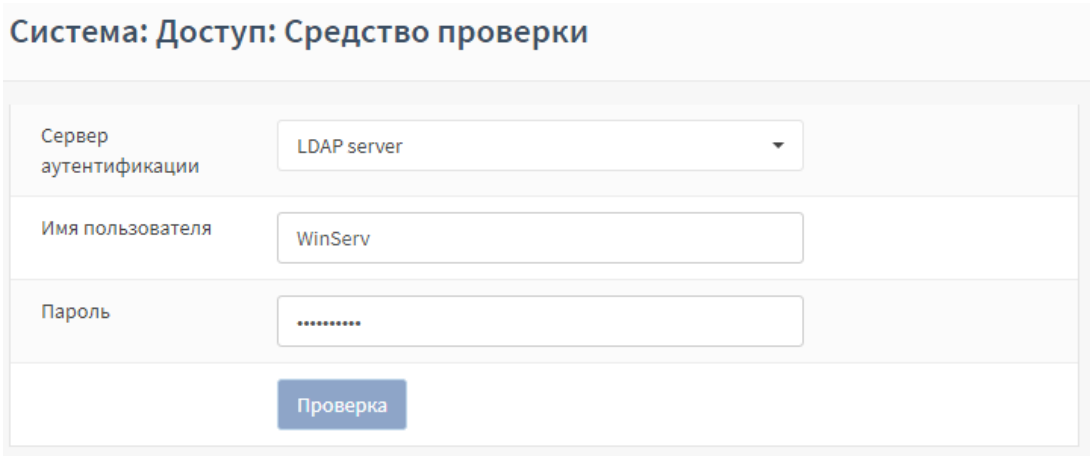

Рисунок 238 – Проверка правильности настройки LDAP-сервера

2. В параметре **«Сервер аутентификации»** выбрать созданный на шаге 1 (см. Раздел 21.4.3.1) LDAP-сервер, в параметрах **«Имя пользователя»** и **«Пароль»** ввести учётные данные для подключения к внешнему LDAP серверу и нажать **кнопку «Проверка»**.
3. В случае корректной настройки появится уведомление об успешной аутентификации (см. Рисунок 239).

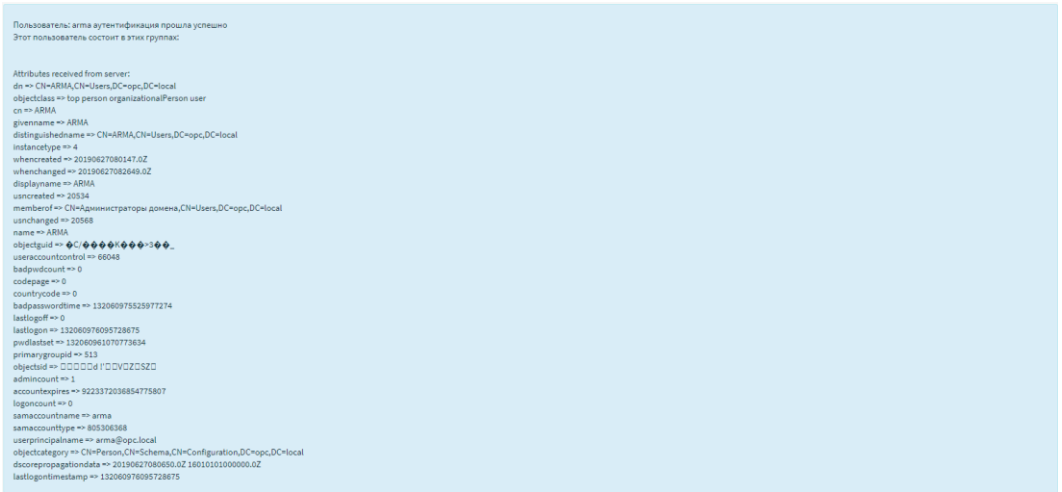

Рисунок 239 – Успешная аутентификация

4. В случае некорректной настройки или ошибки в учетных данных будет отображена ошибка аутентификации (см. Рисунок 240).

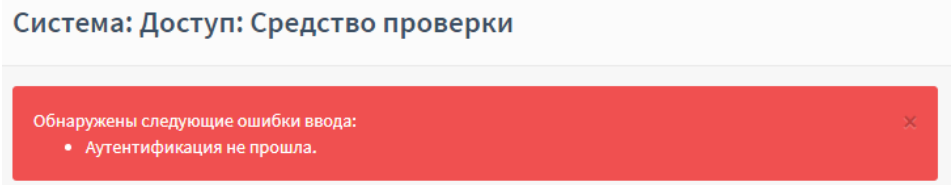

Рисунок 240 – Ошибка аутентификации

21.4.3.3 Шаг 3 – Обновление настроек доступа к системе

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

Для обновления настроек доступа к системе необходимо выполнить следующие действия:

1. Перейти в подраздел настроек **ARMA IF** (**«Система»** - **«Настройки»** - **«Администрирование»**).
2. В блоке **«Аутентификация»** (см. Рисунок 241) добавить сервер аутентификации «LDAP-сервер», созданный на шаге 1 (см. Раздел 21.4.3.1), и нажать **кнопку «Сохранить»**.

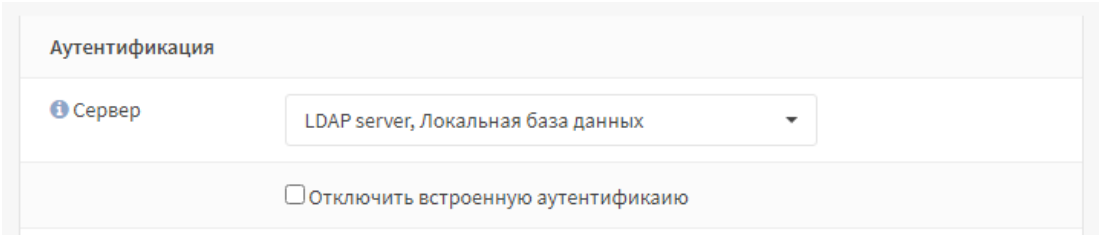

Рисунок 241 – Выбор сервера аутентификации

21.4.3.4 Шаг 4 – Импорт пользовательских УЗ

Для предоставления доступа к веб-интерфейсу пользовательским УЗ внешнего LDAP-сервера, их необходимо импортировать в **ARMA IF**.

Для импорта УЗ необходимо выполнить следующие действия:

1. Перейти в подраздел управления пользователями (**«Система»** - **«Доступ»** - **«Пользователи»**) (см. Рисунок 242).

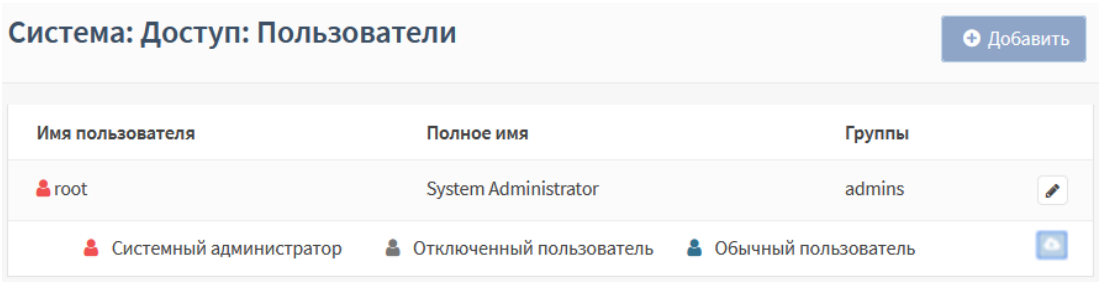

Рисунок 242 – Импорт пользовательских учетных записей LDAP-сервера

2. Нажать появившуюся **кнопку «**  **»** в правом нижнем углу формы.
3. В открывшейся форме установить флажки для импортируемых пользовательских УЗ (см. Рисунок 243) и нажать **кнопку «ОК»**. Импорт произведен успешно, если после нажатия кнопки не появилось сообщений об ошибке и выбранные пользователи отображены в общем списке пользователей.

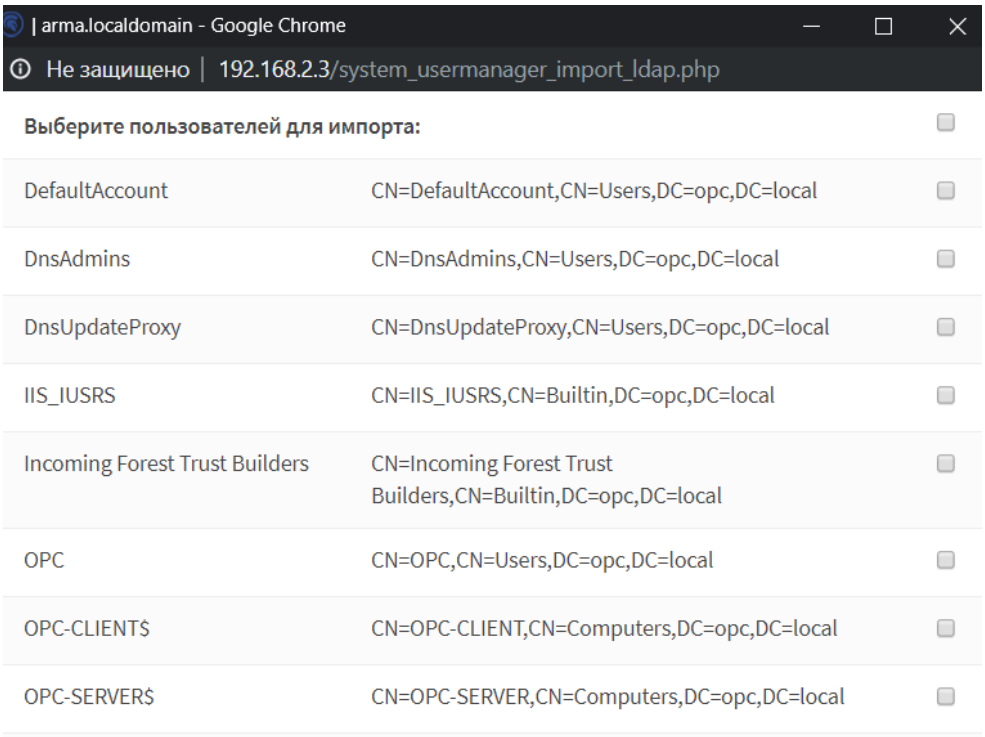

Рисунок 243 – Выбор импортируемых пользовательских учетных записей

21.4.4 Radius

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

ARMA IF поддерживает использование внешнего Radius-сервера для аутентификации пользователей в сервисах VPN (см. Раздел 19) и портала авторизации (см. Раздел 20).

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

21.4.4.1 Добавление внешнего Radius-сервера

Для добавления внешнего Radius-сервера необходимо выполнить следующие действия:

1. Перейти в подраздел редактирования серверов авторизации (**«Система»** - **«Доступ»** - **«Серверы»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме задать настройки в соответствии с таблицей (см. Таблица 42). Значения параметров приведены справочно и зависят от настроек внешнего Radius-сервера.

Таблица 42
Настройки Radius-сервера

Параметр	Значение
Описательное имя	Radius server
Тип	Radius
Имя хоста или IP-адрес	192.168.1.254
Общий секретный ключ	Указать секретный ключ сервера
Предложенные службы	Аутентификация и учет

3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**.

21.4.4.2 Проверка работы внешнего Radius-сервера

Перед проверкой правильности настройки сервера необходимо создать две УЗ:

- **«user»** – с запретом доступа к **ARMA IF**;
- **«user1»** – с разрешением доступа к **ARMA IF**.

Для проверки правильности настройки сервера необходимо выполнить следующие действия:

1. Перейти в подраздел средств проверки (**«Система»** - **«Доступ»** - **«Средство проверки»**).
2. В параметре **«Сервер аутентификации»** выбрать созданный Radius-сервер, в параметрах **«Имя пользователя»** и **«Пароль»** ввести данные УЗ внешнего Radius-сервера и нажать **кнопку «Проверка»**:
    - УЗ **«user»** – не проходит аутентификацию с выводом соответствующего уведомления (см. Рисунок 240);
    - УЗ **«user1»** – проходит аутентификацию с выводом соответствующего уведомления (см. Рисунок 239).

22 МАСТЕР ПЕРВОНАЧАЛЬНОЙ НАСТРОЙКИ

При первом входе пользователя в веб-интерфейс **ARMA IF** автоматически предоставляет мастер первоначальной настройки системы (см. Рисунок 244). Мастер будет запущен на английском языке.

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

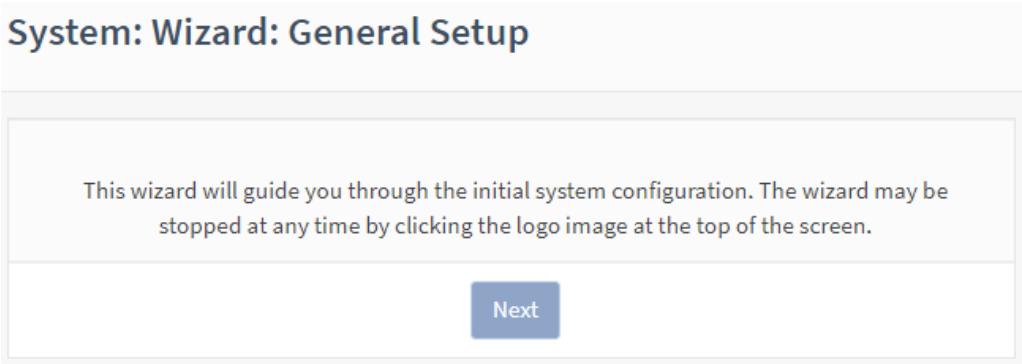

Рисунок 244 – Мастер первоначальной настройки

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

22.1 Шаги Мастера первоначальной настройки

22.1.1 Мастер: шаг 1

На данном шаге предлагается настроить имя хоста, необходимое для идентификации межсетевого экрана, указать домен, в котором находится **ARMA IF**, и сменить язык интерфейса (см. Рисунок 245).

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

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

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

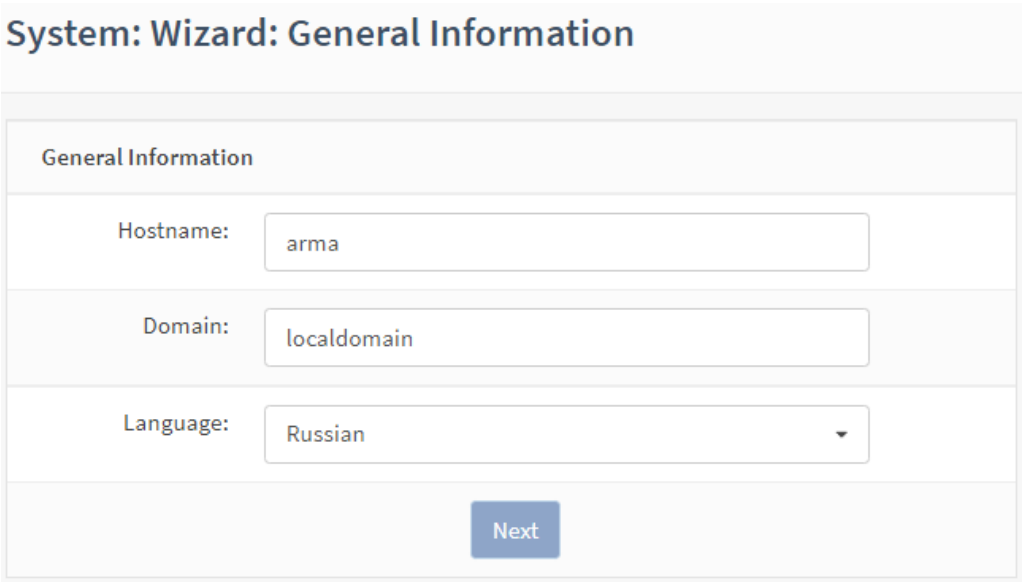

Рисунок 245 – Мастер первоначальной настройки. Шаг 1

22.1.2 Мастер: шаг 2

На данном шаге предлагается задать параметры NTP-сервера и часового пояса (см. Рисунок 246). Для NTP-сервера указывается полное доменное имя или IP-адрес хоста. Если не требуется конкретный NTP-сервер, рекомендуется оставить имя сервера времени по умолчанию. Чтобы использовать несколько серверов времени необходимо добавлять их в одно поле, разделяя каждый сервер пробелом. Часовой пояс рекомендуется выбирать в соответствии с физическим расположением МЭ.

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

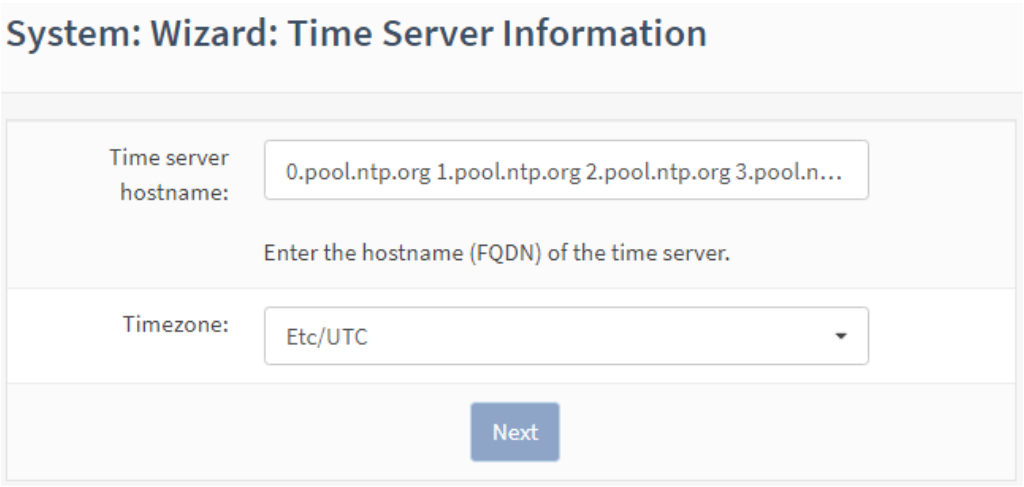

Рисунок 246 – Мастер первоначальной настройки. Шаг 2

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

22.1.3 Мастер: шаг 3

На данном шаге предлагается указать пароль к системной УЗ **«root»** (см. Рисунок 247). Автоматически никакие ограничения к паролю не применяются, рекомендуется использовать надежный пароль.

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

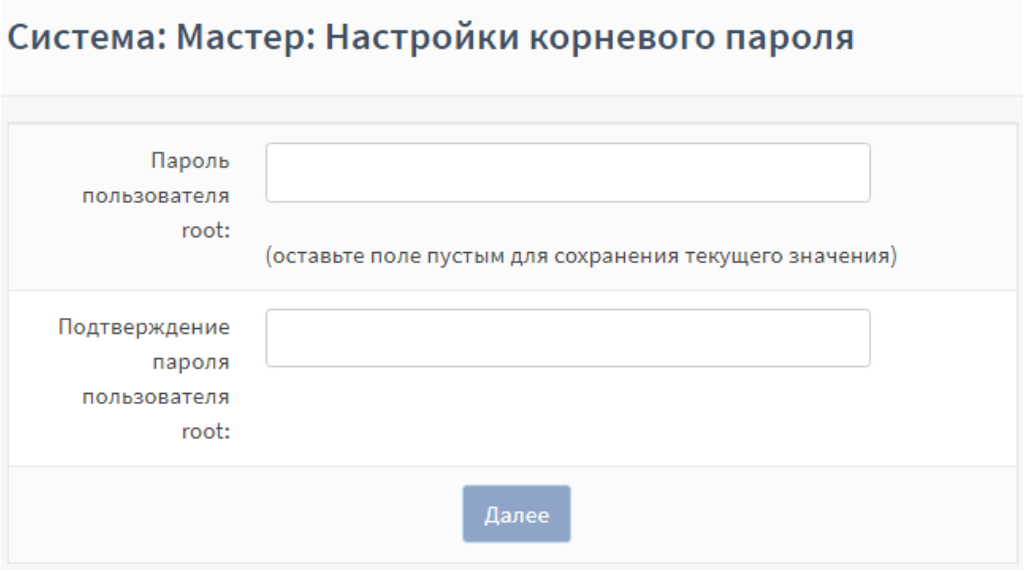

Рисунок 247 – Мастер первоначальной настройки. Шаг 3

22.1.4 Мастер: шаг 4

На данном шаге предлагается выполнить перезагрузку для применения настроек (см. Рисунок 248). Необходимо нажать **кнопку «Перезагрузить»**.

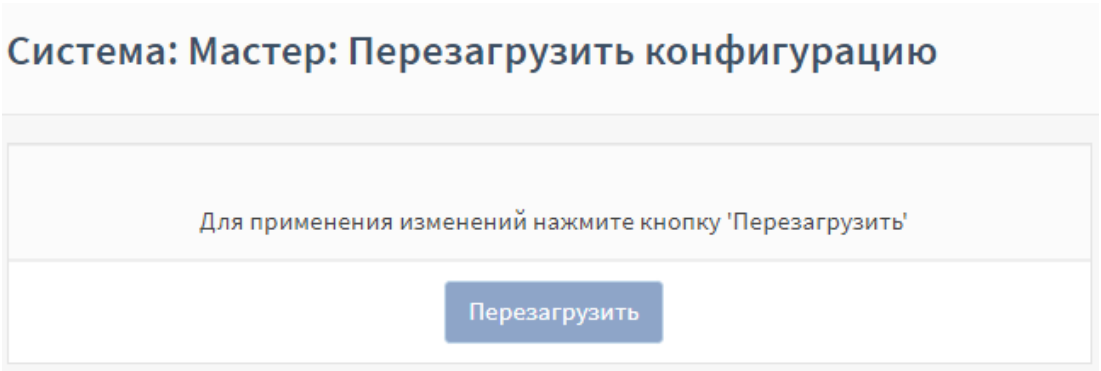

Рисунок 248 – Мастер первоначальной настройки. Шаг 4

В случае, когда необходимо, будет выполнена перезагрузка **ARMA IF**, в остальных случаях будет произведен переход на страницу **«Инструменты»** с виджетами.

23 КОНФИГУРАЦИЯ

Раздел **«Конфигурация»** позволяет выполнять следующие действия:

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

23.1 Резервное копирование

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

Для создания локальной резервной копии конфигурации необходимо выполнить следующие действия:

1. Перейти в подраздел резервного копирования (**«Система»** - **«Конфигурация»** - **«Резервные копии»**) (см. Рисунок 249).
2. Для отключения создания резервной копии БД установить флажок для параметра **«Не делать резервную копию базу данных RRD»**.
3. Задать пароль для резервной копии в полях параметров **«Пароль»** и **«Подтверждение»**, а затем нажать **кнопку «Сохранить конфигурацию»**.

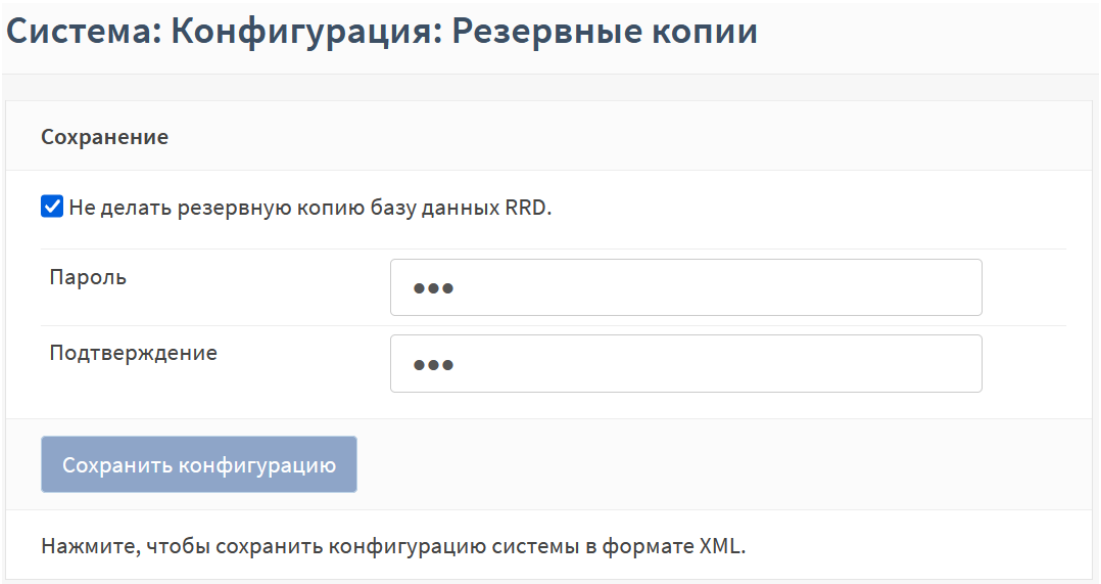

Рисунок 249 – Сохранение текущей конфигурации

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

23.2 История изменений

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

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

23.2.1 Указание количества хранимых резервных копий

Для указания количества хранимых резервных копий конфигурации необходимо в блоке настроек **«Количество резервных копий»** задать требуемое значение (см. Рисунок 250) и нажать **кнопку «Сохранить»**. На каждое изменение конфигурации создается отдельная резервная копия. По истечению заданного количества резервных копий последняя копия будет удалена и создана новая.

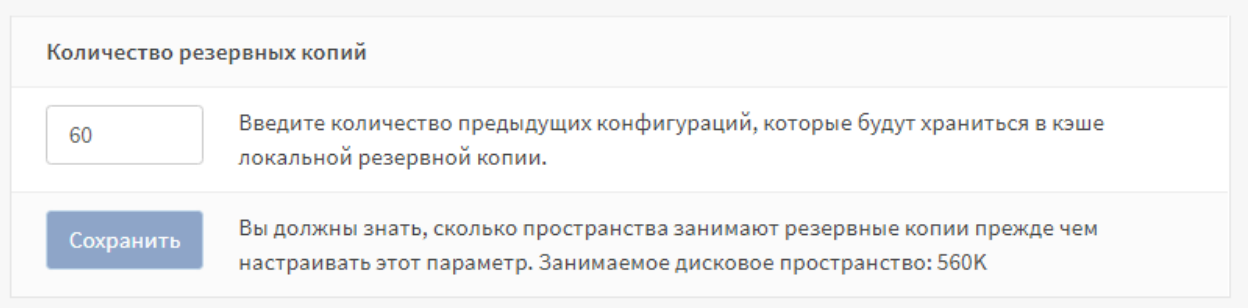

Рисунок 250 – Настройка количества резервных копий

23.2.2 Просмотр истории изменений

Для просмотра истории изменений необходимо выполнить следующие действия:

1. В блоке настроек **«История изменений»**, в списке сохраненных конфигураций, выбрать более раннюю версию в левом столбце, а более позднюю в правом столбце и нажать **кнопку «Просмотреть отличия»**.
2. Отличия между выбранными версиями будут отображены в блоке **«Отличия конфигурации»** в универсальном формате diff-файла:
   - строки, начинающиеся со знака **«-»** показывают, что было удалено из конфигурации;
   - строки, начинающиеся со знака **«+»** показывают, что было добавлено в конфигурацию;
   - строки без знаков показывают, что осталось без изменений (см. Рисунок 251).

Рисунок 251 – Просмотр изменений между конфигурациями

23.2.3 Возврат к предыдущей сохраненной конфигурации

Для возврата к предыдущей сохраненной конфигурации выполнить следующие действия:

1. В строке выбранной конфигурации нажать **кнопку «»** и, в открывшейся форме (см. Рисунок 252), подтвердить действие нажав **кнопку «Да»**.

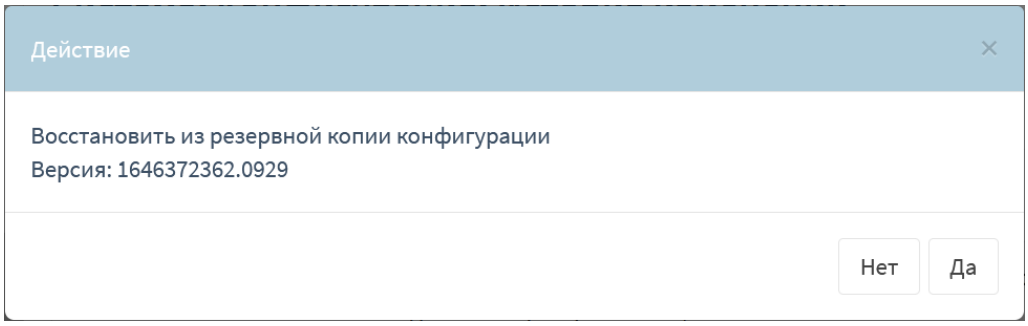

Рисунок 252 – Всплывающее окно о подтверждении действия

2. В случае успешного возврата к предыдущей версии конфигурации появится соответствующее сообщение (см. Рисунок 253).

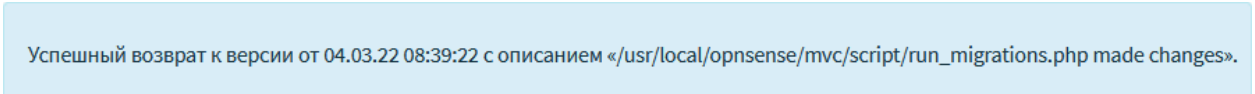

Рисунок 253 – Сообщение об успешном возврате к предыдущей версии конфигурации

23.2.4 Локальное сохранение конфигурации

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

23.3 Восстановление конфигурации

Восстановление конфигурации применяется для:

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

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

Для восстановления конфигурации необходимо выполнить следующие действия:

1. Перейти в подраздел резервного копирования (**«Система»** - **«Конфигурация»** - **«Резервные копии»**).
2. В блоке настроек **«Восстановить зону»** (см. Рисунок 254) выбрать:
   - одну зону для восстановления отдельной зоны конфигурации;
   - несколько зон для восстановления несколько зон конфигурации;
   - значение **«ВСЕ»** для восстановления конфигурации в полном объёме.

   и нажать **кнопку «Обзор...»**.

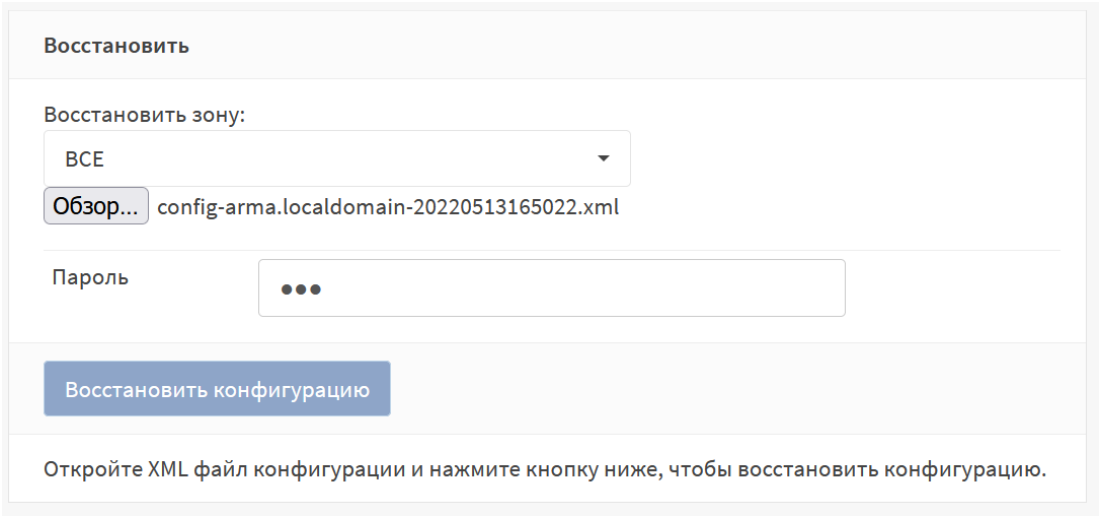

Рисунок 254 – Восстановление конфигурации

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

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

23.3.1 Особенность работы интерфейсов при восстановлении

При восстановлении конфигурации из файла необходимо учитывать следующие особенности:

- при восстановлении конфигурации настройки интерфейсов не восстанавливаются, те есть конфигурация TCP/IP остаётся неизменной;
- при восстановлении конфигурации с режимом работы «Сетевой мост» необходимо предварительно настроить интерфейс для управления **ARMA IF** иначе доступ после восстановления будет потерян.

23.4 Экспорт конфигурации на удаленный FTP/SMB-сервер

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

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

- «config_armaif_[версия ARMA IF]_[дата экспорта]_[время экспорта]_[локация].tar.gz», например, «config_armaif_3.6_20200831_170642_MSK.tar.gz».

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

1. Перейти в подраздел настройки экспорта конфигурации (**«Система»** - **«Конфигурация»** - **«Настройки экспорта»**).
2. Установить флажок в параметре **«Включен»** и указать настройки импорта для требуемого протокола (см. Таблица 43).

Таблица 43

Значения параметров для экспорта конфигурации

Параметр	Значение для FTP	Значение для SMB
Протокол	FTP	SMB
Адрес	Адрес сервера: IP-адрес, хост, доменное имя.	Адрес сервера: IP-адрес, хост, доменное имя.
Общедоступный ресурс Samba	-	Имя общедоступного ресурса Samba.

Параметр	Значение для FTP	Значение для SMB
Имя пользователя	Учётные данные.	Учётные данные.
Пароль	Учетные данные.	Учетные данные.
Путь к корневой папке	Абсолютный путь к корневой папке. Путь должен начинаться с символа «\». Если экспорт производится в корневую директорию, то необходимо оставить только символ «\»	Относительный путь к корневой папке. Путь должен начинаться с символа «\». Если экспорт производится в корневую директорию, то необходимо оставить только символ «\»
Интервал	Интервал ожидания в случае неудачной попытки, задаётся в секундах.	Интервал ожидания в случае неудачной попытки, задаётся в секундах.

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

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

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

23.4.1 Экспорт конфигурации по расписанию

После успешной настройки экспорта конфигурации на удаленный сервер возможно настроить расписание выполнения экспорта с помощью планировщика задах Cron (см. Раздел 26). При создании задачи необходимо выбрать «Экспорт конфигурации» в параметре **«Команда»**.

23.5 Сброс настроек

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

Сброс настроек возможен двумя способами:

- **через веб-интерфейс**;
- **через локальный консольный интерфейс**.

23.5.1 Сброс настроек через веб-интерфейс

Для сброса настроек системы необходимо перейти в подраздел настроек конфигурации (**«Система»** - **«Конфигурация»** - **«Значения по умолчанию»**) и нажать **кнопку «Да»** (см. Рисунок 255). **ARMA IF** будет сброшена к первоначальным настройкам и выполнена перезагрузка.

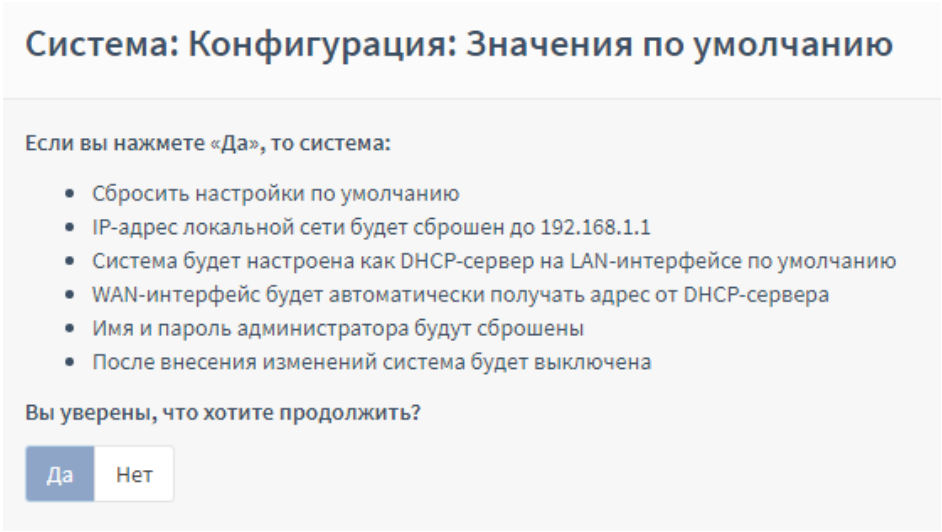

Рисунок 255 – Первоначальные настройки системы

23.5.2 Сброс настроек через локальный консольный интерфейс

Если доступ к веб-интерфейсу невозможен, то сброс настроек возможно выполнить через локальный консольный интерфейс.

Для сброса настроек системы необходимо в локальном консольном интерфейсе выполнить следующие действия:

1. Произвести аутентификацию в интерфейсе.
2. Нажать **клавишу «4»**, а затем **клавишу «Enter»** на клавиатуре для выбора пункта меню **«Reset to factory defaults»**.
3. В выведенной строке **«Do you want to proceed? [y/N]»** нажать **клавишу «y»**, а затем **клавишу «Enter»** (см. Рисунок 256).

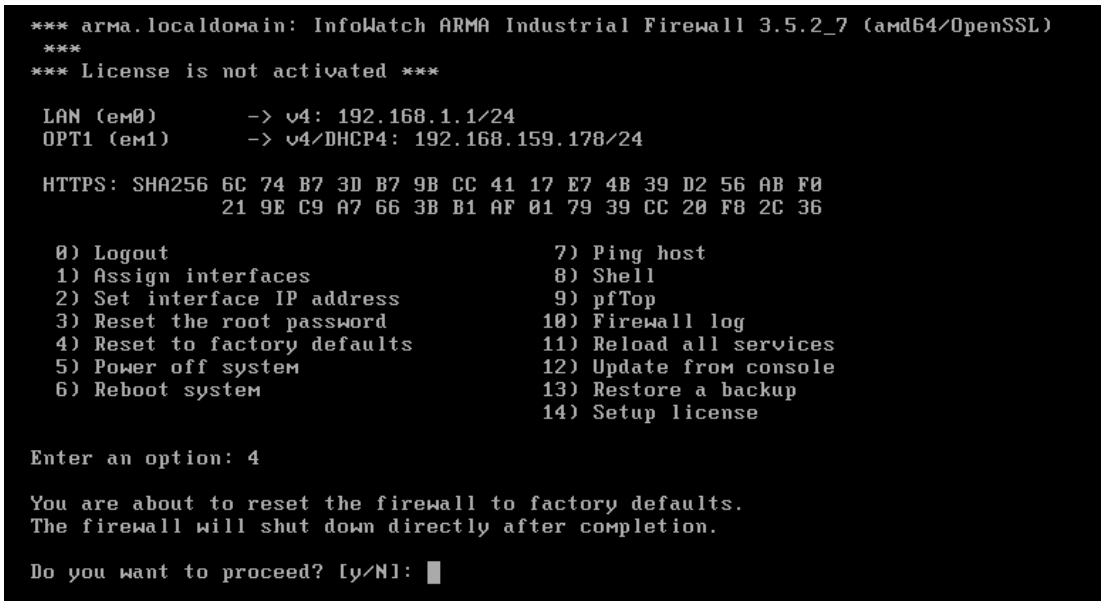

Рисунок 256 – Сброс настроек до заводских значений

23.6 Обновление системы

Обновить встроенное ПО **ARMA IF** возможно двумя способами:

- через веб-интерфейс;
- через локальный консольный интерфейс.

23.6.1 Обновление системы через веб-интерфейс

Для обновления встроенного ПО **ARMA IF** необходимо выполнить следующие действия:

1. Перейти в подраздел установки обновлений (**«Система»** - **«Прошивка»** - **«Обновления»**) (см. Рисунок 257) и нажать **кнопку «Обзор...»**.

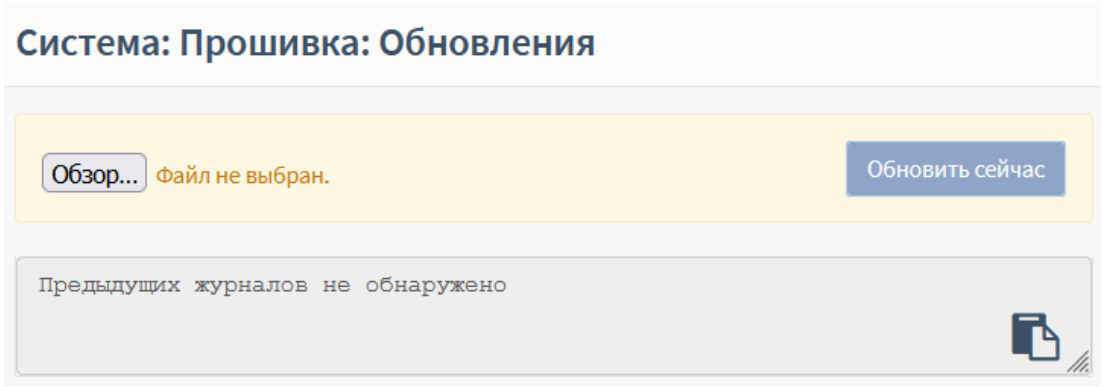

Рисунок 257 – Обновление системы

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

23.6.2 Обновление системы через локальный консольный интерфейс

Для обновления встроенного ПО **ARMA IF** необходимо в локальном консольном интерфейсе выполнить следующие действия:

1. Подготовить USB-носитель с файлом обновления встроенного ПО **ARMA IF** и осуществить подключение носителя к **ARMA IF**.
2. Произвести аутентификацию в интерфейсе.
3. Нажать **клавиши «1»** и **«2»**, а затем **клавишу «Enter»** на клавиатуре для выбора пункта меню **«Update from consol»**.
4. В выведенной строке **«Choose device partition number with update packages or press enter to update list:»** ввести номер раздела диска из списка и нажать **клавишу «Enter»**.
5. В выведенной строке **«Proceed with this action [y/N]»** – нажать **клавишу «y»**, а затем **клавишу «Enter»**. В некоторых случаях будет отображена информация об существенных изменениях.

23.7 Контроль целостности

Контроль целостности необходим для отслеживания неизменности следующих программных частей **ARMA IF** (см. Рисунок 258):

- **«configuration»** – конфигурация системы;
- **«scripts»** – вспомогательные скрипты для различных задач;
- **«site-python»** – вспомогательные модули языка программирования Python, подключаемые в серверный код;
- **«contrib»** – сторонние вспомогательные библиотеки;
- **«version** – версионность продукта;
- **«firmware-product»** – прошивка продукта;
- **«legacy-includes, www, mvc»** – программный код, связанный с веб-сервером;
- **«service»** – программный код, связанный с серверным кодом и не связанный с веб-интерфейсом.

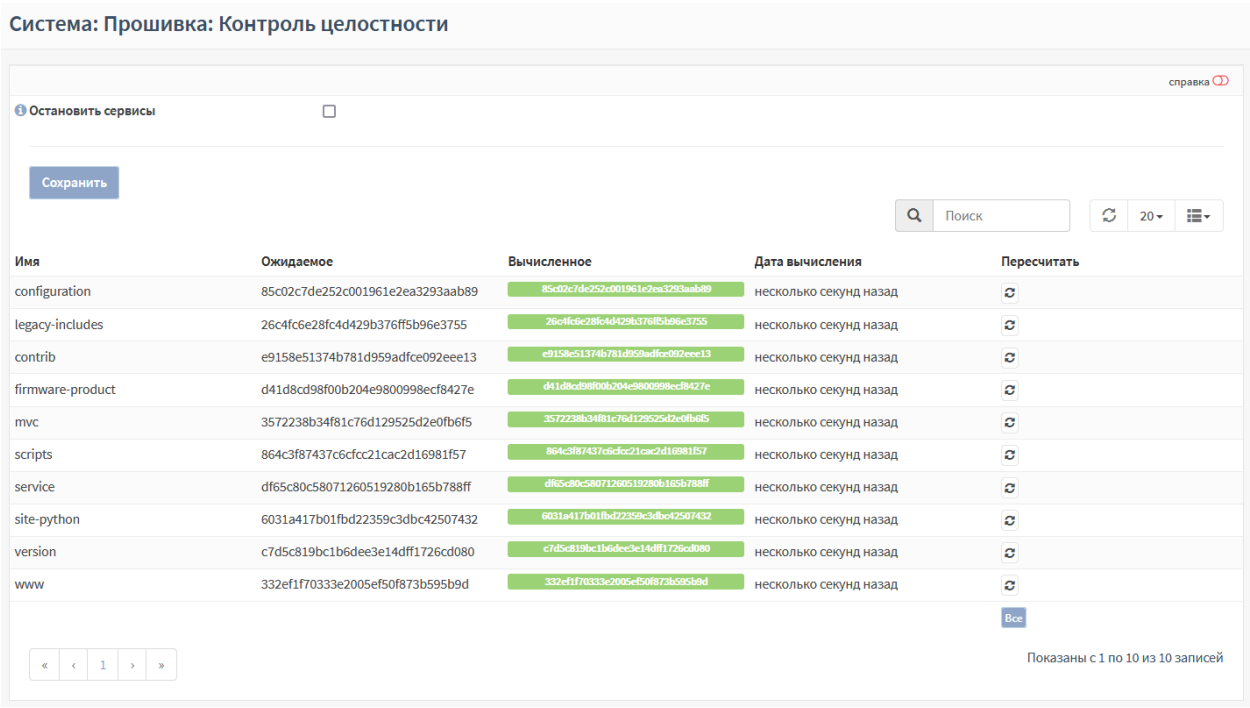

Рисунок 258 – Контроль целостности программных частей системы

Контрольные суммы автоматически пересчитываются при старте системы, но существует дополнительные средств запуска проверки контрольных сумм:

- вручную;
- по расписанию.

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

В случае, если какая-то из частей вышла из строя или была внештатно изменена, то значение столбца **«Вычисленное»** будет выделено красным цветом и появится уведомление о неуспешной проверке целостности вверху страницы (см. Рисунок 259). Уведомление сохраняется при переходе в любой раздел веб-интерфейса.

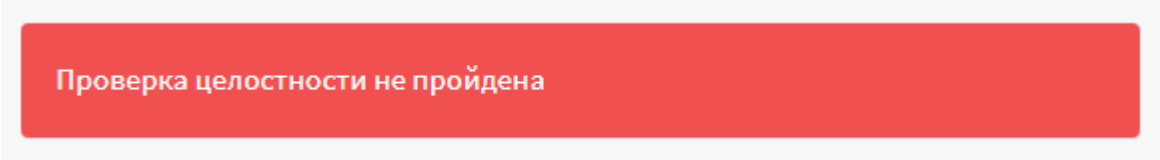

Рисунок 259 – Неуспешная проверка целостности

Дополнительно существует возможность останавливать сервисы в случае нарушения целостности. Для этого необходимо установить флажок напротив поля **«Остановить сервисы»** и нажать **кнопку «Сохранить»**. В случае нарушения целостности любой части **ARMA IF**, блокируется работа всех сервисов **ARMA IF** – дальнейшая эксплуатация невозможна, при этом появится соответствующее уведомление (см. Рисунок 260).

Рисунок 260 – Автоматическая блокировка межсетевого экрана

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

23.7.1 Запуск проверки контрольных сумм вручную

Для запуска проверки контрольных сумм вручную необходимо выполнить следующие действия:

1. Перейти в подраздел контроля целостности системы (**«Система»** - **«Прошивка»** - **«Контроль целостности»**) (см. Рисунок 258).
2. Нажать **кнопку «»** напротив строки программной части, нуждающейся в проверке или нажать **кнопку «Все»** для запуска проверки всех программных частей **ARMA IF**.

23.7.2 Запуск проверки контрольных сумм по расписанию

Возможна настройка расписания выполнения проверки контрольных сумм **ARMA IF** с помощью планировщика задах Cron (см. Раздел 26). При создании задачи необходимо выбрать «Пересчитать все чек-суммы» в параметре **«Команда»**.

24 АНТИВИРУС

Реализацией антивируса в **ARMA IF** является демон «clamd», используемый с подключаемым модулем «C-ICAP» для защиты соединений по протоколам HTTP и HTTPS от вирусов, троянов и прочего вредоносного ПО.

Для настройки и тестирования функции антивирусной защиты используется схема стенда, представленная на рисунке (см. Рисунок 261).

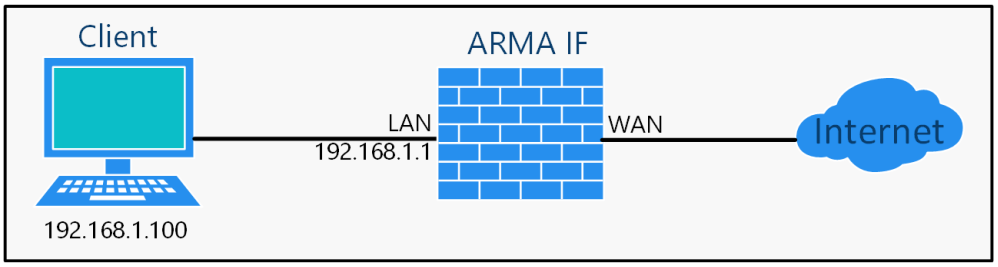

Рисунок 261 – Схема стенда для настройки и тестирования функции антивирусной защиты

Перед настройкой антивирусной защиты необходимо настроить прокси-сервер (см. Раздел 18.1).

Для настройки функции антивирусной защиты необходимо выполнить следующие шаги:

1. Включить ICAP.
2. Включить C-ICAP.
3. Настроить антивирусную защиту.
4. Проверить работу антивирусной защиты.

24.1 Шаг 1. Включение ICAP

Для включения ICAP необходимо выполнить следующие действия:

1. Перейти в подраздел настроек прокси-сервера (**«Службы»** - **«Веб-прокси»** - **«Администрирование»**).
2. Раскрыть вкладку **«Перенаправляющий прокси»** нажав **кнопку «** ▼ **»** и выбрать **«Настройки ICAP»** (см. Рисунок 262).

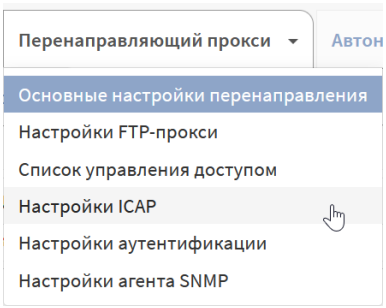

Рисунок 262 – Выбор настроек перенаправляющего прокси-сервера

3. Установить флажок **«Включить ICAP»**, указать следующие значение параметров **«REQMOD URL»** и **«RESPMOD URL»**:

   - «icap://127.0.0.1:1344/avscan»

   и нажать **кнопку «Применить»** (см. Рисунок 263).

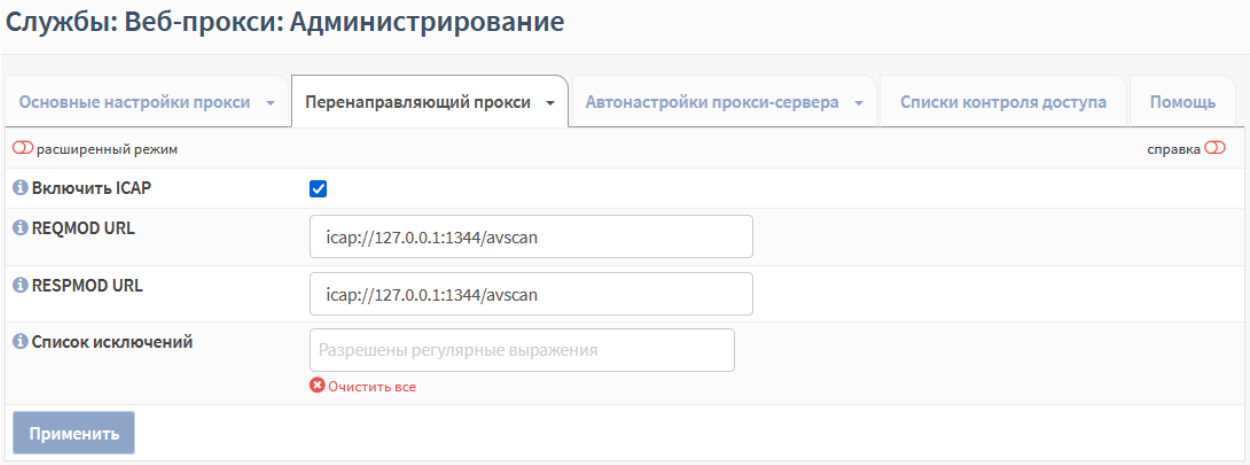

Рисунок 263 – Настройка ICAP

24.2 Шаг 2. Включение C-ICAP

Для включения C-ICAP необходимо выполнить следующие действия:

1. Перейти в подраздел настроек C-ICAP (**«Службы»** - **«C-ICAP»** - **«Конфигурация»**) (см. Рисунок 264).
2. Установить флажок **«Включить службу c-icap»**, указать значение «127.0.0.1» для параметра **«Адрес прослушивания»**, остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

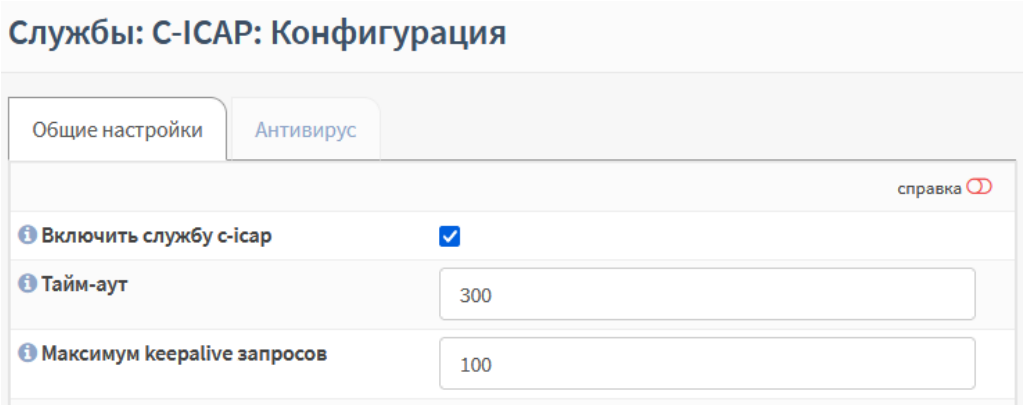

Рисунок 264 – Настройка C-ICAP

3. Перейти во вкладку **«Антивирус»** (см. Рисунок 265), установить флажок **«Включить ClamAV»**, указать «20» в параметре **«Максимальный размер объекта»**, остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

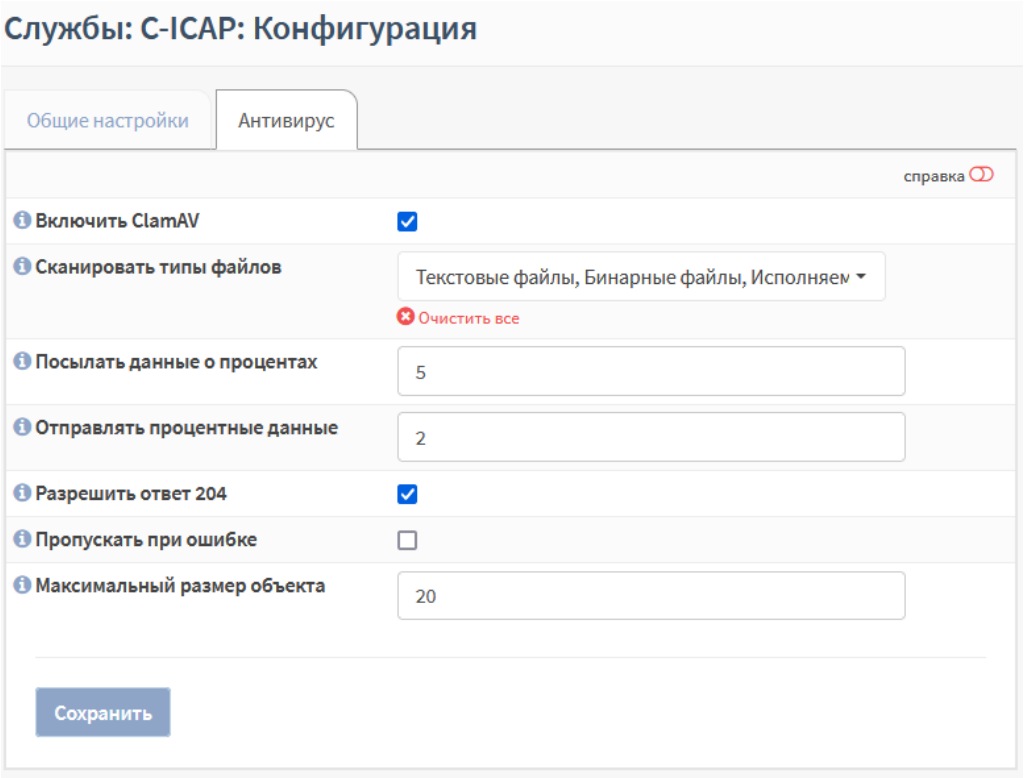

Рисунок 265 – Настройка антивируса C-ICAP

!Важно Размер для параметров **«Отправлять процентные данные»** и **«Максимальный размер объекта»** используется единица измерения Мбайт.

24.3 Шаг 3. Настройка антивирусной защиты

Перед началом рекомендуется обновить сигнатуры ClamAV. Для этого необходимо скачать архив с сигнатурами БД ClamAV, а затем загрузить данные сигнатуры в **ARMA IF**. Для загрузки сигнатур необходимо выполнить следующие действия:

1. Перейти в подраздел настроек антивируса (**«Службы»** - **«Антивирус»** - **«Конфигурация»**), а затем перейти во вкладку **«Версии»** (см. Рисунок 266).

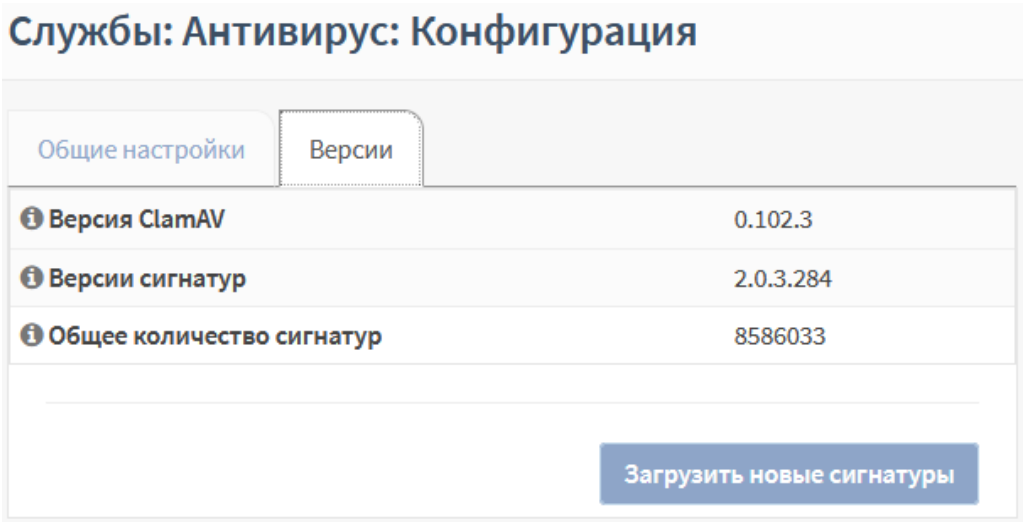

Рисунок 266 – Обновление сигнатур ClamAV

2. Нажать **кнопку «Загрузить новые сигнатуры»**, в открывшемся окне проводника выбрать скаченный ранее файл и нажать **кнопку «Открыть»**.

Для настройки антивирусной защиты необходимо выполнить следующие действия:

1. Перейти в подраздел настроек антивируса (**«Службы»** - **«Антивирус»** - **«Конфигурация»**) (см. Рисунок 267).

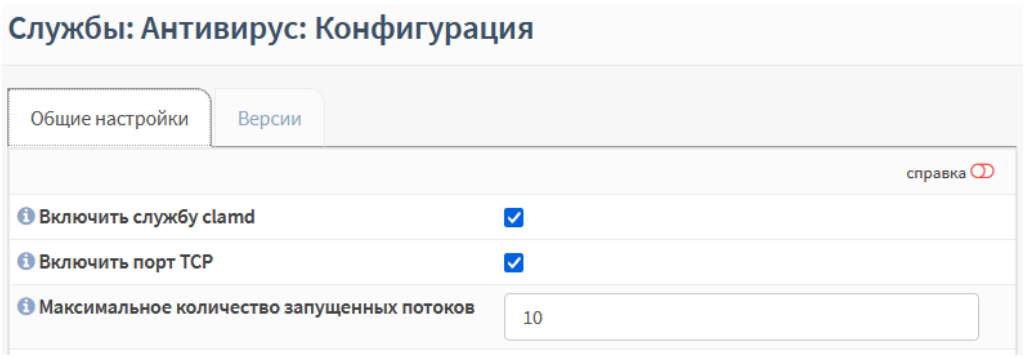

Рисунок 267 – Включение антивируса

2. Установить флажок **«Включить службу clamd»**, при необходимости установить флажки для параметров **«Обнаруживать повреждённые исполняемые файлы»**, **«Блокировать OLE2 макросы»** и **«Блокировать зашифрованные архивы»**, остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

24.4 Шаг 4. Проверка антивирусной защиты

Для проверки работоспособности функции антивирусной защиты необходимо выполнить следующие действия:

1. На ПК **«Client»** запустить веб-браузер, перейти по ссылке:

- «https://www.eicar.org/?page_id=3950»

и скачать файл **«eicar.com.zip»** (см. Рисунок 268).

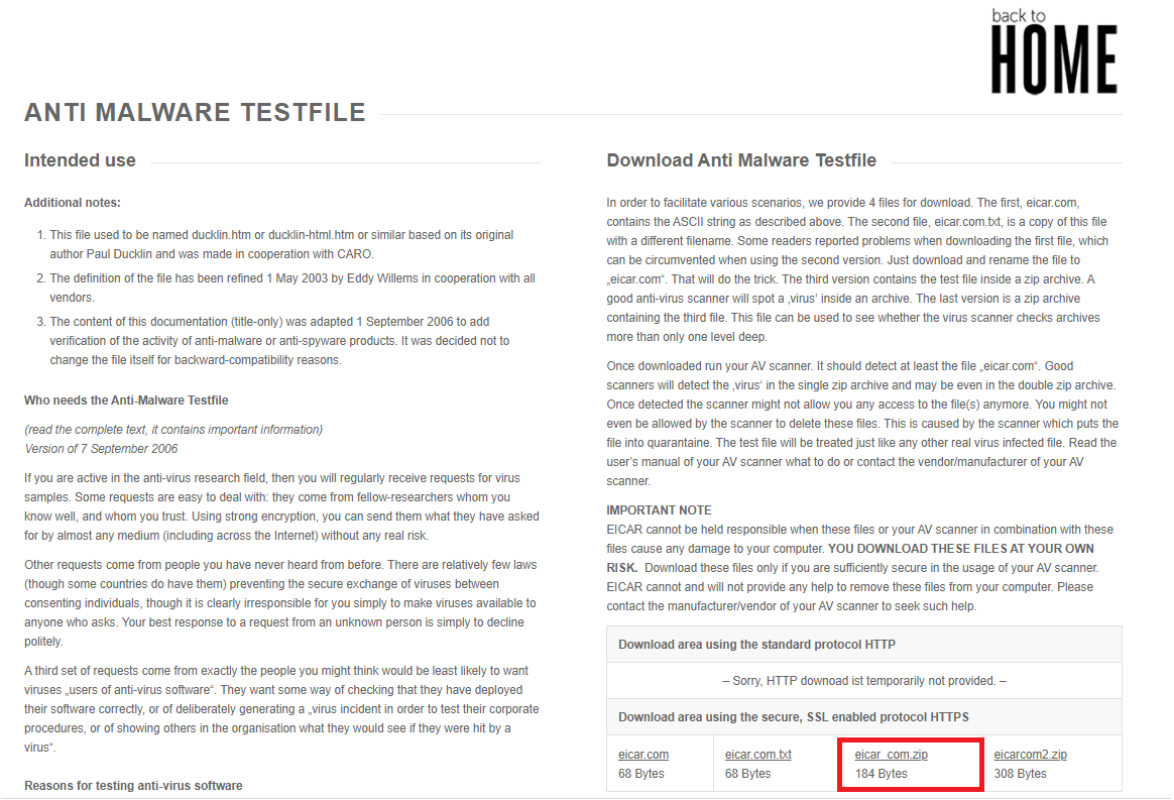

Рисунок 268 – Скачивание файла eicar.com2.zip

2. Убедиться в наличии уведомления в веб-браузере об обнаружении вредоносного ПО при скачивании файла (см. Рисунок 269).

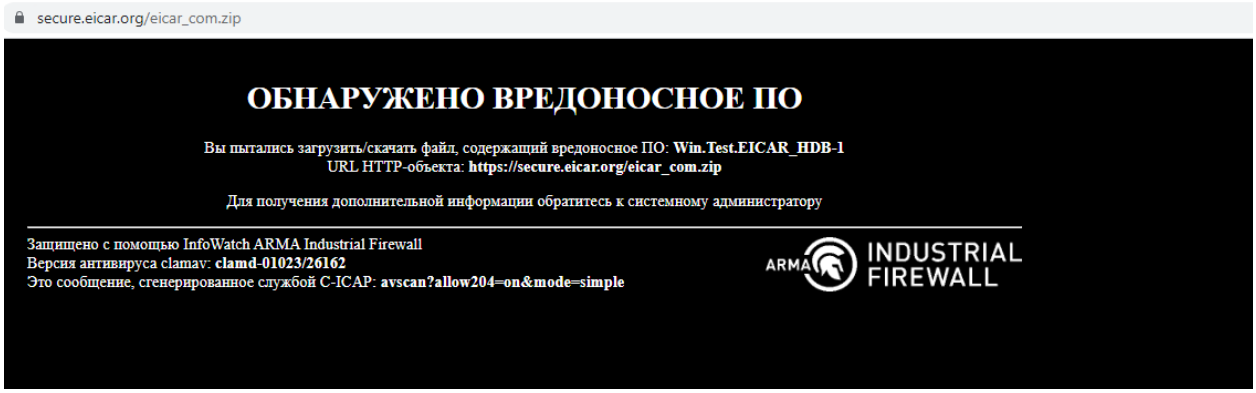

Рисунок 269 – Уведомление антивируса об обнаружении вредоносного ПО

3. Убедиться в наличии записей в журналах:
   - журнала C-ICAP (**«Службы»** - **«C-ICAP»** - **«Журнал»**) (см Рисунок 270);
   - журнала антивируса (**«Службы»** - **«Антивирус»** - **«Логирование/Clamd»**) (Рисунок 271).

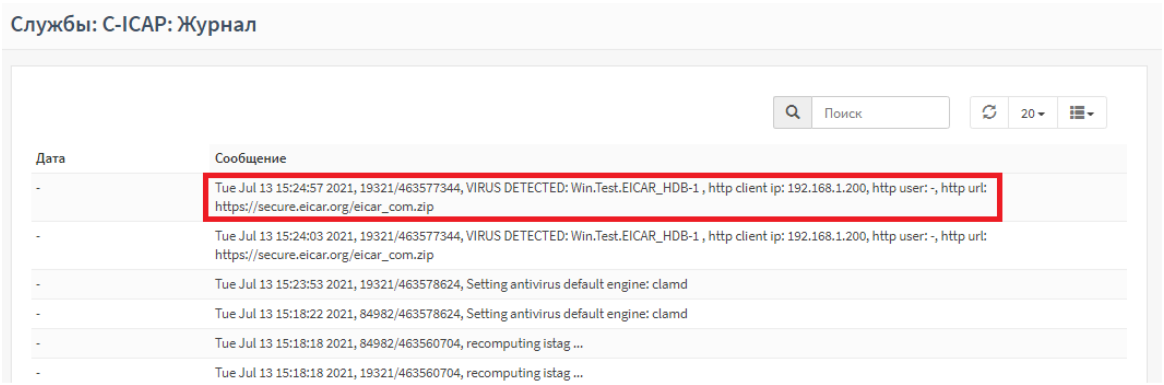

Рисунок 270 – Журнал C-ICAP

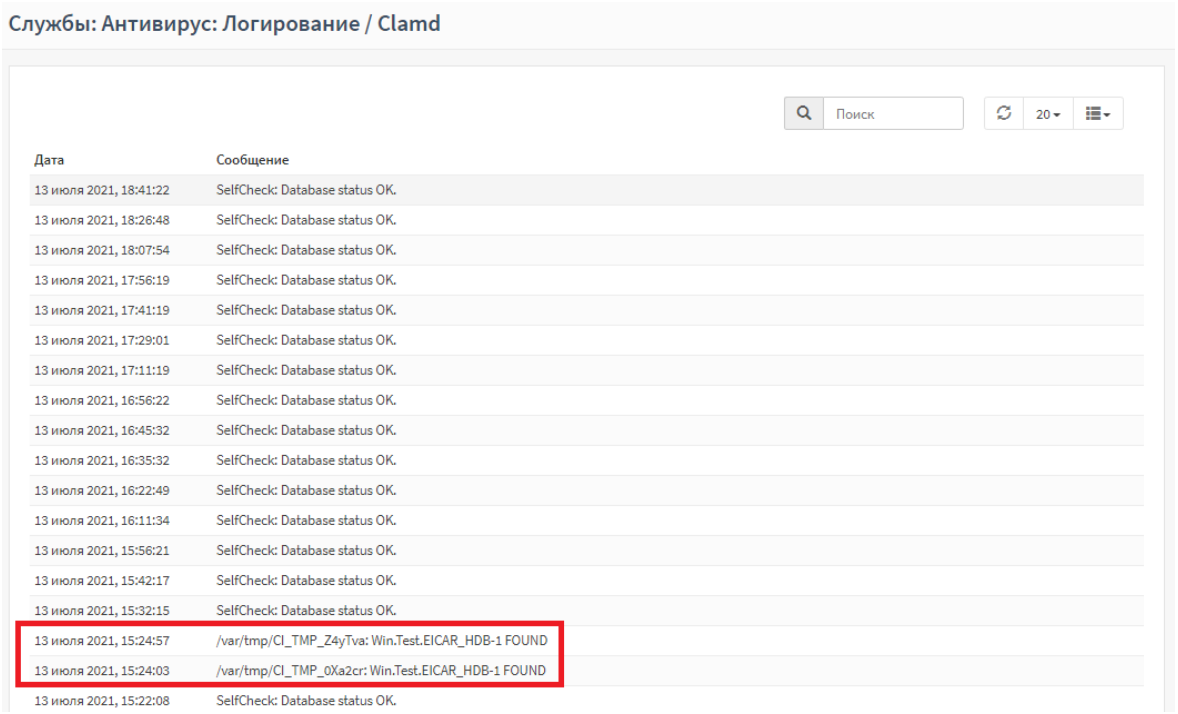

Рисунок 271 – Журнал антивируса

!Важно Включенный антивирус приводит к увеличению потребления ресурсов и повышает требования к аппаратному обеспечению. В случае нехватки ресурсов возможны сбои в работе **ARMA IF**.

25 DNSMASQ DNS

Dnsmasq – легковесный и быстроконфигурируемый проксирующий DNS-, DHCP- и TFTP-сервер, предназначенный для работы в небольших сетях.

В режиме DNS-сервера Dnsmasq обеспечивает доменными именами локальные хосты, не имеющие глобальных DNS-записей. DHCP-сервер интегрирован с DNS-сервером и назначает хостам с IP-адресом доменное имя, сконфигурированное ранее в конфигурационном файле, поддерживает привязку IP-адреса к хосту или автоматическую настройку IP-адресов из заданного диапазона и BOOTP для сетевой загрузки бездисковых машин.

В качестве примера настройки Dnsmasq будет использоваться схема стенда, представленная на рисунке (см. Рисунок 272). На ПК **«Client»** установлена ОС Windows.

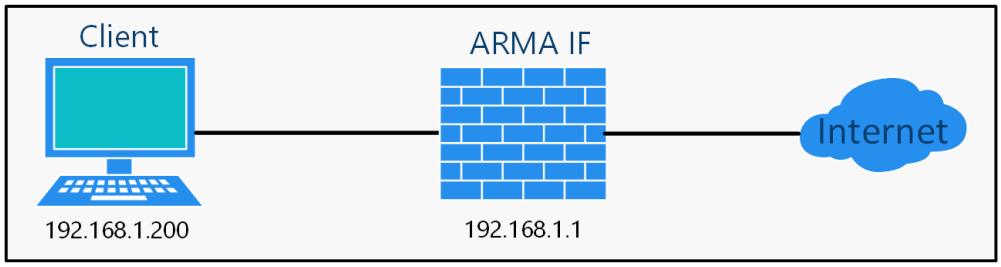

Рисунок 272 – Схема стенда настройки Dnsmasq

25.1 Настройка Dnsmasq DNS

Для настройки Dnsmasq DNS необходимо выполнить следующие действия:

1. Перейти в подраздел настроек кэширующего DNS-сервера (**«Службы»** - **«Кэширующий DNS-сервер»** - **«Общие настройки»**) и убрать флажок для параметра **«Включить»**.
2. Перейти в подраздел настроек Dnsmasq DNS (**«Службы»** - **«Dnsmasq DNS»** - **«Настройки»**) (см. Рисунок 273), установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»**.

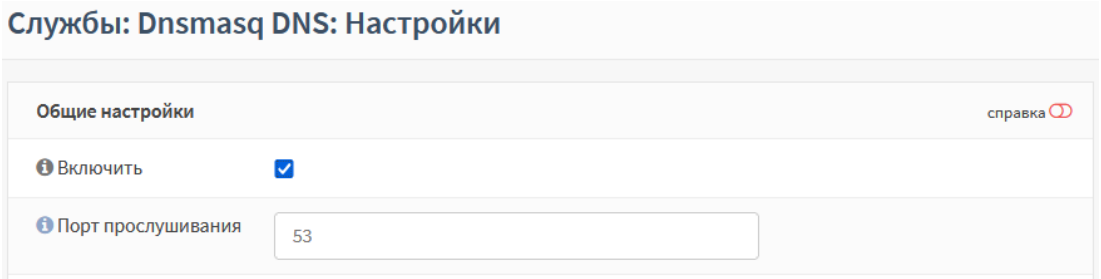

Рисунок 273 – Включение Dnsmasq

!Важно При использовании динамических интерфейсов не рекомендуется привязываться к адресам из этих интерфейсов.

25.1.1 Дополнительные настройки Dnsmasq DNS

Параметр **«DNSSEC»** рекомендуется включать в целях минимизирования атак, связанных с подменой DNS-адреса при разрешении доменных имён.

Вариант **«Перенаправление запросов DNS»** параметра **«Переадресация DNS-запросов»** рекомендуется включать для опроса DNS-серверов по порядку, указанном в блоке настроек DNS-сервера (**«Система»** - **«Общие настройки»**), вместо параллельно запроса всем указанным DNS-серверам.

Для создания отдельных записей определения хоста или домена необходимо нажать **кнопку «+»** в соответствующем блоке (см. Рисунок 274), задать значения в открывшейся форме и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

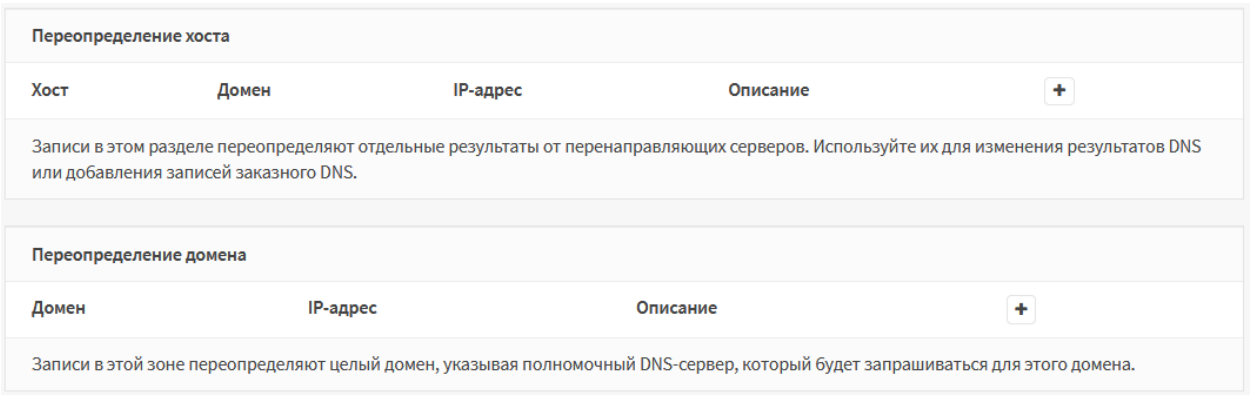

Рисунок 274 – Переопределение хоста или домена

25.2 Проверка работы Dnsmasq DNS

Для проверки работы Dnsmasq DNS необходимо выполнить следующие действия:

1. На ПК **«Client»** указать для используемого сетевого подключения IP-адрес **ARMA IF** в качестве предпочитаемого DNS-сервера (см. Рисунок 275).

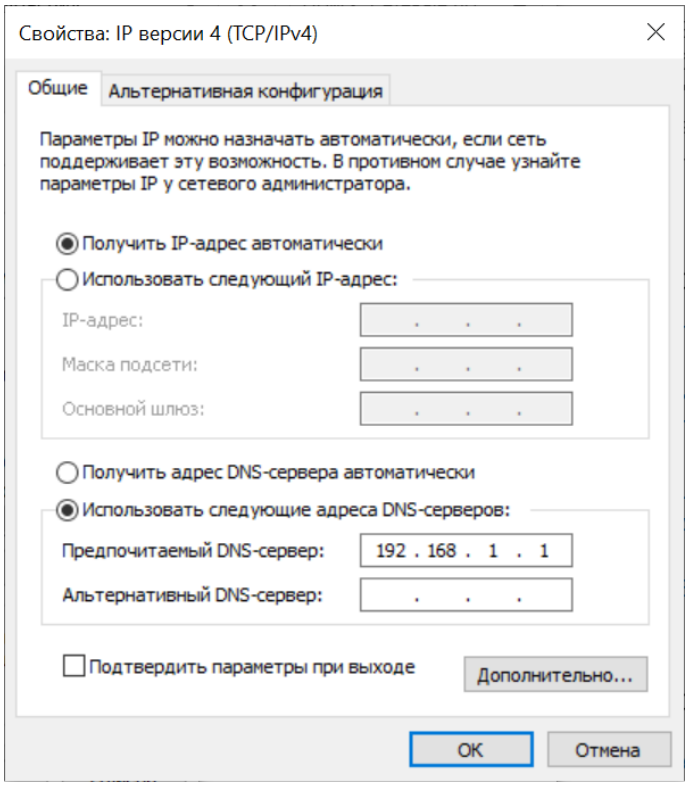

Рисунок 275 – Настройка параметров сети

2. На ПК **«Client»** открыть веб-браузер и перейти на сайт «ya.ru». Работоспособность Dnsmasq DNS проверяется успешным подключением к сайту.

26 CRON

Cron – это служба, использующаяся в качестве планировщика задач в **ARMA IF**.

Планировщик задач позволяет выполнять различные задания в определённое время или с определённой периодичностью.

В качестве примера будет рассмотрен следующий сценарий использования планировщика заданий Cron:

- Действие – перезагрузка **ARMA IF**.
- Периодичность – каждую субботу.
- Время перезагрузки – 18 часов 30 минут.

Для добавления задания необходимо выполнить следующие действия:

1. Перейти в подраздел планировщика задач (**«Система»** - **«Настройки»** - **«Планировщик задач Cron»**) и нажать **кнопку «+»**.
2. В появившейся форме (см. Рисунок 276) указать следующие значения для параметров:
   - **«Мин»** – «30»;
   - **«Ч»** – «18»;
   - **«День недели»** – «6»;
   - **«Команда»** – «Выполнить перезагрузку»;
   - **«Описание»** – «Перезагрузка каждую субботу».

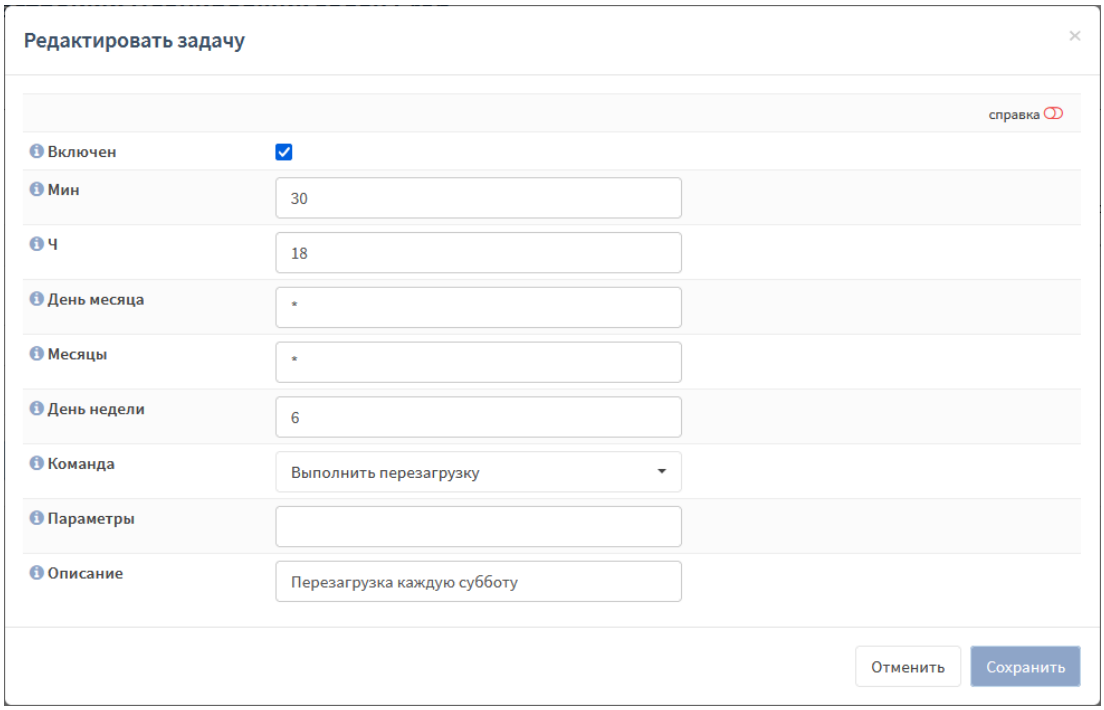

Рисунок 276 – Редактирование задачи

3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

В результате новая задача будет добавлена в список (см. Рисунок 277) и каждую субботу в 18:30 будет выполнена перезагрузка **ARMA IF**.

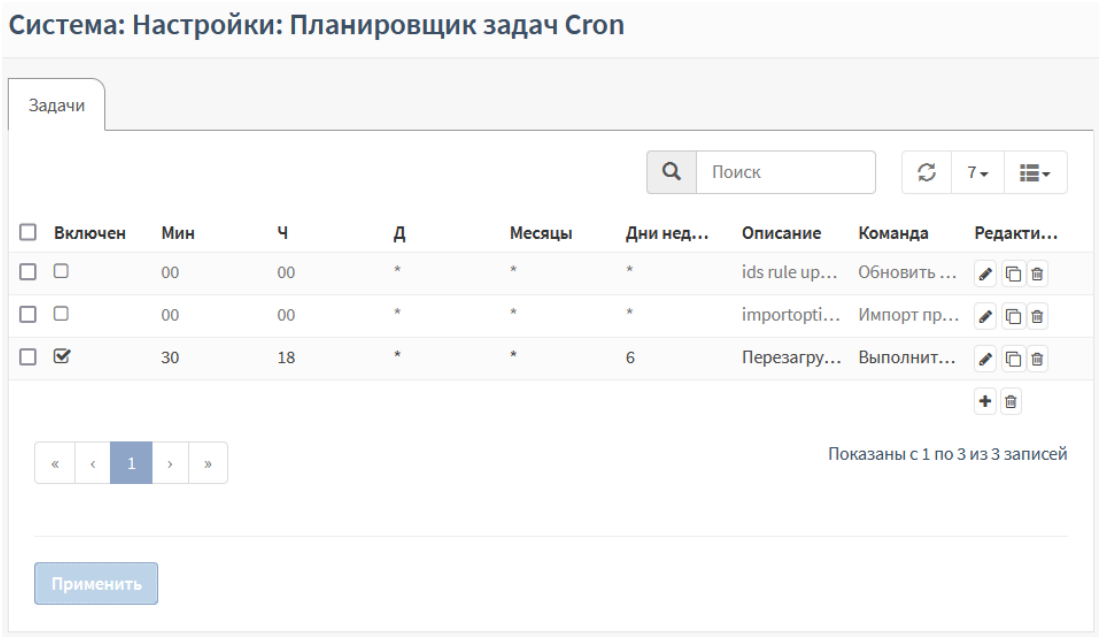

Рисунок 277 – Список планировщика задач

!Важно По умолчанию в планировщике созданы две задачи COB, являющиеся системными и не подлежащие удалению.

26.1 Особенности параметров, используемых в задачах

Во всех полях временных параметров задачи возможно указать единичное значение, перечень значений, разделённых запятой и диапазон, разделённый знаком «минус»:

- «4»;
- «1,3,6»;
- «2-7».

Значения разных параметров будут объединены, например, для параметров:

- **«Мин»** – «20,30»;
- **«Ч»** – «10,22»;
- **«Месяц»** – «1,3»;
- **«День недели»** –«1-5»;

задача будет выполняться с понедельника по пятницу января и марта, в 10:20, 10:30, 22:20 и 22:30.

26.2 Задачи планировщика

Планировщик задач позволяет выполнять следующие задания:

- **«Восстановить DH параметры»** – генерирует DH параметры для введенной длины ключа, указанного в поле **«Параметры»**. Если длина ключа не указана, то параметры генерируется для следующих значений: «1024», «2048», «4096»;
- **«Выполнить перезагрузку»** –выполняет перезагрузку **ARMA IF**;
- **«Выполнить периодическое обновление интерфейса»** – обновляет настройки интерфейса (см. Раздел 14), указанного в поле **«Параметры»**. Если интерфейс не указан, то выполняется обновление интерфейса «WAN»;
- **«Импорт правил СОВ»** – импортирует правила СОВ согласно настройкам, указанным в подразделе настройки импорта правил СОВ (**«Обнаружение вторжений»** - **«Настройка импорта правил»**).
- **«Обновить ACL с внешнего прокси»** – обновляет черный список веб-адресов прокси-сервера (см. Раздел 18) согласно спискам контроля доступа. Списки указываются в подразделе управления списками контроля доступа (**«Веб-прокси»** - **«Администрирование»** - **«Списки контроля доступа»**).
- **«Обновить ACL с внешнего прокси и перезагрузить сервис»** – дополнительно к **«Обновить ACL с внешнего прокси»** производит перезапуск службы, отвечающей за работу прокси-сервера в случае неудачной загрузки черного списка веб-адресов.
- **«Обновить и перезагрузить правила обнаружения вторжений»** – добавляет импортированные правила в действующие правила СОВ и перезапускает службу, отвечающую за правила обнаружения вторжений (см. Раздел 5).
- **«Обновить и перезагрузить псевдонимы межсетевого экрана»** – выполняет перезапуск службы, отвечающей за псевдонимы МЭ (см. Раздел 1.1.3).
- **«Перезагрузить правила обнаружения вторжений»** – выполняет перезапуск службы, отвечающей за правила обнаружения вторжений (см. Раздел 5).
- **«Перезагрузить сервис IPsec»** – выполняет перезапуск службы, отвечающей за VLAN IPsec 9 (см. Раздел 17).
- **«Перезапустить сервис портала авторизации»** – выполняет перезапуск службы, отвечающей за портал авторизации (см. Раздел 20).
- **«Пересчитать все чек-суммы»** – выполняет проверку контроля целостности системы (см. Раздел 23.7).

- **«Экспорт конфигурации»** – выполняет экспорт конфигурации на удалённый сервер (см. Раздел 23.4).

27 МОНИТОРИНГ, СТАТИСТИКА, ДИАГНОСТИКА

27.1 Мониторинг системы с помощью информационных виджетов

ARMA IF позволяет производить мониторинг текущего состояния с помощью различных виджетов.

Панель виджетов доступна в разделе **«Инструменты»**, являющимся по умолчанию стартовым разделом после аутентификации в **ARMA IF** (см. Рисунок 278).

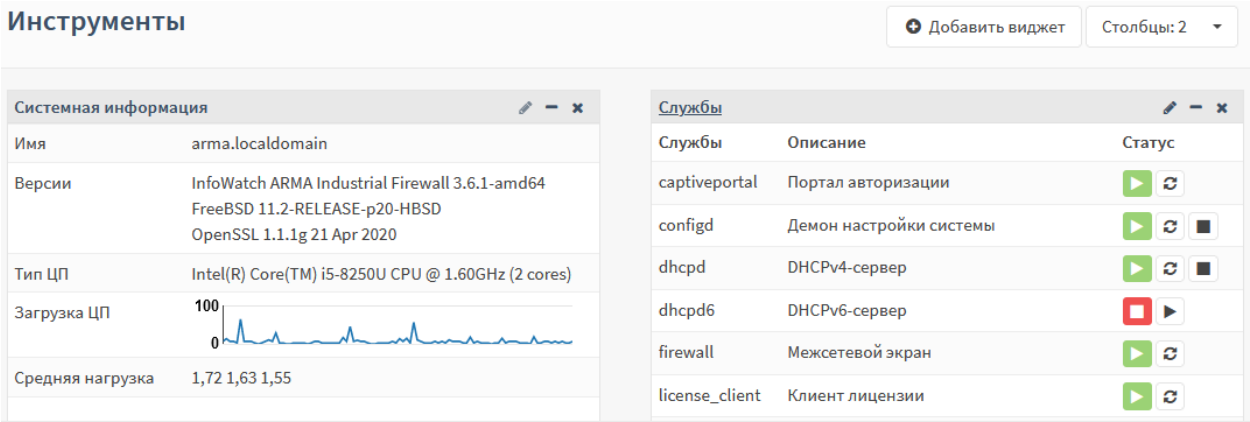

Рисунок 278 – Панель виджетов

Существует возможность перемещения виджетов с помощью мыши. Для этого необходимо навести курсор мыши на заголовок виджета, зажать **левую кнопку мыши**, переместить виджет в требуемое положение и отпустить **левую кнопку мыши**.

Количество отображаемых столбцов выбирается с помощью выпадающего списка **«Столбцы»** в верхней правой части раздела.

Для сохранения местоположения виджетов и количества столбцов необходимо нажать **кнопку «Сохранить настройки»**.

27.1.1 Добавление виджетов

Для добавления виджета необходимо выполнить следующие действия:

1. Нажать **кнопку «+Добавить виджет»** и выбрать требуемый виджет в открывшейся форме доступных виджетов (см. Рисунок 279). За один раз возможно выбрать несколько виджетов.
2. Нажать **кнопку «Закрыть»**, а затем нажать **кнопку «Сохранить настройки»**.

Рисунок 279 – Добавление виджетов

В **ARMA IF** доступны следующие виджеты для мониторинга текущего состояния:

- **«CARP»** – отображает статус устройства в режиме работы кластера;
- **«Использование ЦП»** – отображает график загрузки ЦП в режиме реального времени;
- **«Шлюзы»** – отображает статус работы настроенных шлюзов, время приема-передачи и процент потерь;
- **«Интерфейсы»** – отображает включенные сетевые интерфейсы и их основные параметры: имя, скорость и режим передачи, IP-адрес;
- **«Статистика интерфейса»** – отображает сводную таблицу по всем настроенным интерфейсам в режиме реального времени;
- **«IPsec»** – отображает настроенные IPsec туннели;
- **«Информация о лицензии»** – отображает информацию о лицензии;
- **«Журнал межсетевого экрана»** – отображает таблицу событий МЭ в режиме реального времени;
- **«Monit»** – отображает состояния почтовых серверов, доступность различных сервисов и ресурсов, состояние сетевых сервисов;
- **«Сетевое время»** – отображает текущее время системы, а также информацию о сервере синхронизации времени;
- **«OpenVPN»** – отображает настроенные OpenVPN серверы;
- **«Службы»** – отображает статус работы настроенных служб и позволяет остановить/запустить/перезапустить выбранную службу;
- **«Системная информация»** – отображает основную информацию о системе;

- **«Журнал Syslog»** – отображает таблицу журнала Syslog в режиме реального времени;
- **«Тепловые датчики»** – отображает по данным ACPI температуру ЦП, МП, позволяет задавать различные пороговые значения температуры;
- **«Графики трафика»** – отображает график входящего/исходящего трафика в режиме реального времени.

27.2 Сбор и статистика Netflow

NetFlow – сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems. Протокол захватывает полные потоки пакетов, включая источник, IP-адрес назначения и номер порта.

ARMA IF позволяет собирать данные NetFlow, проходящие через МЭ для последующего анализа, а также экспортировать эти данные для анализа сторонним ПО.

27.2.1 Настройка NetFlow

Для настройки NetFlow необходимо выполнить следующие действия:

1. Перейти в подраздел настройки NetFlow (**«Создание отчетов»** - **«NetFlow»**) (см. Рисунок 280).

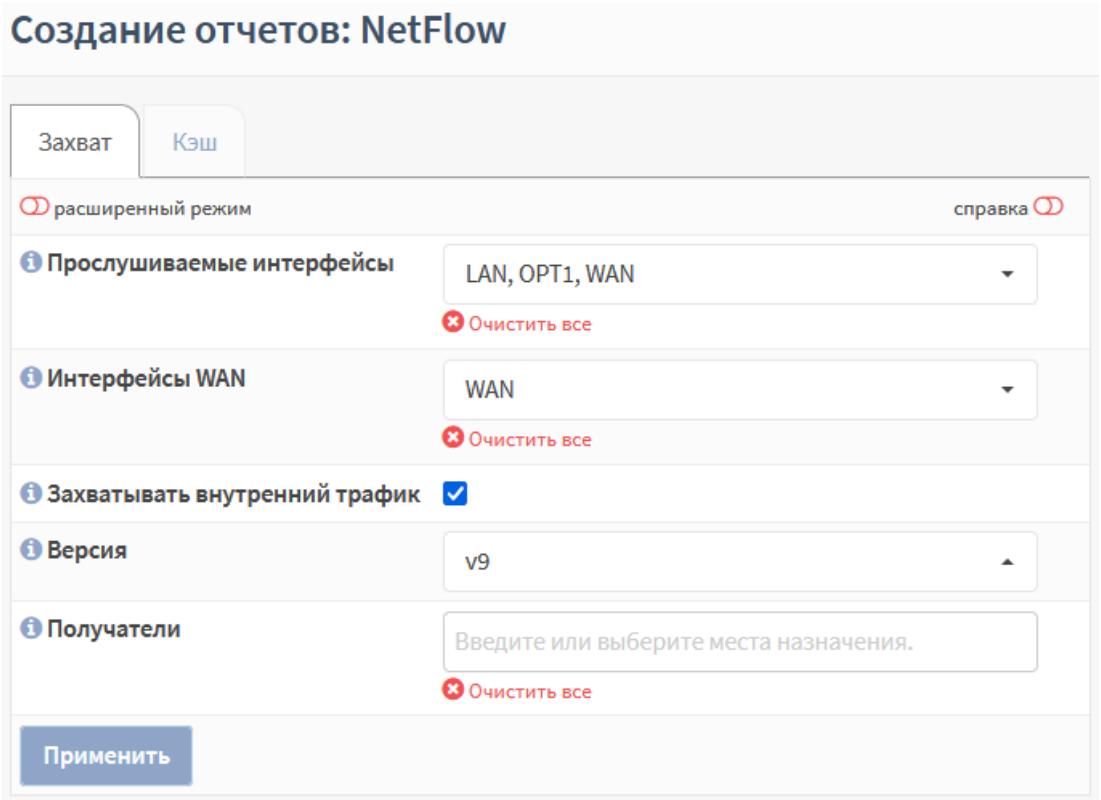

Рисунок 280 – Параметры работы NetFlow

2. Указать интерфейсы, для которых необходимо собирать данные NetFlow.

3. Указать интерфейс, используемый в качестве выхода в глобальную сеть – WAN.
4. Установить флажок для параметра **«Захватывать внутренний трафик»** для сбора локальных данных на **ARMA IF**. Локальный кэш хранит только последние 100 Мбайт данных.
5. При необходимости выбрать версию NetFlow, по умолчанию выбрано значение «v9».
6. В параметре **«Получатели»** указать адреса получателей данных, если поле оставить пустым – будет осуществляться только локальный сбор данных. Формат заполнения:
    - «IP-адрес:номер порта», например «192.168.1.100:2550».
7. Нажать **кнопку «Применить»**.

!Важно При использовании стороннего сборщика данных NetFlow, в большинстве случаев, необходимо настроить передачу SNMP (см. Раздел 7) и создать правило МЭ (см. Раздел 1.1.1), разрешающее трафик SNMP на выбранном интерфейсе.

В случае сбора локальных данных на вкладке **«Кэш»** подраздела **«NetFlow»** будет отображено количество собранных пакетов на различных интерфейсах (см. Рисунок 281).

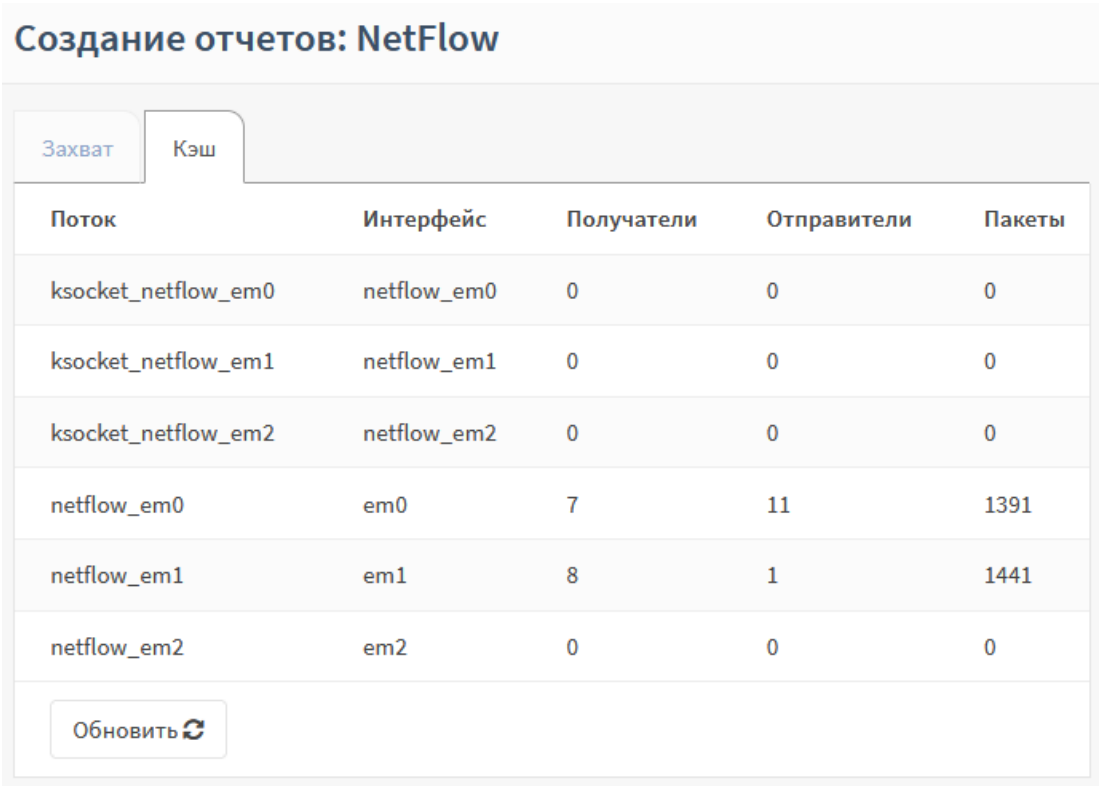

Рисунок 281 – Данные кэша NetFlow

27.2.2 Анализ данных Netflow

В случае успешной настройки NetFlow (см. Раздел 27.2.1) в подразделе анализа трафика (**«Создание отчетов»** - **«Анализ»**) будет отображена информация о трафике (см. Рисунок 282).

В верхней части страницы существует возможность выбора временного промежутка представления из выпадающего списка.

При выборе значения на диаграмме будет произведен переход на вкладку **«Подробности»** для более детального представления данных.

На вкладке **«Экспорт»** подраздела **«Анализ»** возможно произвести экспорт данных NetFlow. Для этого необходимо выбрать требуемые значения в выпадающих списках и нажать **кнопку «Экспорт»**.

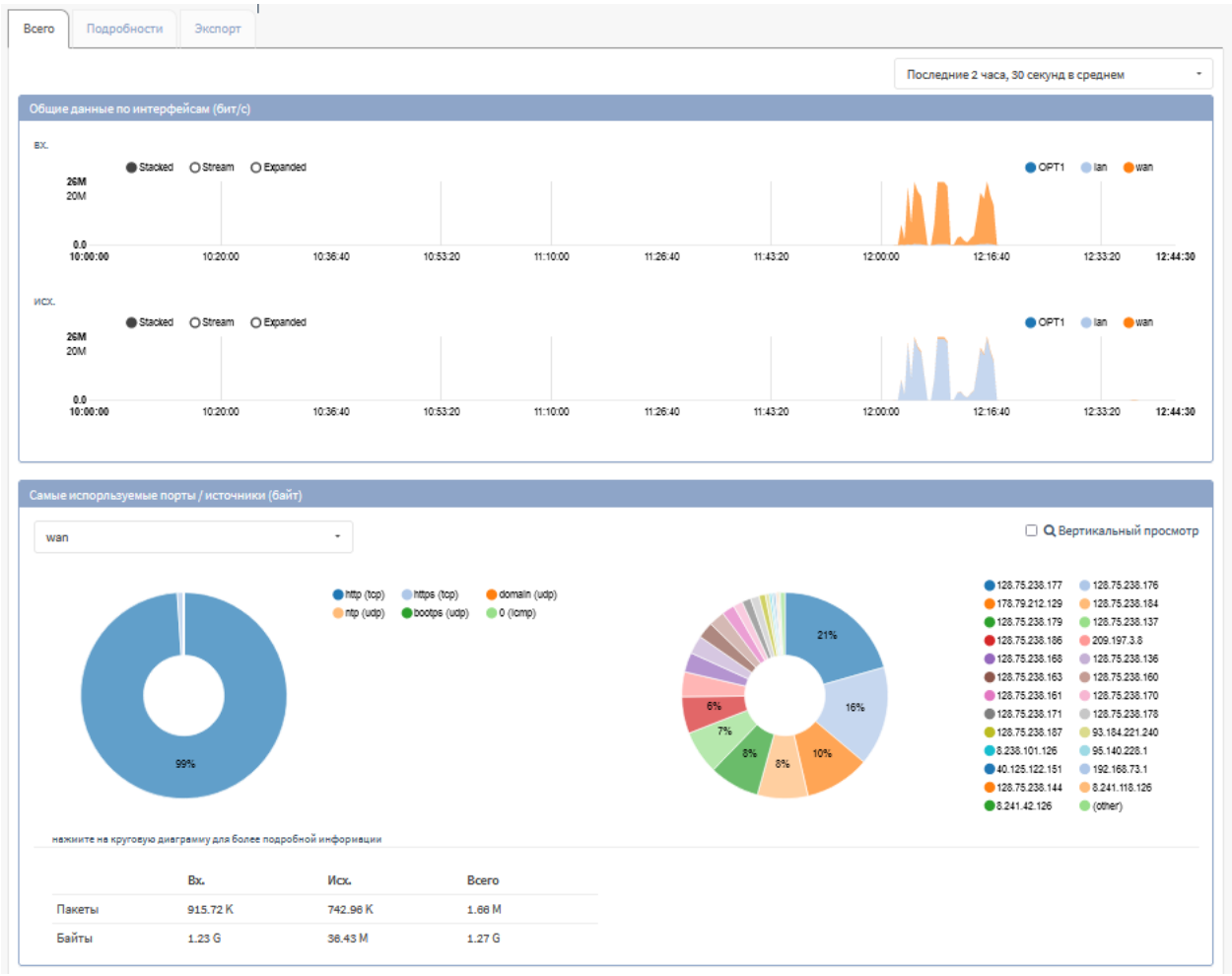

Рисунок 282 – Сводная информация на основании данных NetFlow

27.3 Диагностика МЭ

Диагностика МЭ позволяет просматривать общую информацию и статистику МЭ, активные в текущее время маршруты, IP-адреса, записанные как псевдонимы, прослушивающие сокеты для IPv4 и IPv6, активные состояния, отсортированные

состояния по различным критериям. Помимо просмотра информации имеется возможность удаления активных состояний и отслеживания источника.

27.3.1 Диагностика pfInfo

Для просмотра общей информации об МЭ необходимо перейти в подраздел диагностики pfInfo (**«Межсетевой экран»** - **«Диагностика»** - **«pfInfo»**) (см. Рисунок 283).

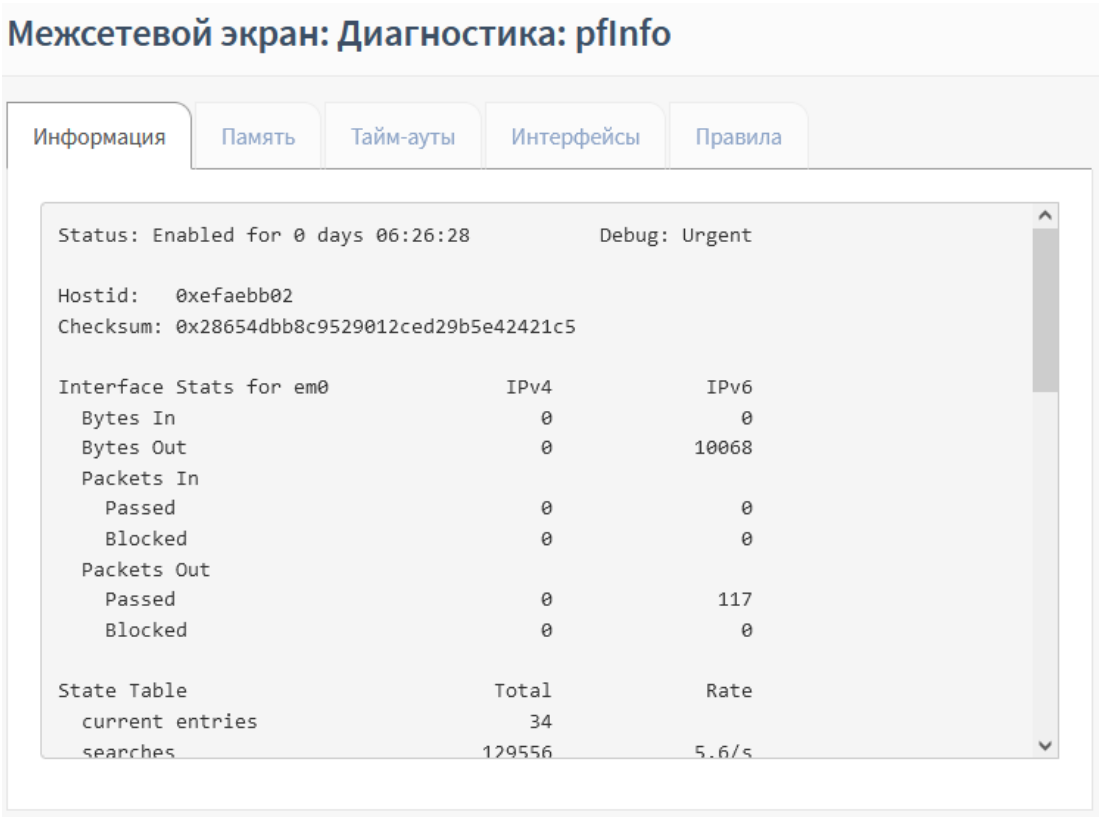

Рисунок 283 – Диагностика pfinfo

Существует возможность переключения по вкладкам:

- **«Информация»** – отображает различную общую информацию о работе МЭ;
- **«Память»** – отображает заданные ограничения памяти;
- **«Тайм-ауты»** – отображает информацию об тайм-аутах;
- **«Интерфейсы»** – отображает информацию об интерфейсах;
- **«Правила»** – отображает информацию о правилах МЭ.

27.3.2 Диагностика pfTop

Для просмотра доступных маршрутов в текущее время необходимо перейти в подраздел диагностики pfTop (**«Межсетевой экран»** - **«Диагностика»** - **«pfTop»**) (см. Рисунок 284).

Существует возможность изменить вид, настроить сортировку или указать количество строк в соответствующих выпадающих строках.

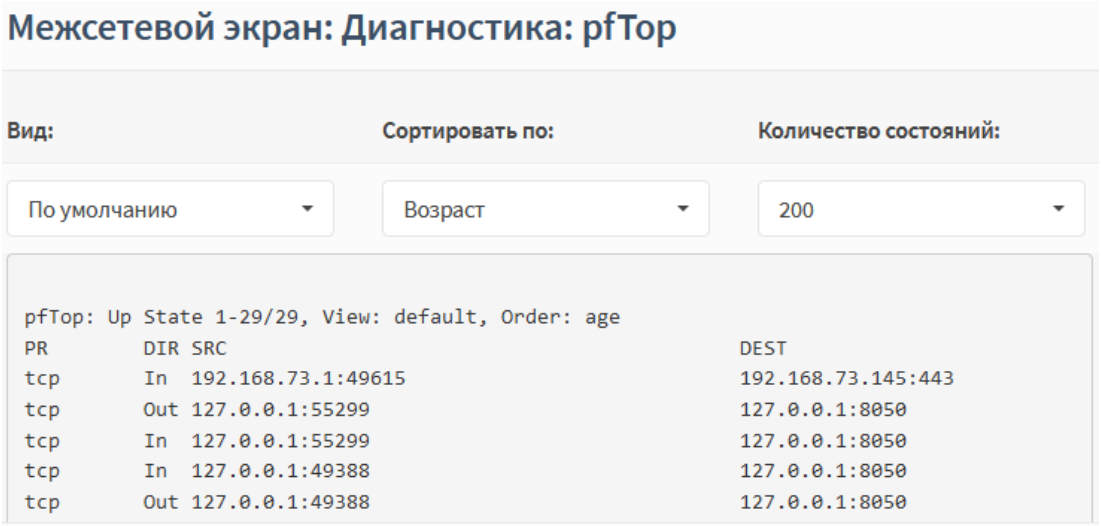

Рисунок 284 –Диагностика pfTop

27.3.3 Диагностика pfTables

Для просмотра IP-адресов, указанных в псевдонимах необходимо перейти в подраздел диагностики pfTables (**«Межсетевой экран»** - **«Диагностика»** - **«pfTables»**) (см. Рисунок 285).

Выпадающие списки позволяют выбрать псевдоним, очистить и обновить базу псевдонима, нажав соответствующие кнопки.

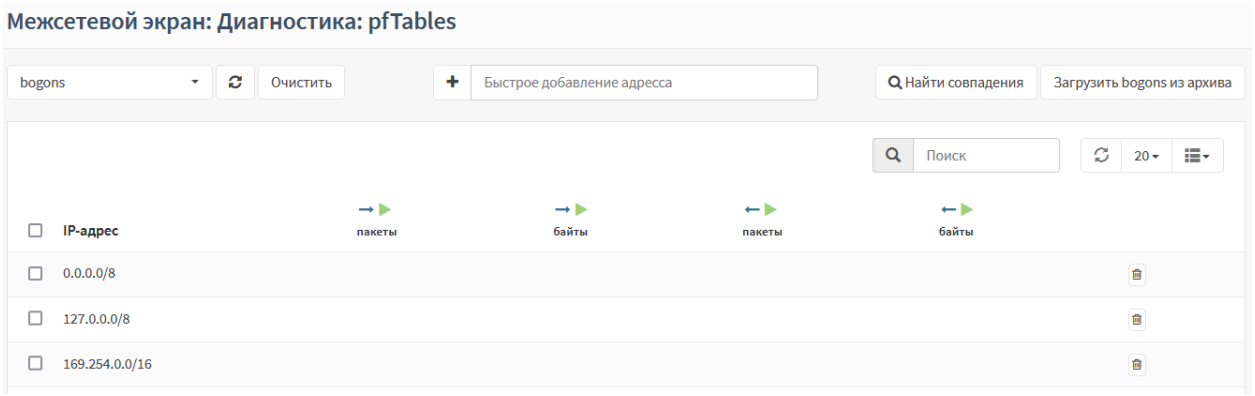

Рисунок 285 – Диагностика pfTables

27.4 Диагностика системы

27.4.1 Действия пользователей

Для просмотра действий пользователей, в том числе системных пользователей, необходимо перейти в подраздел отслеживания активности пользователей (**«Система»** - **«Диагностика»** - **«Активность»**) (см. Рисунок 286).

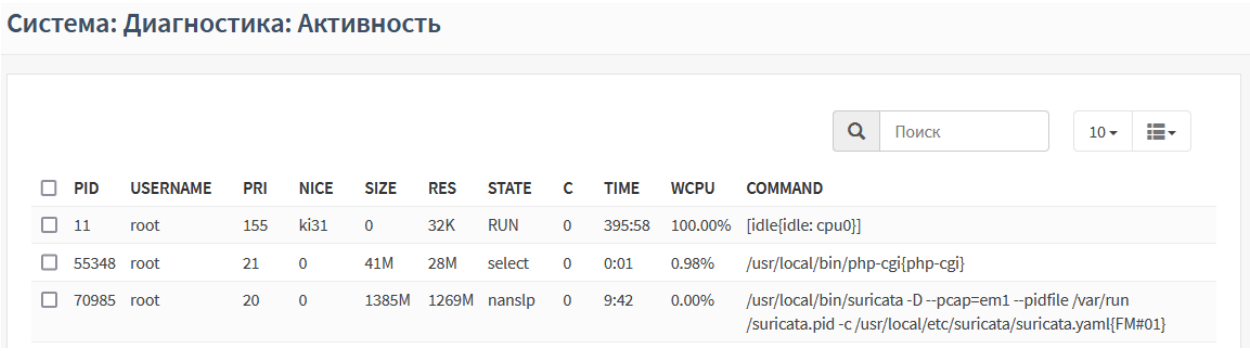

Рисунок 286 – Активность

27.4.2 Службы

Для просмотра и управления настроенными службами необходимо перейти в подраздел управления службами (**«Система»** - **«Диагностика»** - **«Службы»**) (см. Рисунок 287).

Для служб возможны следующие действия при нажатии соответствующей кнопки:

- **кнопка «■»** – остановить службу;
- **кнопка «▶»** – запустить службу;
- **кнопка «↻»** – перезапустить службу.

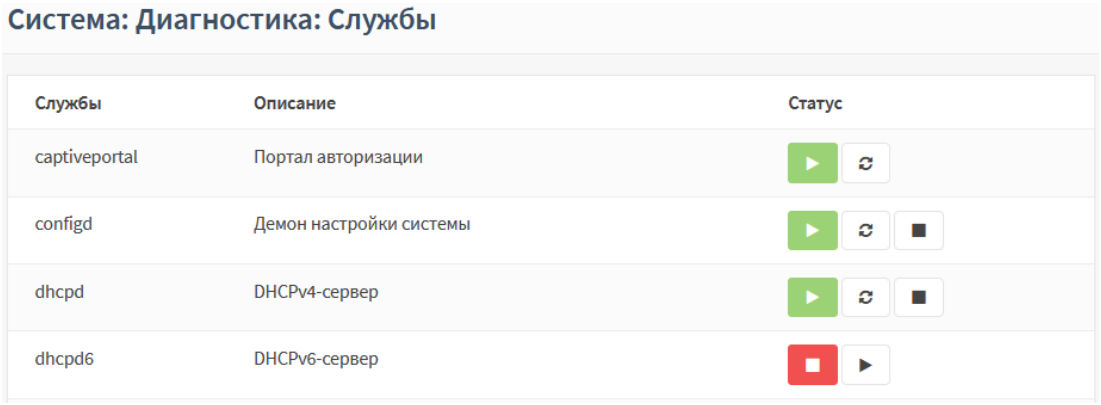

Рисунок 287 – Службы

27.5 Диагностика сетевых интерфейсов

Диагностика сетевых интерфейсов позволяет выполнять следующие действия:

- просматривать таблицу ARP;
- запускать сканирование ARP;
- просматривать таблицу DNS-записей;
- просматривать таблицу NDP-записей;
- экспортировать дамп трафика определенного сетевого интерфейса;
- выполнять и просматривать результаты команды «ping»;

- выполнять проверку порта на наличие подключения;
- выполнять маршрут трассировки.

27.5.1 ARP-таблица

Для просмотра ARP-таблицы необходимо перейти в подраздел просмотра ARP-таблицы (**«Интерфейсы»** - **«Диагностика»** - **«ARP-таблица»**) (см. Рисунок 288).

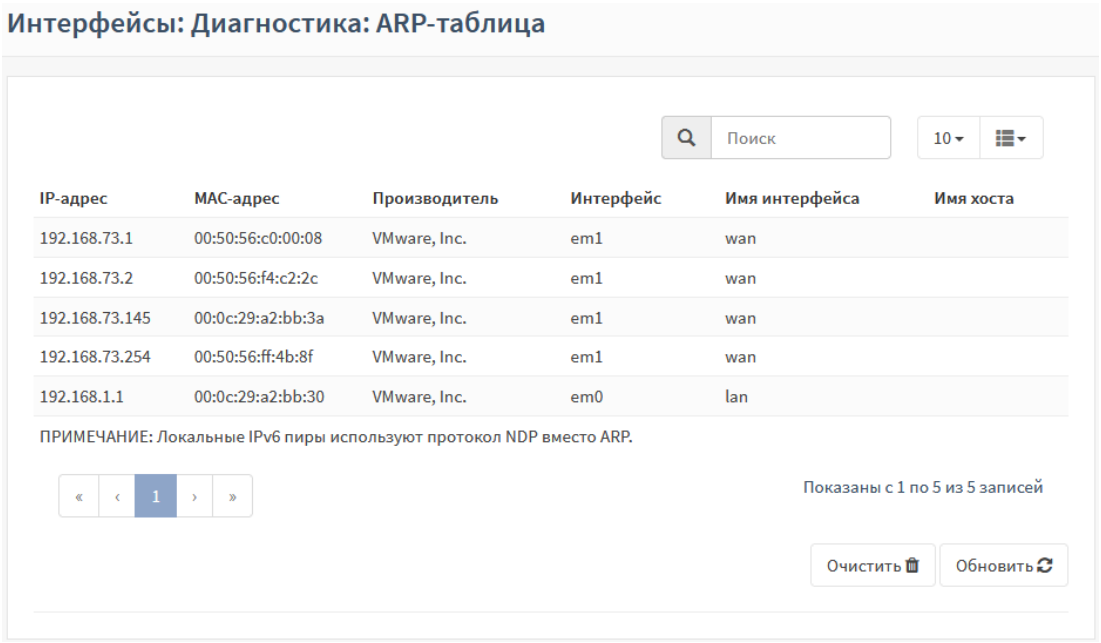

Рисунок 288 – ARP-таблица

27.5.2 Просмотр DNS-записей

Для поиска IP-адресов и записей, принадлежащих заданному имени хоста необходимо перейти в подраздел просмотра DNS-записей (**«Интерфейсы»** - **«Диагностика»** - **«Просмотр DNS-записей»**) (Рисунок 289), указать в параметре **«Имя хоста или IP-адрес»** IP-адрес и нажать **кнопку «Просмотр DNS-записей»**.

Рисунок 289 – Просмотр DNS-записей

27.5.3 NDP-таблица

Для просмотра NDP-таблицы, в которой перечислены локально подключенные узлы IPv6 необходимо перейти в подраздел просмотра NDP-таблицы (**«Интерфейсы»** - **«Диагностика»** - **«NDP-таблица»**) (см. Рисунок 290).

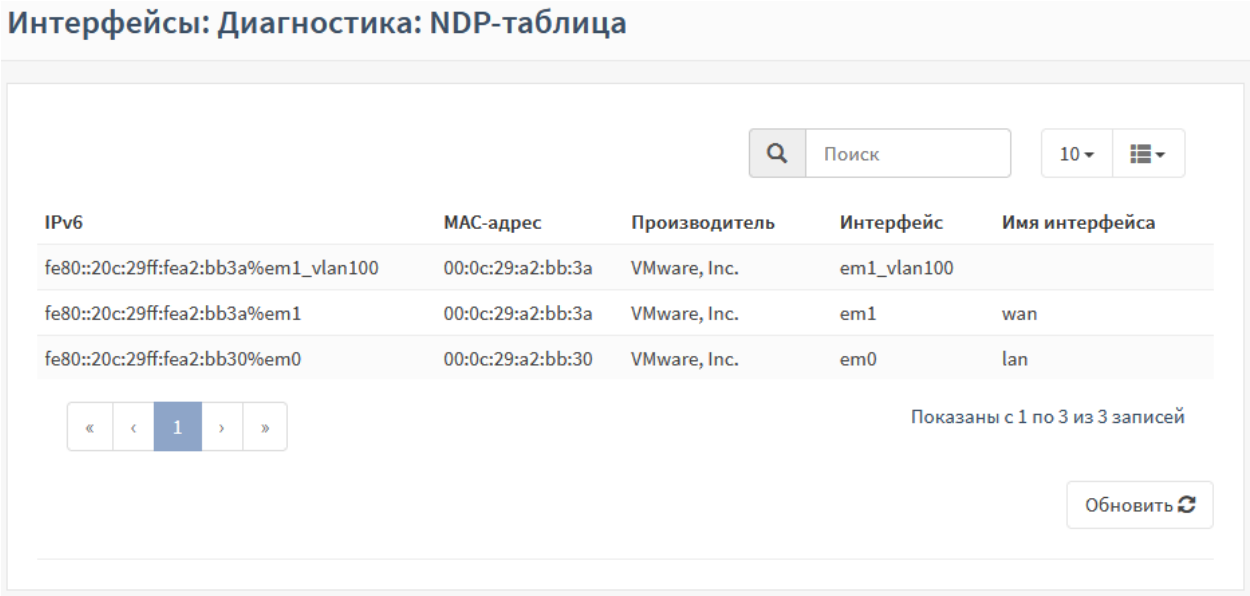

Рисунок 290 – NDP-таблица

27.5.4 Netstat

Для просмотра статистики работы с сетевыми интерфейсами необходимо перейти в подраздел диагностики Netstat (**«Интерфейсы»** - **«Диагностика»** - **«Netstat»**) (см. Рисунок 291).

Статистика работы с сетевыми интерфейсами отображается в группированном виде во вкладках:

- **«Bpf»** – bpf-статистика;
- **«Интерфейсы»** – статистика по интерфейсам;
- **«Память»** – mbuf-статистика;
- **«Netisr»** – netisr-статистика;
- **«Протокол»** – статистика по протоколам;
- **«Сокеты»** –статистика по сокетам.

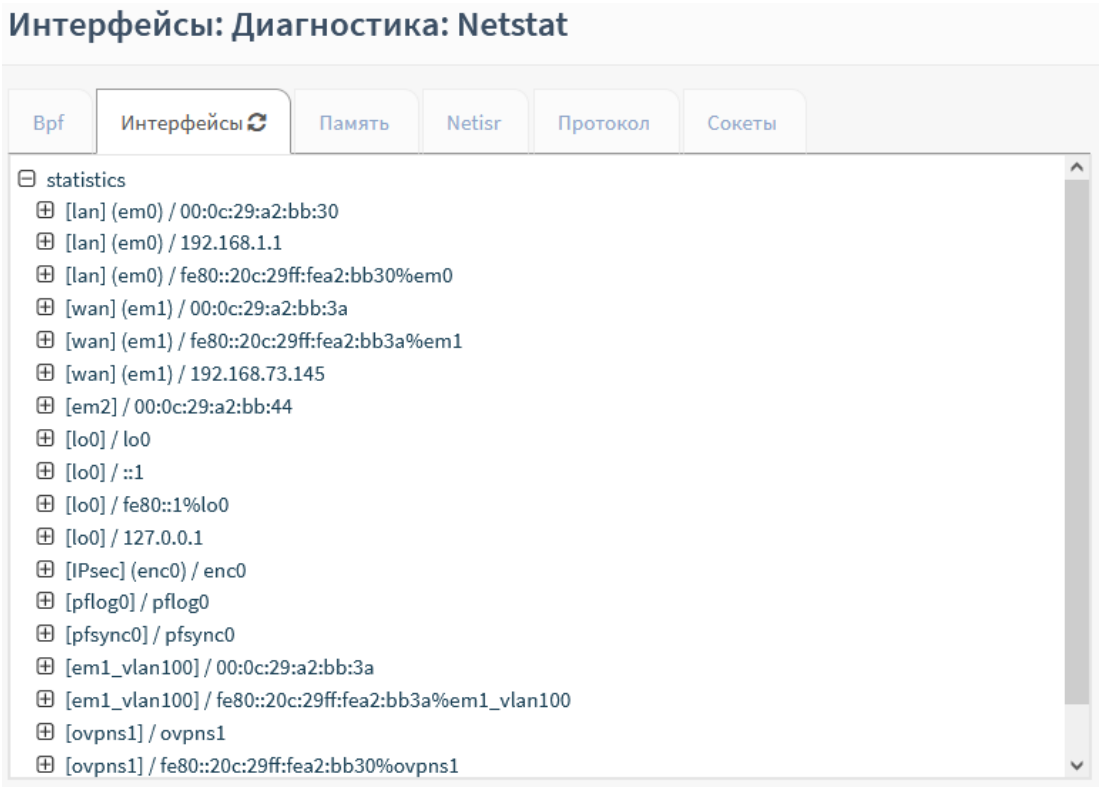

Рисунок 291 – Статистика работы Netstat

27.5.5 Захват пакетов

Функция захвата пакетов предоставляет возможность записи дампов графика с последующим экспортом в файл с расширением «.cap», например, для проведения расследования инцидентов ИБ.

В качестве примера будет рассмотрен захват HTTP-трафика с ПК **«Admin»** до ПК **«Webserver»** по интерфейсу «LAN» (см. Рисунок 292).

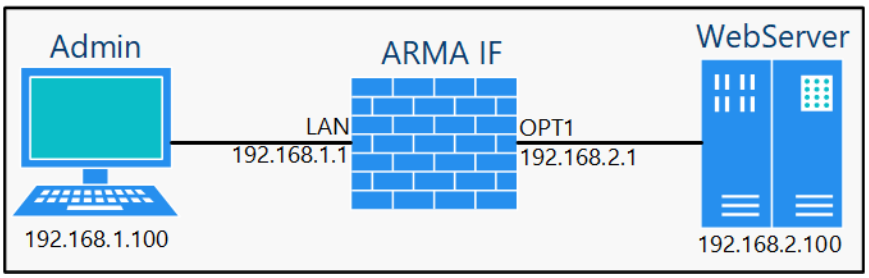

Рисунок 292 – Схема стенда для проверки функции захвата пакетов

Для запуска механизма сбора дампов необходимо выполнить следующие действия:

1. Перейти в подраздел диагностики захватом пакетов (**«Интерфейсы»** – **«Диагностика»** – **«Захват пакетов»**) (см. Рисунок 293).

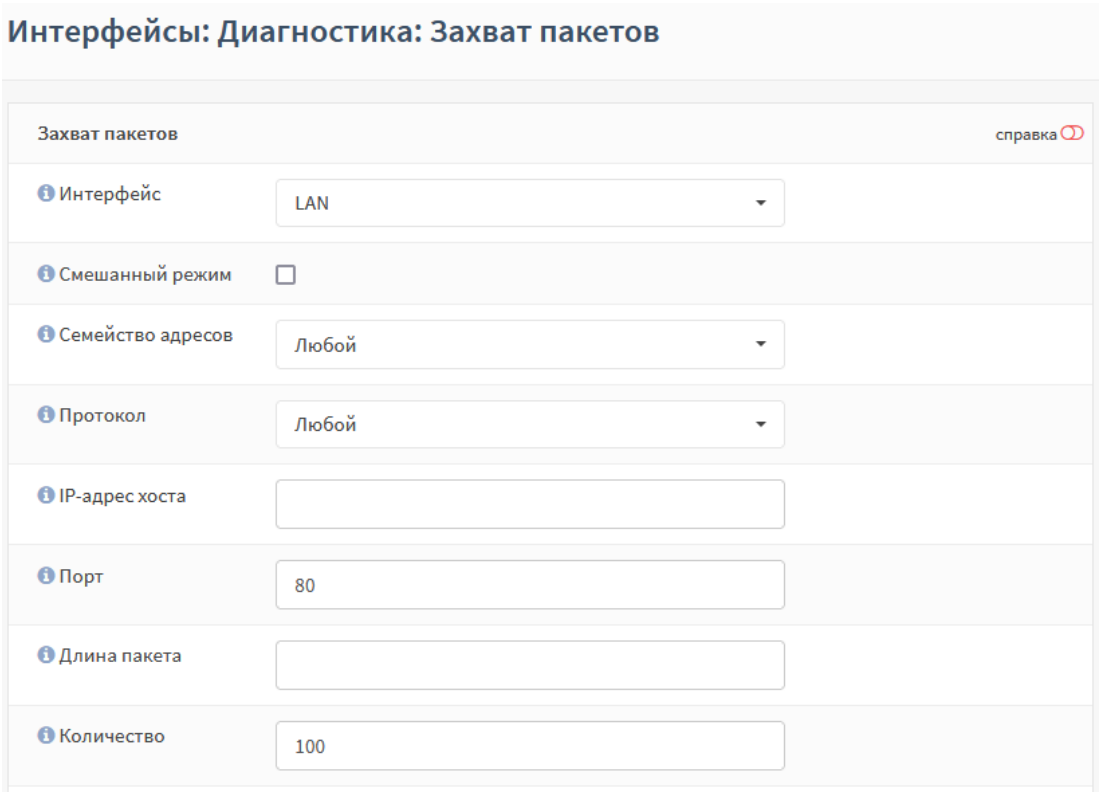

Рисунок 293 – Захват пакетов

2. Указать следующие значения параметров:
   - **«Интерфейс»** – «LAN»;
   - **«Порт»** – «80»;

   остальные параметры отставить без изменений и нажать **кнопку «Запустить»**.
3. На ПК **«Admin»** открыть веб-браузер и перейти по адресу «192.168.2.100».
4. В подразделе **«Захват пакетов»** нажать **кнопку «Остановить»**. Дамп трафика будет отображен в нижней части страницы подраздела (см. Рисунок 294).

Для просмотра захваченных пакетов в веб-интерфейсе **ARMA IF** необходимо нажать **кнопку «Просмотр захваченных пакетов»**. Уровень детализации просматриваемых пакетов выбирается в выпадающем списке **«Уровень детализации»**.

Для сохранения дампа захваченных пакетов на локальный ПК необходимо нажать на гиперссылку **«packetcapture_emX.cap»**, где **«X»** – это номер физического интерфейса, и выполнить сохранение с помощью интерфейса веб-браузера.

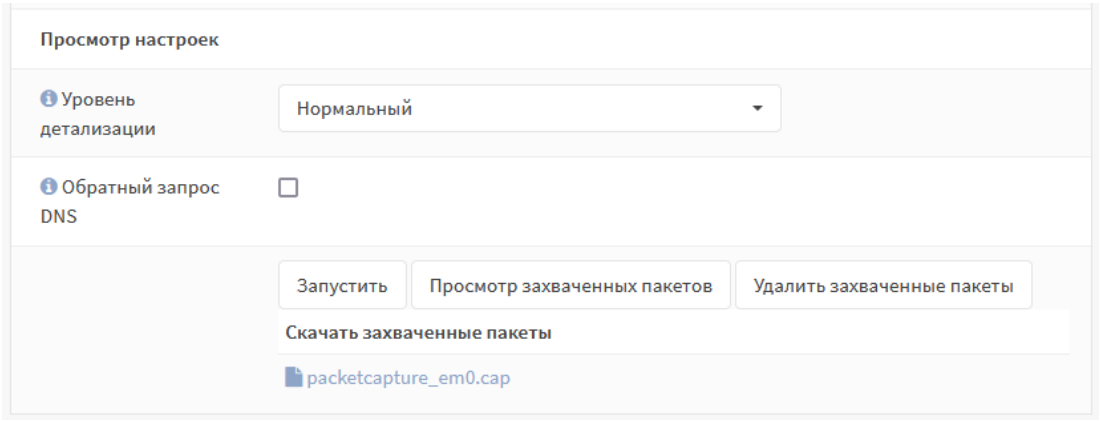

Рисунок 294 – Дамп трафика

Краткое описание параметров при захвате пакетов:

- **«Смешанный режим»** – установка флажка позволяет принимать все пакеты трафика, независимо от адресата;
- **«Семейство адресов»** – позволяет оставлять только трафик IPv4 или IPv6;
- **«IP-адрес хоста»** – указывает IP-адрес или подсеть получателя или источника, также существует возможность указания исключения или множество значений используя логическое выражение со аргументами **«not»** и **«and»**;
- **«Порт»** – указывается порт получателя или источника;
- **«Длина пакета»** – указывается значение количества бит каждого захваченного пакета;
- **«Количество»** – указывается значение количества захватываемых пакетов;
- **«Обратный запрос DNS»** – установка флажка позволяет захватывать пакеты трафика, ассоциируемые со всеми IP-адресами обратного запроса DNS:

  для этого в группе настроек **«Захват пакетов»** в поле **«Интерфейсы»** необходимо выбрать интерфейсы для захвата трафика. В поле **«Смешанный режим»** необходимо установить флажок для того, чтобы принимать все пакеты, независимо от того, кому они адресованы. В поле **«Семейство адресов»** необходимо выбрать тип трафика для захвата. В поле **«Протокол»** необходимо выбрать протокол для захвата трафика. В поле **«IP-адрес хоста»** необходимо ввести IP-адрес источника. В поле **«Порт»** необходимо ввести порт. В поле **«Длина пакета»** необходимо ввести длину пакета (в битах). В поле **«Количество»** необходимо ввести количество пакетов, которые будут захватываться

27.5.6 Ping

Ping – утилита для проверки целостности и качества соединений в сетях TCP/IP.

Функция ping используется, например, для проверки наличия доступа к устройству сети. В качестве примера будет рассмотрена проверка наличия доступа к ПК **«Admin»** (см. Рисунок 292).

Для запуска утилиты ping необходимо выполнить следующие действия:

1. Перейти в подраздел диагностики ping (**«Интерфейсы»** – **«Диагностика»** – **«Ping»**) (см. Рисунок 295).
2. Указать IP-адрес «192.168.1.100» в параметре **«Хост»** и нажать **кнопку «Ping»**.

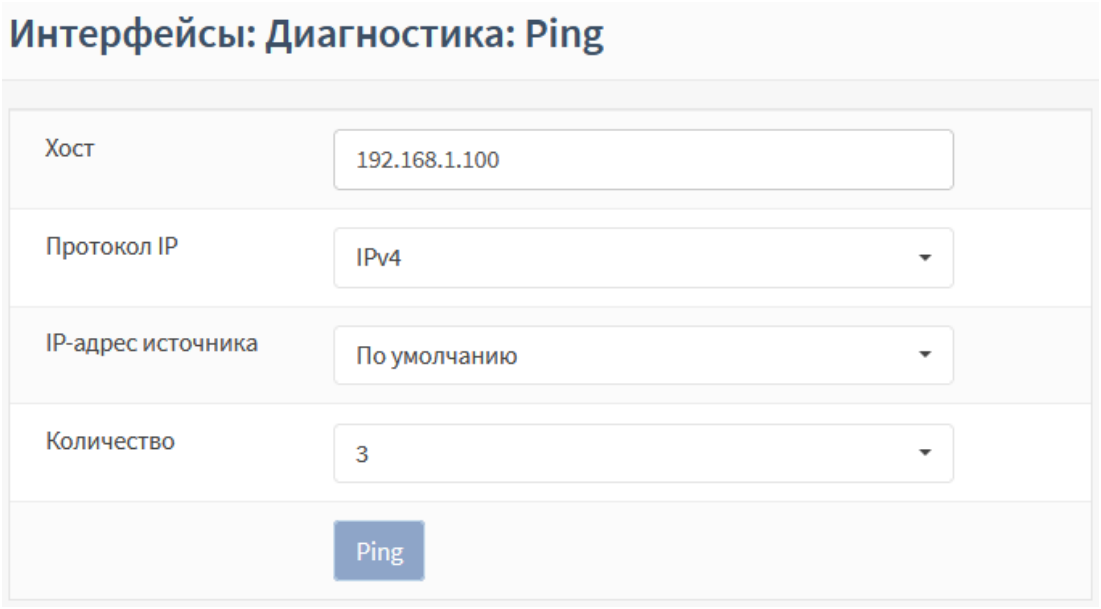

Рисунок 295 – Ping

3. Результат команды отобразится в нижней части страницы (Рисунок 296).

```
# /sbin/ping -c '3' '192.168.1.100'
PING 192.168.1.100 (192.168.1.100): 56 data bytes
64 bytes from 192.168.1.100: icmp_seq=0 ttl=128 time=0.380 ms
64 bytes from 192.168.1.100: icmp_seq=1 ttl=128 time=0.441 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=128 time=0.383 ms

--- 192.168.1.100 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.380/0.401/0.441/0.028 ms
```

Рисунок 296 – Результат выполнения команды Ping

27.5.7 Проверка порта

Функция проверки порта используется для выполнения простого теста TCP-соединения по указанному порту. В качестве примера будет рассмотрена проверка наличия доступа к ПК **«WebServer»** по порту «443» (см. Рисунок 292).

Для проверки соединения необходимо выполнить следующие действия:

1. Перейти в подраздел проверки порта (**«Интерфейсы»** – **«Диагностика»** – **«Проверка порта»**) (см. Рисунок 297).

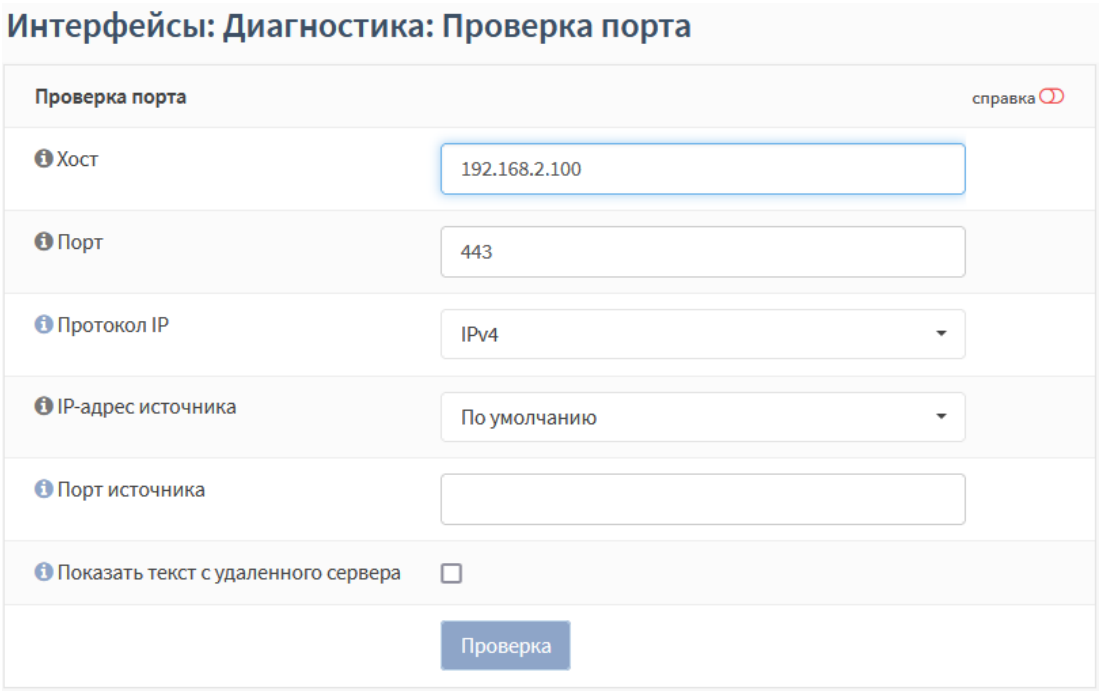

Рисунок 297 – Проверка порта

2. Указать следующие значения параметров:
   - **«Хост»** – «192.168.2.100»;
   - **«Порт»** – «443»;

   остальные параметры отставить без изменений и нажать **кнопку «Проверка»**.
3. Результат команды отобразится в нижней части страницы (см. Рисунок 298).

```
# /usr/bin/nc -w 10 -z  -4 '192.168.2.100' '443'
Connection to 192.168.2.100 443 port [tcp/https] succeeded!
```

Рисунок 298 – Результат выполнения команды проверка порта

27.5.8 Маршрут трассировки

Трассировка маршрута предназначена для определения маршрутов следования данных в сетях TCP/IP. В качестве примера будет рассмотрено определение маршрута к ПК **«Admin»** (см. Рисунок 292).

Для выполнения трассировки маршрута необходимо выполнить следующие действия:

1. Перейти в подраздел трассировки маршрутов (**«Интерфейсы»** – **«Диагностика»** – **«Маршрут трассировки»**) (см. Рисунок 299).

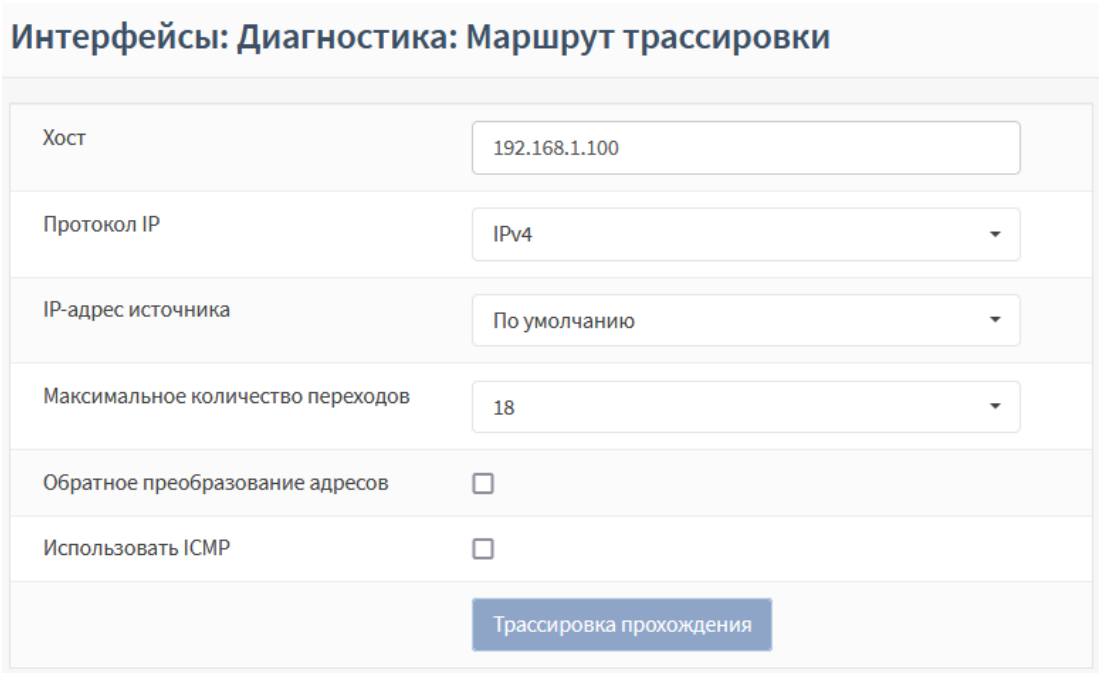

Рисунок 299 – Маршрут трассировки

2. Указать «192.168.1.100» в параметре **«Хост»** и нажать **кнопку «Трассировка прохождения»**.
3. Результат команды отобразится в нижней части страницы (см. Рисунок 300).

```
# /usr/sbin/traceroute -w 2 -n  -m '18'  '192.168.1.100'
traceroute to 192.168.1.100 (192.168.1.100), 18 hops max, 40 byte packets
 1  192.168.1.100  0.719 ms  0.335 ms  0.428 ms
```

Рисунок 300 – Результат выполнения команды трассировки

27.5.9 Обзор

Диаграммы трафика, обработанного **ARMA IF**, представлены в подразделе обзора журналов (**«Межсетевой экран»** - **«Журналы»** - **«Обзор»**). В подразделе представленные следующие диаграммы:

- **«Действия»** – Рисунок 301;
- **«Интерфейсы»** – Рисунок 302;
- **«Протоколы»** – Рисунок 303;
- **«IP-адреса источника»** – Рисунок 304;
- **«IP-адреса назначения»** – Рисунок 305;
- **«Порты источника»** – Рисунок 306;
- **«Порты назначения»** – Рисунок 307.

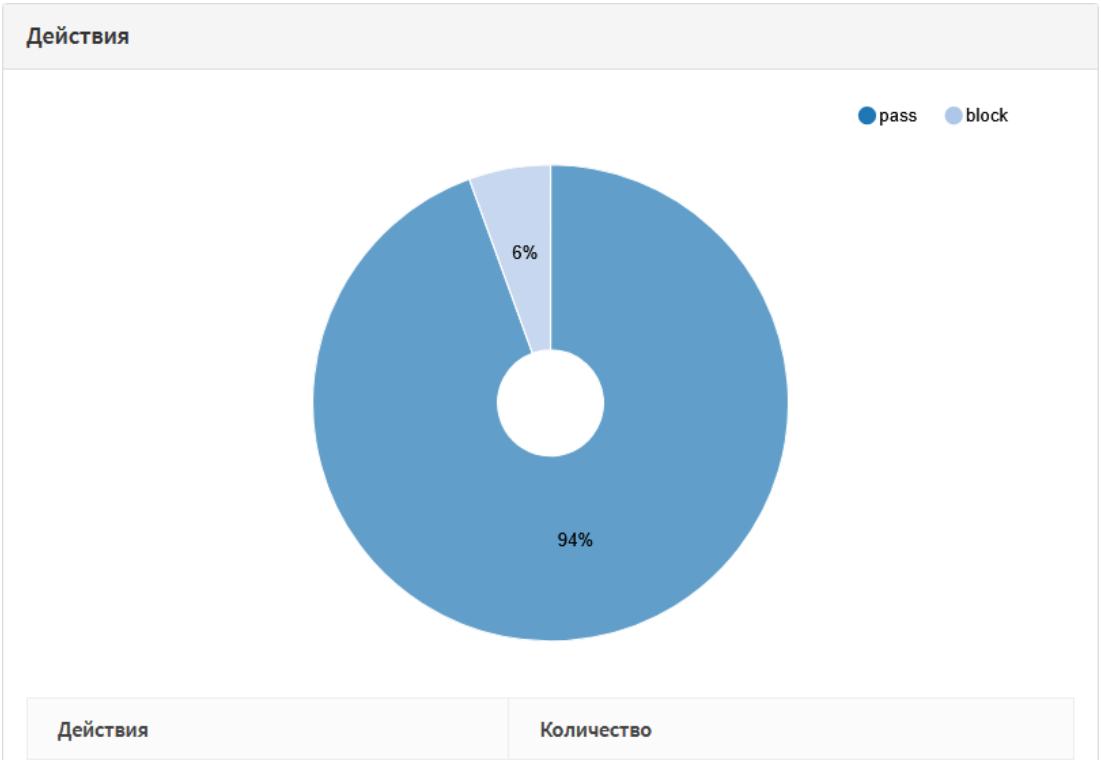

Рисунок 301 – Действия

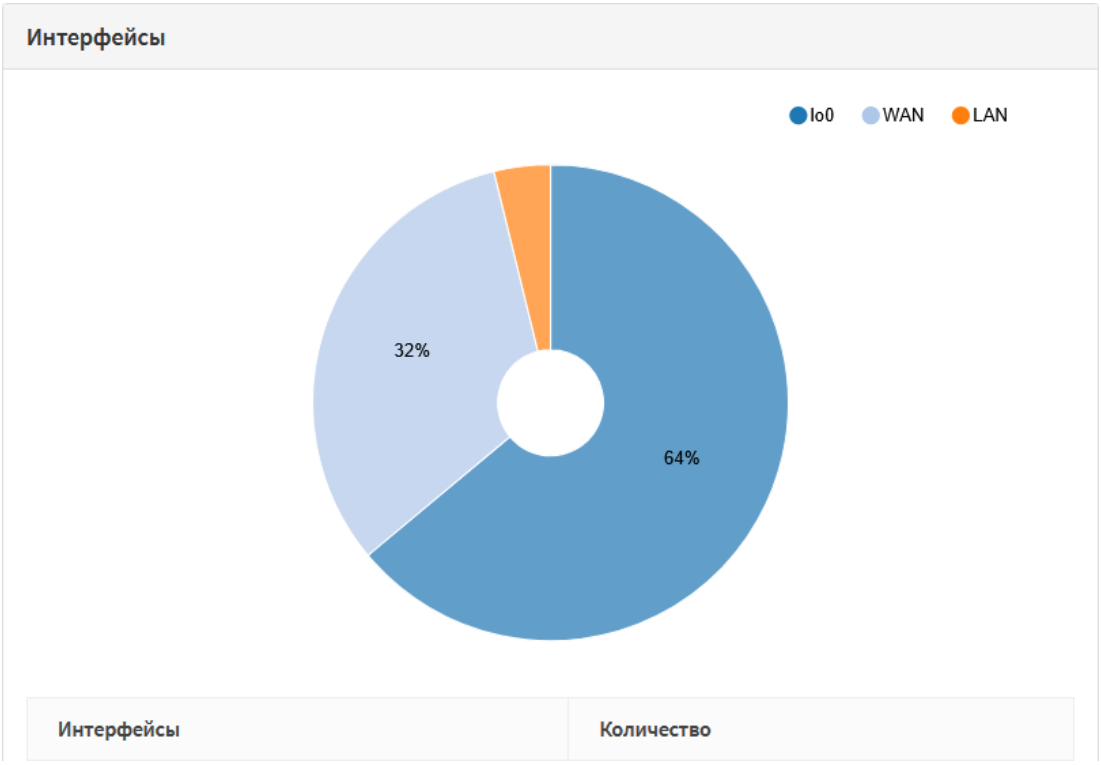

Рисунок 302 – Интерфейсы

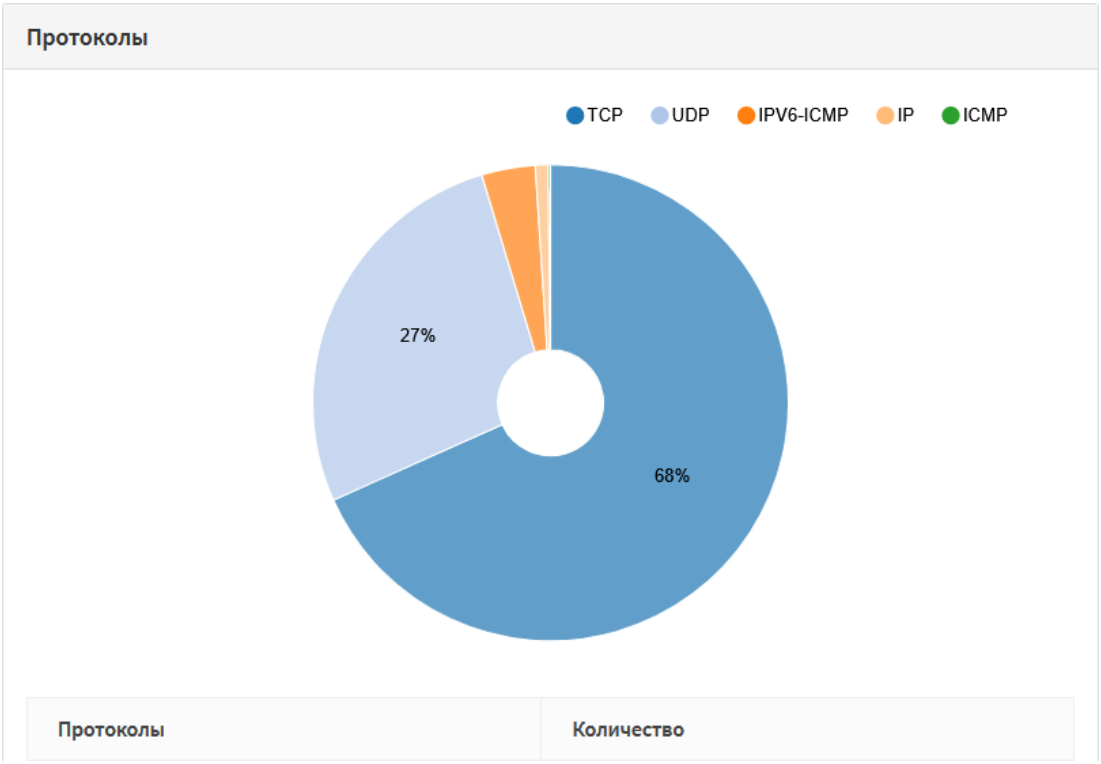

Рисунок 303 – Протоколы

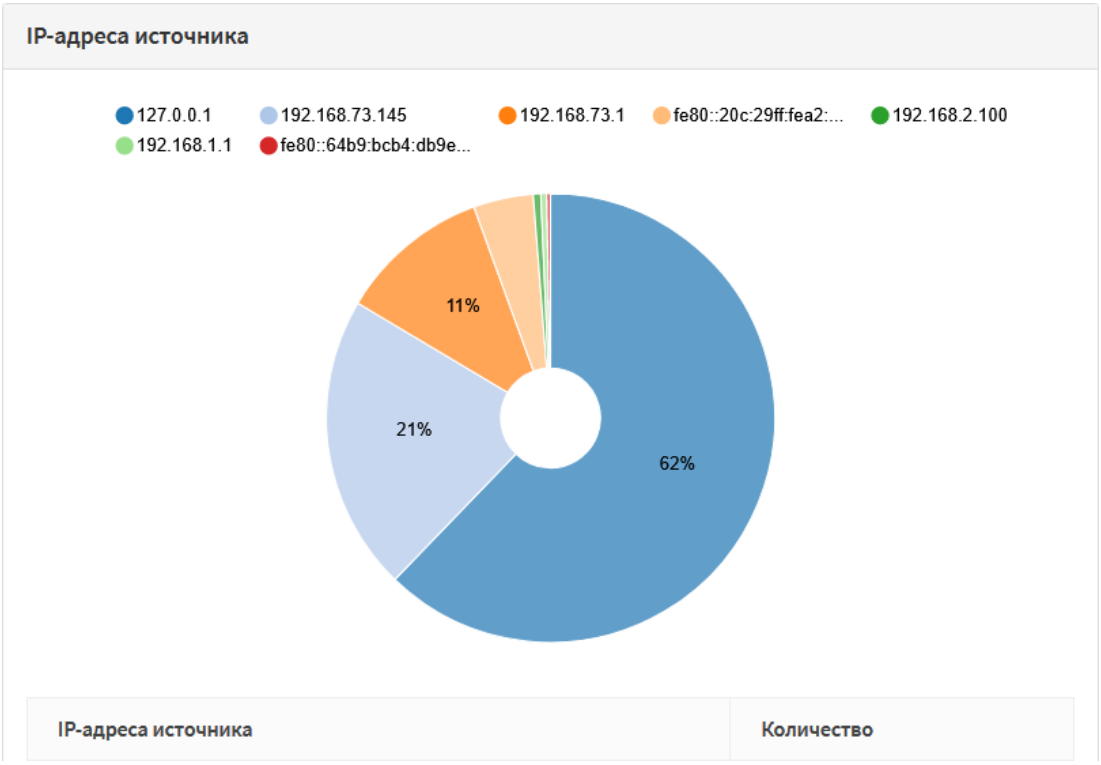

Рисунок 304 – IP-адреса источника

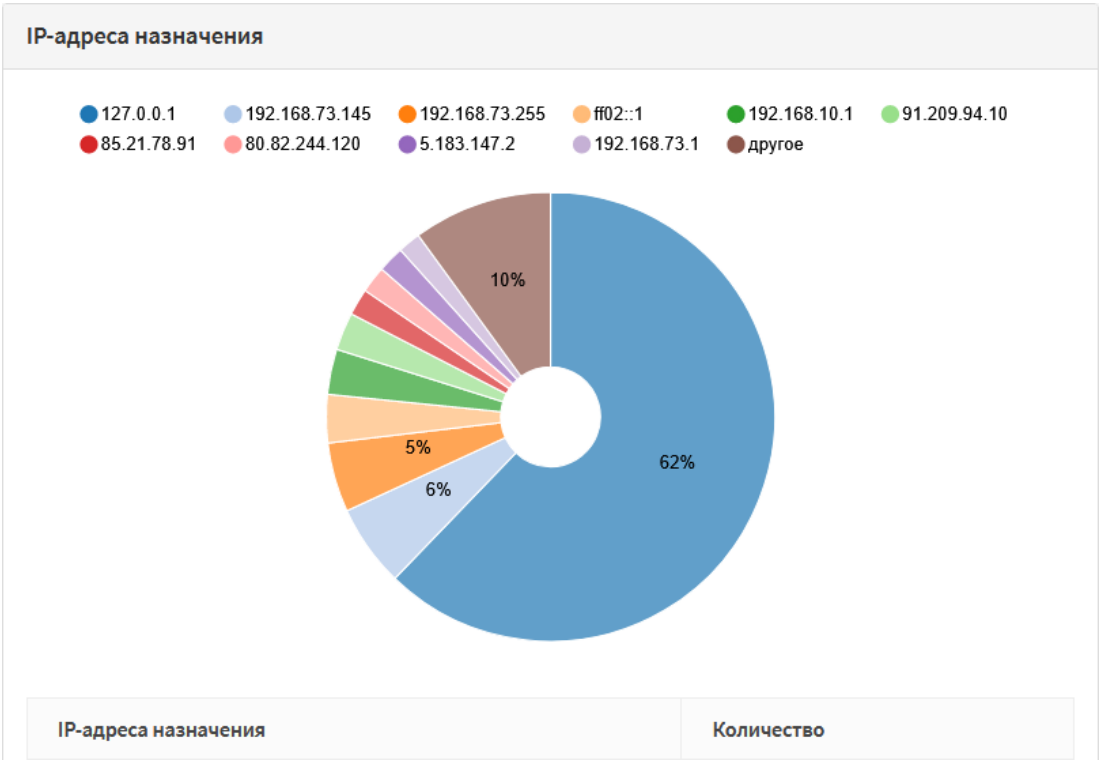

Рисунок 305 – IP-адреса назначения

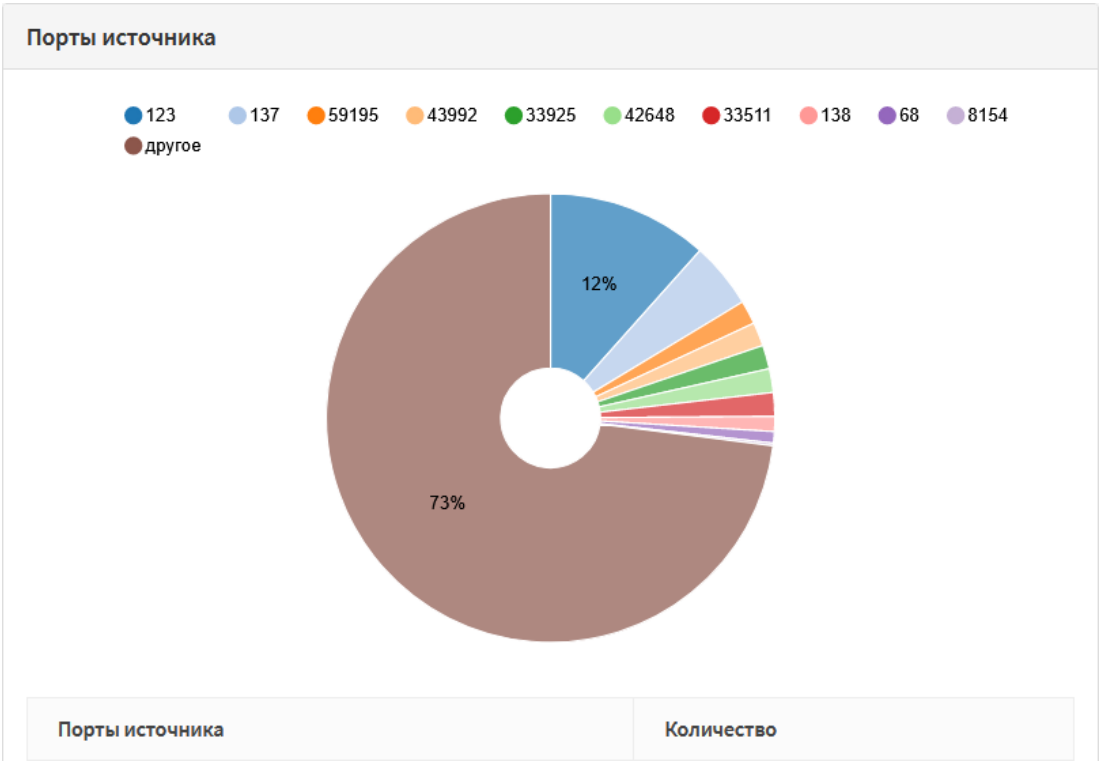

Рисунок 306 – Порты источника

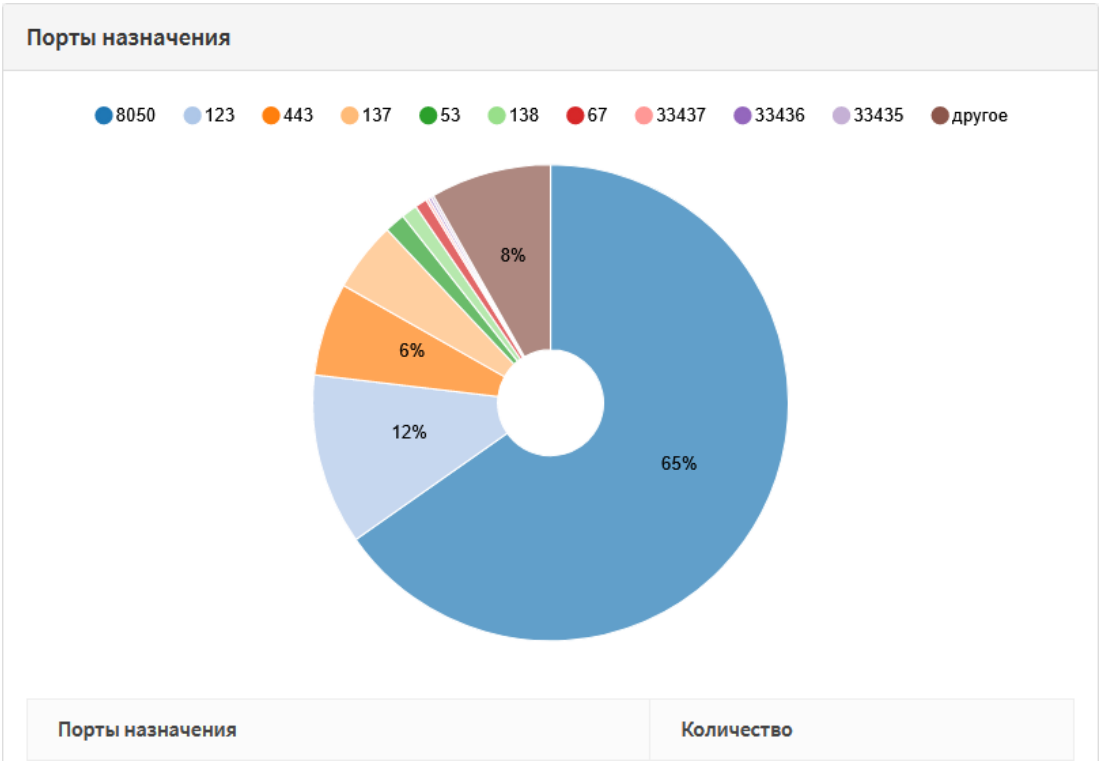

Рисунок 307 – Порты назначения

27.6 Диагностика статической маршрутизации

Для диагностики статической маршрутизации в **ARMA IF** предусмотрены два подраздела:

- статус маршрутизации (**«Система»** - **«Маршруты»** - **«Статус»**) – в подразделе приведена таблица маршрутов системы (см. Рисунок 308);

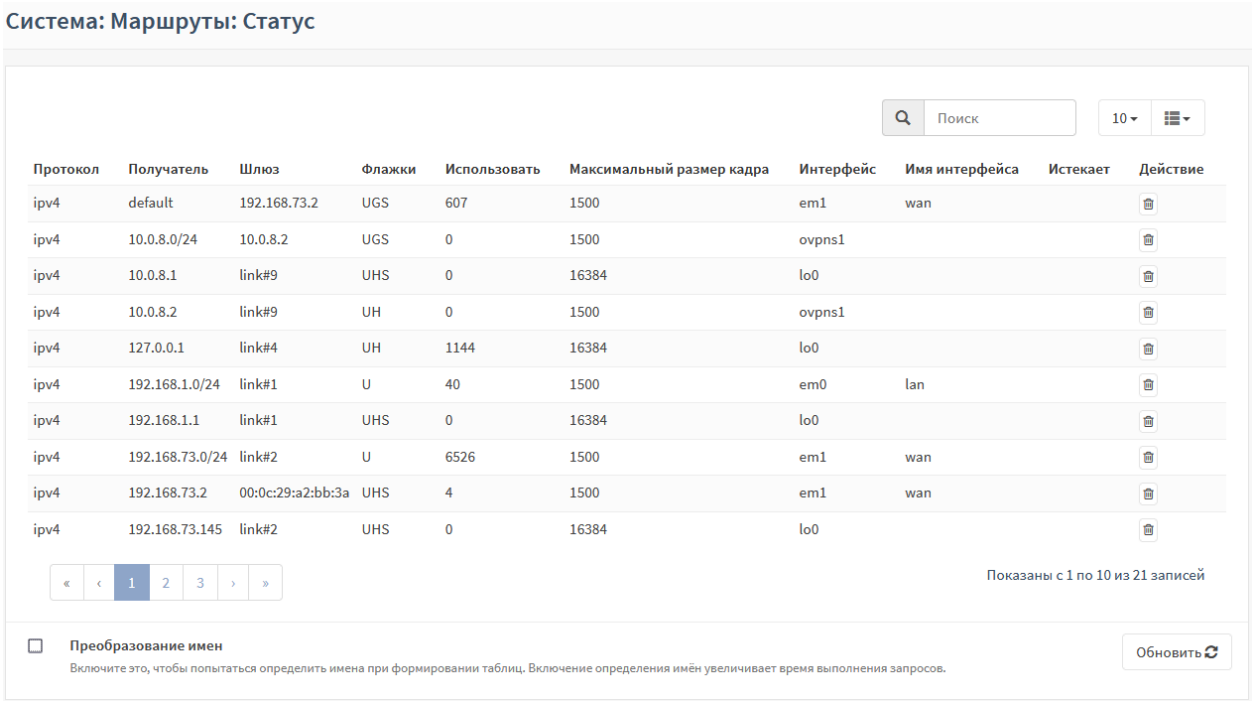

Рисунок 308 – Диагностика статической маршрутизации

- журнал маршрутизации (**«Система»** - **«Маршруты»** - **«Журнал»**) – в подразделе отображены события изменения маршрутов (см. Рисунок 309).

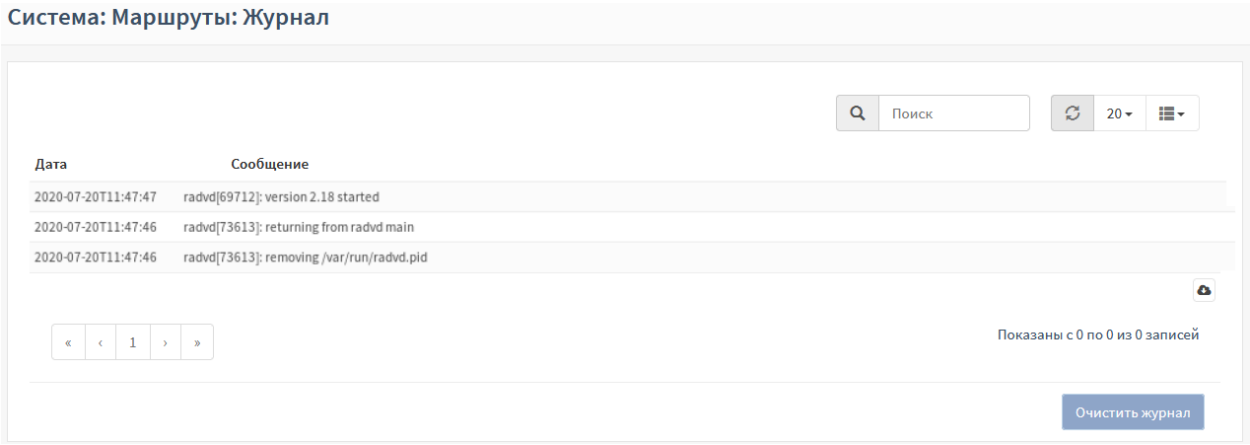

Рисунок 309 – Журнал статической маршрутизации

27.7 Диагностика динамической маршрутизации

Для диагностики динамической маршрутизации в **ARMA IF** предусмотрены следующие вкладки в подразделе общих настроек динамической маршрутизации (**«Маршрутизация»** - **«Диагностика»** - **«Общие настройки»**):

- **«Маршруты IPv4»** – отображает данные о маршрутах IPv4 (см. Рисунок 310);

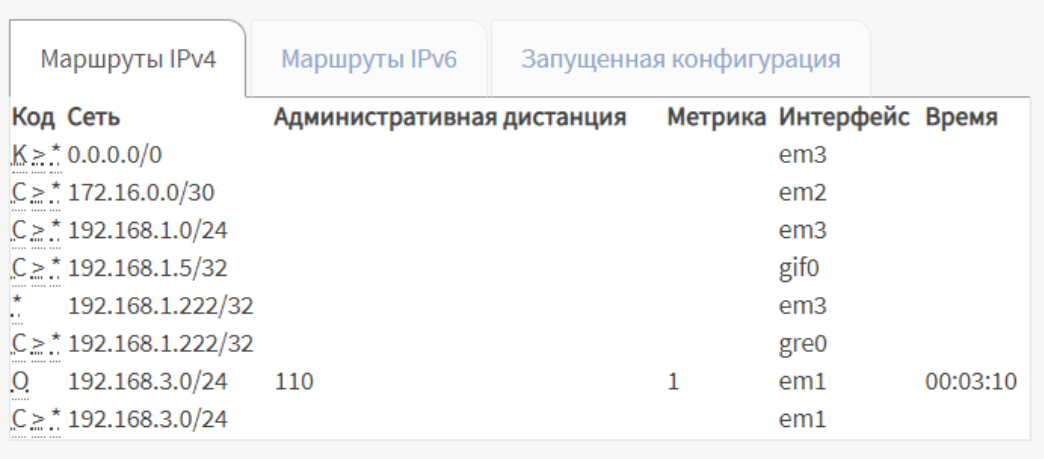

Рисунок 310 – Маршруты IPv4

- **«Маршруты IPv6»** – отображает данные о маршрутах IPv6 (см. Рисунок 311);

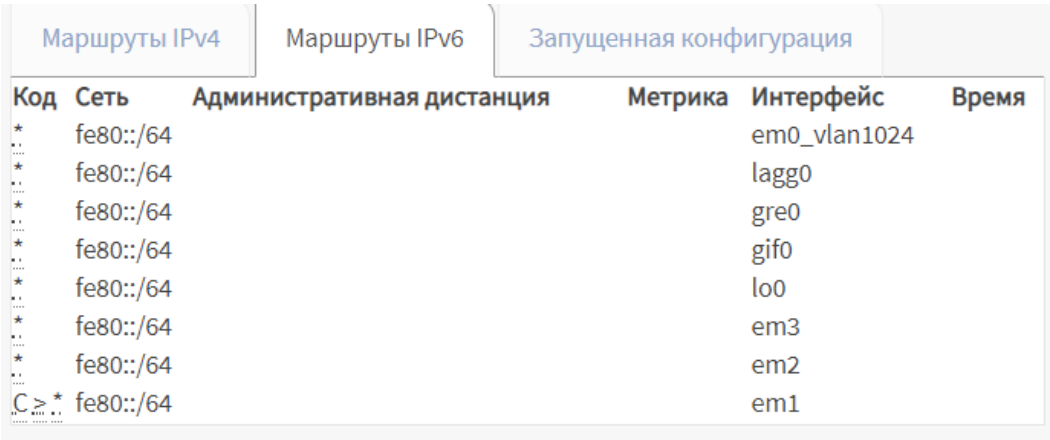

Рисунок 311 – Маршруты IPv6

- **«Запущенная конфигурация»** – отображает общую конфигурацию настроенных динамических маршрутов (см. Рисунок 312).

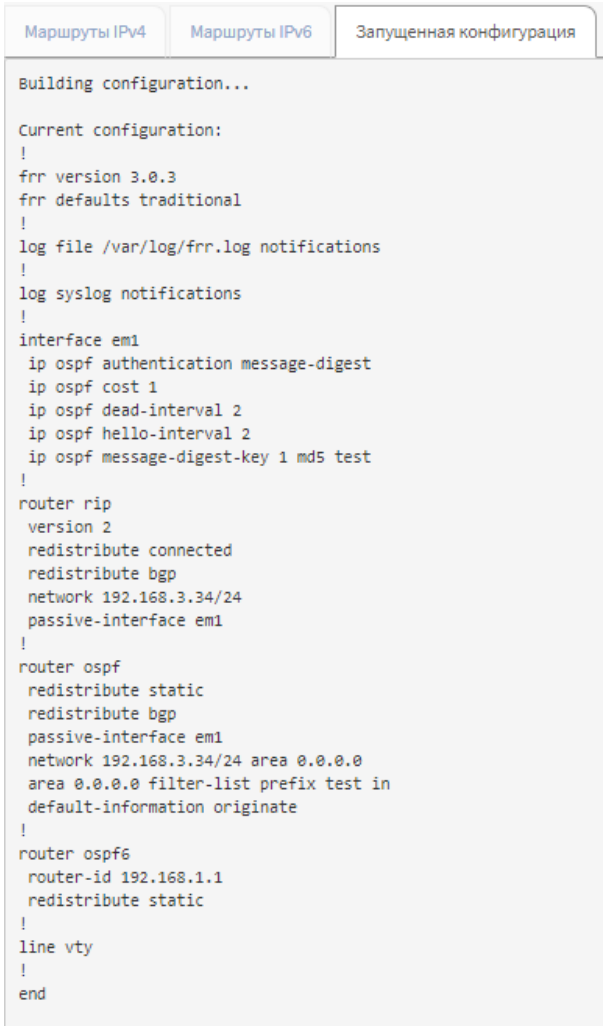

Рисунок 312 – Запущенная конфигурация

27.7.1 OSPF

Для просмотра данных о настройке динамической маршрутизации по протоколу OSPF в **ARMA IF** предусмотрены следующие вкладки в подразделе OSPF динамической маршрутизации (**«Маршрутизация»** - **«Диагностика»** - **«OSPF»**):

- **«Обзор»** – отображает общие данные о настройке динамической маршрутизации по протоколу OSPF (см. Рисунок 313);

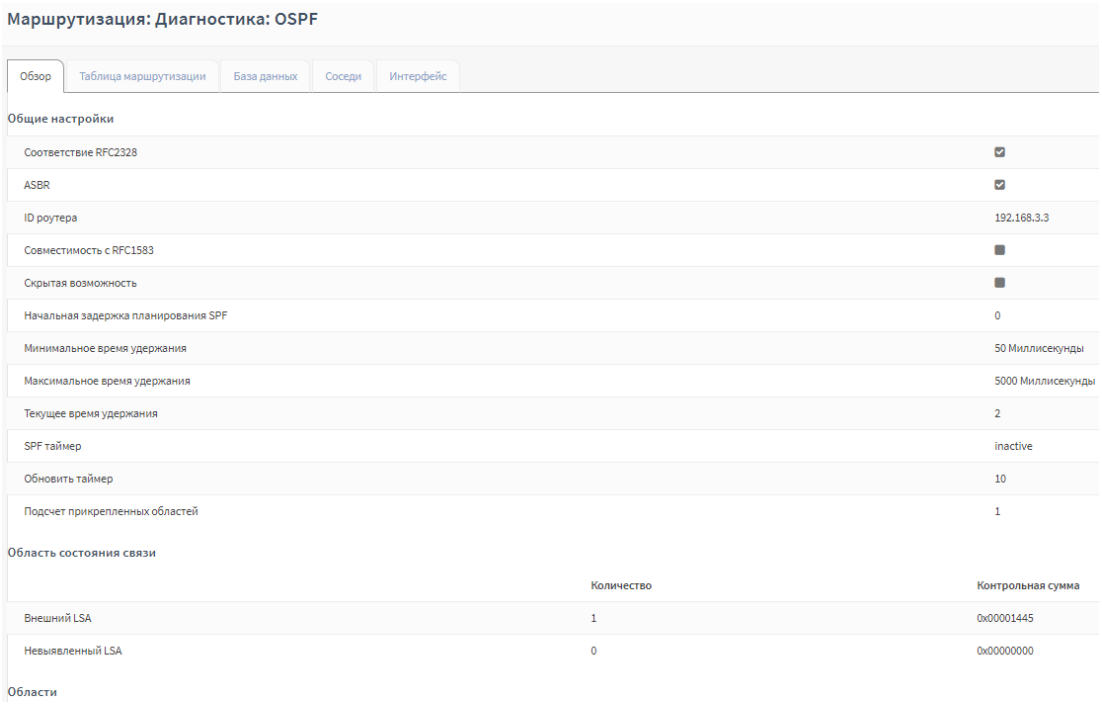

Рисунок 313 – Обзор

- **«Таблица маршрутизация»** – отображает таблицу маршрутизации сети/роутера, внешнюю таблицу маршрутизации (см. Рисунок 314);

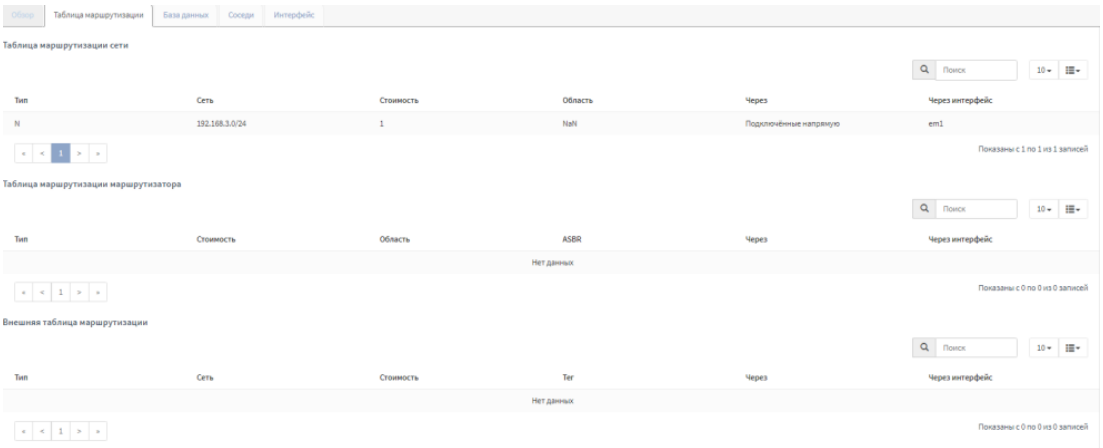

Рисунок 314 – Таблица маршрутизации

- **«База данных»** – отображает таблицы состояний связи (см. Рисунок 315);

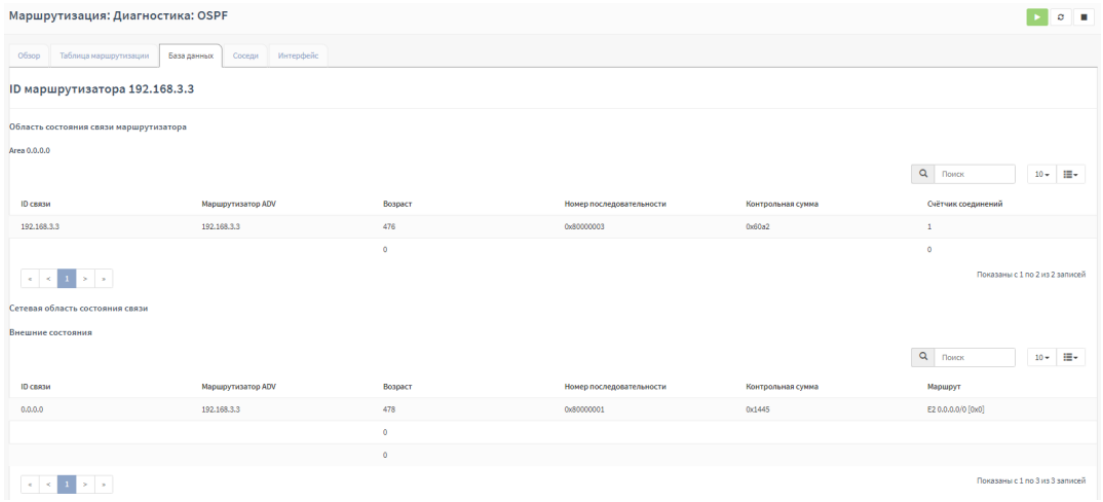

Рисунок 315 – База данных

- **«Соседи»** – отображает таблицу соседей (см. Рисунок 316);

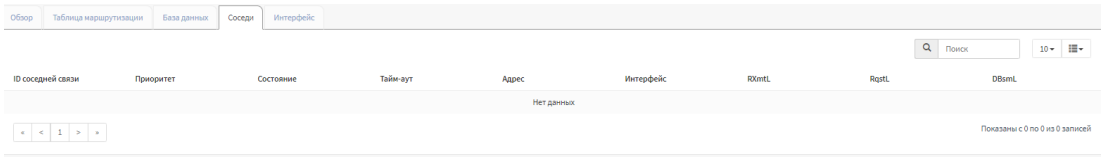

Рисунок 316 – Соседи

- **«Интерфейс»** – отображает данные о настроенных интерфейсах (см. Рисунок 317).

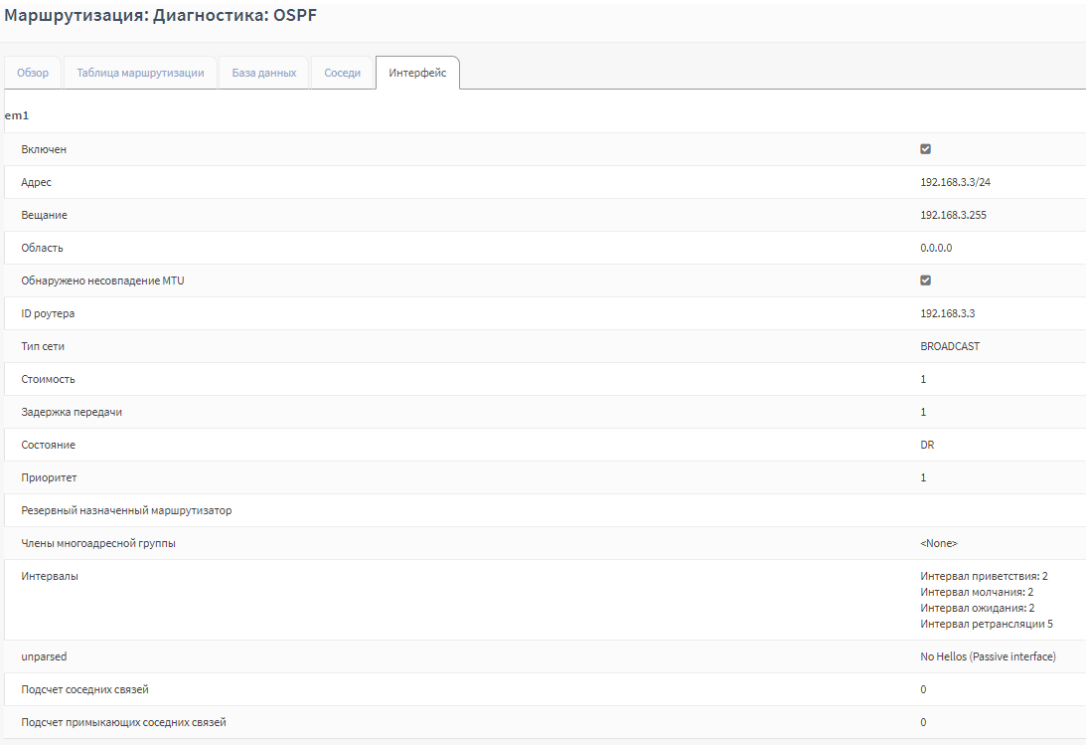

Рисунок 317 – Интерфейс

27.8 Диагностика COB/IPS

Для просмотра данных COB/IPS в **ARMA IF**, в подразделе администрирования COB (**«Обнаружение вторжений»** - **«Администрирование»**), предусмотрена вкладка **«Журналирование»** (см. Рисунок 318).

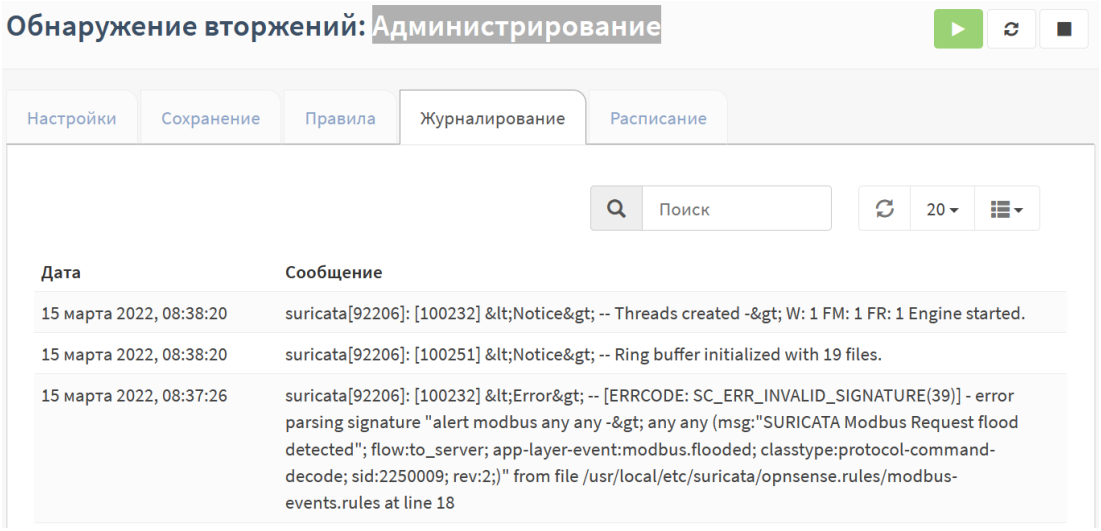

Рисунок 318 – Диагностика COB/IPS

27.9 Диагностика синхронизации времени

Для просмотра данных об синхронизации времени в **ARMA IF** предусмотрен подраздел статуса сетевого времени (**«Службы»** - **«Сетевое время»** - **«Статус»**) (см. Рисунок 319), показывающий текущий статус сетевого времени.

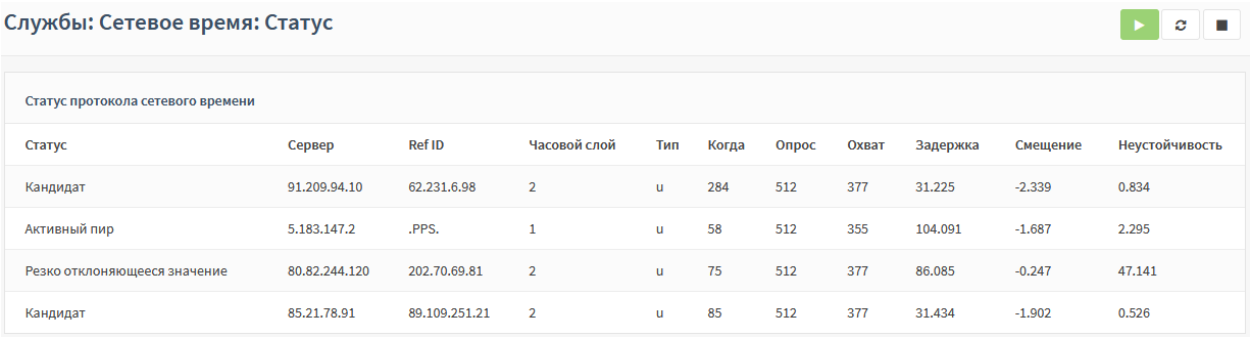

Рисунок 319 – Диагностика синхронизации времени

27.10 Анализ дампа трафика

Для просмотра и анализа дампа трафика, захваченного COB, в **ARMA IF** предусмотрен подраздел журналирования (**«Сеть»** - **«Анализ трафика»** - **«Журналирование»**) (см. Рисунок 320). Для отображения записей необходимо выбрать из выпадающего списка в верхней левой части формы требуемый файл журнала. Разбиение журналов осуществляется по дате и времени начала записи.

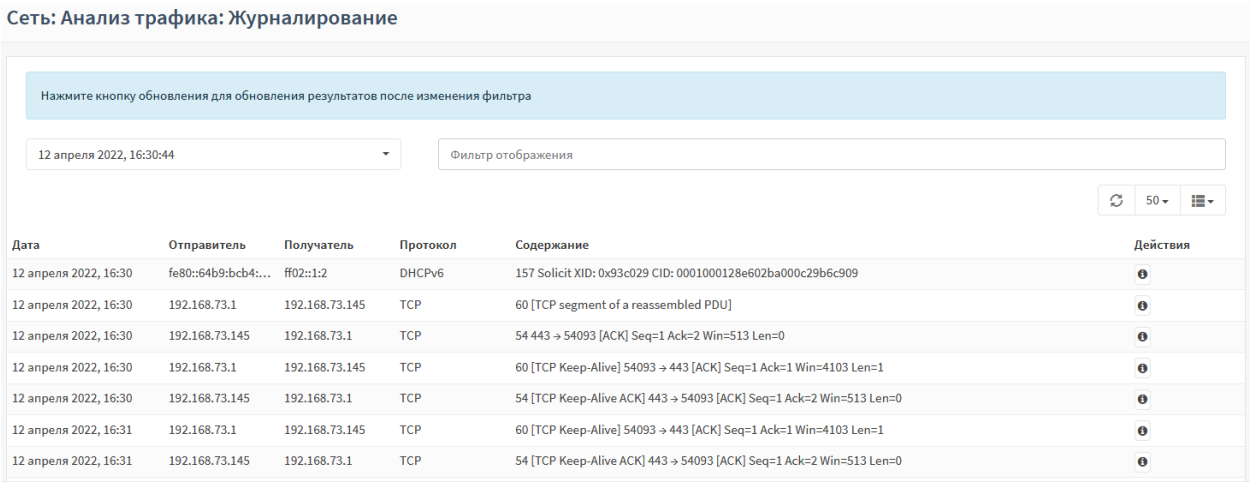

Рисунок 320 – Анализ трафика

27.11 Диагностика состояния ARMA IF

27.11.1 Снимок состояний

Для просмотра активных состояний в текущий момент времени в **ARMA IF** предусмотрен подраздел состояний **ARMA IF** (**«Межсетевой экран»** - **«Диагностика»** - **«Снимок состояний»**) (см. Рисунок 321).

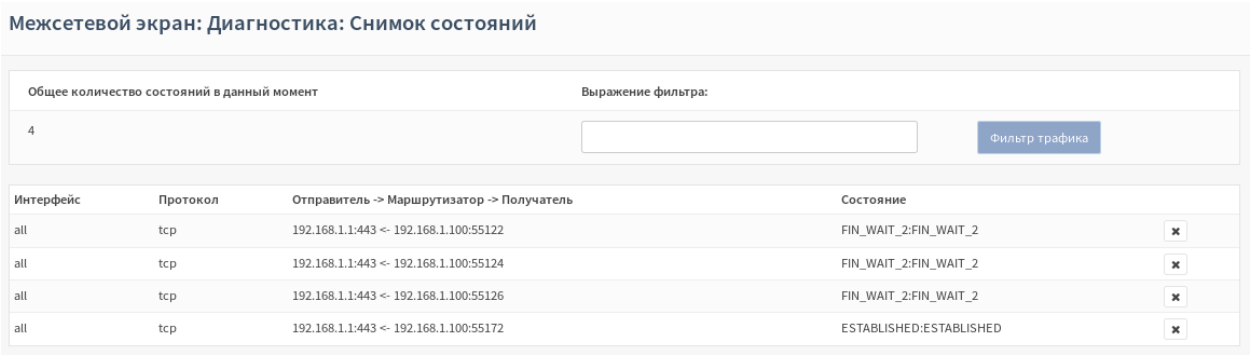

Рисунок 321 – Снимок состояний МЭ

27.11.2 Сброс состояний

Для удаления активных состояний и/или отслеживания источника в **ARMA IF** предусмотрен подраздел сброса состояний (**«Межсетевой экран»** - **«Диагностика»** - **«Сброс состояний»**) (см. Рисунок 322). Для выполнения данных действий необходимо установить соответствующий флажок и нажать **кнопку «Очистить»**.

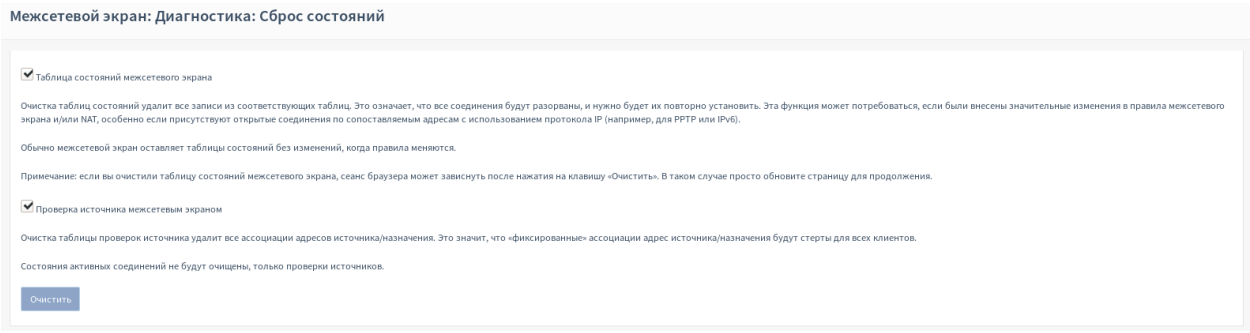

Рисунок 322 – Сброс состояний МЭ

27.11.3 Сводка состояний

Для просмотра состояний МЭ в **ARMA IF** предусмотрен подраздел сводки состояний (**«Межсетевой экран»** - **«Диагностика»** - **«Сводка состояний»**).

Подраздел позволяет просматривать данные, отсортированные по таблицам:

- **«По IP-адресу источника»** – Рисунок 323;

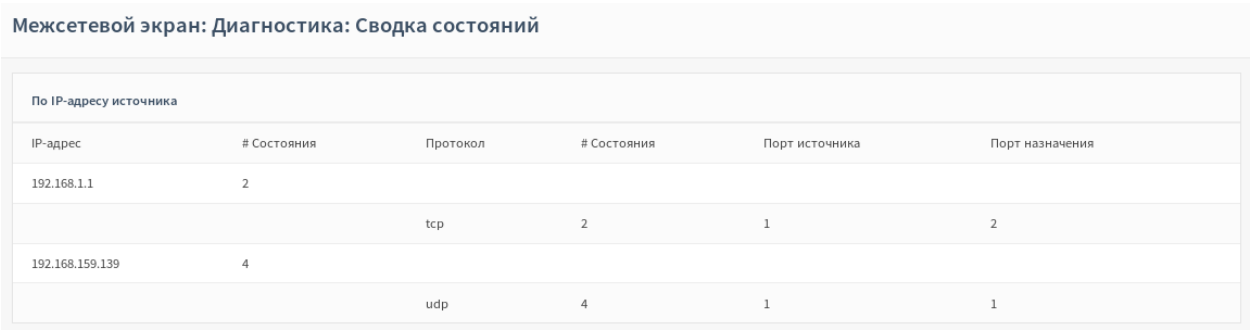

Рисунок 323 – Сводка состояний МЭ «По IP-адресу источника»

- **«По IP-адресу назначения»** – Рисунок 324;

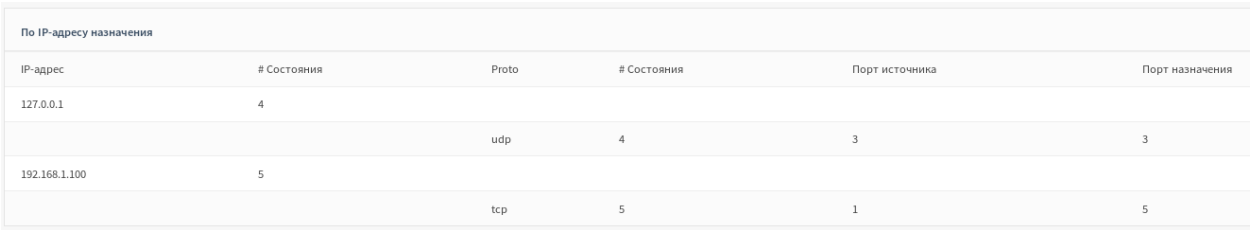

Рисунок 324 – Сводка состояний МЭ «По IP-адресу назначения»

- **«Всего по IP-адресу»** – Рисунок 325;

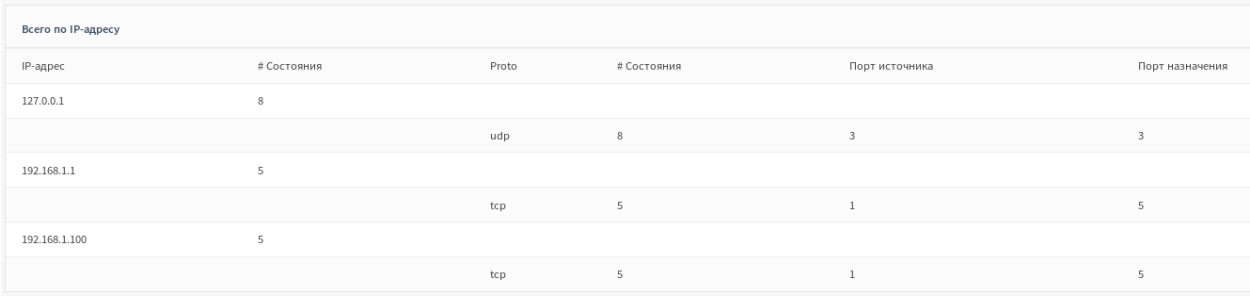

Рисунок 325 – Сводка состояний МЭ «Всего по IP-адресу»

- **«По паре IP-адресов»** – Рисунок 326.

Рисунок 326 – Сводка состояний МЭ «По паре IP-адресов»

27.12 Статистика трафика

Для просмотра текущей загрузки всех сетевых интерфейсов в режиме реального времени в **ARMA IF** предусмотрен подраздел отслеживания трафика (**«Создание отчетов»** - **«Трафик»**) (см. Рисунок 327).

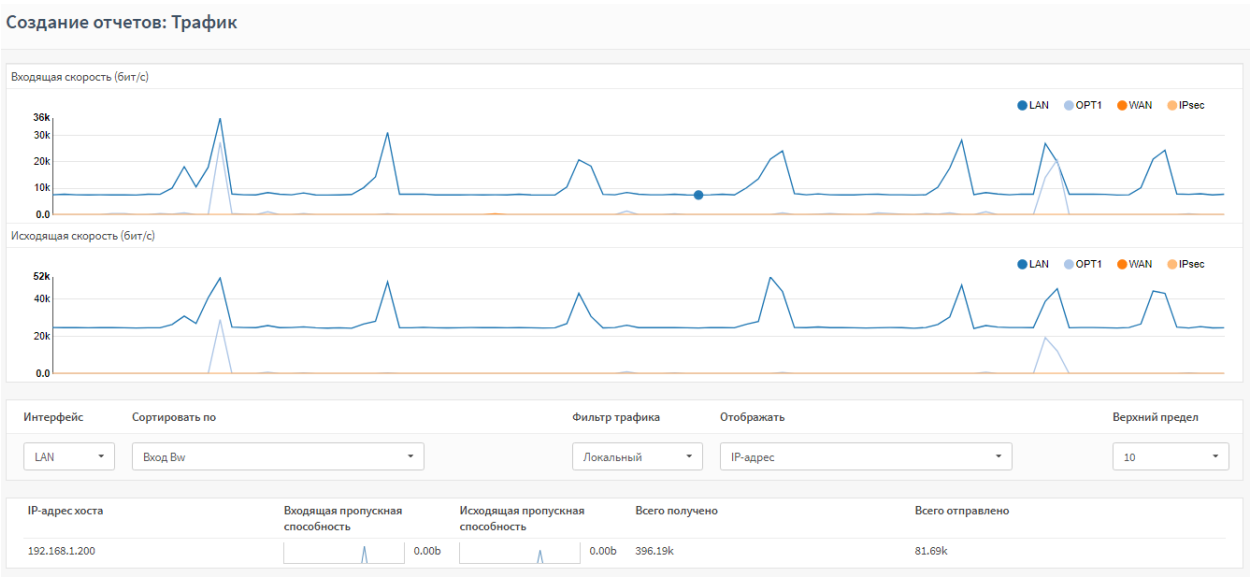

Рисунок 327 – Трафик

27.13 Monit

Сервис Monit является встроенным в систему пакетом. Это утилита мониторинга с возможностью выполнения скриптов в качестве реакции на заданное событие.

Monit используется для следующих действий:

- **отслеживание состояния серверов** – доступность, потребление ресурсов;
- **мониторинг сервисов** – состояние, потребляемые ресурсы, количество дочерних процессов;
- **мониторинг сетевых сервисов** – возможность подключения и корректность ответа;
- **выполнение действий** – встроенных или собственных, созданных с помощью скриптов, при достижении определенных событий;

- **отправка уведомлений** – по электронной почте или в централизованный веб-интерфейс Monit.

28 УПРАВЛЕНИЕ ПИТАНИЕМ

Раздел **«Питание»** позволяет перезагрузить и выключить систему, а также выйти из учетной записи пользователя.

28.1 Перезагрузка

Для перезагрузки системы необходимо перейти в подраздел управления питанием (**«Система»** - **«Питание»** - **«Перезагрузка»**) и нажать **кнопку «Да»** (см. Рисунок 328). После перезагрузки системы откроется окно входа в систему.

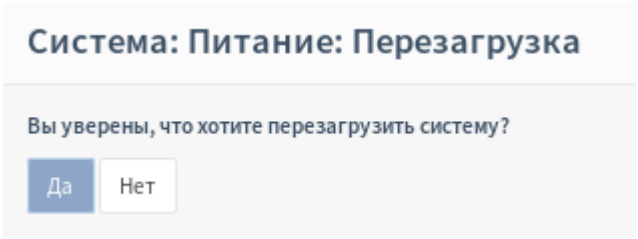

Рисунок 328 – Перезагрузка системы

28.2 Выключение

Для выключения системы необходимо перейти в подраздел управления питанием (**«Система»** - **«Питание»** - **«Выключение»**) и нажать **кнопку «Да»** (см. Рисунок 329). Система завершит свою работу.

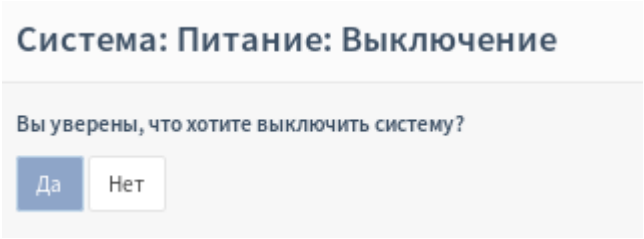

Рисунок 329 – Выключение системы

28.3 Выход

Для выхода из УЗ пользователя необходимо нажать на иконку пользователя в верхней правой части веб-интерфейса и выбрать **«Выйти»** (см. Рисунок 330). Произойдет моментальный выход из системы и откроется окно входа в систему.

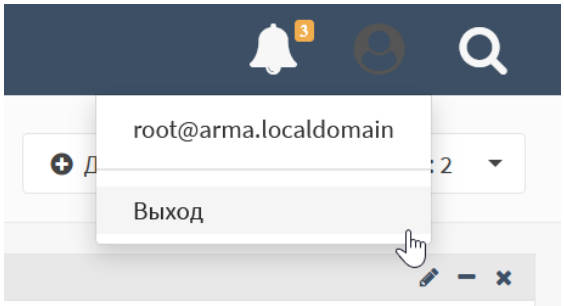

Рисунок 330 – Выход из УЗ

29 ЖУРНАЛИРОВАНИЕ

29.1 Общие настройки журналирования

В подразделе журналирования (**«Система»** - **«Настройки»** - **«Журналирование»**) содержаться настройки, позволяющие управлять журналированием в системе.

Общие параметры журналирования:

- **«Обратный порядок отображения»** – при включении данного параметра последние записи в журнале отображаются сверху списка;
- **«Размер журнала (байт)»** – в поле существует возможность задать размер файлов журнала. По умолчанию размер 500 Кб;
- **«Журнал веб-сервера»** – при включении данного параметра ошибки веб-сервера, в том числе портала авторизации, будут записаны в главный системный журнал;
- **«Локальные записи»** – при включении данного параметра запись журнала на локальный диск производиться не будет;
- **«Сброс записей»** – при нажатии **кнопки «Очистить файлы журналов»** будет произведена очистка всех локальных журналов.

29.1.1 Настройки журналирования событий МЭ

Выбор регистрируемых событий для журналирования межсетевого экрана производится в подразделе журналирования (**«Система»** - **«Настройки»** - **«Журналирование»**).

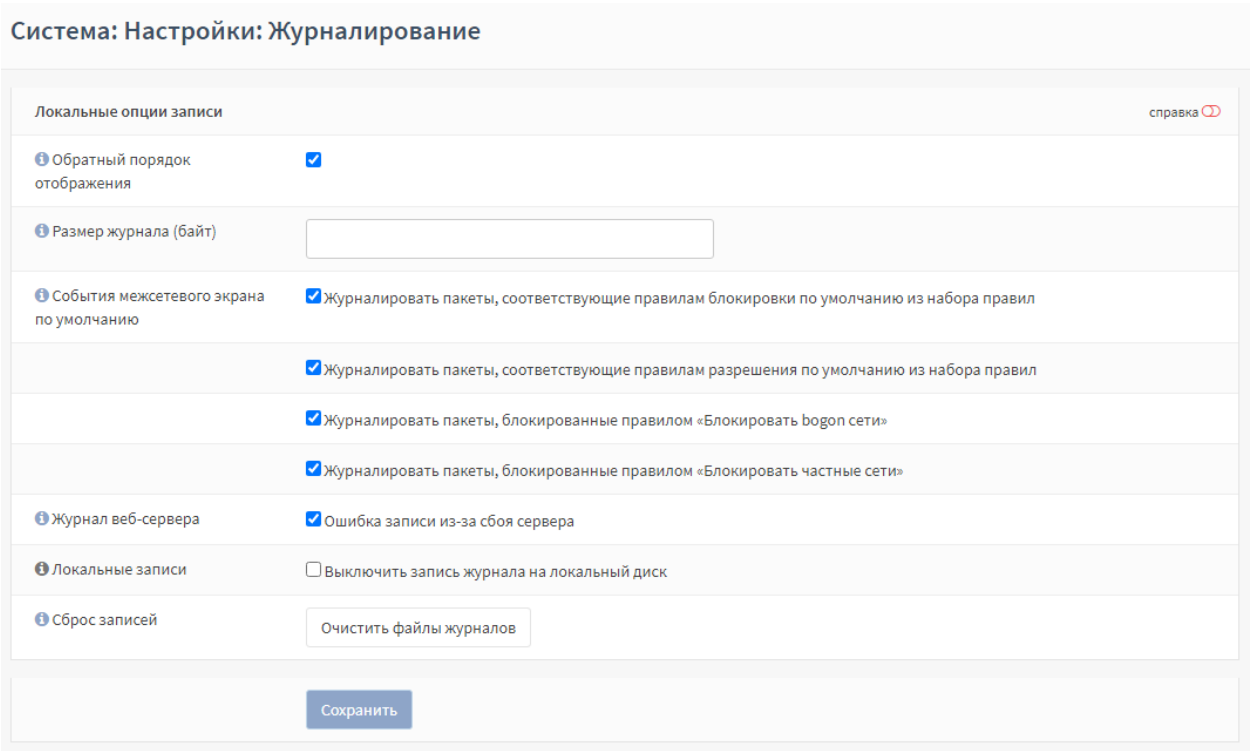

Рисунок 331 – Настройка журналирования

В данном подразделе существует возможность выбрать события, генерируемые **ARMA IF** и подлежащие журналированию.

Выбор событий осуществляется установкой/снятия флажка напротив события, для применения изменения необходимо нажать **кнопку «Сохранить»**. По умолчанию флажки установлены напротив всех событий.

Существует возможность журналировать пакеты, соответствующие правилам МЭ. Для этого необходимо в параметрах создаваемого/созданного правила (см. Раздел 1.1.1) установить флажок напротив параметра **«Журналирование»** (см. Рисунок 332).

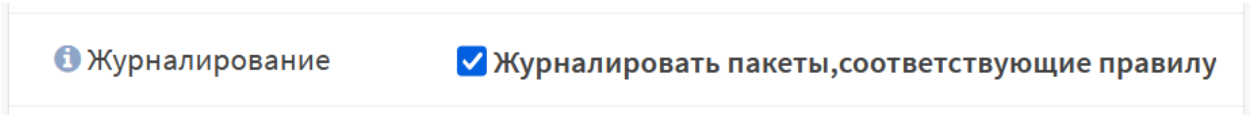

Рисунок 332 – Включение журналирования для правил МЭ

29.1.2 Настройки журналирования действий пользователей

Для включения журналирования действий пользователей необходимо перейти в подраздел администрирования **ARMA IF** (**«Система»** - **«Настройки»** - **«Администрирование»**) и поставить флажок в поле **«Журнал доступа»**. Для сохранения изменений необходимо нажать кнопку **«Сохранить»**.

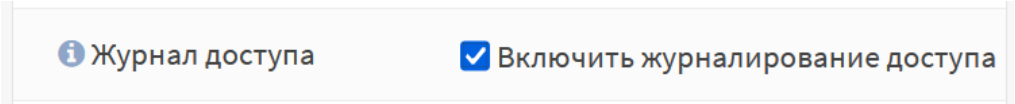

Рисунок 333 – Включение журналирования доступа пользователей

29.2 Журналы МЭ

Журналы МЭ находятся в подразделе журналов МЭ (**«Межсетевой экран»** - **«Журналы»**).

Журналы МЭ в **ARMA IF** делятся на два вида:

- **«В реальном времени»**;
- **«Открытый вид»**.

Дополнительно присутствует подраздел **«Обзор»**, содержащий в себе различные круговые диаграммы.

29.2.1 Журнал «В реальном времени»

Журнал отображает события МЭ в режиме реального времени в виде списка с динамическим изменением (см. Рисунок 334). Блокированные пакеты выделяются красным цветом, разрешённые – зелёным.

Нажатие **кнопки** «  » напротив записи откроет форму с дополнительной информацией о записи.

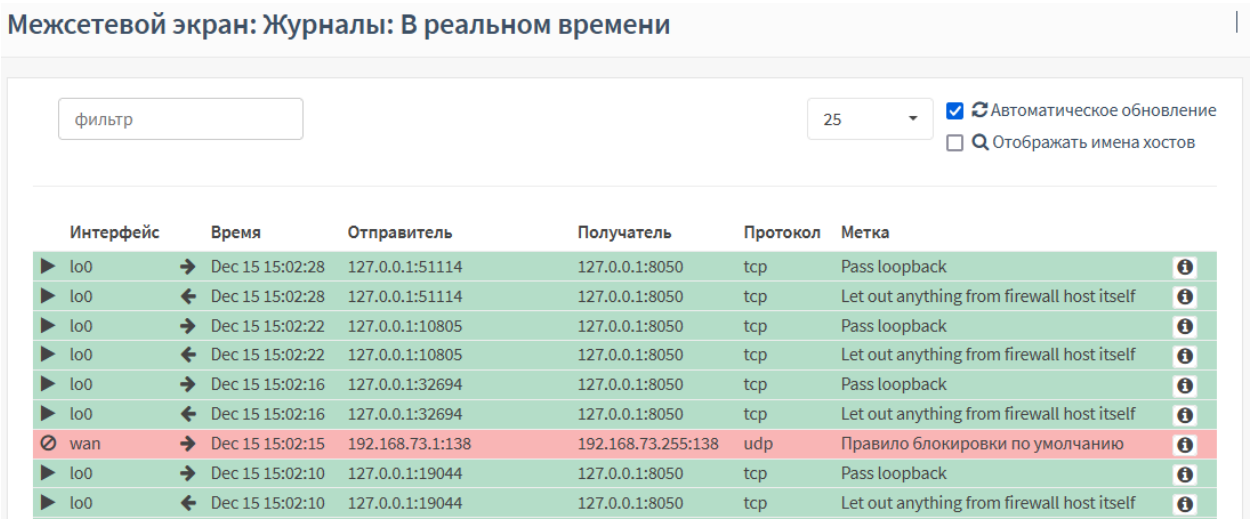

Рисунок 334 – Журнал событий МЭ в реальном времени

29.2.2 Журнал «Открытый вид»

Журнал (см. Рисунок 335) хранит в оригинальном формате, в виде одной текстовой строки, без дополнительной обработки, следующие события МЭ:

- общие правила;
- правила конкретных интерфейсов;
- API правила;
- автоматически генерируемые правила МЭ при включении отдельных опций веб-интерфейса.

При нажатии **кнопки «Очистить журнал»** в нижней части страницы будет предложено удалить весь журнал МЭ.

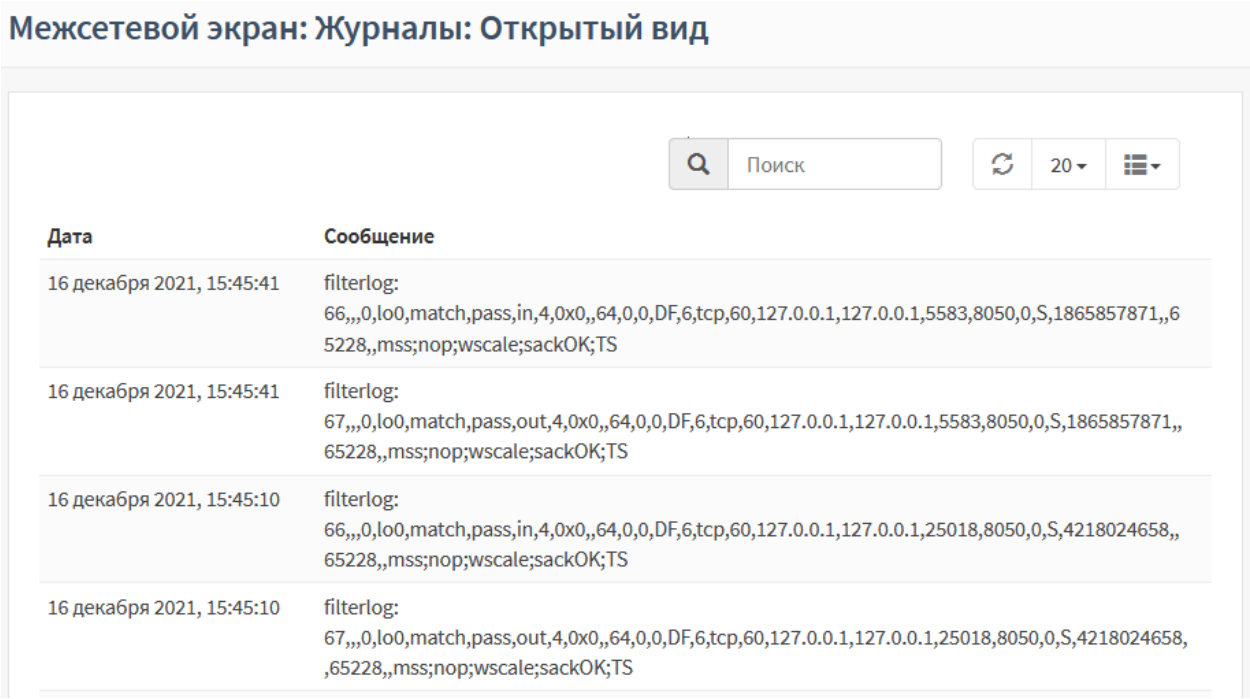

Рисунок 335 – Журнал событий МЭ, открытый вид

29.2.3 Подраздел «Обзор»

Подраздел содержит в себе следующие круговые диаграммы:

- **«Действия»** – отображает процентное соотношение основных действий, которые были применены правилами: «pass» – разрешить / «block»(«drop»/«reject») – блокировать;
- **«Интерфейсы»** – отображает процентное соотношение интерфейсов, на которых срабатывали правила. На данной диаграмме возможно проанализировать, на каком интерфейсе правила срабатывают чаще;
- **«Протоколы»** – отображает процентное соотношение протоколов, при работе которых были сработаны правила МЭ: UDP, TCP, ICMP, и т.д.;
- «**IP-адреса источника»** – отображает процентное соотношение IP-адресов, с которых отправлялись пакеты, отмеченные в сработавшем правиле МЭ;
- **«IP-адреса назначения»** – отображает процентное соотношение IP-адресов, для которых отправлялись пакеты, отмеченные в сработавшем правиле МЭ;
- **«Порты источника»** – отображает процентное соотношение портов источников, с которых отправлялись пакеты, отмеченные в сработавшем правиле МЭ;

- **«Порты назначения»** – отображает процентное соотношение портов назначения, для которых отправлялись пакеты, отмеченные в сработавшем правиле МЭ.

29.3 Журналы СОВ

Настройка журналирования СОВ производится в подразделе администрирования СОВ (**«Обнаружение вторжений»** - **«Администрирование»**), вкладка **«Настройка»**.

Имеется 4 параметра для управления журналированием событий СОВ:

- **«Архивировать журнал»** – задаёт периодичность архивирования журналов предупреждений СОВ. По умолчанию – каждое воскресенье в 23:00;
- **«Сохранить журналы»** – указывает количество файлов журналов СОВ, хранящихся в **ARMA IF**;
- **«Содержимое пакета для журнала»** – добавляет в журнал полезную нагрузку пакета трафика;
- **«Журналировать пакет»** – добавляет в журнал весь пакет трафика.

Последние два параметра доступны при переключении выключателя **«расширенный режим»**.

Для СОВ предусмотрено два журнала:

- **«Журнал работы СОВ»**;
- **«Журнал ошибок работы сигнатур СОВ»**.

29.3.1 Журнал ошибок работы сигнатур СОВ

Журнал (см. Рисунок 336) расположен на вкладке **«Журналирование»** подраздела администрирования СОВ (**«Обнаружение вторжений»** - **«Администрирование»**) и разделен на две части:

- **«Журнал СОВ»** – хранит записи, содержащие ошибки и предупреждения ПО «Suricata» о невозможности запустить или включить какие-либо сигнатуры с указанием причины;
- **«Журнал загрузки правил»** – хранит записи, содержащие ошибки и предупреждения загрузки правил СОВ.

Переключение происходит в выпадающем списке в верхней части формы подраздела. Также в верхней части формы подраздела находятся форма поиска и выпадающий список выбора уровня сообщений.

При нажатии **кнопки «Очистить журнал»** в нижней части формы будет предложено удалить весь журнал МЭ.

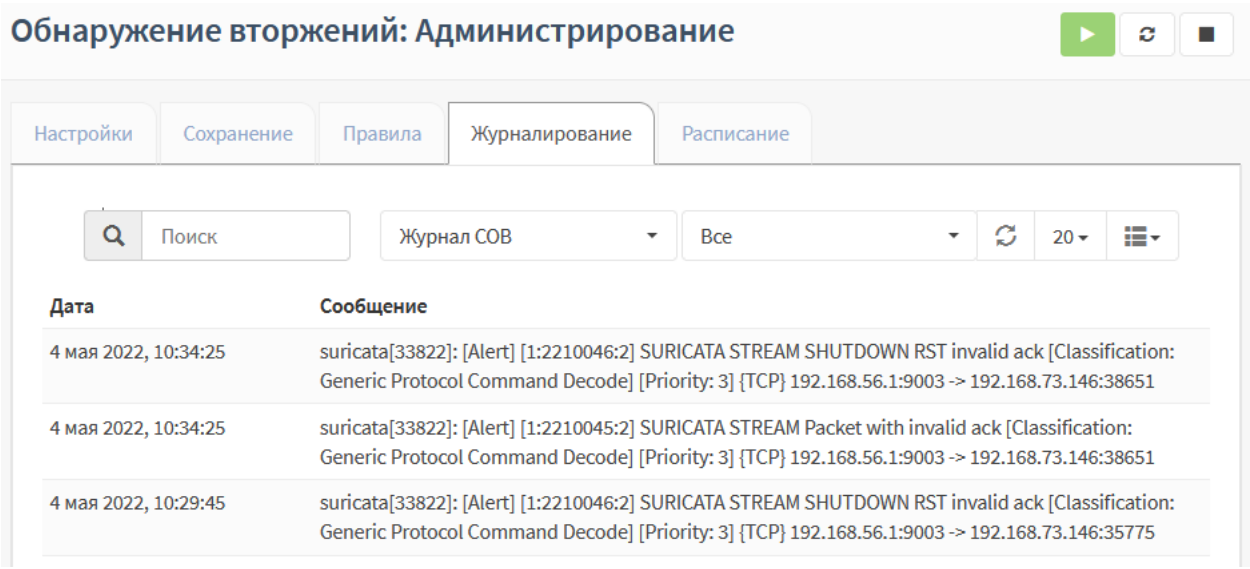

Рисунок 336 – Журнал ошибок работы сигнатур СОВ

29.3.2 Журнал предупреждений СОВ

Журнал (см. Рисунок 337) хранит записи о срабатывании правилах СОВ.

Журнал расположен в подразделе предупреждений СОВ (**«Обнаружение вторжений»** - **«Предупреждения (Alerts)»**).

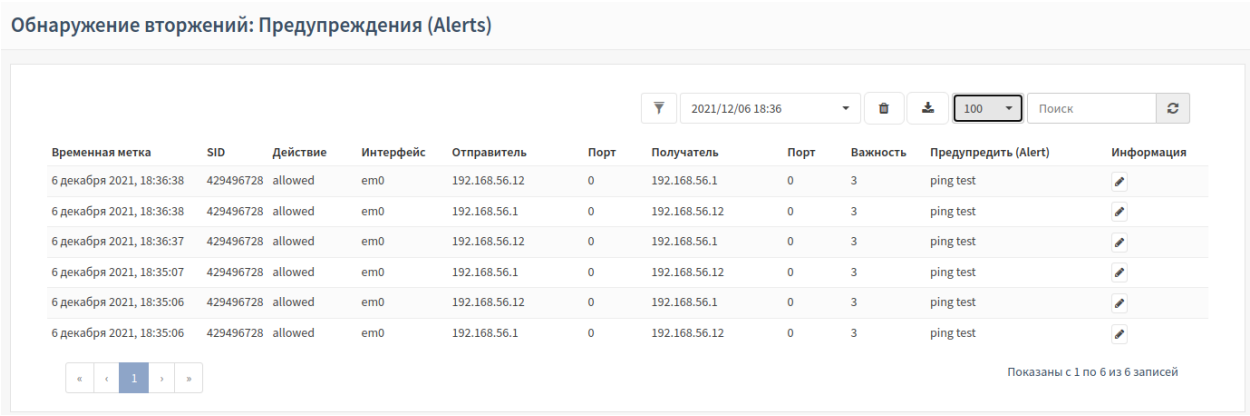

Рисунок 337 – Журнал предупреждений СОВ

29.4 Системные журналы

Системные журналы располагаются в подразделе журналирования (**«Система»** - **«Журналы»**). Всего в подразделе содержится 6 журналов:

- **«Журнал syslog»**;
- **«Backend журнал»**;
- **«Журнал веб-интерфейса»**;
- **«Журнал событий безопасности»**;
- **«Журнал системных событий»**;
- **«Журнал действий пользователя»**.

В большинстве системных журналов доступна возможность сохранения записей в текстовый файл с помощью кнопок:

- «  » – сохраняет записи журнала, представленные в данный момент в форме;
- «  » – сохраняет все записи журнала.

29.4.1 Журнал syslog

Журнал (см. Рисунок 338) хранит записи, содержащие события следующих типов:

- успешность входа в систему;
- изменение внутреннего представления времени;
- изменение пароля пользователя;
- изменение настроек системы;
- добавление, изменение, удаление и получение информации об элементах системы – пользователях, правил МЭ, правил и групп правил СОВ;
- уведомления об отказе модулей;
- успешность доступа пользователей к различным страницам системы;
- сообщения от syslog-парсеров;
- сообщения, связанные с активацией или проверкой лицензии.

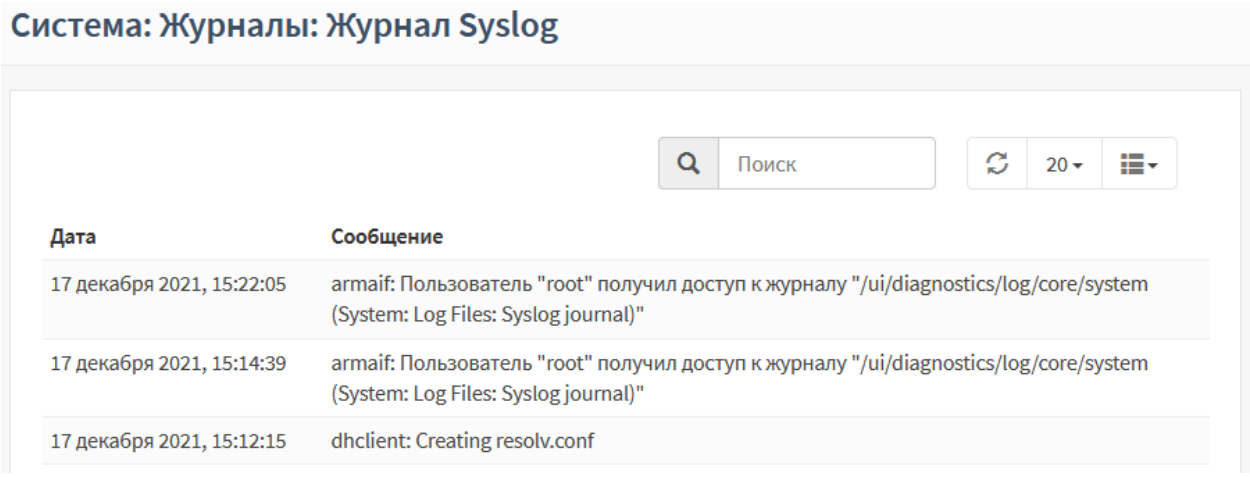

Рисунок 338 – Журнал Syslog

В вни

29.4.2 Backend журнал

Журнал (см. Рисунок 339) хранит записи, содержащие события следующих типов:

- сгенерированные за счет использования API сервера – перезагрузка, остановка, запуск сервисов;

- изменение конфигурации – генерирование конфигураций сервисов при сохранении форм.

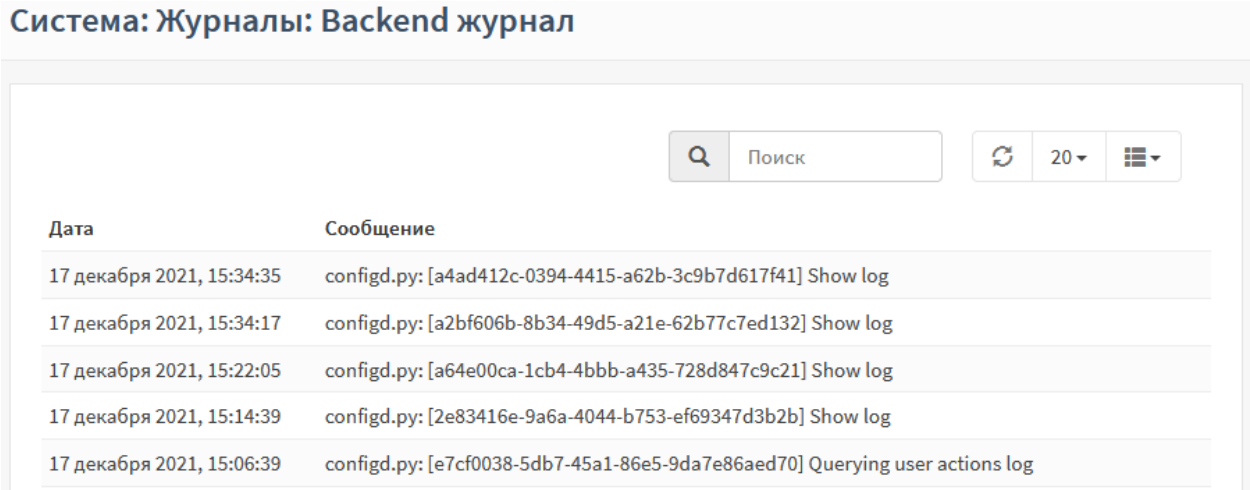

Рисунок 339 – Backend журнал

29.4.3 Журнал веб-интерфейса

Журнал (см. Рисунок 340) хранит записи, содержащие события веб-сервера lighthttpd.

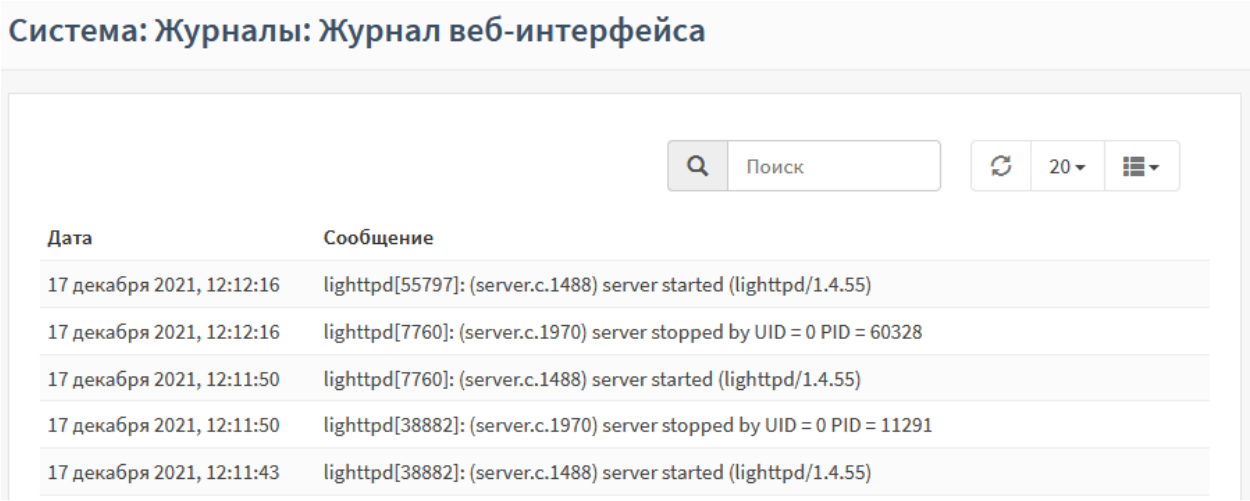

Рисунок 340 – Журнал веб-интерфейса

29.4.4 Журнал событий безопасности

Журнал (см. Рисунок 341) хранит записи, содержащие события следующих типов:

- Для СОВ – срабатывание сигнатур;
- Для МЭ – срабатывания правил межсетевого экрана;
- Для arpwatch:
    - подключение несанкционированного устройства;
    - обнаружение конфликта IP-адресов;
    - обнаружение изменения IP, MAC адреса;

- обнаружение подмены IP-адресов;

- Для портала авторизации – запуск/остановка/перезагрузка портала авторизации и лог-файлы с записями о событиях в хронологическом порядке.

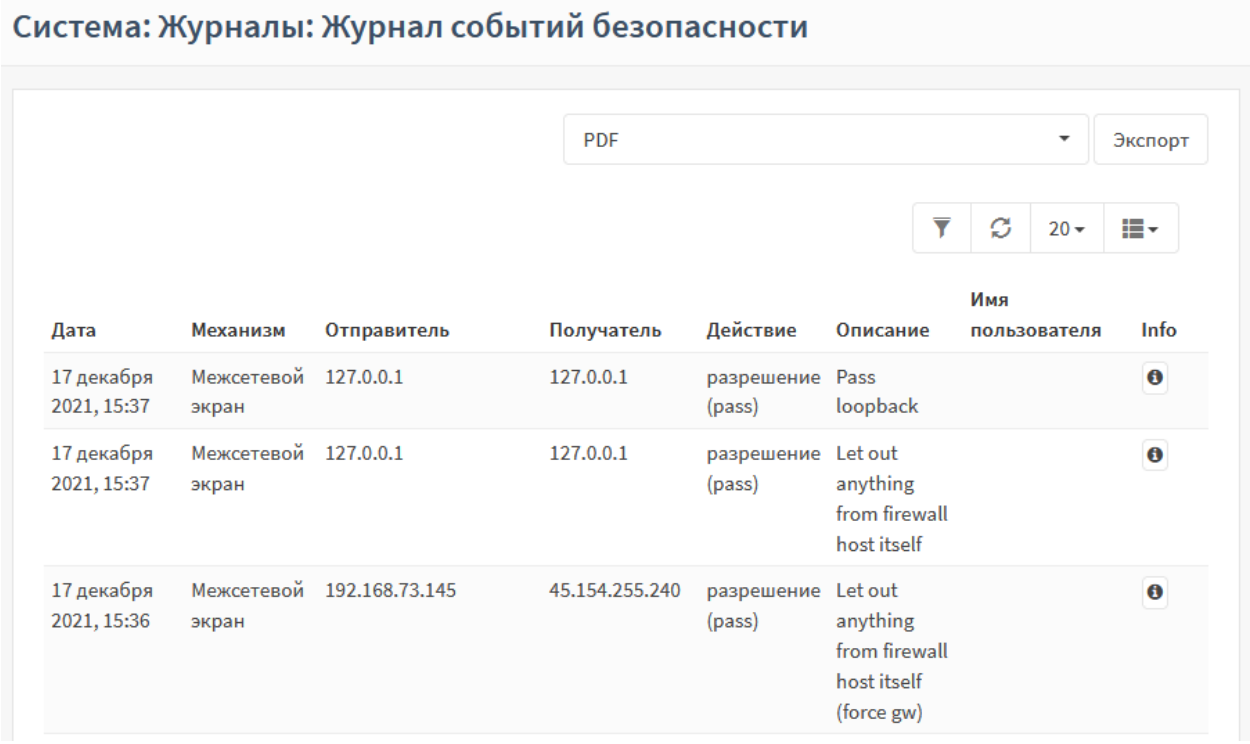

Рисунок 341 – Журнал событий безопасности

Нажатие **кнопки «**  **»** напротив записи откроет форму с дополнительной информацией о записи.

Для экспорта журнала необходимо в верхней части страницы выбрать формат файла и нажать **кнопку «Экспорт»**.

29.4.5 Журнал системных событий

Журнал (см. Рисунок 342) хранит записи, содержащие события следующих типов:

- NTP-сервер:
  - запуск, остановка или перезагрузка сервера;
  - успешная синхронизация времени;
  - отсутствие подключение к NTP-серверу;
- Сбой портала авторизации – неуспешная попытка входа в портал авторизации;
- СОВ:
  - запуск, остановка или перезагрузка СОВ;
  - сбой СОВ;

- События, связанные с состоянием интерфейса CARP;
- События контроля целостности;
- Запуск веб-сервера;
- Неуспешный доступ к странице веб-интерфейса;
- Сообщения при загрузке системы.

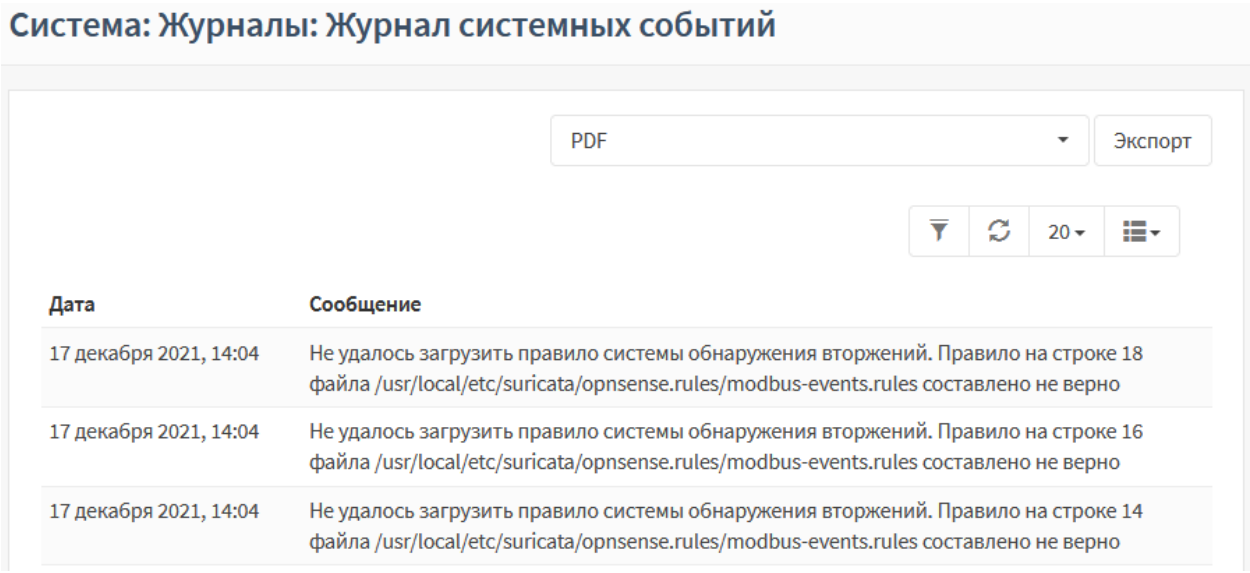

Рисунок 342 – Журнал системных событий

Для экспорта журнала необходимо в верхней части страницы выбрать формат файла и нажать **кнопку «Экспорт»**.

29.4.6 Журнал действий пользователя

Журнал (см. Рисунок 343) хранит записи, содержащие события следующих типов:

- включение/отключение МЭ;
- включение/отключение СОВ;
- добавление/изменение/удаление правил МЭ;
- изменение настроек МЭ;
- изменение правил СОВ;
- изменение настроек СОВ;
- успешная/неуспешная авторизация в граф. интерфейс и интерфейс консоли;
- изменение размера записей в webgui журнале;
- сообщения при работе с пользователями и группами пользователей;
- сообщения, связанные с изменением настроек мониторинга состояния системы на странице анализа трафика, настроек monit;

- перезагрузка системы;
- информация о нештатном завершении системы.

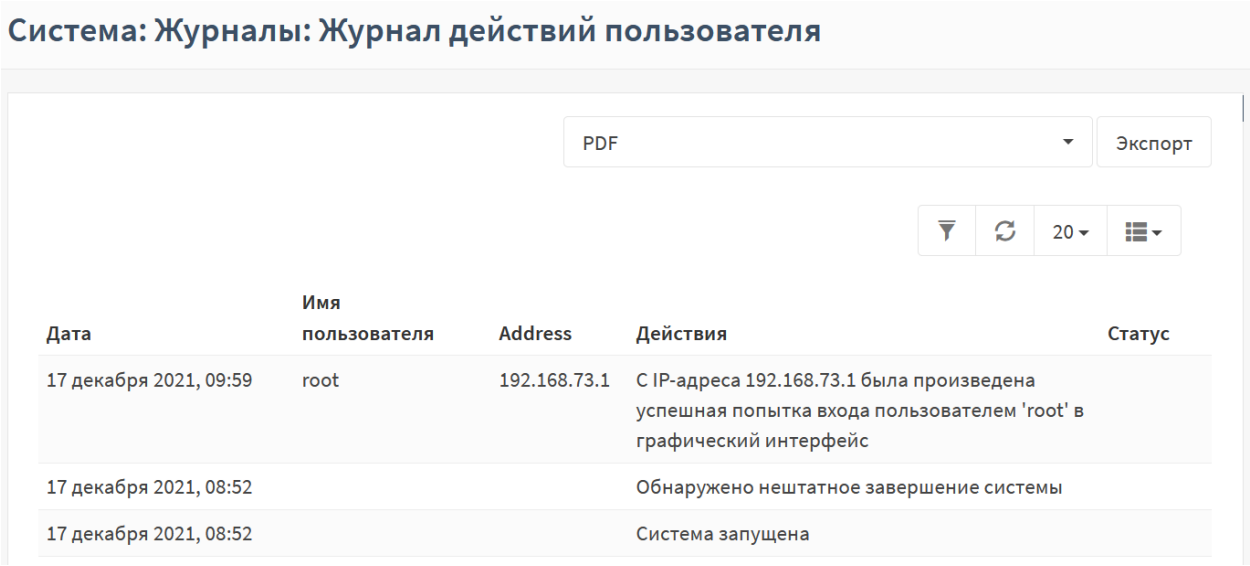

Рисунок 343 – Журнал действий пользователя

Для экспорта журнала необходимо в верхней части страницы выбрать формат файла и нажать **кнопку «Экспорт»**.

29.5 Журналы маршрутизации

Журналы маршрутизации делятся на два типа:

- **«Журнал статической маршрутизации»**;
- **«Журнал динамической маршрутизации»**.

29.5.1 Журнал статической маршрутизации

Журнал (см. Рисунок 344) хранит записи, содержащие сообщения от протоколов маршрутизации ZEBRA, OSPF/OSPF6, RIP, а также от других сервисов, работающих со статическими маршрутами сети, например, radvd и rtsold.

Журнал расположен в подразделе журналирования маршрутизации (**«Система»** - **«Маршруты»** - **«Журнал»**).

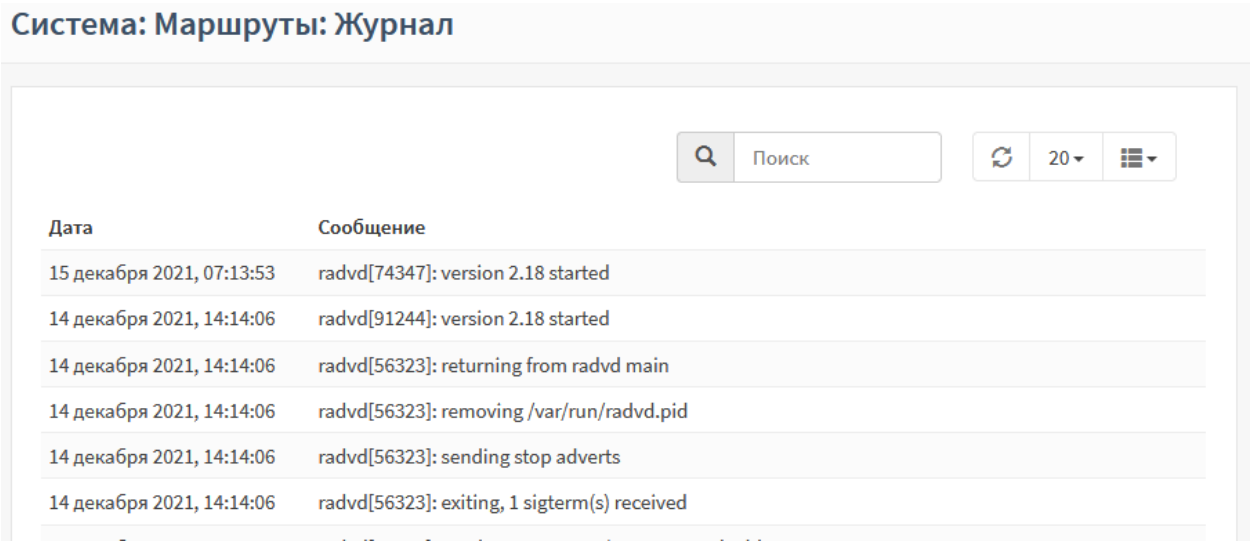

Рисунок 344 – Журнал статической маршрутизации

29.5.2 Журнал динамической маршрутизации

Основой работы данного журнала является ПО Quagga. По умолчанию ведение данного журнала выключено.

Журнал (см. Рисунок 345) хранит записи, содержащие сообщения от протоколов маршрутизации ZEBRA, OSPF/OSPF6, RIP, задействованных в процессе динамической маршрутизации, следующих типов:

- hello-сообщения от ZEBRA и другие сообщения протокола ZEBRA;
- сообщения от OSPF/OSPF6;
- сообщения от протокола RIP;
- ошибки конфигурации протоколов динамической маршрутизации;
- запуск, остановка или перезагрузка сервиса quagga (frr).

Журнал расположен в подразделе журналирования маршрутизации (**«Маршрутизация»** - **«Диагностика»** - **«Журналирование»**).

Для включения наполнения журнала необходимо перейти в подраздел общих настроек маршрутизации (**«Маршрутизация»** - **«Общие настройки»**), установить флажки для параметров **«Включить»** и **«Создание файла журнала»** и нажать **кнопку «Сохранить».**

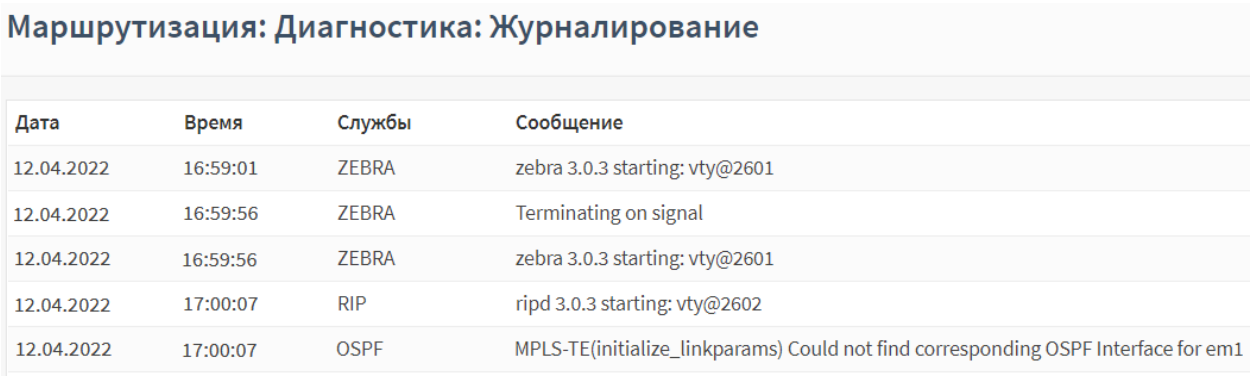

Рисунок 345 – Журнал динамической маршрутизации

29.6 Журнал портала авторизации

Журнал (см. Рисунок 346) хранит записи, содержащие информацию о работе сервиса Captive Portal, отвечающего за работу портала авторизации. В журнале представлены следующие типы событий:

- сообщение об отсутствии у пользователя доступа к определенному URL;
- запуск, остановка или перезагрузка сервиса;
- ошибки сервиса.

Журнал расположен в подразделе журналирования портала авторизации (**«Службы»** - **«Портал авторизации»** - **«Журнал»**).

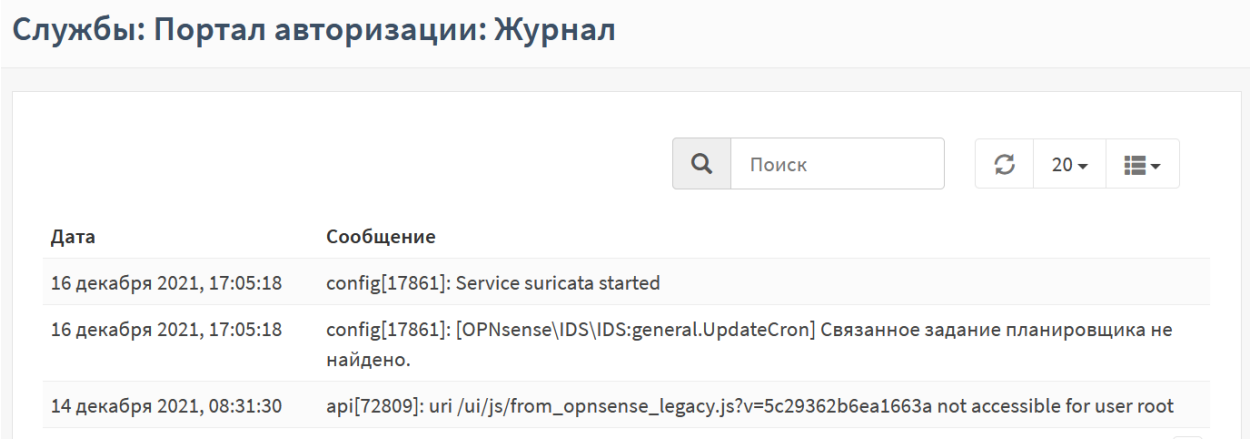

Рисунок 346 – Журнал портала авторизации

29.7 Журнал DHCPv4

Журнал (см. Рисунок 347) хранит записи, содержащие события о работе DHCP-сервера на сетевых интерфейсах следующих типов:

- включение DHCP-сервера на интерфейсе;
- назначение IP-адреса устройству в сети.

Журнал расположен в подразделе журналирования DHCP (**«Службы»** - **«DHCPv4»** - **«Журнал»**).

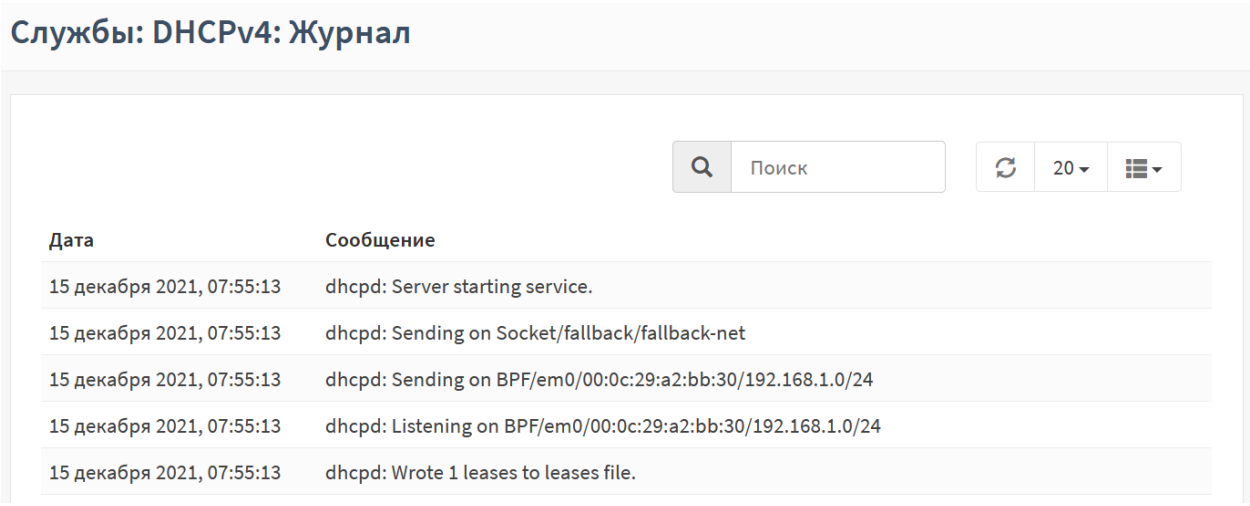

Рисунок 347 – Журнал DHCPv4

29.8 Журнал NTP

Журнал (см. Рисунок 348) хранит записи, содержащие события о работе сервиса NTP следующих типов:

- запуск, остановка или перезагрузка сервиса;
- ошибки сервиса;
- успешность синхронизации времени.

Журнал расположен в подразделе журналирования сетевого времени (**«Службы»** - **«Сетевое время»** - **«Журнал»**).

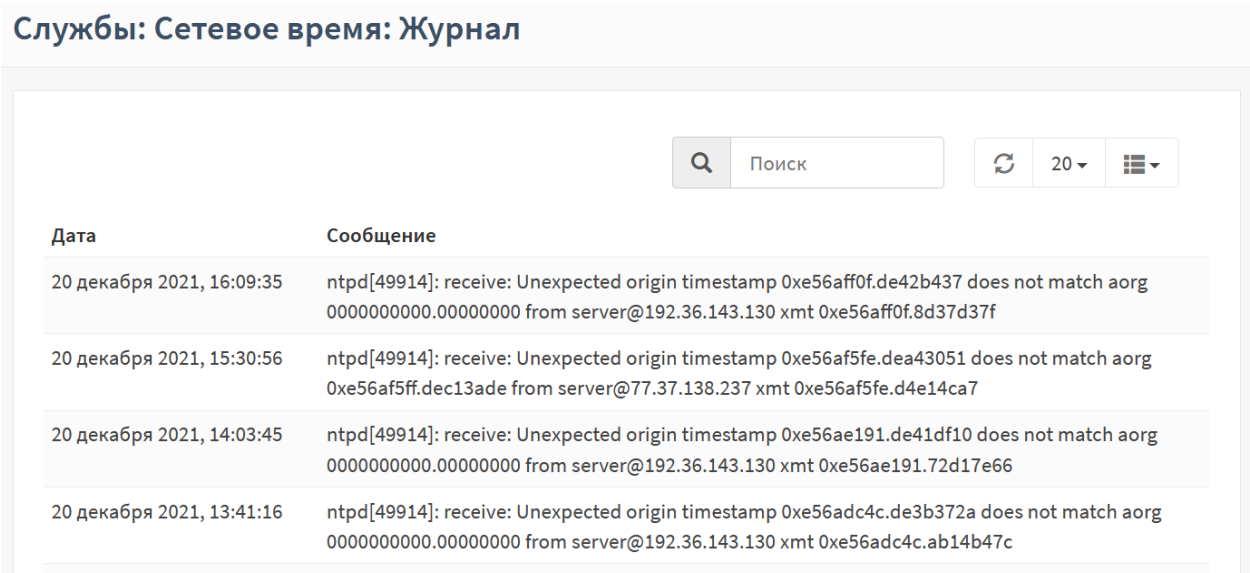

Рисунок 348 – Журнал сетевого времени

29.9 Журнал веб-прокси

Журналы веб-прокси делятся на три типа:

- **«Журнал кэша»**;

- **«Журнал доступа»**;
- **«Журнал хранения»**.

29.9.1 Журнал кэша

Журнал (см. Рисунок 349) хранит записи, содержащие сообщения отладки и ошибок, генерируемые ПО «Squid».

Журнал расположен в подразделе журналирования прокси-сервера (**«Службы»** - **«Веб-прокси»** - **«Журнал кэша»**).

Рисунок 349 – Журнал кэша

29.9.2 Журнал доступа

Журнал (см. Рисунок 350) хранит записи, содержащие сведения о подключениях к веб-прокси.

Журнал расположен в подразделе журналирования прокси-сервера (**«Службы»** - **«Веб-прокси»** - **«Журнал доступа»**).

Рисунок 350 – Журнал доступа

29.9.3 Журнал хранения

Журнал (см. Рисунок 351) хранит записи, содержащие информацию об объектах кэша, как хранящихся в данный момент на диске, так и удалённых.

Журнал расположен в подразделе журналирования прокси (**«Службы»** - **«Веб-прокси»** - **«Журнал хранения»**).

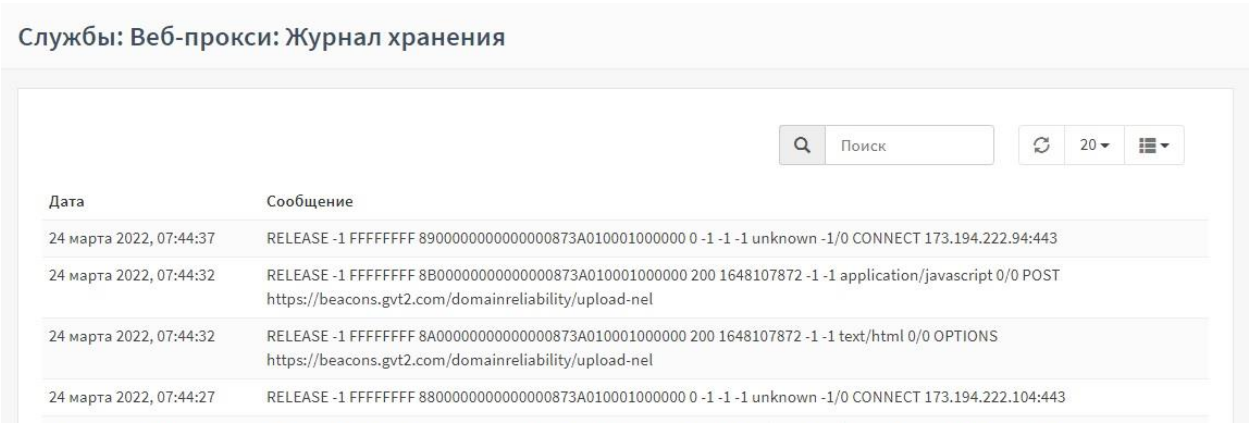

Рисунок 351 – Журнал хранения

29.10 Журнал антивируса

Журнал (см. Рисунок 352) хранит записи, содержащие события работы сервиса антивирусного ПО Clamd следующих типов:

- сообщения о включении плагинов, входящих в состав ПО Clamd;
- сообщения о проверке статуса БД ПО Clamd;
- сообщения об обнаружении вируса;
- сообщения об ошибках работы ПО Clamd.

Журнал расположен в подразделе журналирования антивируса (**«Службы»** - **«Антивирус»** - **«Журнал Clamd»**).

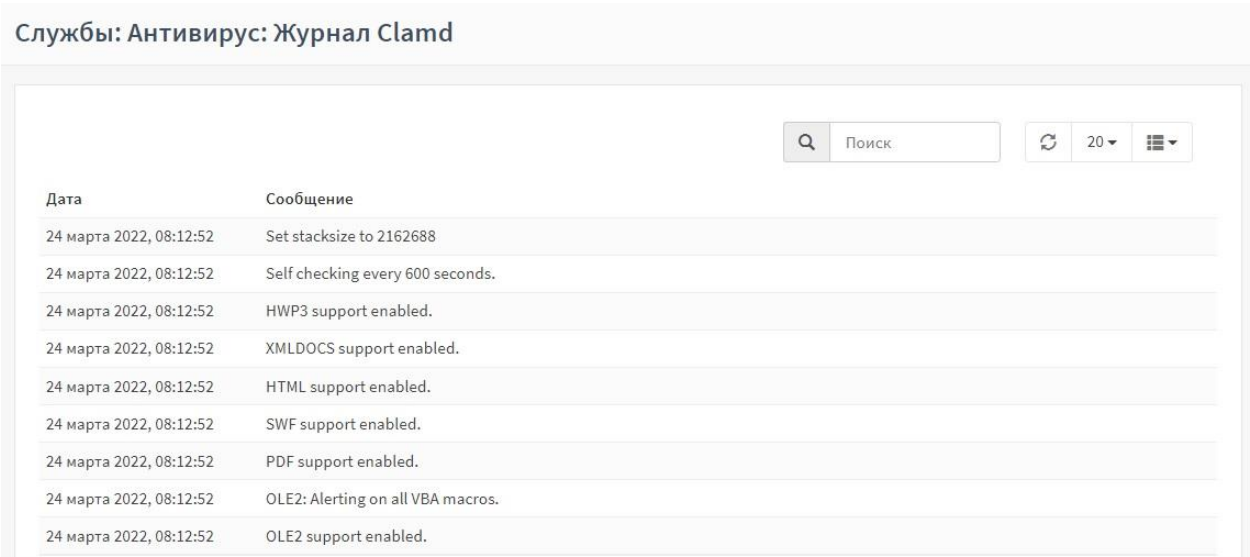

Рисунок 352 – Журнал антивируса

29.11 Журнал Dnsmasq

Журнал (см. Рисунок 353) хранит записи, содержащие события работы сервиса dnsmasq следующих типов:

- запуск, остановка и перезагрузка сервиса;

- успешное чтение адресов из каталогов:
  - «/etc/hosts»;
  - «var/etc/dnsmasq-hosts»;
- успешное чтение конфигурации из каталога «/etc/resolv.conf»;
- используемые пространства имен.

Журнал расположен в подразделе журналирования dnsmasq (**«Службы»** - **«Dnsmasq DNS»** - **«Журнал»**).

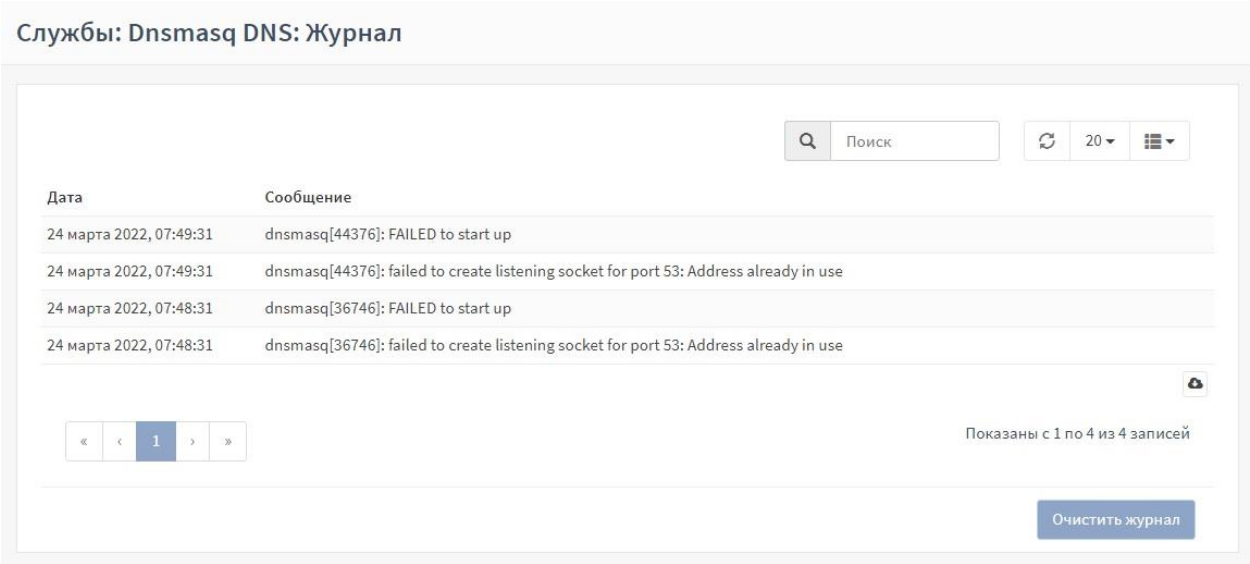

Рисунок 353 – Журнал Dnsmasq DNS

29.12 Журнал C-ICAP

Журнал (см. Рисунок 354) хранит записи, содержащие события работы сервера C-ICAP, позволяющим работать с протоколом ICAP.

Типы событий, содержащихся в журнале:

- ошибки сервера;
- запуск, остановка или перезагрузка сервера;
- обнаружение вируса.

Журнал расположен в подразделе журналирования ICAP (**«Службы»** - **«C-ICAP»** - **«Журнал»**).

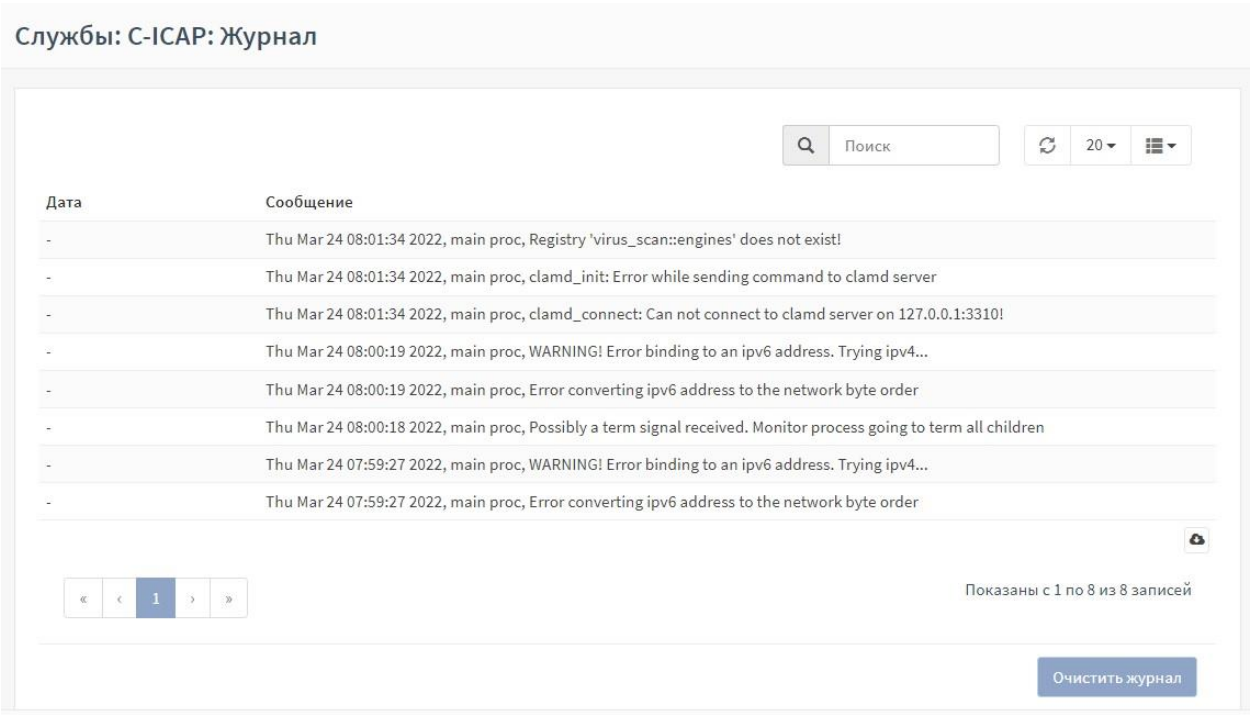

Рисунок 354 – Журнал C-ICAP

29.13 Журнал кэширующего DNS

Журнал (см. Рисунок 355) хранит записи, содержащие события работы DNS-сервера следующих типов:

- запуск, остановка и перезагрузка сервера;
- общие сведения о кэшировании и рекурсии на сервере.

Журнал расположен в подразделе журналирования DNS (**«Службы»** - **«Кэширующий DNS-сервер»** - **«Журнал»**).

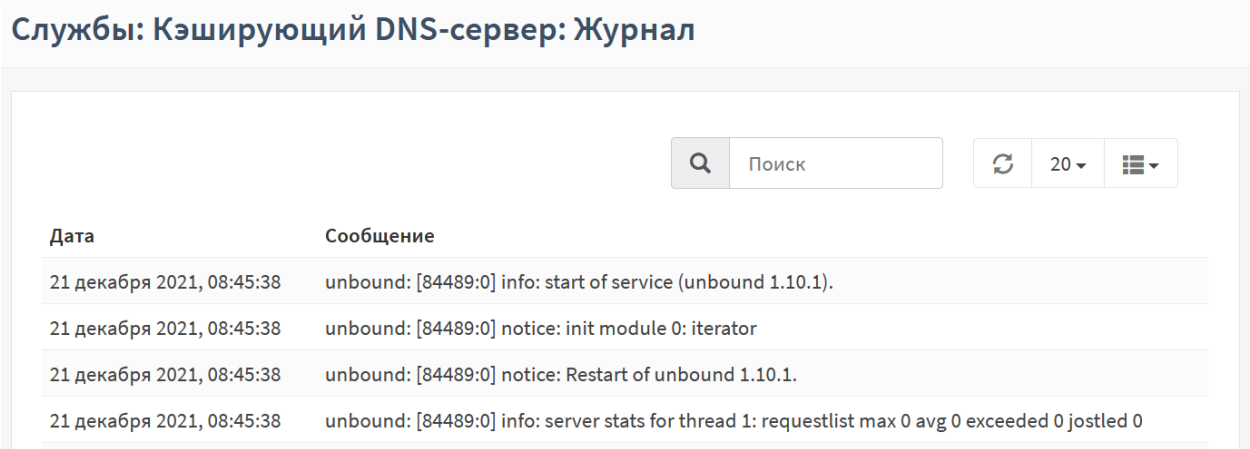

Рисунок 355 – Журнал кэширующего DNS

29.14 Журнал IPsec

Журнал (см. Рисунок 357) хранит записи, содержащие события работы протокола IPsec VPN следующих типов:

- подключение нового клиента к туннелю:
    - IP-адрес;
    - Логин;
- отключение клиента;
- успешность аутентификации;
- включение, выключение и перезагрузка IPsec-туннеля;
- ошибки и предупреждения IPsec-туннеля.

Журнал расположен в подразделе журналирования IPsec (**«VPN»** - **«IPсec»** - **«Журнал»**).

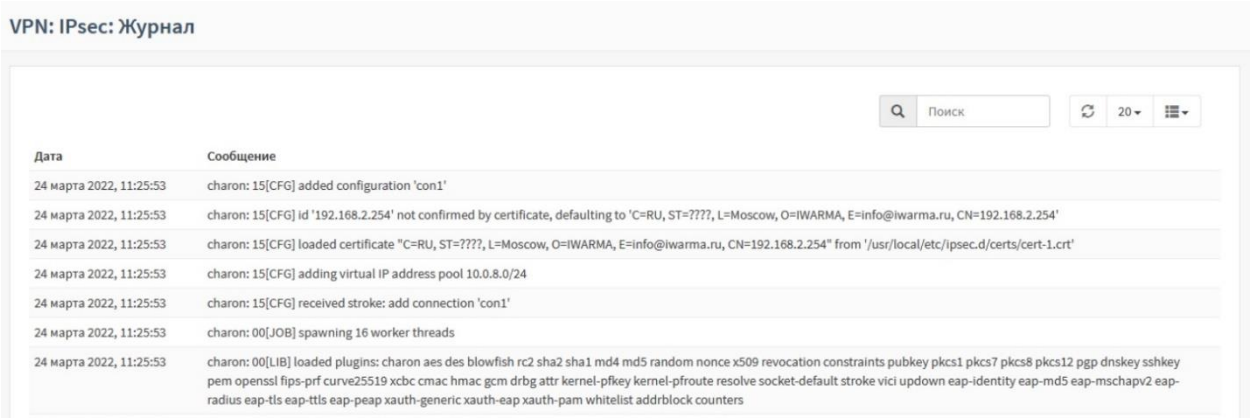

Рисунок 356 – Журнал IPsec

29.15 Журнал OpenVPN

Журнал (см. Рисунок 357) хранит записи, содержащие события работы сервиса OpenVPN следующих типов:

- подключение нового клиента;
- назначение IP-адреса;
- успешность аутентификации;
- тип аутентификации:
    - логин/пароль;
    - общий ключ;
- включение, выключение и перезагрузка сервера;
- ошибки и предупреждения сервера.

Предусмотрено разделение событий по настроенным серверам OpenVPN с помощью выпадающего списка **«Тип фильтра»** в верхней части страницы.

Журнал расположен в подразделе журналирования OpenVPN (**«VPN»** - **«OpenVPN»** - **«Журнал»**).

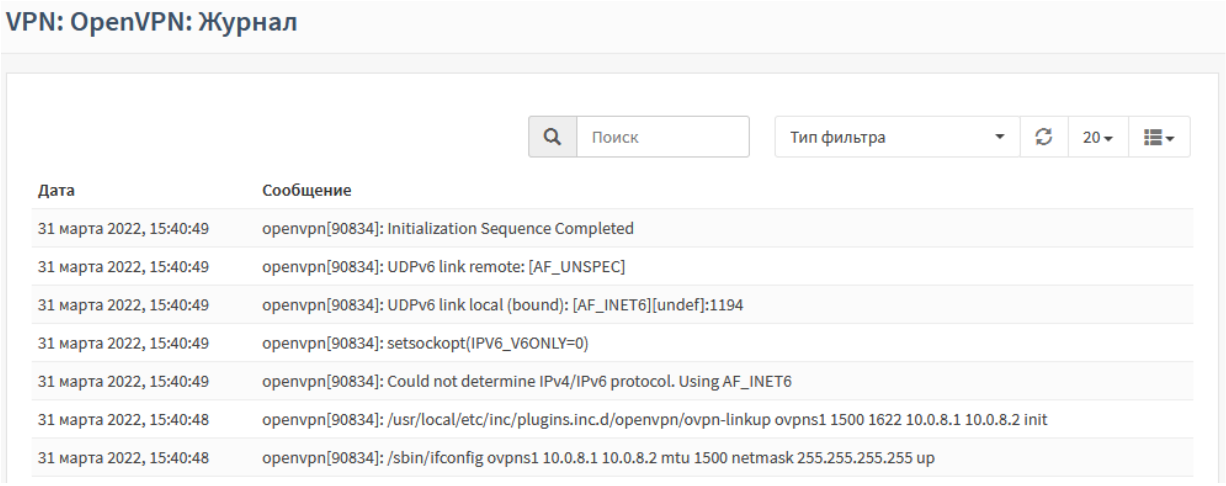

Рисунок 357 – Журнал OpenVPN