УТВЕРЖДЕН
НПЕШ.465614.005РП-ЛУ

МЕЖСЕТЕВОЙ ЭКРАН И СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ «РУБИКОН»

Руководство пользователя

НПЕШ.465614.005РП

Листов 256

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

2022

АННОТАЦИЯ

В документе содержатся сведения о назначении, области применения, функциональных возможностях изделия «Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005 (далее – «Рубикон», изделие), представлены методы работы с пользовательским интерфейсом, настройки функций безопасности.

Оформление программного документа «Руководство пользователя» произведено по требованиям ЕСПД:

1) ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов;

2) ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов;

3) ГОСТ 19.104-78 ЕСПД. Основные надписи;

4) ГОСТ 19.105-78 ЕСПД. Общие требования к программным документам;

5) ГОСТ 19.106-78 ЕСПД. Общие требования к программным документам, выполненным печатным способом.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение и область применения

Изделие представляет собой программно-аппаратный комплекс, реализующий функции межсетевого экрана типа «А» второго класса защиты и системы обнаружения вторжений уровня сети второго класса защиты, используемые в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, и иной информации ограниченного доступа и обеспечивающие защиту от преднамеренного несанкционированного доступа или специальных воздействий на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена.

1.2. Функциональные возможности

«Рубикон» реализует следующие основные функциональные возможности:

1) возможность осуществлять фильтрацию сетевого трафика для отправителей информации, получателей информации и всех операций передачи, контролируемой «Рубикон» информации к узлам информационной системы и от них;

2) возможность осуществлять фильтрацию для всех операций перемещения через межсетевой экран информации к узлам информационной системы и от них;

3) возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности субъектов: сетевой адрес узла отправителя; сетевой адрес узла получателя; и информации: сетевой протокол, который используется для взаимодействия; интерфейс межсетевого экрана (на уровне сетевого адреса), через который проходит пакет; интерфейс межсетевого экрана (на физическом уровне);

4) возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности информации: сетевой протокол, который используется для взаимодействия; атрибуты, указывающие на фрагментацию пакетов; транспортный протокол, который используется для взаимодействия, порты источника и получателя в рамках сеанса (сессии); разрешенные/запрещенные команды, разрешенный/запрещенный мобильный код; параметры команд; последовательности используемых команд; разрешенные/запрещенные протоколы прикладного уровня;

5) возможность явно разрешать информационный поток, базируясь на устанавливаемом администратором «Рубикон» наборе правил фильтрации, основанном на идентифицированных атрибутах;

6) возможность запрещать информационный поток, базируясь на устанавливаемом администратором «Рубикон» наборе правил фильтрации, основанном на идентифицированных атрибутах;

7) возможность блокирования всех информационных потоков, проходящих через нефункционирующий или функционирующий некорректно «Рубикон»;

8) возможность осуществлять политику фильтрации пакетов с учетом управляющих команд от взаимодействующих с «Рубикон» средств защиты информации других видов;

9) возможность осуществлять проверку каждого пакета по таблице состояний для определения того, не противоречит ли состояние (статус, тип) пакета ожидаемому состоянию;

10) возможность осуществлять проверку использования пользователями отдельных команд, для которых администратором «Рубикон» установлены разрешительные или запретительные атрибуты безопасности;

11) возможность осуществлять проверку использования пользователями отдельных команд (последовательностей отдельных команд), для которых администратором «Рубикон» установлены разрешительные или запретительные атрибуты безопасности;

12) возможность осуществлять проверку использования сетевых ресурсов, содержащих мобильный код, для которого администратором «Рубикон» установлены разрешительные или запретительные атрибуты безопасности;

13) возможность осуществлять проверку использования пользователями прикладного программного обеспечения (приложений), для которых администратором «Рубикон» установлены разрешительные или запретительные атрибуты безопасности;

14) возможность разрешать информационный поток, основываясь на результатах проверок;

15) возможность запрещать информационный поток, основываясь на результатах проверок;

16) возможность осуществлять фильтрацию пакетов с учетом управляющих команд от взаимодействующих с «Рубикон» средств защиты информации других видов, основанную на атрибутах, указывающих на признаки нарушения безопасности в информации сетевого трафика;

17) возможность разрешать информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на отсутствие нарушений безопасности информации;

18) возможность запрещать информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на наличие нарушений безопасности информации;

19) возможность осуществлять фильтрацию при импорте (перехвате) информации сетевого трафика из-за пределов «Рубикон»;

20) возможность осуществлять передачу информационных потоков с переназначением сетевых адресов отправителя и (или) получателя (трансляция адресов и посредничество в передаче), фильтрацию при экспорте (передаче от своего имени) информации сетевого трафика за пределы межсетевого экрана;

21) возможность экспортировать (передавать от своего имени) информацию сетевого трафика при положительных результатах фильтрации и других проверок;

22) возможность осуществлять посредничество в передаче информации сетевого трафика, основанное на типе сетевого трафика;

23) возможность маскирования наличия «Рубикон» способами, затрудняющими нарушителям его выявление;

24) возможность осуществлять проверку параметров отдельных команд, для которых администратором «Рубикон» установлены допустимые или недопустимые значения параметров;

25) возможность осуществлять проверку последовательностей используемых отдельных команд, для которых администратором «Рубикон» установлены признаки допустимых и (или) недопустимых последовательностей;

26) возможность регистрации и учета выполнения проверок информации сетевого трафика;

27) возможность читать информацию из записей аудита уполномоченным администраторам;

28) возможность выбора совокупности событий, подвергающихся аудиту, из совокупности событий, в отношении которых возможно осуществление аудита;

29) возможность оповещения уполномоченных лиц о критичных видах событий безопасности, в том числе – сигнализация о попытках нарушения правил «Рубикон»;

30) возможность выборочного просмотра данных аудита (поиск, сортировка, упорядочение данных аудита);

31) возможность регистрации возникновения событий, которые в соответствии с национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» включены в детализированный уровень аудита;

32) возможность идентификации администратора «Рубикон» до разрешения любого действия (по администрированию), выполняемого при посредничестве «Рубикон» от имени этого администратора;

33) возможность аутентификации администратора «Рубикон» до разрешения любого действия (по администрированию), выполняемого при посредничестве «Рубикон» от имени этого администратора;

34) возможность осуществления идентификации субъектов межсетевого взаимодействия до передачи «Рубикон» информационного потока получателю;

35) возможность осуществления аутентификации субъектов межсетевого взаимодействия до передачи «Рубикон» информационного потока получателю;

36) поддержку определенных ролей по управлению «Рубикон»;

37) возможность со стороны администраторов управлять режимом выполнения функций безопасности «Рубикон»;

38) возможность со стороны администраторов управлять данными «Рубикон», используемыми функциями безопасности «Рубикон»;

39) возможность со стороны администраторов управлять атрибутами безопасности;

40) возможность поддержки списка типов сетевого трафика для осуществления посредничества в передаче, предусматривающего разделение трафика по типам;

41) ассоциацию типов сетевого трафика из списка с конкретным сетевым трафиком для осуществления посредничества в передаче и обработки соответствующих типов сетевого трафика прокси-агентами;

42) возможность изменения области значений информации состояния соединения со стороны администраторов «Рубикон»;

43) возможность присвоения информации состояния соединения допустимых значений, таких как установление соединения, использование соединения, завершение соединения и других;

44) возможность ведения для каждого соединения таблицы состояний, основанной на информации состояния соединения;

45) предоставление возможности администраторам «Рубикон» модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности для используемых пользователями отдельных команд для осуществления «Рубикон» фильтрации;

46) предоставление возможности администраторам «Рубикон» модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности использования сетевых ресурсов, содержащих отдельные типы мобильного кода, для осуществления «Рубикон» фильтрации;

47) предоставление возможности администраторам «Рубикон» модифицировать, удалять атрибуты безопасности, определяющие допустимые и (или) недопустимые значения параметров используемых отдельных команд, для осуществления «Рубикон» фильтрации;

48) предоставление возможности администраторам «Рубикон» модифицировать, удалять атрибуты безопасности, определяющие признаки допустимых и (или) недопустимых последовательностей используемых отдельных команд, для осуществления «Рубикон» фильтрации;

49) возможность перехода в режим аварийной поддержки, который предоставляет возможность возврата «Рубикон» к штатному функционированию;

50) возможность генерации надежных меток времени при проведении аудита безопасности;

51) возможность тестирования (самотестирования) функций безопасности «Рубикон» (контроль целостности исполняемого кода «Рубикон»);

52) возможность сохранения штатного функционирования «Рубикон» при некритичных типах сбоев;

53) возможность согласованно интерпретировать управляющие команды, атрибуты сетевого трафика и иные данные, получаемые от взаимодействующих с «Рубикон» средств защиты информации других видов;

54) поддержку правил интерпретации данных, получаемых от взаимодействующих с «Рубикон» средств защиты информации других видов;

55) возможность завершения работы или восстановления (для предусмотренных сценариев сбоев) штатного функционирования «Рубикон»;

56) возможность тестирования средств защиты информации других видов, взаимодействующих с «Рубикон», и управляющие команды которых использует «Рубикон» для управления потоками информации;

57) возможность при определенных типах сбоев/прерываний обслуживания автоматического возврата «Рубикон» к штатному функционированию;

58) возможность кластеризации «Рубикон»;

59) возможность приоритизации контроля и фильтрации разных информационных потоков, а также выделения ресурсов, доступных для разных информационных потоков, обрабатываемых одновременно (в течение определенного периода времени);

60) возможность сбора информации о сетевом трафике;

61) возможность выполнения анализа собранных данных «Рубикон» о сетевом трафике в режиме, близком к реальному масштабу времени, и по результатам анализа фиксировать информацию о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для проведения вторжения;

62) возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием сигнатурного и эвристических методов;

63) возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика на заданном уровне эвристического анализа;

64) возможность обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня базовой эталонной модели взаимосвязи открытых систем;

65) возможность фиксации факта обнаружения вторжений или нарушений безопасности в журналах аудита;

66) возможность задания правил фильтрации данных «Рубикон» с возможностью сохранения отфильтрованной информации в отдельных файлах;

67) возможность блокирования вторжений и нарушений безопасности, в том числе путем выдачи управляющих сигналов «Рубикон»;

68) уведомление администратора «Рубикон» об обнаруженных вторжениях по отношению к контролируемым узлам информационной системе (далее – ИС) и нарушениях безопасности с помощью отображения соответствующего сообщения на консоли управления, отсылки сообщений электронной почты;

69) возможность автоматизированного обновления базы решающих правил (далее – БРП);

70) возможность верификации целостности БРП системы обнаружения вторжений (далее – СОВ);

71) возможность маскирования наличия датчика «Рубикон» в составе контролируемой ИС, противодействие выявлению его на сетевом уровне стандартными средствами операционной системы (далее – ОС);

72) возможность со стороны уполномоченных администраторов (ролей) управлять режимом выполнения функций безопасности «Рубикон»;

73) возможность со стороны уполномоченных администраторов (ролей) управлять данными «Рубикон» (установление и контроль ограничений и значений; внесения новых правил контроля в БРП СОВ);

74) поддержку определенных ролей для «Рубикон» и их ассоциацию с конкретными администраторами и пользователями ИС;

75) возможность локального и удалённого администрирования «Рубикон»;

76) наличие графического интерфейса администрирования «Рубикон»;

77) возможность генерации записей аудита для событий, потенциально подвергаемых аудиту;

78) возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;

79) возможность читать информацию из записей аудита;

80) ограничение доступа к чтению записей аудита;

81) поиск, сортировку, упорядочение данных аудита.

1.3. Уровень подготовки пользователя

Пользователь изделия должен обладать уровнем знаний и навыков в области информационной безопасности не ниже CISSP (Certified Information Security Systems Professional – сертифицированный специалист по информационной безопасности), опытом реализации политик безопасности информационных систем, пройти авторизованное обучение в АО «НПО «Эшелон» по использованию продуктов «Рубикон».

1.4. Перечень эксплуатационной документации, необходимой к ознакомлению

Перечень эксплуатационных документов, с которыми необходимо ознакомиться перед началом работы с изделием:

1) данный документ «Межсетевой экран и система обнаружения вторжений «Рубикон». Руководство пользователя» НПЕШ.465614.005РП;

2) «Межсетевой экран и система обнаружения вторжений «Рубикон». Руководство администратора» НПЕШ.465614.005РА;

3) «Межсетевой экран и система обнаружения вторжений «Рубикон». Руководство по эксплуатации» (в соответствии с вариантом исполнения эксплуатируемого изделия «Рубикон»);

4) «Межсетевой экран и система обнаружения вторжений «Рубикон». Формуляр» (в соответствии с вариантом исполнения эксплуатируемого изделия «Рубикон»).

2. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Назначение изделия

Программно-аппаратный комплекс «Межсетевой экран и система обнаружения вторжений «Рубикон» предназначен для защиты информации ограниченного доступа в локальных вычислительных сетях от внешних программно-аппаратных воздействий путем фильтрации потоков информации между защищаемой сетью и внешней незащищенной сетью, а также для обнаружения и блокирования атак на ресурсы защищаемой сети.

2.2. Реализуемые функции безопасности

Программно-аппаратный комплекс «Межсетевой экран и система обнаружения вторжений «Рубикон» реализует следующие функции безопасности:

1) контроль и фильтрация;
2) идентификация и аутентификация;
3) разграничение доступа к управлению изделием;
4) регистрация событий безопасности (аудит);
5) обеспечение бесперебойного функционирования и восстановление;
6) тестирование и контроль целостности;
7) преобразование сетевых адресов;
8) маскирование;
9) приоритизация информационных потоков;
10) управление (администрирование);
11) взаимодействие с другими средствами защиты информации;
12) управление параметрами системы обнаружения вторжений;
13) управление установкой обновлений (актуализации) БРП СОВ;
14) анализ данных системы обнаружения вторжений;
15) сбор данных о событиях и активности в контролируемой информационной системе;

16) реагирование системы обнаружения вторжений.

2.3. Режимы работы

Изделие предусматривает следующие режимы работы:

1) рабочий режим – предусматривает штатное выполнение функций безопасности;

2) сервисный режим – предусматривает штатное обновление программного обеспечения (далее – ПО);

3) аварийный режим – предусматривает прекращение или неопределенность выполнения функций безопасности.

2.4. Принципы безопасной работы средства

Безопасная работа изделия обеспечивается реализацией следующих основных принципов:

1) регламентированием запрета доступа непривилегированных пользователей из внешней сети в защищаемые сети по всем типам протоколов, за исключением специально созданной для такого доступа демилитаризованной сети;

2) обеспечением физической сохранности технических средств (межсетевого экрана, средства вычислительной техники, на котором он функционирует и терминалов, с которых выполняется его управление) и исключение возможности доступа к ним посторонних лиц;

3) обеспечением установки, конфигурирования и управления «Рубикон» в соответствии с эксплуатационной документацией.

Представленные принципы реализуются посредством принятия организационных и технических мер, предусмотренных политикой безопасности защищаемой информационной системы.

3. ПОДГОТОВКА К РАБОТЕ

3.1. Первый запуск изделия

Первый запуск изделия производится в следующем порядке:

1) последовательно выполнить действия, указанные в подразделе «Подготовка изделия к использованию» руководства по эксплуатации на изделие;

2) последовательно выполнить действия, указанные в подразделе «Подключение изделия» руководства по эксплуатации на изделие;

3) последовательно выполнить действия, указанные в подразделе «Включение изделия» руководства по эксплуатации на изделие;

Примечание. Для авторизации, как администратор, необходимо ввести логин и пароль. По умолчанию логин – **admin**. Пароль – **radmin**. В случае выполнения трех неуспешных попыток ввода логина и пароля – доступ к «Рубикон» будет заблокирован. Спустя 5 минут можно повторить попытку входа.

4) при первом подключении к административному интерфейсу, для обеспечения безопасности, пароль по умолчанию необходимо изменить в подразделе «Пользователи» раздела «Система» в главном меню веб-интерфейса изделия;

5) после выполнения указанных выше шагов пользователь с полномочиями администратора безопасности будет перенаправлен в раздел «Система», подраздел «Начало» (стартовая страница).

3.2. Настройка функций безопасности

Настройка функций безопасности изделия осуществляется в соответствии с политикой информационной безопасности, защищаемой ИС.

3.3. Установка изделия

По завершению настройки функций безопасности изделие должно быть установлено и подключено согласно монтажным схемам и схемам подключений защищаемой ИС.

3.4. Проверка целостности установленного ПО

Перед началом эксплуатации необходимо выполнить проверку контрольных сумм установленного ПО «Рубикон-А».

В изделии предусмотрена возможность верификации целостности исполняемых файлов и файлов конфигурации администратором после успешного прохождения им процедуры авторизации.

Контроль целостности исполняемых файлов и файлов конфигурации проводится автоматически с периодичностью 1 час и дополнительно по запросу пользователя (администратора) (см. п. 4.3.8 настоящего руководства).

3.5. Проверка работоспособности

Проверка работоспособности считается выполненной при успешном завершении процедур первого запуска и корректных результатах проверки контрольных сумм компонентов ПО «Рубикон-А», установленных на аппаратной платформе «Рубикон».

4. ОПИСАНИЕ ИНТЕРФЕЙСА

4.1. Описание видов и функциональных возможностей интерфейса меню

4.1.1. Навигационное меню

Навигационное меню изделия отображается в веб-браузере, располагается вверху экрана и служит для быстрого переключения между разделами и вспомогательными окнами.

Навигационное меню изделия содержит элементы, представленные в таблице 1.

Таблица 1 – Описание элементов навигационного меню

Элемент	Описание
	Кнопка «Открыть развернутое меню разделов»
	Кнопка «Перейти в подраздел «Начало» (стартовая страница)»
	Кнопка «Закрыть развернутое меню разделов»
	Кнопка «Открыть всплывающее окно уведомлений»
	Кнопка «Перейти в полноэкранный режим»

4.1.2. Сокращенное функциональное меню

Сокращенное меню (см. рис. 1) отображается при наведении курсора на кнопку «  » и представляет собой колонку символов разделов основного меню.

Сокращенное функциональное меню изделия

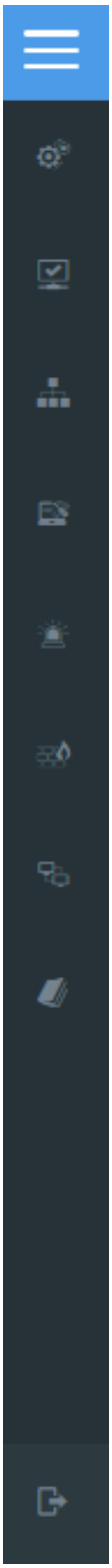

Рис. 1

Сокращенное меню содержит элементы, указанные в таблице 2.

Таблица 2 – Описание элементов сокращенного меню

Элемент	Описание
	Кнопка выбора раздела «Система»
	Кнопка выбора раздела «Состояние»
	Кнопка выбора раздела «Сеть»
	Кнопка выбора раздела «Службы»
	Кнопка выбора раздела «Система Обнаружения Вторжений»
	Кнопка выбора раздела «Межсетевой экран»
	Кнопка выбора раздела «VPN»
	Кнопка выбора раздела «Журналы»
	Кнопка «Закрепить развернутое меню на экране»
	Кнопка «Снять закрепление развернутого меню на экране»
	Кнопка выхода из текущей учетной записи

При нажатии на сокращенное меню откроется развернутое меню.

4.1.3. Развернутое функциональное меню

Развернутое меню (см. рис. 2) содержит символы отображения, названия разделов и подразделов.

Развернутое функциональное меню

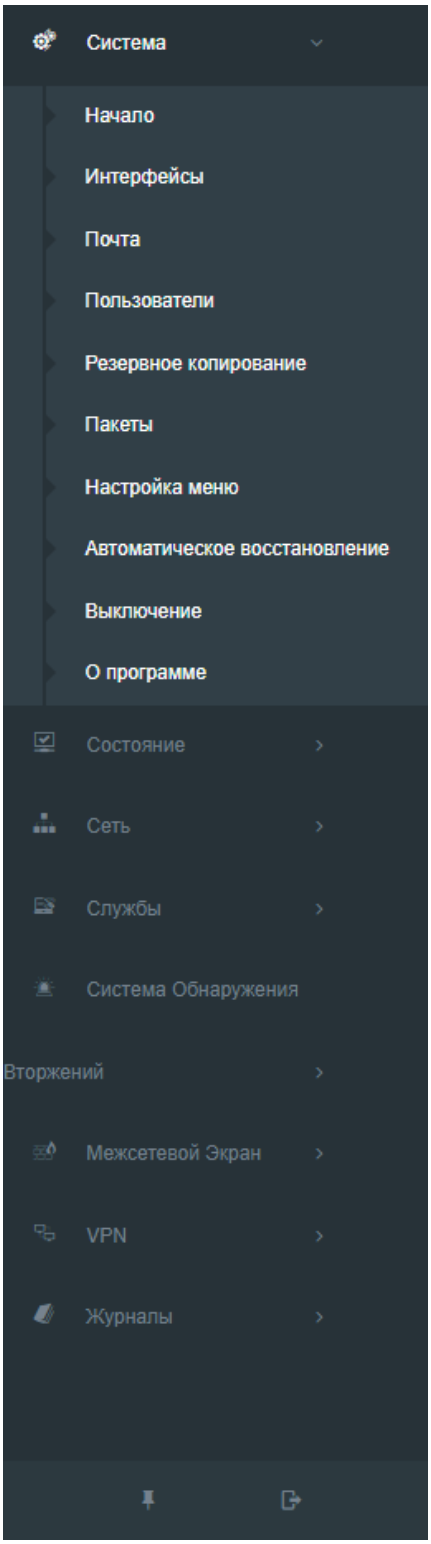

Рис. 2

Настройка отображения пунктов навигационного меню производится с помощью подраздела «Настройка меню» (см. п. 4.2.7 настоящего руководства).

Развернутое меню содержит элементы, указанные в таблице 3.

Таблица 3 – Описание элементов развернутого меню

Элемент	Описание
	Кнопка «Развернуть список подразделов меню»
	Кнопка «Свернуть список подразделов меню»

4.1.4. Всплывающее окно «Уведомления»

Всплывающее окно «Уведомления» отображает перечень полученных уведомлений.

При нажатии на кнопку «Открыть всплывающее окно уведомлений» будет отображен перечень полученных пользователем уведомлений в форме всплывающего окна (см. рис. 3).

Всплывающее окно уведомлений изделия

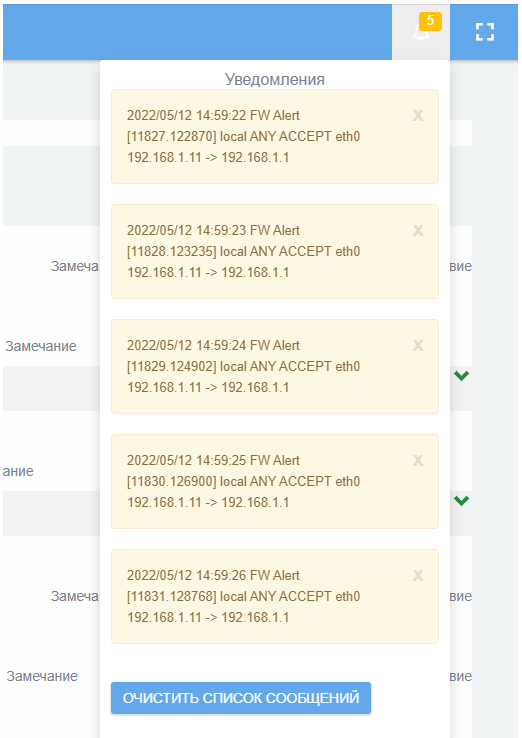

Рис. 3

Для очистки перечня полученных пользователем уведомлений необходимо нажать кнопку «Очистить список сообщений».

4.2. Раздел «Система»

Раздел «Система» содержит следующие подразделы:

1) «Начало»;

2) «Интерфейсы»;

3) «Почта»;

4) «Пользователи»;

5) «Резервное копирование»;

6) «Пакеты»;

7) «Настройка меню»;

8) «Автоматическое восстановление»;

9) «Выключение»;

10) «О программе».

4.2.1. Подраздел «Начало»

Подраздел «Начало» является стартовой страницей и представлен в виде информационного окна (см. рис. 4).

Подраздел «Начало» (стартовая страница)

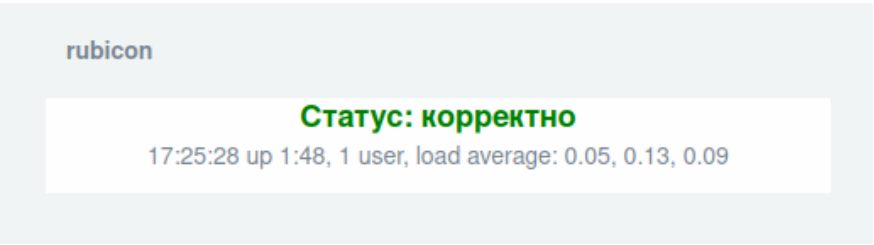

Рис. 4

Подраздел «Начало» отображает следующую информацию:

1) текущее календарное время;

2) длительность непрерывной работы сервера;

3) количество пользователей на сервере;

4) «load average» – средние значения нагрузки;

5) объем трафика на «красных» интерфейсах (при наличии активных чекбоксов «Подсчёт трафика включен» и «Отображать подсчитанный трафик на стартовой странице» (см. рис. 5) в разделе «Состояние» → перейти в подраздел «Подсчет трафика» → по нажатию кнопки «Конфигурация подсчета трафика» → откроется страница «Монитор трафика»);

Примечание. На стартовой странице изделия предусмотрена возможность отображения информации о подсчете трафика по следующим критериям:

— объем трафика по красным интерфейсам за неделю;

— объем трафика по красным интерфейсам за месяц.

Страница «Монитор трафика»

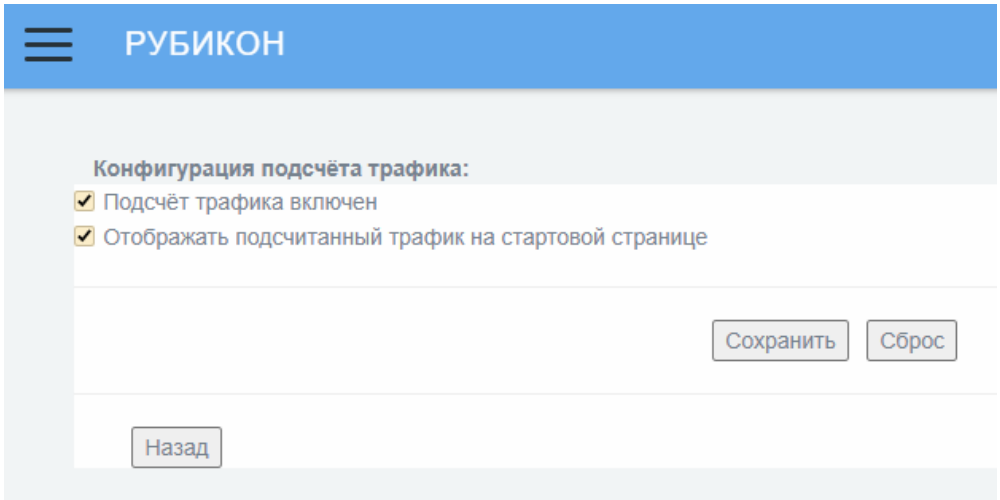

Рис. 5

6) статус самотестирования сервера (состоянии контрольных сумм функционирующего ПО «Рубикон-А» по результатам периодических автоматических пересчетов указанных контрольных сумм (запись: «Статус: корректно»).

В случае изменений контрольных сумм выдается сообщение об ошибке (см. рис. 6).

Сообщение об ошибке в случае изменений контрольных сумм

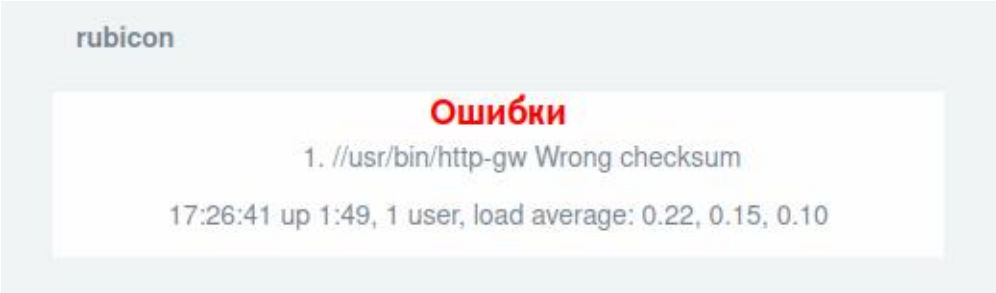

Рис. 6

При наличии одного и более «красных» интерфейсов в подразделе «Начало» отображаются функциональные кнопки (см. рис. 7).

Примечание. Доступные для изделия цветовые политики интерфейсов представлены подробно в подразделе «Настройка межсетевого экрана» руководства администратора НПЕШ.465614.005РА.

Отображение функциональных кнопок подраздела «Начало»

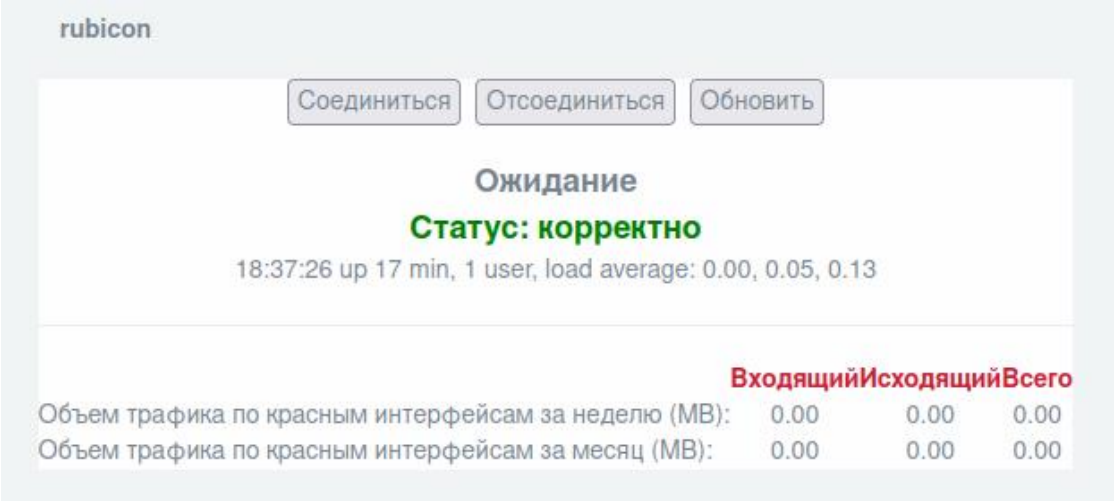

Рис. 7

В подразделе «Начало» могут отображаться следующие кнопки, имеющие отношение к «красным» интерфейсам:

1) кнопка «Соединиться» предназначена для включения прохождения трафика через «красный» интерфейс. Кнопка может применяться, если предварительно была нажата кнопка «Отсоединиться»;

2) кнопка «Отсоединиться» предназначена для отключения прохождения трафика через «красный» интерфейс;

3) кнопка «Обновить» предназначена для проверки возможности запуска «красных» интерфейсов, например, в случае восстановления файлов с корректными контрольными суммами.

4.2.2. Подраздел «Интерфейсы»

Подраздел «Интерфейсы» (см. рис. 8) предназначен для настройки сетевых интерфейсов.

Подраздел «Интерфейсы» раздела «Система»

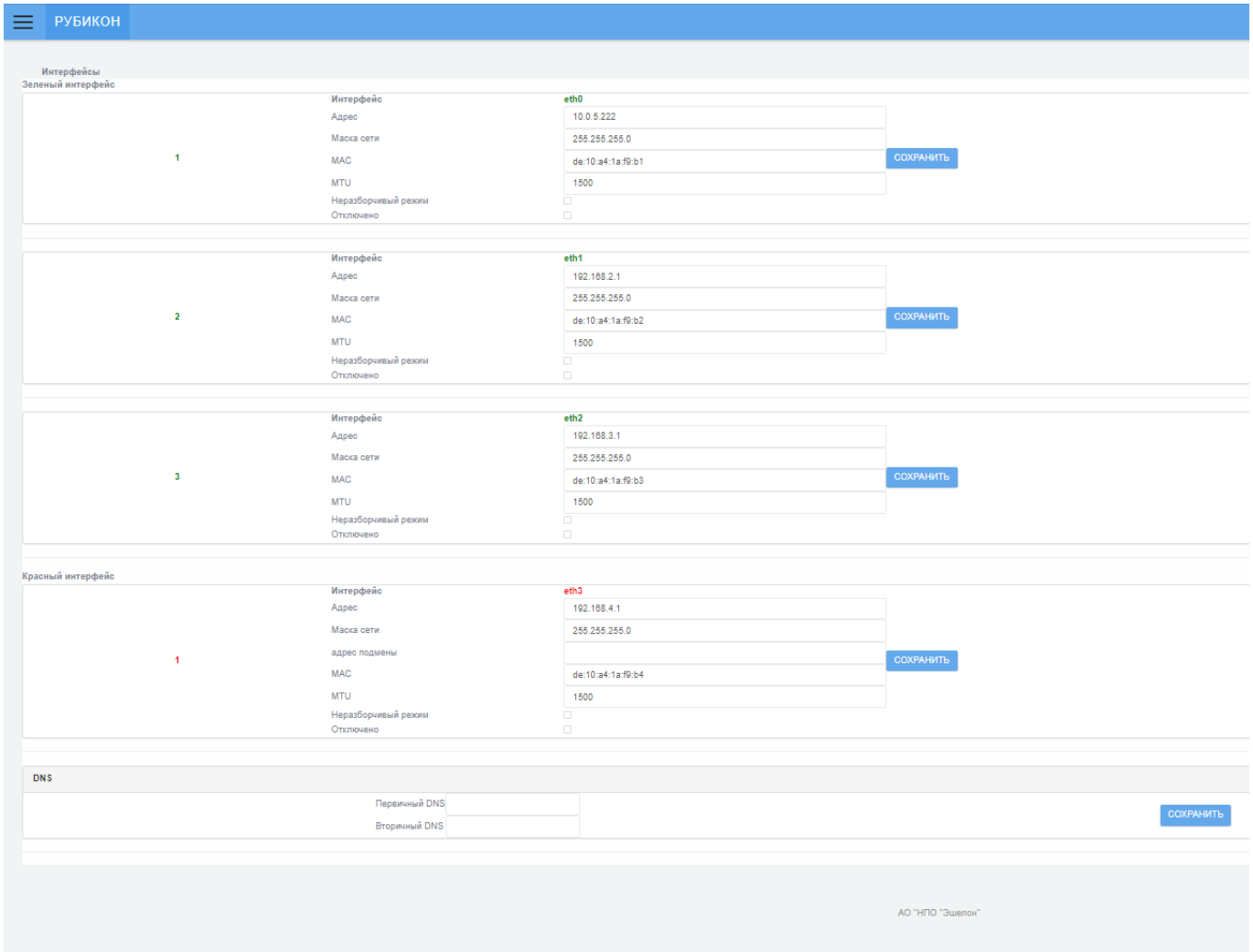

Рис. 8

В таблице 4 приведено описание элементов подраздела «Интерфейсы».

Таблица 4 – Описание элементов подраздела «Интерфейсы»

Элемент	Описание
Интерфейсы	
Информационное поле «Интерфейс»	Название и тип интерфейса
Поле «Адрес»	Поле для ввода IP-адреса интерфейса
Поле «Маска сети»	Поле для ввода маски сети интерфейса
Поле «адрес подмены»	Поле для ввода замены сетевого адреса на маскирующий адрес (подставной адрес)
Поле «MAC»	Поле для ввода MAC-адреса оборудования интерфейса
Поле «MTU»	Поле для ввода максимального размера пакета, передаваемого по сетям
Чекбокс «Неразборчивый режим»	Предназначен для включения режима приема всех сетевых пакетов, появляющихся на сетевом адаптере независимо от назначения
Чекбокс «Отключено»	Отключение интерфейса
Кнопка «Сохранить»	Предназначена для сохранения введенной информации и настроек
DNS	
Поле «Первичный DNS»	Поле для ввода IP-адреса первичного DNS-сервера
Поле «Вторичный DNS»	Поле для ввода IP-адреса вторичного DNS-сервера

4.2.3. Подраздел «Почта»

Подраздел «Почта» (см. рис. 9) предназначен для настройки процедур отправки уведомлений на заданные адреса электронной почты.

Подраздел «Почта» раздела «Система»

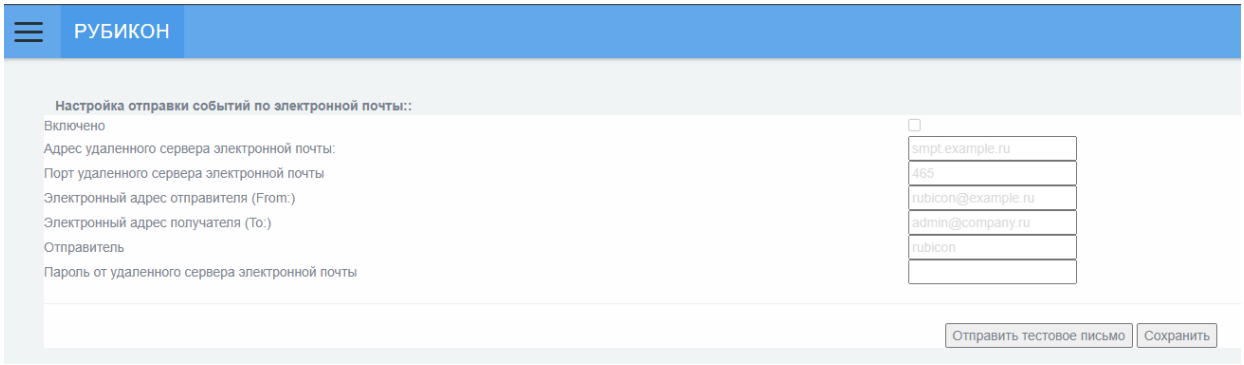

Рис. 9

В таблице 5 приведено описание элементов подраздела «Почта».

Таблица 5 – Описание элементов подраздела «Почта»

Элемент	Описание
Чекбокс «Включено»	Чекбокс включения/отключения отправки уведомлений на заданный почтовый адрес
Поле «Адрес удаленного сервера электронной почты»	Поле ввода для адреса сервера электронной почты отправителя
Поле «Порт удаленного сервера электронной почты»	Поле ввода для порта сервера электронной почты отправителя
Поле «Электронный адрес отправителя (From:)»	Поле ввода для адреса электронной почты отправителя
Поле «Электронный адрес получателя (To:)»	Поле ввода для адреса электронной почты получателя
Поле «Отправитель»	Поле ввода для имени отправителя
Поле «Пароль от удаленного сервера электронной почты»	Поле ввода для пароля отправителя
Кнопка «Отправить тестовое письмо»	Предназначена для отправки тестового письма

4.2.4. Подраздел «Пользователи»

Подраздел «Пользователи» (см. рис. 10) предназначен для управления учетными записями пользователей и позволяет:

1) создать нового пользователя;

2) редактировать учетную запись пользователя;

3) удалить учетную запись пользователя.

Подраздел «Пользователи»

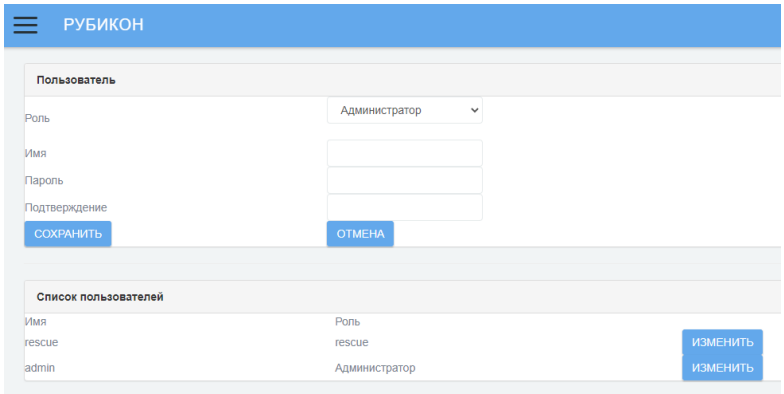

Рис. 10

Для учетных записей пользователей предусмотрены следующие роли:

1) «Администратор» – учетная запись для первоначальной установки, развертывания и настройки ПО. Администратор имеет доступ к просмотру веб-интерфейса и настройке «Рубикон»;

2) «Аудитор» – имеет доступ к стартовой странице, разделам «Состояние» и «Журналы» **без возможности внесения изменений** в настройки «Рубикон»;

3) «Пользователь» – **не имеет доступа к просмотру веб-интерфейса** (кроме стартовой страницы) и страницы установки соединения «https://**<ip-address>**:8443/cgi-bin/connect.cgi».

После аутентификации «Рубикон» фиксирует IP-адрес пользователя и предоставляет соответствующие правила. Пользователь включает правила нажатием кнопки «Запуск правил» на стартовой странице «Рубикон».

Примечание. При возможном изменении IP-адреса пользователя сессия будет принудительно закрыта. Для продолжения работы будет необходима повторная процедура подключения пользователя к изделию.

При необходимости обеспечения мониторинга состояния функционирования «Рубикон» следует использовать роль «Аудитор». Если при эксплуатации изделия необходимо вносить изменения в настройки, используйте роль «Администратор».

В таблице 6 приведено описание элементов подраздела «Пользователь».

Таблица 6 – Описание элементов подраздела «Пользователь»

Элемент	Описание
Пользователь	
Выпадающий список «Роль»	Выпадающий список выбора роли для новой учетной записи или при редактировании существующей учетной записи. Доступны для выбора роли: администратор, аудитор или пользователь
Поле «Имя»	Поле для ввода имени
Поле «Пароль»	Поле для ввода пароля
Поле «Подтверждение»	Поле для ввода подтверждения пароля

Элемент	Описание
Список пользователей	
Колонка «Имя»	Отображает список имен в колонке таблицы
Колонка «Роль»	Отображает список ролей в колонке таблицы
Кнопка «Изменить»	Предназначена для редактирования учетной записи в выбранной строке «Имя»/«Роль»
Кнопка «Удалить»	Предназначена для удаления учетной записи в выбранной строке «Имя»/«Роль». Удаление роли производится без возможности восстановления. Недоступны для удаления роли: «rescue» и «Администратор»

4.2.5. Подраздел «Резервное копирование»

Подраздел «Резервное копирование» (см. рис. 11) предназначен для управления резервными копиями.

Файл резервной копии имеет вид «rubicon-2021-11-10_10-11-47.dat».

Подраздел «Резервное копирование»

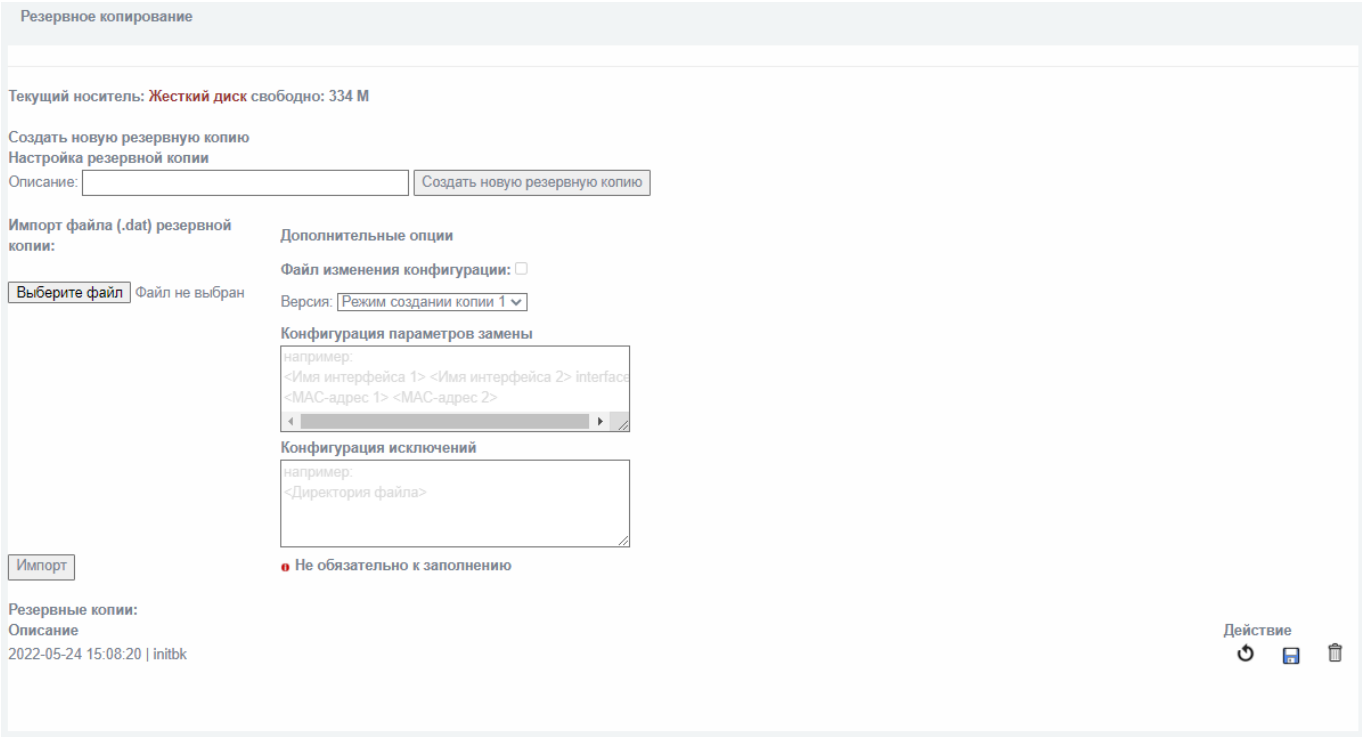

Рис. 11

В таблице 7 приведено описание элементов подраздела «Резервное копирование».

Таблица 7 – Описание элементов подраздела «Резервное копирование»

Элемент	Описание
Резервное копирование	
Информационное поле «Текущий носитель»	Описание текущего носителя с указанием оставшегося свободного места для хранения резервных копии
Настройка резервной копии	
Поле «Описание»	Поле для ввода описания резервной копии. Название может состоять **только из символов латинского алфавита и цифр**. Примечание. Использование кириллицы, пробелов и специальных символов не допускается!
Кнопка «Создать новую резервную копию»	Предназначена для создания новой резервной копии с введенным описанием
Импорт файла (.dat) резервной копии	
Кнопка «Выберите файл»	Предназначена для выбора резервной копии, хранящейся на рабочем месте администратора
Чекбокс «Файл изменения конфигурации»	Предназначен для включения функции преобразования файла резервной копии
Выпадающий список «Версия»	Предназначен для выбора соответствующего способа преобразования, зависящий от версии изделия «Рубикон». Доступные режимы создания копии следует уточнять у предприятия-производителя
Поле «Конфигурация параметров замены»	Предназначено для указания соответствия имен и MAC-адресов, содержащихся в резервной копии и в текущей конфигурации. Общая информация: <С чего меняем> <На что меняем> [<flag>] Формат процесса: <Имя интерфейса1> <Имя интерфейса 2> interface. *Пример: eth1 lan-1 interface* Формат процесса: <MAC-адрес 1> <MAC-адрес 2>. *Пример: 11:22:33:44:55:66 66:55:44:33:22:11*
Поле «Конфигурация исключений»	Не обязательное поле. Предназначено для заполнения в случае необходимости исключения части элементов конфигурации из файла резервной копии. **Не требуется при штатной работе. При использовании необходима консультация с предприятием-изготовителем**
Кнопка «Импорт»	Предназначена для импорта выбранной резервной копии
Резервные копии	
Информационное поле «Описание»	Отображение столбца информации о имеющихся в системе резервных копиях в формате «дата/время/описание»
	Кнопка «Применить выбранную резервную копию». Восстанавливает настройки из выбранной резервной копии
	Кнопка «Сохранить выбранную резервную копию на рабочее место администратора»
	Кнопка «Удалить резервную копию»

Блок элементов управления «Дополнительные опции» предназначен для преобразования содержимого файла резервной копии, перенесенных с других изделий «Рубикон», в том числе более старых версий, а также при отличающихся аппаратных настройках изделий.

Особенности использования:

1) с помощью кнопки «Выберите файл» стандартным способом производится выбор файла резервной копии, при чем:

— могут использоваться файлы резервной копии текущей версии изделия («Режим создания копии 1»);

— могут использоваться файлы резервной копии предыдущих версий изделия (режимы требуется уточнять у предприятия-изготовителя).

Примечание. При использовании резервных копий от предыдущих версий (при значительном отличии в конфигурации), может быть нарушена работа системы (требуется консультация с предприятием-изготовителем).

4.2.6. Подраздел «Пакеты»

Подраздел «Пакеты» (см. рис. 12) предназначен для установки дополнительных пакетов и обновлений, требуемых для функционирования изделия и возможного исправления найденных ошибок.

Подраздел «Пакеты»

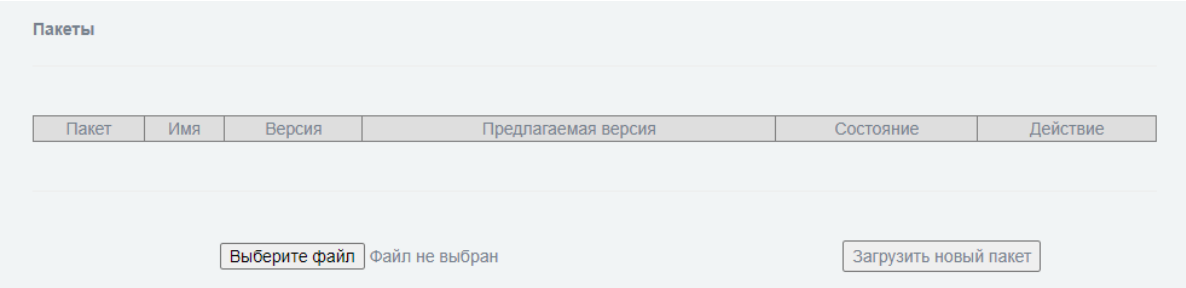

Рис. 12

Пользователь может выбрать необходимый файл обновления из локального каталога с помощью нажатия кнопки «Выберите файл», затем, осуществить загрузку выбранного пакета в файловую систему изделия с помощью кнопки «Загрузить новый пакет». Подробнее процесс установки пакетов и обновлений представлен в подразделе «Процедуры обновления изделия» руководства администратора НПЕШ.465614.005РА.

Описание активных элементов подраздела «Пакеты» представлено в таблице 8.

Таблица 8 – Описание элементов подраздела «Пакеты»

Элемент	Описание
Таблица «Пакеты»	Предназначена для отображения и установки загруженных пакетов
Кнопка «  »	Кнопка «Установить». Предназначена для установки загруженного пакета в изделие
Кнопка «Выберите файл»	Предназначена для выбора пакета из локального каталога рабочего места администратора
Кнопка «Загрузить новый пакет»	Предназначена для загрузки выбранного пакета в изделие

4.2.7. Подраздел «Настройка меню»

Подраздел «Настройка меню» раздела «Система» (см. рис. 13 и рис. 14) предназначен для включения и отключения отображения разделов и подразделов в навигационном меню.

Подраздел «Настройка меню». Часть 1

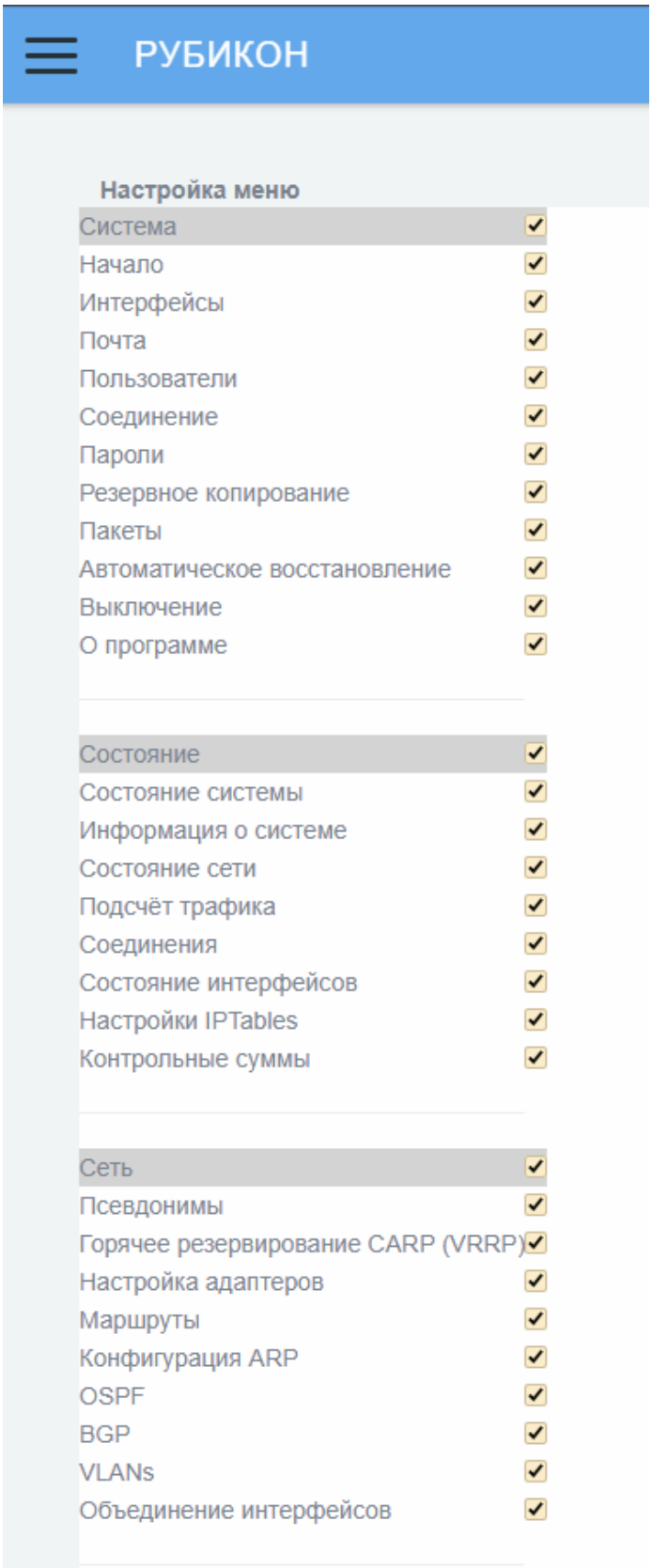

Рис. 13

Подраздел «Настройка меню». Часть 2

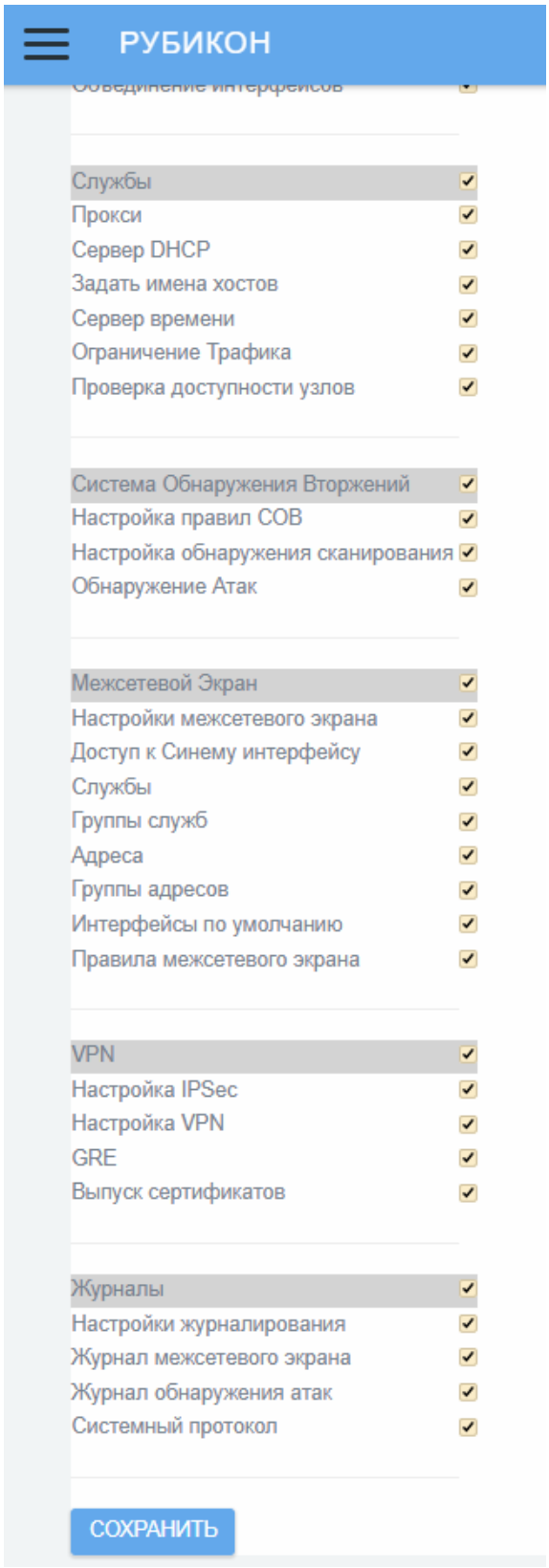

Рис. 14

Подраздел «Настройка меню» содержит элементы, указанные в таблице 9.

Таблица 9 – Описание элементов подраздела «Настройка меню»

Элемент	Описание
Таблица «Настройка меню»	Предназначена для отображения разделов и подразделов меню
Чекбокс «Активировать/деактивировать»	Предназначен для выбора отобразить (при активации) или скрыть (при снятом флажке) раздел/подраздел меню
Примечание. Дополнительное расширение меню также предусмотрено в разделе «Межсетевой экран», посредством выбора чекбокса «Расширенный режим» в поле «Настройки» подраздела «Настройки межсетевого экрана».	

4.2.8. Подраздел «Автоматическое восстановление»

Подраздел «Автоматическое восстановление» (см. рис. 15) предназначен для настройки автоматических действий при возникновении указанных в подразделе неисправностей.

Подраздел «Автоматическое восстановление»

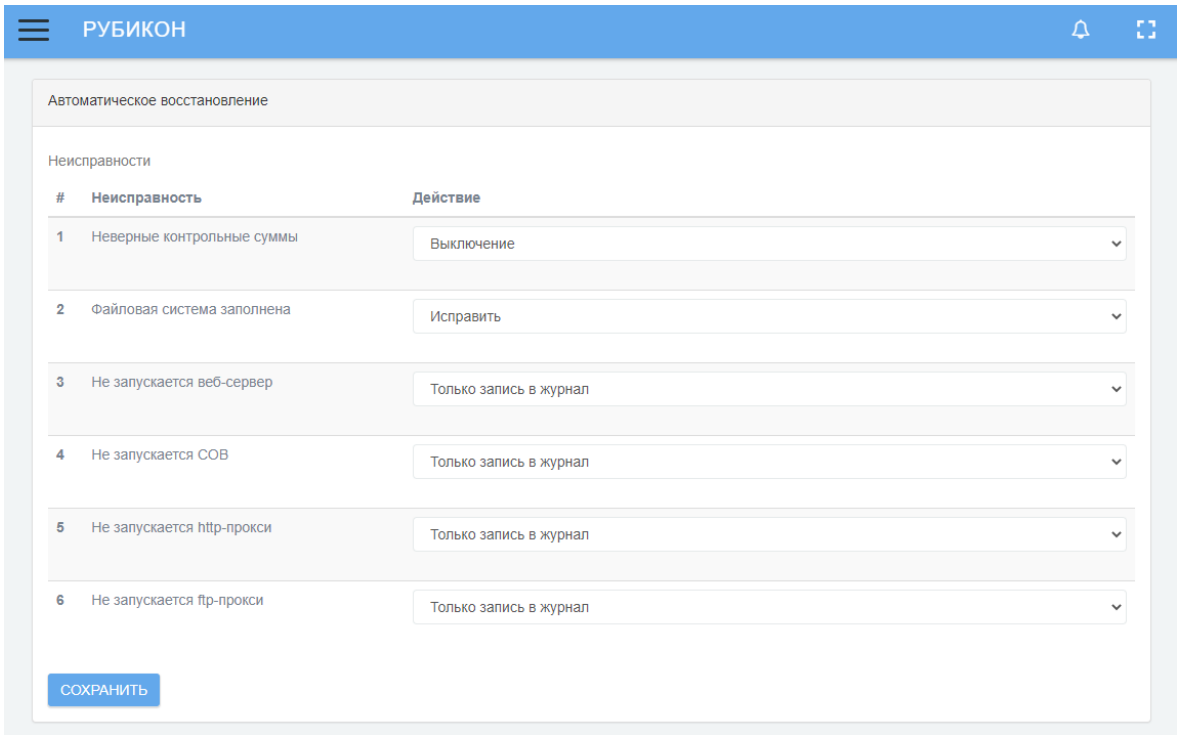

Рис. 15

В подразделе выделены определенные типы неисправностей, а также напротив каждой из них доступен выпадающий список с выбором автоматического действия при возникновении данной неисправности.

Соответствие типа неисправности и доступных для выбора автоматических действий представлены в таблице .

Таблица 10 – Соответствие типов неисправности и доступных для выбора автоматических действий

Неисправность	Доступные варианты выбора в выпадающем списке «Действие»
Неверные контрольные суммы	– только запись в журнал и блокировка «информационных потоков»; – выключение; – восстановить последнюю резервную копию настроек
Файловая система заполнена	– выключение; – исправить
Не запускается веб-сервер	– только запись в журнал; – выключение; – исправить; – восстановить последнюю резервную копию настроек
Не запускается СОВ	– только запись в журнал; – выключение; – исправить; – восстановить последнюю резервную копию настроек
Не запускается http-прокси	– только запись в журнал; – выключение; – исправить; – восстановить последнюю резервную копию настроек
Не запускается ftp-прокси	– только запись в журнал; – выключение; – исправить; – восстановить последнюю резервную копию настроек
Примечание. После настройки/смены выбора автоматического набора действий необходимо сохранить изменения, нажав кнопку «Сохранить».	

4.2.9. Подраздел «Выключение»

Подраздел «Выключение» (см. рис. 16) предназначен для программного выключения или перезагрузки аппаратной части изделия.

Подраздел «Выключение»

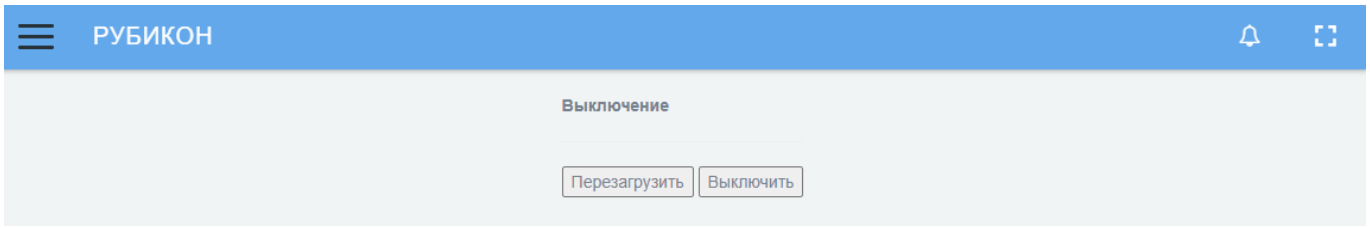

Рис. 16

Подраздел «Выключение» содержит элементы, указанные в таблице 11Таблица 9.

Таблица 11 – Описание элементов подраздела «Выключение»

Элемент	Описание
Кнопка «Перезагрузить»	Предназначена для перезагрузки изделия
Кнопка «Выключение»	Предназначена для выключения изделия

4.2.10. Подраздел «О программе»

Подраздел «О программе» (см. рис. 17) предназначен для отображения основной информации о ПО.

Подраздел «О программе»

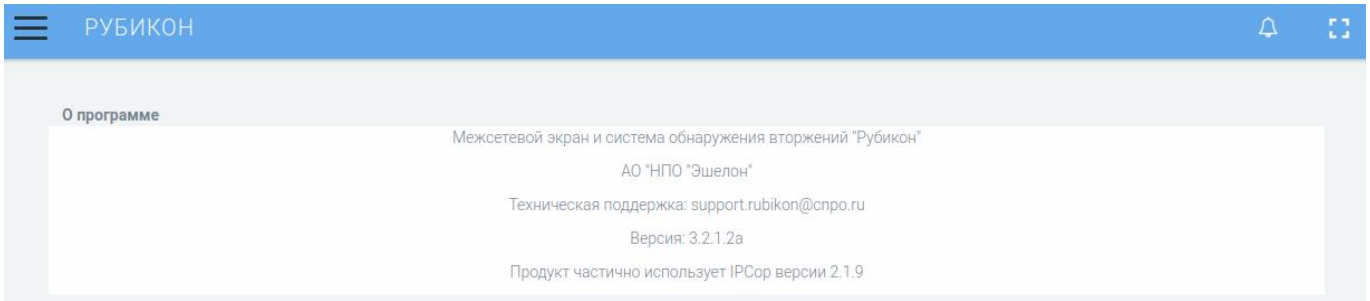

Рис. 17

В данном подразделе отображается следующая информация:

1) полное название программы;

2) предприятие-изготовитель;

3) электронная почта технической поддержки;

4) версия программы;

5) версия используемых плагинов.

4.3. Раздел «Состояние»

Раздел «Состояние» содержит следующие подразделы:

1) подраздел «Состояние системы»;

2) подраздел «Информация о системе»;

3) подраздел «Состояние сети»;

4) подраздел «Подсчет трафика»;

5) подраздел «Соединения»;

6) подраздел «Состояние интерфейсов»;

7) подраздел «NFTables»;

8) подраздел «Контрольные суммы».

4.3.1. Подраздел «Состояние системы»

Подраздел «Состояние системы» (см. рис. 18) предназначен для отображения полной информации о состоянии изделия.

Подраздел «Состояние системы»

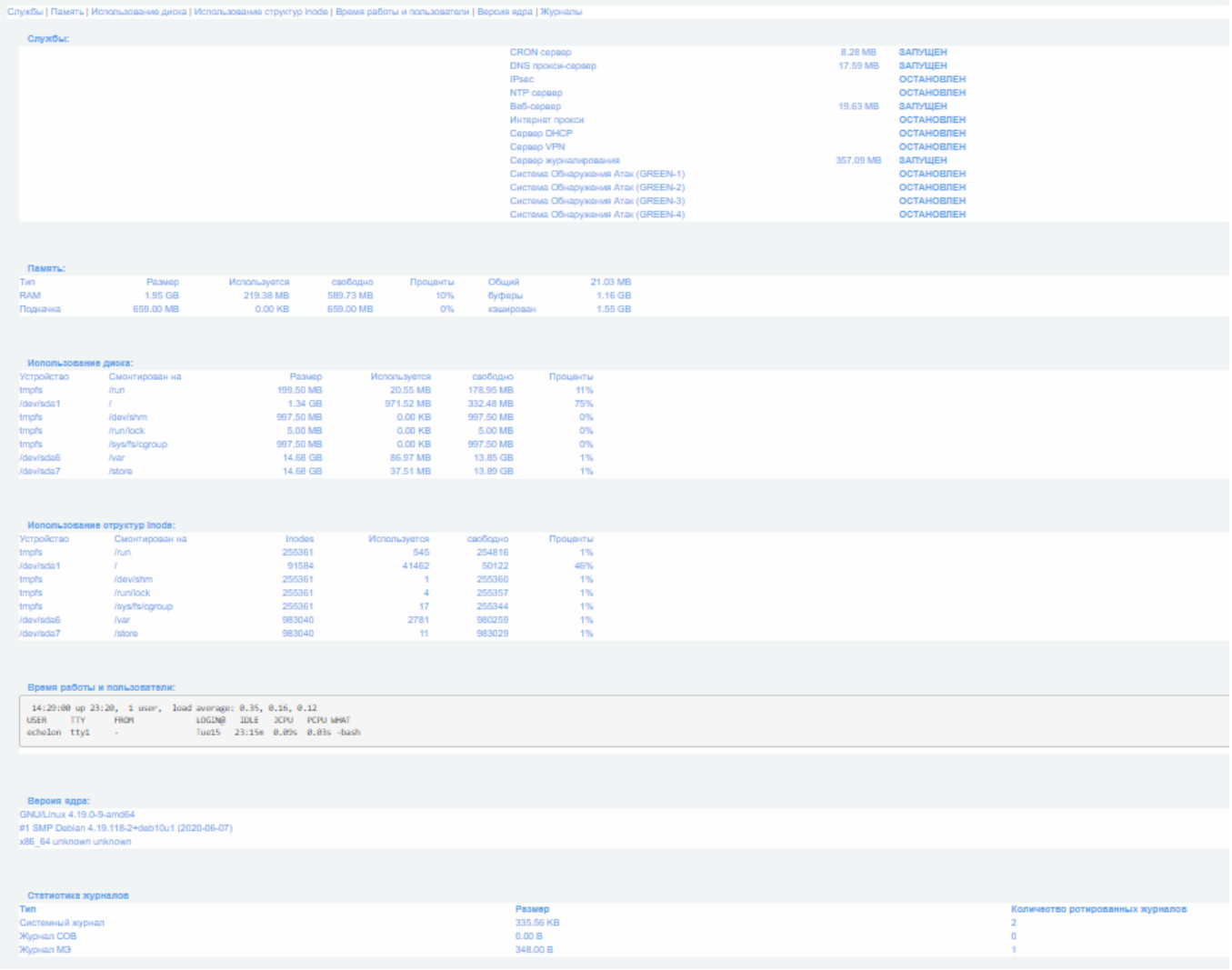

Рис. 18

Для удобства навигации по подразделу вверху страницы (см. рис. 19) предусмотрены ссылки на блоки.

Ссылки на блоки подраздела «Состояние системы»

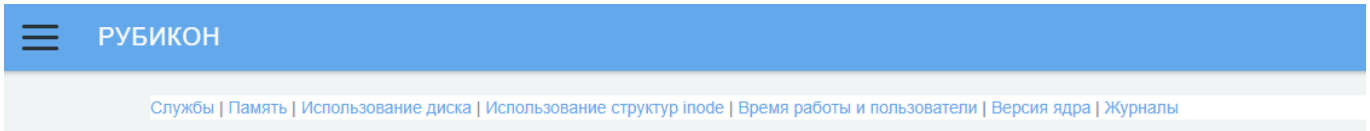

Рис. 19

Подраздел «Состояние системы» содержит следующие блоки:

1) блок «Службы»;

2) блок «Память»;

3) блок «Использование диска»;

4) блок «Использование структур inode»;

5) блок «Время работы и пользователи»;

6) блок «Версия ядра»;

7) блок «Журналы».

4.3.1.1. Блок «Службы»

В блоке «Службы» (см. рис. 20) отображается перечень служб, объем используемой ими оперативной памяти, их статус («ОСТАНОВЛЕН» или «ЗАПУЩЕН»).

Вкладка «Службы»

Службы:

CRON сервер	8.28 MB	ЗАПУЩЕН
DNS прокси-сервер	17.59 MB	ЗАПУЩЕН
IPsec	-	ОСТАНОВЛЕН
NTP сервер	-	ОСТАНОВЛЕН
Веб-сервер	19.50 MB	ЗАПУЩЕН
Интернет прокси	-	ОСТАНОВЛЕН
Сервер DHCP	-	ОСТАНОВЛЕН
Сервер VPN	-	ОСТАНОВЛЕН
Сервер журналирования	357.09 MB	ЗАПУЩЕН
Система Обнаружения Атак (GREEN-1)	-	ОСТАНОВЛЕН
Система Обнаружения Атак (GREEN-2)	-	ОСТАНОВЛЕН
Система Обнаружения Атак (GREEN-3)	-	ОСТАНОВЛЕН
Система Обнаружения Атак (GREEN-4)	-	ОСТАНОВЛЕН

Рис. 20

4.3.1.2. Блок «Память»

В блоке «Память» (см. рис. 21) отображается информация о всех видах памяти в изделии.

Блок «Память»

Память:

Тип	Размер	Используется	свободно	Проценты	Общий	21.03 MB
RAM	1.95 GB	219.38 MB	589.73 MB	10%	буферы	1.16 GB
Подкачка	659.00 MB	0.00 KB	659.00 MB	0%	кэширован	1.55 GB

Рис. 21

Информация о памяти представлена в виде таблицы со следующими параметрами:

1) «Тип» – тип памяти;

2) «Размер» – объем памяти;

3) «Используется» – количество задействованной памяти;

4) «Свободно» – количество свободной памяти;

5) «Проценты» – процент используемой памяти на устройстве;

6) «Общий» – объем общей памяти;

7) «Буферы» – объем буферной памяти;

8) «Кэширован» – объем кэш-памяти.

4.3.1.3. Блок «Использование диска»

В блоке «Использование диска» (см. рис. 22) отображается информация о всех физических и виртуальных дисках.

Блок «Использование диска»

Использование диска:

Устройство	Смонтирован на	Размер	Используется	свободно	Проценты
tmpfs	/run	199.50 MB	20.55 MB	178.95 MB	11%
/dev/sda1	/	1.34 GB	970.89 MB	333.11 MB	75%
tmpfs	/dev/shm	997.50 MB	0.00 KB	997.50 MB	0%
tmpfs	/run/lock	5.00 MB	0.00 KB	5.00 MB	0%
tmpfs	/sys/fs/cgroup	997.50 MB	0.00 KB	997.50 MB	0%
/dev/sda6	/var	14.68 GB	86.71 MB	13.85 GB	1%
/dev/sda7	/store	14.68 GB	37.51 MB	13.89 GB	1%

Рис. 22

Информация о дисках представлена в виде таблицы со следующими параметрами:

1) «Устройство» – название устройства;

2) «Смонтирован на» – адрес устройства;

3) «Размер» – размер диска;

4) «Используется» – используемое место на диске;

5) «Свободно» – свободное место на диске;

6) «Проценты» – процентное заполнение диска.

4.3.1.4. Блок «Использование структур inode»

В блоке «Использование структур inode» (см. рис. 23) отображается информация об использовании структур с индексными дескрипторами.

Блок «Использование структур inode»

Использование структур inode:

Устройство	Смонтирован на	Inodes	Используется	свободно	Проценты
tmpfs	/run	255361	545	254816	1%
/dev/sda1	/	91584	41462	50122	46%
tmpfs	/dev/shm	255361	1	255360	1%
tmpfs	/run/lock	255361	4	255357	1%
tmpfs	/sys/fs/cgroup	255361	17	255344	1%
/dev/sda6	/var	983040	2781	980259	1%
/dev/sda7	/store	983040	11	983029	1%

Рис. 23

Информация об использовании структур с индексными дескрипторами представлена в виде таблицы со следующими параметрами:

1) «Устройство» – название устройства;

2) «Смонтирован на» – адрес устройства;

3) «Inodes» – количество индексных дескрипторов;

4) «Используется» – используется дескрипторов;

5) «Свободно» – свободно дескрипторов;

6) «Проценты» – процентное соотношение используемых дескрипторов.

4.3.1.5. Блок «Время работы и пользователи»

В блоке «Время работы и пользователи» (см. рис. 24) отображается информация о времени беспрерывной работы изделия и количестве пользователей в сети.

Блок «Время работы и пользователи»

Время работы и пользователи:

```
 14:29:00 up 23:20,  1 user,  load average: 0.35, 0.16, 0.12
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
echelon  tty1     -                Tue15   23:15m  0.09s  0.03s -bash
```

Рис. 24

4.3.1.6. Блок «Версия ядра»

В блоке «Версия ядра» (см. рис. 25) отображается информация о версии ядра.

Блок «Версия ядра»

Версия ядра:

GNU/Linux 4.19.0-9-amd64
#1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07)
x86_64 unknown unknown

Рис. 25

4.3.1.7. Блок «Статистика журналов»

В блоке «Статистика журналов» (см. рис. 26) отображается информация о журналах.

Блок «Статистика журналов»

Статистика журналов

Тип	Размер	Количество ротированных журналов
Системный журнал	335.56 KB	2
Журнал СОВ	0.00 B	0
Журнал МЭ	348.00 B	1

Рис. 26

Информация о журналах представлена в виде таблицы со следующими параметрами:

1) «Тип» – тип журнала;

2) «Размер» – размер журнала;

3) «Количество ротированных журналов» – количество фактов переноса активного журнала в архивную область.

4.3.2. Подраздел «Информация о системе»

Подраздел «Информация о системе» предназначен для отображения подробной информации о физических компонентах изделия.

Для удобства навигации по подразделу вверху страницы (см. рис. 27) предусмотрены ссылки на блоки.

Ссылки на блоки подраздела «Информация о системе»

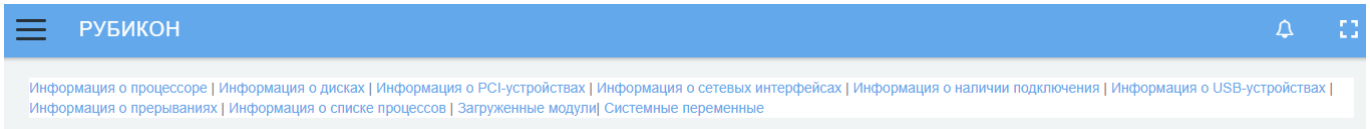

Рис. 27

Подраздел «Информация о системе» содержит следующие блоки:

1) блок «Информация о процессоре»;

2) блок «Информация о дисках»;

3) блок «Информация о PCI-устройствах»;

4) блок «Информация о сетевых интерфейсах»;

5) блок «Информация о наличии подключения»;

6) блок «Информация о USB-устройствах»;

7) блок «Информация о прерываниях»;

8) блок «Информация о списке процессов»;

9) блок «Загруженные модули»;

10) блок «Системные переменные».

4.3.2.1. Блок «Информация о процессоре»

В блоке «Информация о процессоре» (см. рис. 28) отображается полная техническая информация о процессоре.

Блок «Информация о процессоре»

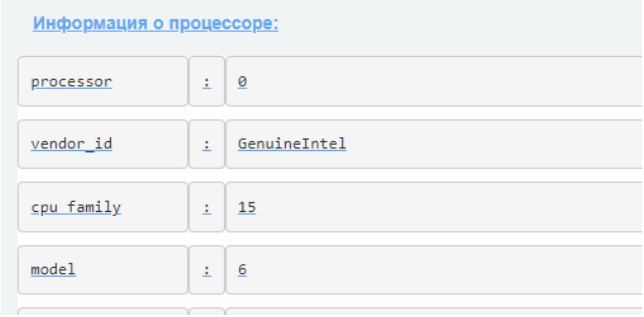

Рис. 28

4.3.2.2. Блок «Информация о дисках»

В блоке «Информация о дисках» (см. рис. 29) отображается техническая информация о подключенных физических носителях данных.

Вкладка «Информация о дисках»

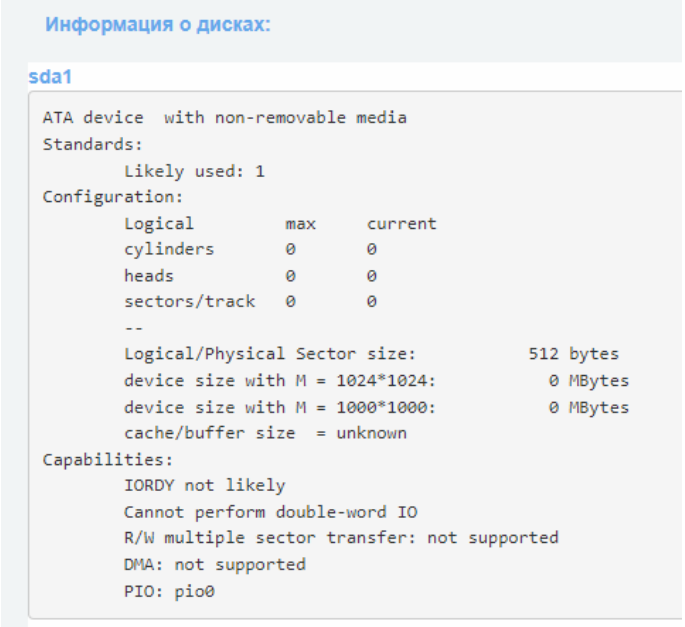

Рис. 29

Информация по каждому носителю данных отображается в отдельном поле.

4.3.2.3. Блок «Информация о PCI-устройствах»

В блоке «Информация о PCI-устройствах» (см. рис. 30) отображается информация о подключенных устройствах к шине PCI.

Блок «Информация о PCI-устройствах»

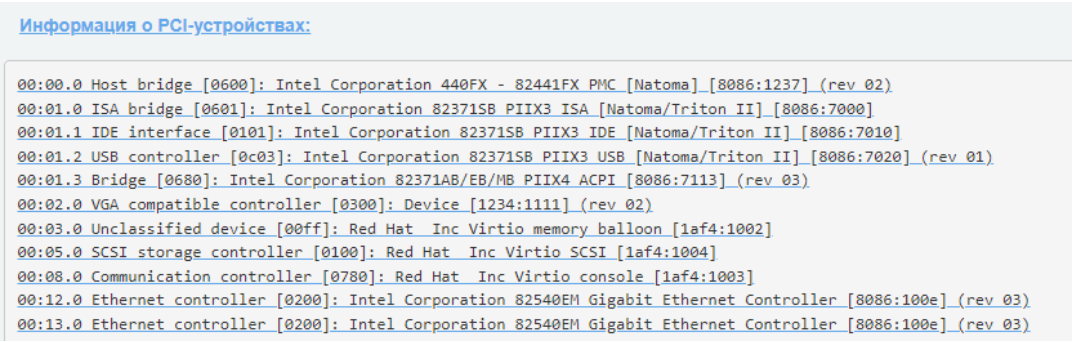

Рис. 30

4.3.2.4. Блок «Информация о сетевых интерфейсах»

В блоке «Информация о сетевых интерфейсах» (см. рис. 31) отображается информация о сетевых контроллерах.

Блок «Информация о сетевых интерфейсах»

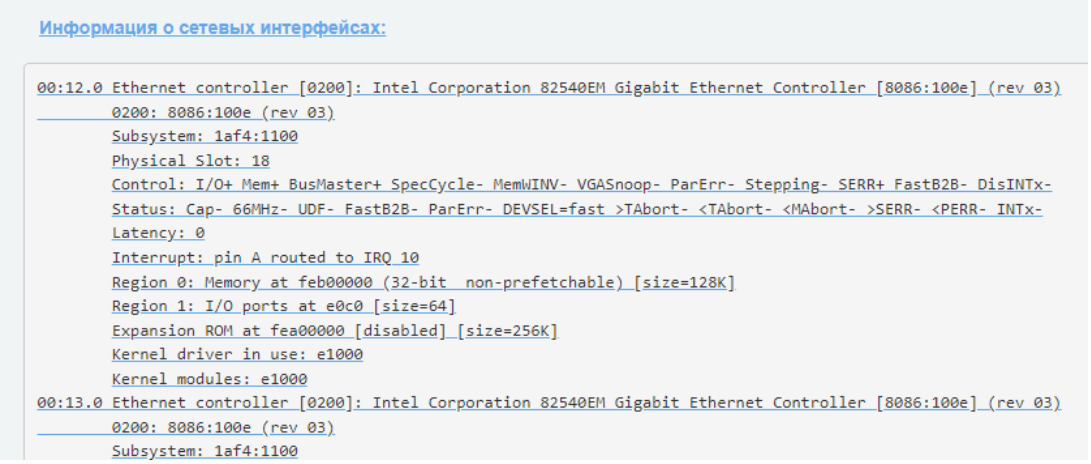

Рис. 31

4.3.2.5. Блок «Информация о наличии подключения»

В блоке «Информация о наличии подключения» (см. рис. 32) приведена информация о подключении по сетевым интерфейсам.

Блок «Информация о наличии подключения»

Информация о наличии подключения:

```
Состояние соединения (MII):

erspan0: link status: unknown (MII not supported)
eth0: negotiated 1000baseT-FD flow-control, link ok

eth1: negotiated 1000baseT-FD flow-control, link ok

eth2: negotiated 1000baseT-FD flow-control, link ok

eth3: negotiated 1000baseT-FD flow-control, link ok

gre0: link status: unknown (MII not supported)
gretap0: link status: unknown (MII not supported)
ifb0: link status: unknown (MII not supported)
ifb1: link status: unknown (MII not supported)
ifb2: link status: unknown (MII not supported)
ifb3: link status: unknown (MII not supported)

Состояние соединения (ethtool):

Settings for erspan0:

Settings for eth0:
        Speed: 1000Mb/s
        Duplex: Full
        Link detected: yes

Settings for eth1:
        Speed: 1000Mb/s
        Duplex: Full
        Link detected: yes

Settings for eth2:
        Speed: 1000Mb/s
```

Рис. 32

4.3.2.6. Блок «Информация о USB-устройствах»

В блоке «Информация о USB-устройствах» (см. рис. 33) приведена информация о подключениях по портам USB.

Блок «Информация о USB устройствах»

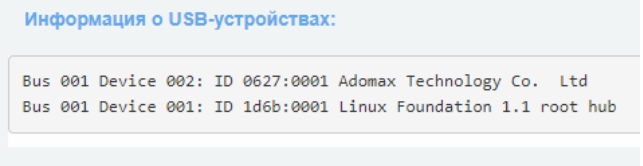

Рис. 33

4.3.2.7. Блок «Информация о прерываниях»

В блоке «Информация о прерываниях» (см. рис. 34) приведена информация о прерываниях.

Вкладка «Информация о прерываниях»

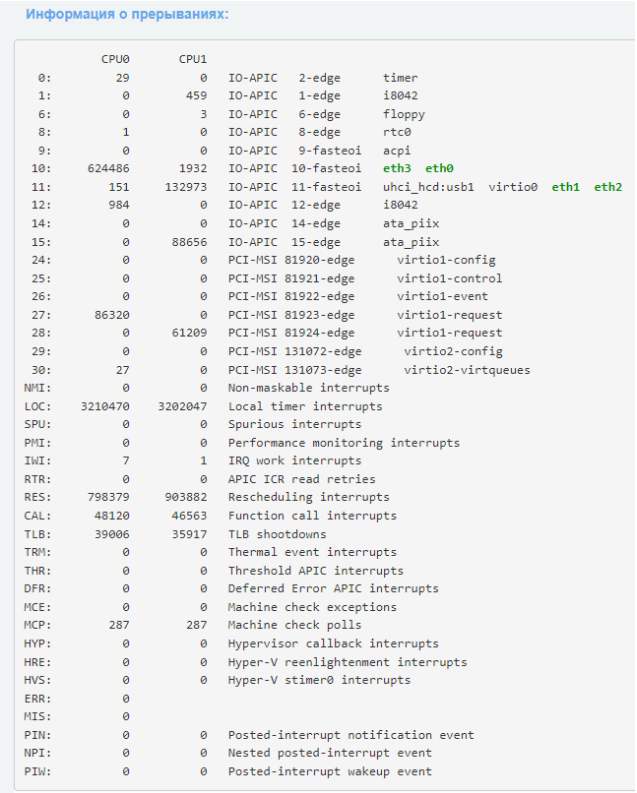

Рис. 34

4.3.2.8. Блок «Информация о списке процессов»

В блоке «Информация о списке процессов» (см. рис. 35) приводится информация о всех программных процессах, запущенных в изделии.

Вкладка «Информация о списке процессов»

Информация о списке процессов:

USER	PID	PPID	%CPU	%MEM	VSZ	RSS	TT	STAT	STARTED	TIME	COMMAND
root	2	0	0.0	0.0	0	0	?	S	May 24	00:00:00	[kthreadd]
root	3	2	0.0	0.0	0	0	?	I<	May 24	00:00:00	_ [rcu_gp]
root	4	2	0.0	0.0	0	0	?	I<	May 24	00:00:00	_ [rcu_par_gp]
root	6	2	0.0	0.0	0	0	?	I<	May 24	00:00:00	_ [kworker/0:0H-kblockd]
root	7	2	0.0	0.0	0	0	?	I	May 24	00:00:01	_ [kworker/u4:0-events_unbound]
root	8	2	0.0	0.0	0	0	?	I<	May 24	00:00:00	_ [mm_percpu_wq]
root	9	2	0.0	0.0	0	0	?	S	May 24	00:00:03	_ [ksoftirqd/0]
root	10	2	0.0	0.0	0	0	?	I	May 24	00:00:19	_ [rcu_sched]

Рис. 35

Информация о списке программных процессов представлена в виде таблицы со следующими параметрами:

1) «USER» – пользователь, запустивший процесс;

2) «PID» – идентификатор процесса;

3) «PPID» – идентификатор родительского процесса;

4) «%CPU» – процент использования процессорной мощности;

5) «%MEM» – процент использования памяти;

6) «VSZ» – размер виртуальной памяти;

7) «RSS» – размер задействованной оперативной памяти;

8) «TT» – терминал TTY;

9) «STAT» – текущее состояние процесса;

10) «STARTED» – время начала процесса;

11) «TIME» – время работы процесса;

12) «COMMAND» – префикс процесса.

4.3.2.9. Блок «Загруженные модули»

В блоке «Загруженные модули» (см. рис. 36) приводится информация о всех загруженных модулях.

Блок «Загруженные модули»

Загруженные модули:

Module	Size	Used by
tun	49152	0
xt_secmark	16384	0
ifb	16384	0
ip_gre	32768	0
ip_tunnel	24576	1 ip_gre
gre	16384	1 ip_gre

Рис. 36

Информация о загруженных модулях представлена в виде таблицы со следующими параметрами:

1) «Module» – название модуля;

2) «Size» – размер модуля;

3) «Used by» – используется сетевым интерфейсом.

4.3.2.10. Блок «Системные переменные»

В блоке «Системные переменные» (см. рис. 37) приводится информация о системных переменных.

Вкладка «Системные переменные»

Системные переменные:

net.ipv4.neigh.default.gc_thresh1	2048
net.ipv4.neigh.default.gc_thresh2	2048
net.ipv4.neigh.default.gc_thresh3	2048
net.ipv4.route.max_size	2147483647

Рис. 37

4.3.3. Подраздел «Состояние сети»

Подраздел «Состояние сети» предназначен для отображения информации по всем сетевым интерфейсам.

Для удобства навигации по подразделу вверху страницы (см. рис. 38) предусмотрены ссылки на блоки.

Ссылки на блоки подраздела «Состояние сети»

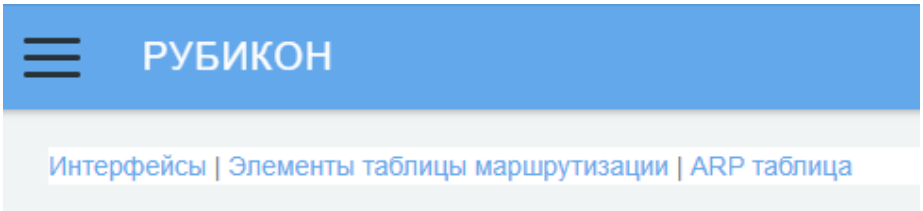

Рис. 38

Подраздел «Состояние сети» содержит следующие блоки:

1) блок «Интерфейсы»;

2) блок «Элементы таблицы маршрутизации»;

3) блок «ARP таблица».

При нажатии на ссылку, экран переносится на соответствующий блок с информацией.

4.3.3.1. Блок «Интерфейсы»

В блоке «Интерфейсы» (см. рис. 39) представлена информация о всех сетевых интерфейсах.

Информация приводится по каждому сетевому интерфейсу.

Блок «Интерфейсы»

Интерфейсы:

```
erspan0: flags=4098<BROADCAST,MULTICAST>  mtu 1450
        ether 00:00:00:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.5.222  netmask 255.255.255.0  broadcast 0.0.0.0
        ether de:10:a4:1a:f9:b1  txqueuelen 1000  (Ethernet)
        RX packets 418503  bytes 74545386 (71.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 248933  bytes 92145180 (87.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Рис. 39

4.3.3.2. Блок «Элементы таблицы маршрутизации»

В блоке «Элементы таблицы маршрутизации» (см. рис. 40) приведена информация по всем таблицам маршрутизации.

Блок «Элементы таблицы маршрутизации»

Элементы таблицы маршрутизации:

```
0:      from all lookup local
32766:  from all lookup main
32767:  from all lookup default

default via 10.0.5.1 dev eth0
10.0.5.0/24 dev eth0 proto kernel scope link src 10.0.5.222
192.168.2.0/24 dev eth1 proto kernel scope link src 192.168.2.1
192.168.3.0/24 dev eth2 proto kernel scope link src 192.168.3.1
192.168.4.0/24 dev eth3 proto kernel scope link src 192.168.4.1
broadcast 10.0.5.0 dev eth0 table local proto kernel scope link src 10.0.5.222
```

Рис. 40

4.3.3.3. Блок «ARP таблица»

В блоке «ARP таблица» (см. рис. 41) приведена информация по всем MAC-адресам, привязанным к IP-адресам.

Блок «ARP таблица»

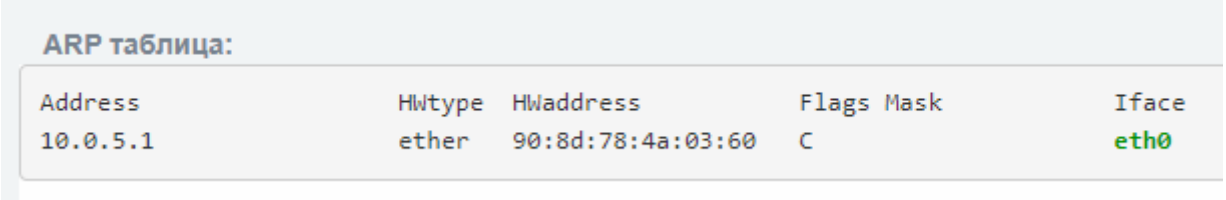

Рис. 41

Информация о ARP таблицах представлена в виде таблицы со следующими параметрами:

1) «Address» – IP-адрес устройства;

2) «HWtype» – тип устройства;

3) «HWaddress» – MAC-адрес устройства;

4) «Flags Mask» – тип записи;

5) «Iface» – название интерфейса.

4.3.4. Подраздел «Подсчет трафика»

Подраздел «Подсчет трафика» (см. рис. 42) предназначен для отображения количества трафика в детализации по аппаратным сетевым интерфейсам за определенный период времени.

Подраздел «Подсчет трафика»

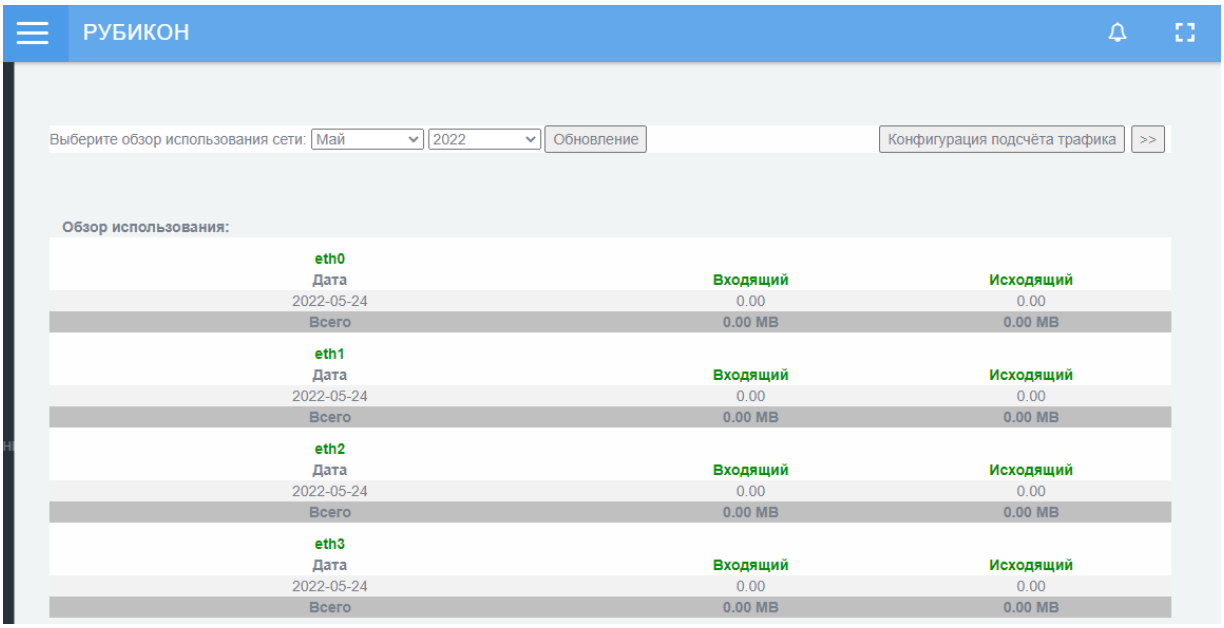

Рис. 42

В таблице 12 приведено описание элементов подраздела «Подсчет трафика».

Таблица 12 – Описание элементов подраздела «Подсчет трафика»

Элемент	Описание
Выпадающий список «Месяц»	Предназначен для выбора необходимого для отображения месяца
Выпадающий список «Год»	Предназначен для выбора необходимого для отображения года
Кнопка «Обновление»	Предназначена для применения выбранных временных параметров выпадающих списков и обновлении информации в таблице вывода подсчета трафика
Кнопка «Конфигурация подсчета трафика»	Предназначена для открытия страницы конфигурации подсчета трафика: – подсчет трафика производится при активном чекбоксе «Подсчёт трафика включен»; – при активном чекбоксе «Отображать подсчитанный трафик на стартовой странице» на стартовой странице отображается информация о подсчитанном трафике **только для «красных» интерфейсов** (см. рис. 5 и 7)
Кнопка « >> »	Кнопка «Переход к расширенной конфигурации». Предназначена для открытия страницы расширенной конфигурации подсчета трафика
Таблица «Обзор использования»	Предназначена для отображения информации о подсчитанном трафике

Информация по подсчету трафика представлена в виде таблицы со следующими параметрами:

1) «Дата» – дата, на которую произведен подсчет трафика;

2) «Входящий» – количество входящего трафика;

3) «Исходящий» – количество исходящего трафика.

Отображение информации о подсчитанном трафике может быть представлено в следующих интервалах:

1) ежедневное отображение за период в один месяц (по умолчанию – текущий);

2) ежедневное отображение за выбранный интервал времени.

4.3.5. Подраздел «Соединения»

Подраздел «Соединения» (см. рис. 43) предназначен для отображения информации об активных соединениях.

Подраздел «Соединения»

Трассировка связи по NFTables

Отображать: Трафик

Сохранить

Протокол	Исходный IP-адрес:Порт источника	Исходный IP-адрес:Порт назначения	Пакеты / Байты	Ответ IP-адрес:Порт источника	Ответ IP-адрес:Порт назначения	Пакеты / Байты
tcp	192.168.56.101 :36828	192.168.56.1 :8443	14 / 2504	192.168.56.1 :8443	192.168.56.101 :36828	9 / 1678
tcp	192.168.56.101 :36852	192.168.56.1 :8443	12 / 1740	192.168.56.1 :8443	192.168.56.101 :36852	9 / 1045
tcp	192.168.56.101 :36838	192.168.56.1 :8443	11 / 1691	192.168.56.1 :8443	192.168.56.101 :36838	10 / 1097
tcp	192.168.56.101 :36866	192.168.56.1 :8443	13 / 2450	192.168.56.1 :8443	192.168.56.101 :36866	9 / 1678
tcp	192.168.56.101 :36884	192.168.56.1 :8443	9 / 2389	192.168.56.1 :8443	192.168.56.101 :36884	7 / 917
tcp	192.168.56.101 :36872	192.168.56.1 :8443	13 / 2454	192.168.56.1 :8443	192.168.56.101 :36872	9 / 1678
tcp	192.168.56.101 :36826	192.168.56.1 :8443	13 / 2452	192.168.56.1 :8443	192.168.56.101 :36826	9 / 1678
tcp	192.168.56.101 :36874	192.168.56.1 :8443	14 / 2502	192.168.56.1 :8443	192.168.56.101 :36874	9 / 1678
tcp	192.168.56.101 :36836	192.168.56.1 :8443	12 / 1743	192.168.56.1 :8443	192.168.56.101 :36836	8 / 993
tcp	192.168.56.101 :36830	192.168.56.1 :8443	12 / 1743	192.168.56.1 :8443	192.168.56.101 :36830	8 / 993
tcp	192.168.56.101 :36864	192.168.56.1 :8443	13 / 2454	192.168.56.1 :8443	192.168.56.101 :36864	9 / 1678
tcp	192.168.56.101 :36882	192.168.56.1 :8443	14 / 2502	192.168.56.1 :8443	192.168.56.101 :36882	8 / 1626

Легенда: ЛВС | ИНТЕРНЕТ | Беспроводная сеть | Демилитаризованная Зона (DMZ) | IPCop | IPsec | OpenVPN

Рис. 43

Информационный блок подраздела может отражать одну из следующих таблиц:

1) таблица «Трафик» (по умолчанию);

2) таблица «Состояние».

Для переключения между таблицами необходимо в блоке «Трассировка связи по NFTables» выбрать название таблицы в выпадающем списке «Отображать» и нажать кнопку «Сохранить». Страница будет автоматически обновлена и отобразит выбранную ранее таблицу.

4.3.5.1. Таблица «Трафик»

Таблица «Трафик» (см. рис. 44) подсчитывает количество переданных пакетов в действующих соединениях.

Таблица «Трафик»

Протокол	Исходный IP-адрес:Порт источника	Исходный IP-адрес:Порт назначения	Пакеты / Байты	Ответ IP-адрес:Порт источника	Ответ IP-адрес:Порт назначения	Пакеты / Байты
tcp	192.168.56.101 :36828	192.168.56.1 :8443	14 / 2504	192.168.56.1 :8443	192.168.56.101 :36828	9 / 1678
tcp	192.168.56.101 :36852	192.168.56.1 :8443	12 / 1740	192.168.56.1 :8443	192.168.56.101 :36852	9 / 1045
tcp	192.168.56.101 :36838	192.168.56.1 :8443	11 / 1691	192.168.56.1 :8443	192.168.56.101 :36838	10 / 1097
tcp	192.168.56.101 :36866	192.168.56.1 :8443	13 / 2450	192.168.56.1 :8443	192.168.56.101 :36866	9 / 1678
tcp	192.168.56.101 :36884	192.168.56.1 :8443	9 / 2389	192.168.56.1 :8443	192.168.56.101 :36884	7 / 917
tcp	192.168.56.101 :36872	192.168.56.1 :8443	13 / 2454	192.168.56.1 :8443	192.168.56.101 :36872	9 / 1678
tcp	192.168.56.101 :36826	192.168.56.1 :8443	13 / 2452	192.168.56.1 :8443	192.168.56.101 :36826	9 / 1678
tcp	192.168.56.101 :36874	192.168.56.1 :8443	14 / 2502	192.168.56.1 :8443	192.168.56.101 :36874	9 / 1678
tcp	192.168.56.101 :36836	192.168.56.1 :8443	12 / 1743	192.168.56.1 :8443	192.168.56.101 :36836	8 / 993
tcp	192.168.56.101 :36830	192.168.56.1 :8443	12 / 1743	192.168.56.1 :8443	192.168.56.101 :36830	8 / 993
tcp	192.168.56.101 :36864	192.168.56.1 :8443	13 / 2454	192.168.56.1 :8443	192.168.56.101 :36864	9 / 1678
tcp	192.168.56.101 :36882	192.168.56.1 :8443	14 / 2502	192.168.56.1 :8443	192.168.56.101 :36882	8 / 1626

Легенда: ЛВС | ИНТЕРНЕТ | Беспроводная сеть | Демилитаризованная Зона (DMZ) | IPCop | IPsec | OpenVPN

Рис. 44

Информация по соединениям представлена в виде таблицы со следующими параметрами:

1) «Протокол» – название протокола соединения;

2) «Исходный IP-адрес: Порт источника» – запрос на адрес и порт источника;

3) «Исходный IP-адрес: Порт назначения» – информация, содержащая IP-адрес и порт сетевого соединения-запроса;

4) «Пакеты / Байты» – количество переданных пакетов в байтах;

5) «Ответ IP-адрес: Порт источника» – ответ на адрес и порт источника;

6) «Ответ IP-адрес: Порт назначения» – информация, содержащая IP-адрес и порт сетевого соединения-ответа;

7) «Пакеты / Байты» – количество переданных пакетов в байтах.

Под таблицей представлена легенда цветовой политики настройки сетевых интерфейсов.

4.3.5.2. Таблица «Состояние»

Таблица «Состояние» (см. рис. 45) отображает актуальное состояние действующих соединений.

Таблица «Состояние»

Протокол	Запрос IP-адрес:Порт источника	Запрос IP-адрес:Порт назначения	Ответ IP-адрес:Порт источника	Ответ IP-адрес:Порт назначения	Истекает (Секунды)	Состояние	Выделенный	Использовано
tcp	192.168.56.101 :36860	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36860	5	CLOSE	0	1
tcp	192.168.56.101 :36828	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36828	51	TIME_WAIT	0	1
tcp	192.168.56.101 :36826	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36826	51	TIME_WAIT	0	1
tcp	192.168.56.101 :36836	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36836	70	TIME_WAIT	0	1
tcp	192.168.56.101 :36818	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36818	19	TIME_WAIT	0	1
tcp	192.168.56.101 :36858	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36858	5	CLOSE	0	1
tcp	192.168.56.101 :36838	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36838	76	TIME_WAIT	0	1
tcp	192.168.56.101 :36862	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36862	431999	ESTABLISHED	0	1
tcp	192.168.56.101 :36830	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36830	58	TIME_WAIT	0	1
tcp	192.168.56.101 :36852	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36852	93	TIME_WAIT	0	1
tcp	192.168.56.101 :36820	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36820	25	TIME_WAIT	0	1

Легенда: ЛВС | ИНТЕРНЕТ | Беспроводная сеть | Демилитаризованная Зона (DMZ) | IPCop | IPsec | OpenVPN

Рис. 45

Информация по соединениям представлена в виде таблицы со следующими параметрами:

1) «Протокол» – название протокола соединения;

2) «Запрос IP-адрес: Порт источника» – запрос на адрес и порт источника;

3) «Запрос IP-адрес: Порт назначения» – информация, содержащая IP-адрес и порт сетевого соединения-запроса;

4) «Ответ IP-адрес: Порт источника» – ответ на адрес и порт источника;

5) «Ответ IP-адрес: Порт назначения» – информация, содержащая IP-адрес и порт сетевого соединения-ответа;

6) «Истекает (Секунды)» – время до конца сессии;

7) «Состояние» – состояние соединения;

8) «Выделенный» – принадлежность к выделенным каналам;

9) «Использовано» – использовано на данный момент.

Под таблицей представлена легенда цветовой политики настройки сетевых интерфейсов.

4.3.6. Подраздел «Состояние интерфейсов»

Подраздел «Состояние интерфейсов» (см. рис. 46) предназначен для отображения текущего состояния сетевых интерфейсов.

Подраздел «Состояние интерфейсов»

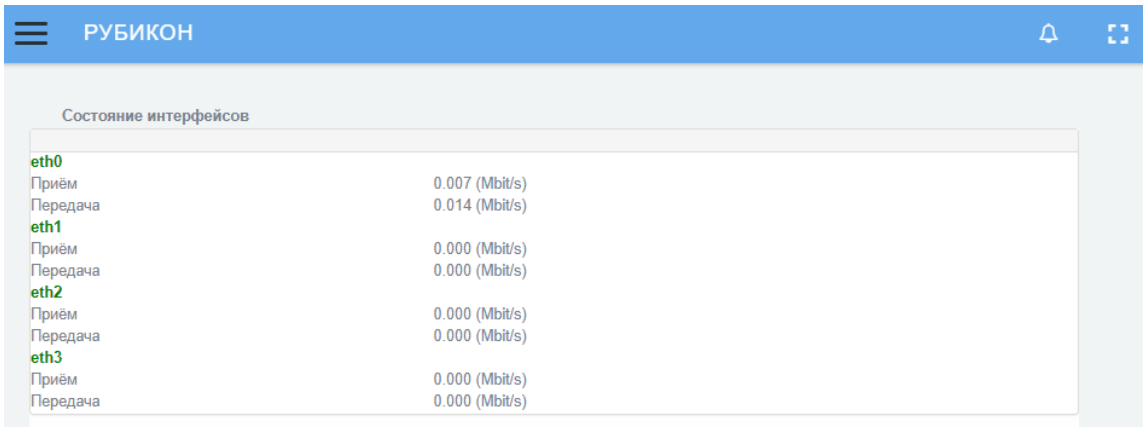

Рис. 46

Для каждого сетевого интерфейса отображается скорость приема (Mbit/s) и скорость передачи (Mbit/s).

4.3.7. Подраздел «NFTables»

Подраздел «NFTables» (см. рис. 47) предназначен для отображения информации по NFTables.

Подраздел «NFTables»

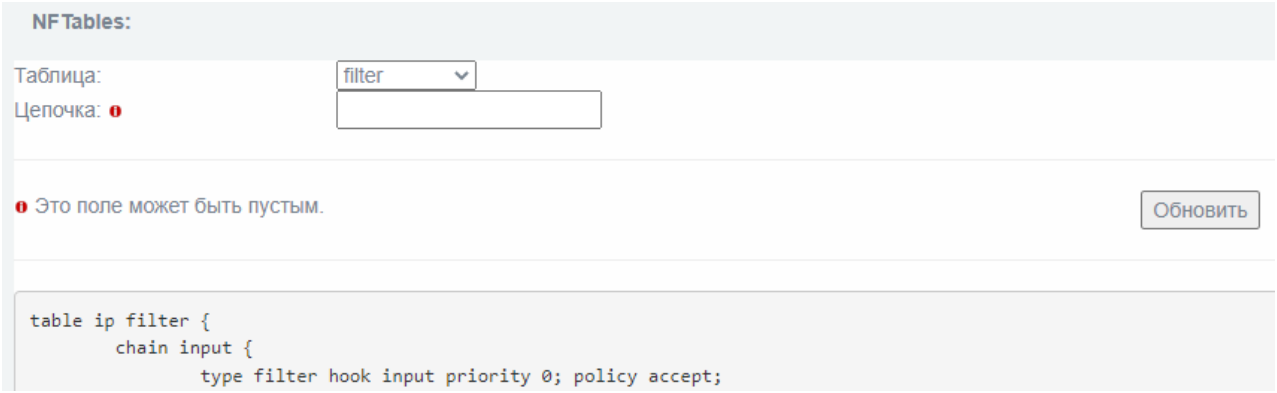

Рис. 47

Для изменения типа таблицы необходимо выбрать соответствующий тип в ниспадающем списке (см. рис. 48) и нажать кнопку «Обновить».

Выбор типа таблицы «NFTables»

Рис. 48

4.3.7.1. Виды доступных к отображению таблиц

Таблицы могут быть следующих типов:

1) «filter» – таблица, предназначена для отображения правил фильтрации по различным полям сетевого пакета (см. рис. 49);

Таблица «filter»

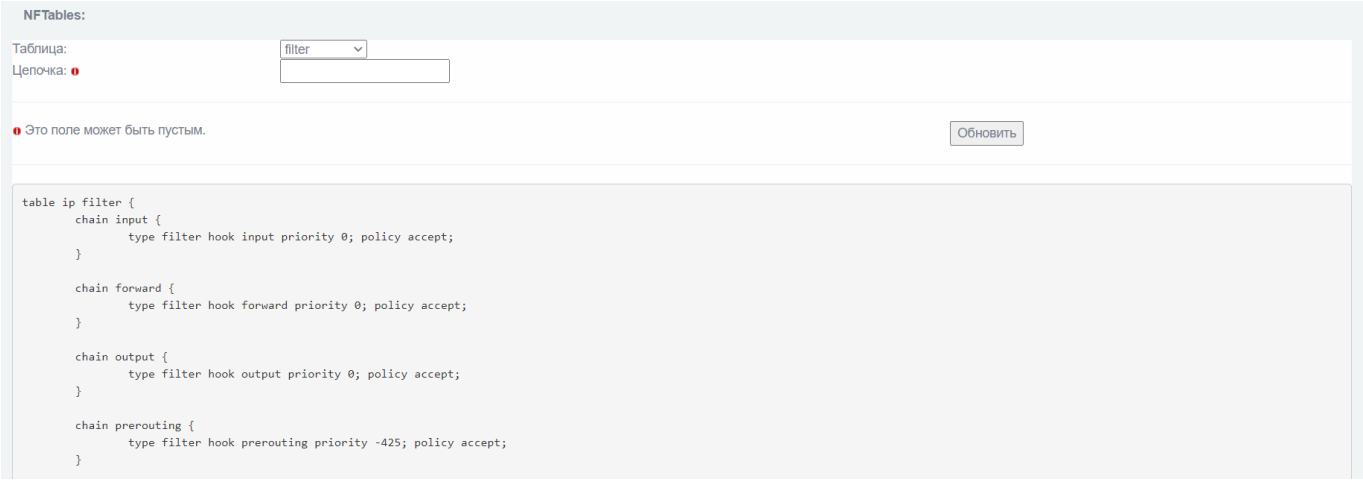

Рис. 49

2) «mangle» – таблица, предназначена для отображения правил классификации и маркировки пакетов, а также модификации заголовков TTL и TOS (см. рис. 50);

Таблица «mangle»

NFTables:

Таблица: mangle

Цепочка:

Это поле может быть пустым.

Обновить

```
table ip mangle {
        chain PREROUTING {
                type filter hook prerouting priority -150; policy accept;
                counter packets 9045 bytes 1409881 jump MANGLEMARK
                counter packets 9045 bytes 1409881 jump PROXYMANGLE
                counter packets 9045 bytes 1409881 jump PORTFWMANGLE
        }

        chain INPUT {
                type filter hook input priority -150; policy accept;
        }

        chain FORWARD {
                type filter hook forward priority -150; policy accept;
        }

        chain OUTPUT {
                type route hook output priority -150; policy accept;
        }
```

Рис. 50

3) «nat» – таблица, предназначена для отображения правил изменения полей сетевого пакета при осуществлении трансляции NAT/PAT (см. рис. 51);

Таблица «nat»

NFTables:

Таблица: nat

Цепочка:

Это поле может быть пустым.

Обновить

```
table ip nat {
        chain PREROUTING {
                type nat hook prerouting priority -100; policy accept;
                counter packets 1264 bytes 77800 jump CUSTOMPREROUTING
                counter packets 1264 bytes 77800 jump SQUID
                counter packets 1264 bytes 77800 jump PROXY
                counter packets 1264 bytes 77800 jump PORTFW
        }

        chain INPUT {
                type nat hook input priority 100; policy accept;
        }

        chain POSTROUTING {
                type nat hook postrouting priority 100; policy accept;
                counter packets 4 bytes 280 jump CUSTOMPOSTROUTING
                counter packets 4 bytes 280 jump REDNAT
                counter packets 4 bytes 280 jump PROXYNAT
                counter packets 4 bytes 280 jump PORTFWNAT
        }
```

Рис. 51

4) «raw» – таблица предназначена для отображения правил фильтрации пакетов, предназначенных для обработки системой обнаружения вторжений (см. рис. 52);

Примечание. Правила фильтрации пакетов записываются в данную таблицу при настройке правил по кнопке «СОВ» в подразделе «Межсетевой Экран» → «Правила межсетевого экрана».

Таблица «raw»

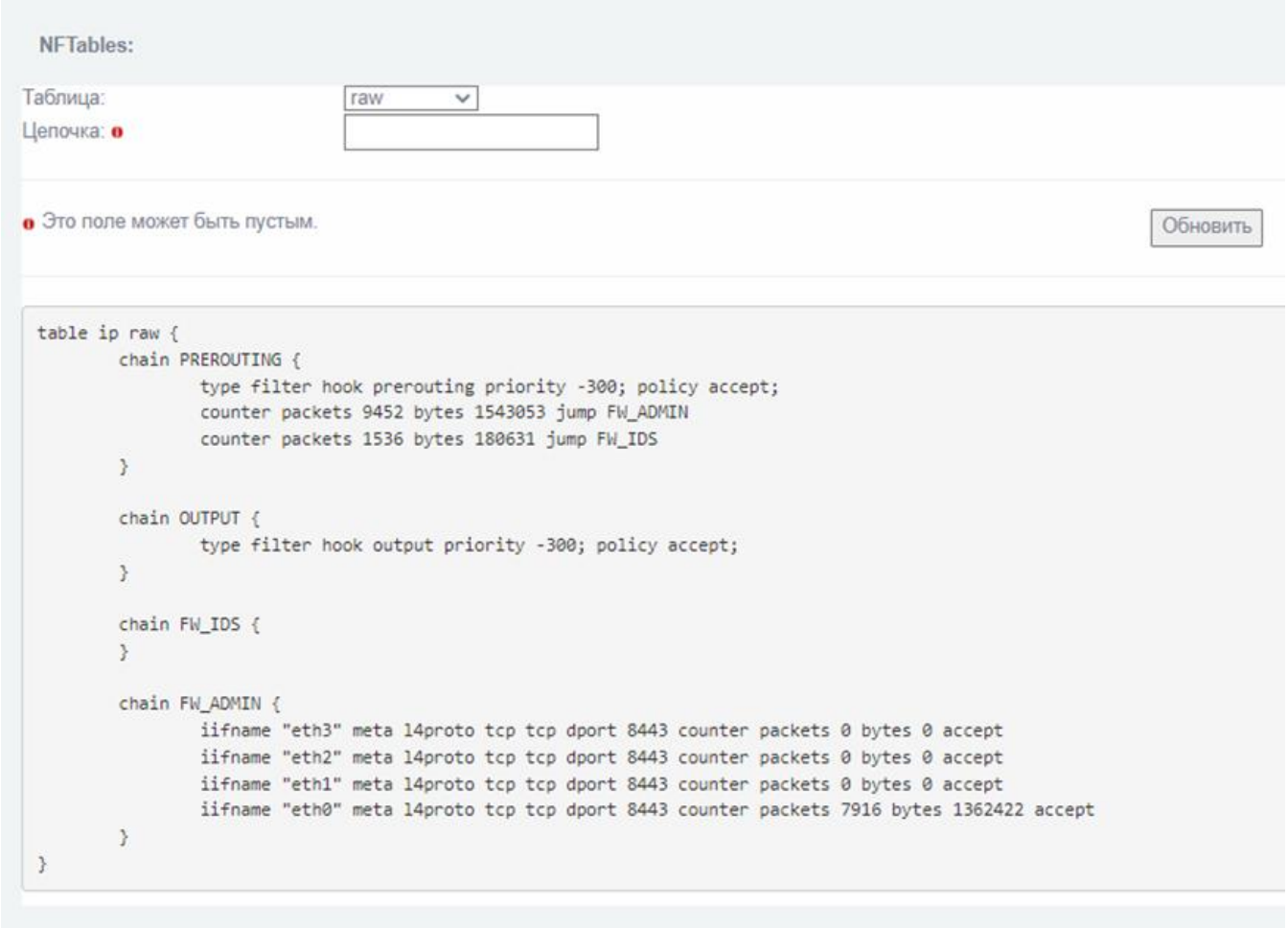

Рис. 52

5) «bridge filter» – таблица предназначена для отображения правил фильтрации сетевого пакета, выполняемых до процедуры отслеживания соединения (см. рис. 53).

Таблица «bridge filter»

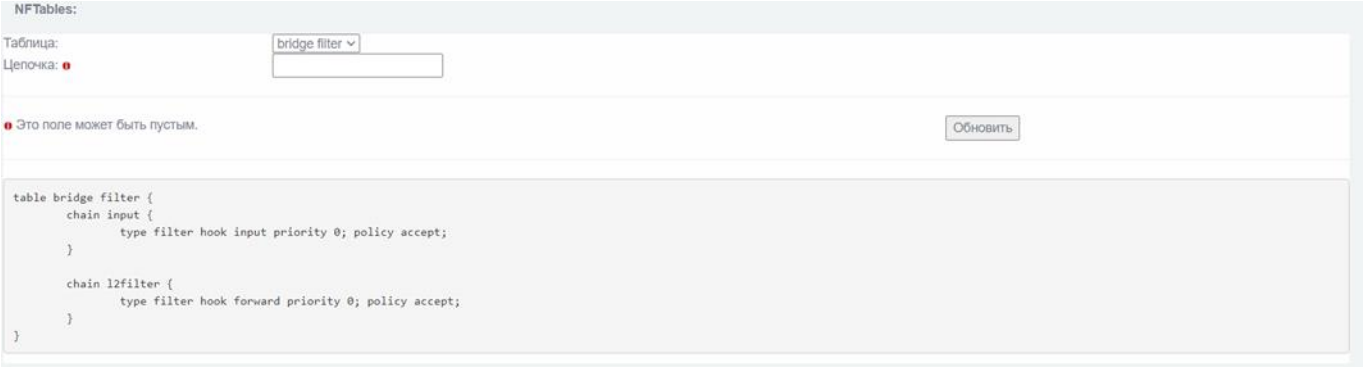

Рис. 53

4.3.7.2. Поле «Цепочка»

Поле «Цепочка» предназначено для выполнения фильтрации по конкретному параметру. Для этого необходимо ввести параметр в текстовое поле «Цепочка» и нажать кнопку «Обновить» (см. рис. 54).

Поле «Цепочка»

Рис. 54

4.3.8. Подраздел «Контрольные суммы»

Подраздел «Контрольные суммы» (см. рис. 55) предназначен для проверки контрольных сумм изделия и сопоставления этих сумм с эталонными суммами.

Подраздел «Контрольные суммы»

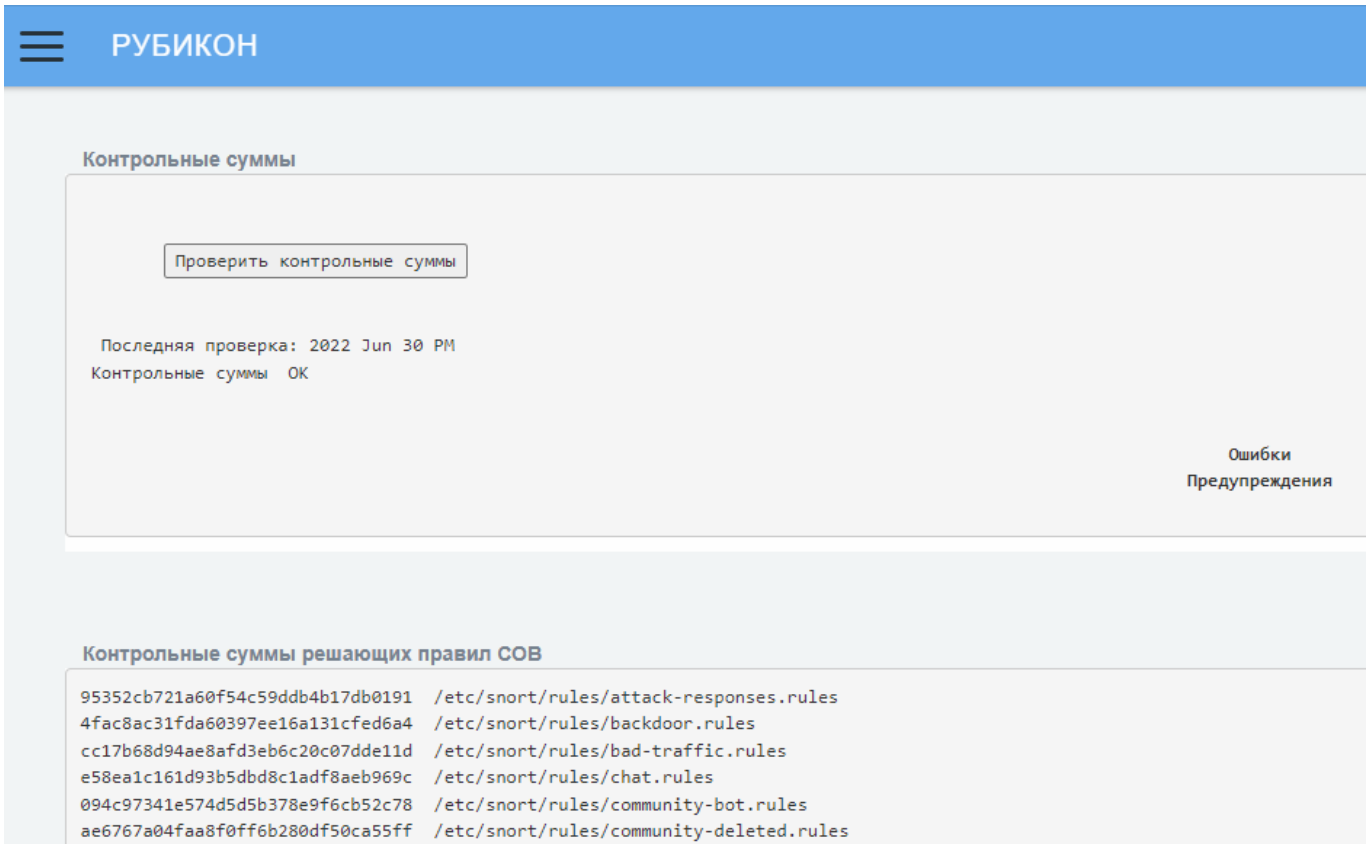

Рис. 55

Проверка контрольных сумм происходит по следующим категориям:

1) контрольные суммы решающих правил СОВ;

2) контрольная сумма файла конфигурации межсетевого экрана;

3) контрольные суммы модулей.

Результат проверки контрольных сумм отображается в виде самой контрольной суммы и адреса решающих правил.

Для начала проверки контрольных сумм необходимо нажать кнопку «Проверить контрольные суммы».

В случае успешной проверки изделие выдаст сообщение – «Контрольные суммы ОК» (см. рис. 55).

В случае возникновения неисправностей или разночтений появятся сообщения в полях «Ошибки» или «Предупреждения» (см. рис. 56).

Поля «Ошибки» и «Предупреждения»

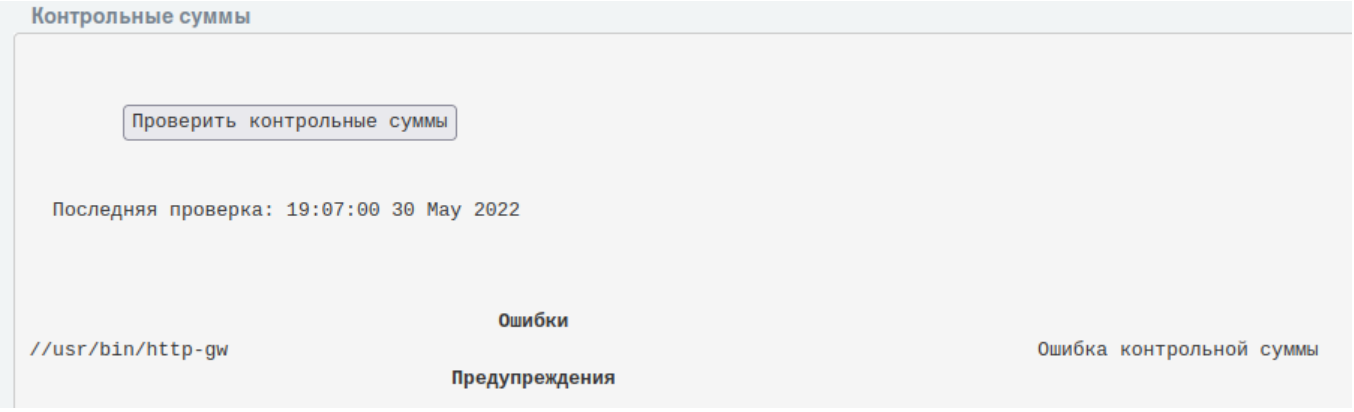

Рис. 56

4.4. Раздел «Сеть»

Раздел «Сеть» содержит следующие подразделы:

1) «Псевдонимы»;

2) «Горячее резервирование CARP»;

3) «Настройка адаптеров»;

4) «Маршруты»;

5) «Конфигурация ARP»;

6) «OSPF»;

7) «BGP»;

8) «VLANs»;

9) «Мосты»;

10) «Объединение интерфейсов».

4.4.1. Подраздел «Псевдонимы»

Подраздел «Псевдонимы» (см. рис. 57) предназначен для задания псевдонимов сетевых адресов. Данная возможность применяется для назначения нескольких сетевых псевдонимов для разделения внутренних ресурсов по сетевому адресу.

Подраздел «Псевдонимы»

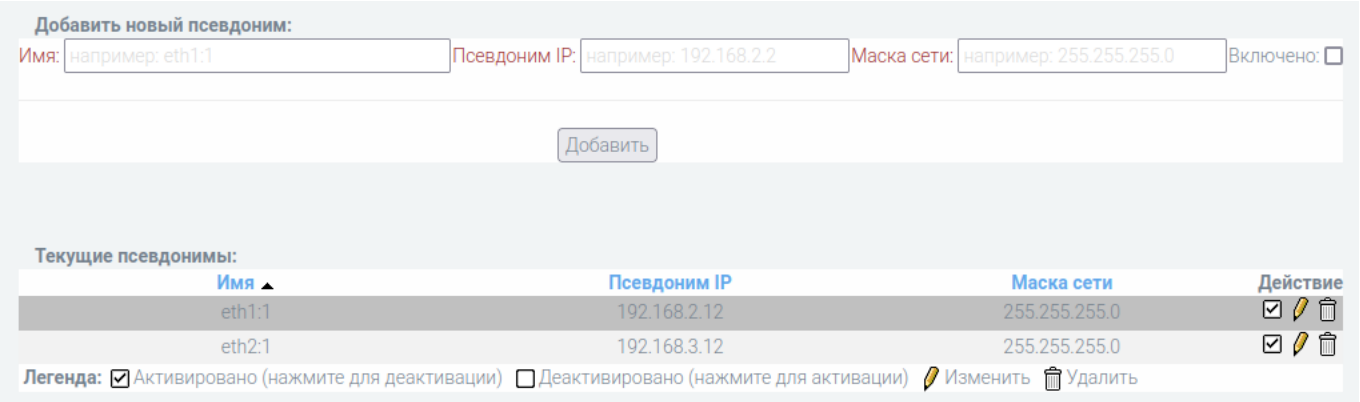

Рис. 57

В таблице 13 приведено описание элементов подраздела «Псевдонимы».

Таблица 13 – Описание элементов подраздела «Псевдонимы»

Элемент	Описание
Поле «Имя»	Предназначено для указания имени псевдонима сетевого адреса
Поле «Псевдоним IP»	Предназначено для указания адреса псевдонима
Поле «Маска сети»	Предназначено для указания маски сети
Чекбокс «Включено»	Предназначен для включения/отключения данного псевдонима
Кнопка «Добавить»	Предназначена для сохранения настроек псевдонима сетевого адреса
Кнопка « Имя »	Заголовок с возможностью включения сортировки в колонке таблицы
Таблица «Текущие псевдонимы»	Предназначена для отображения списка псевдонимов сетевых интерфейсов
Чекбокс «Действие»	Предназначен для выбора определенного псевдонима
Кнопка « »	Кнопка «Изменить». Предназначена для изменения выбранного псевдонима
Кнопка « »	Кнопка «Удалить». Предназначена для удаления выбранного псевдонима

Информация о списке псевдонимов сетевых интерфейсов представлена в виде таблицы «Текущие псевдонимы» со следующими параметрами:

1) «Имя»;

2) «Псевдоним IP»;

3) «Маска сети»;

4) «Действие».

Параметр «Действие» позволяет редактировать или удалить выбранный псевдоним в таблице «Текущие псевдонимы».

Под таблицей представлена легенда всех возможных действий с псевдонимами.

4.4.2. Подраздел «Горячее резервирование CARP (VRRP)»

Подраздел «Горячее резервирование CARP (VRRP)» (см. рис. 58) предназначен для установки параметров специального режима резервирования, предусматривающий наличие двух устройств, которые, за исключением сетевых интерфейсов, настроены одинаково (правила, маршруты, туннели и т. п.). При этом одно из устройств находится в активном рабочем состоянии, а второе в резервном. Активное устройство периодически оповещает резервное о своем статусе. В случае если активное устройство выходит из строя и перестает отправлять оповещения, резервное устройство принимает функции активного. Передача информации по сети через комплекс «Рубикон» восстанавливается. Когда вышедшее из строя устройство вновь оказывается в рабочем состоянии, то оно отправляет сообщение активному резервному о своей работоспособности. Резервное устройство снова переходит в пассивный режим ожидания.

Примечание. Для осуществления функции горячего резервирования используется протокол резервирования CARP (созданный на основе протокола VRRP (RFC 2281, RFC 3768)).

Подраздел «Горячее резервирование CARP (VRRP)»

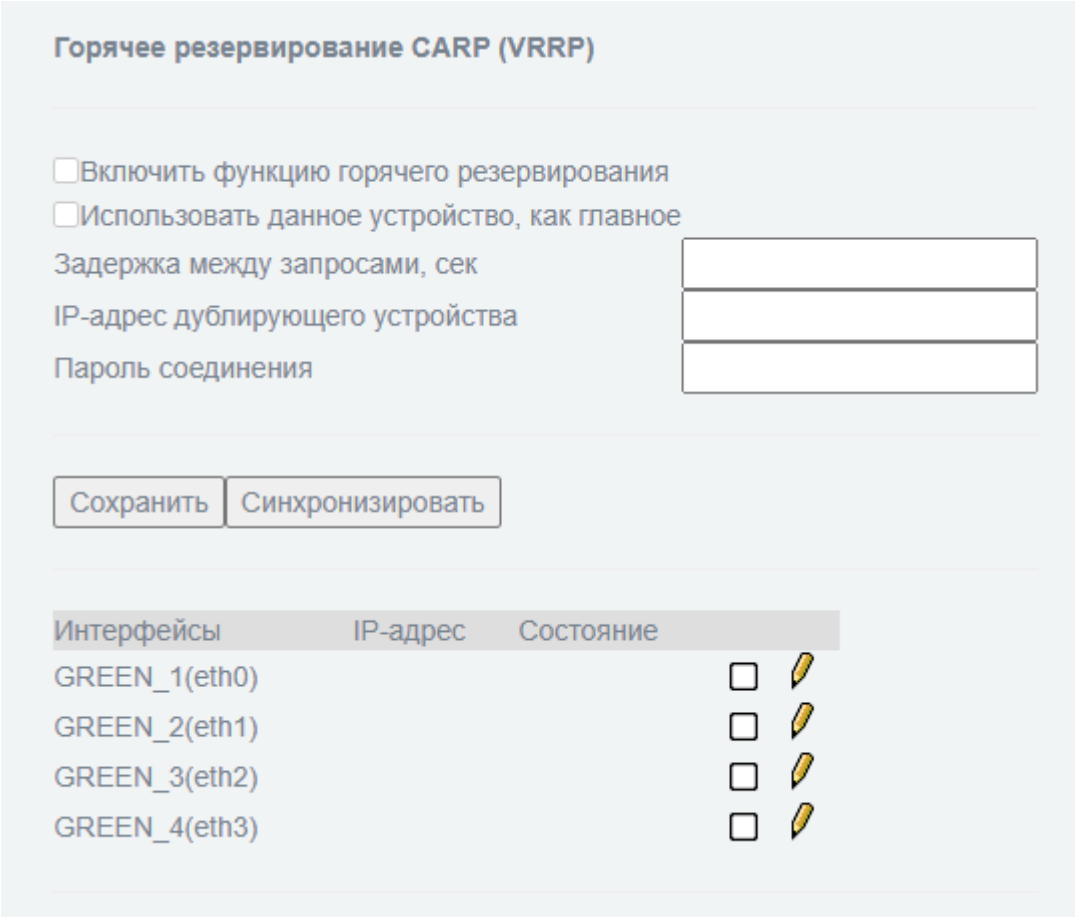

Рис. 58

В таблице 13 приведено описание элементов подраздела «Горячее резервирование CARP (VRRP)».

Таблица 14 – Описание элементов подраздела «Горячее резервирование CARP (VRRP)»

Элемент	Описание
Чекбокс «Включить функцию горячего резервирования»	Предназначен для включения функции горячего резервирования
Чекбокс «Использовать данное устройство, как главное»	Предназначен для включения/отключения использования изделия в качестве главного устройства
Поле «Задержка между запросами, сек»	Предназначено для ввода задержки между запросами об активности изделия
Поле «IP-адрес дублирующего устройства»	Предназначено для указания IP-адреса устройства, которое находится в резерве. По указанному адресу будет осуществляться синхронизация устройств

Элемент	Описание
Поле «Пароль соединения»	Предназначено для ввода пароля соединения
Кнопка «Сохранить»	Предназначена для сохранения установленных параметров функции горячего резервирования
Кнопка «Синхронизировать»	Предназначена для обновления данных в подразделе
Таблица «Перечень интерфейсов»	Предназначена для включения интерфейсов в список резервируемых, а также отображения информации о настроенных интерфейсах. Отображается виртуальный адрес и текущее состояние интерфейса
Чекбокс «Состояние интерфейса»	Предназначен для индикации состояния (ВКЛ/ВЫКЛ) сервиса резервирования указанного интерфейса. Если стоит галочка, указанный интерфейс будет резервироваться в случае отказа устройства
Кнопка « »	Кнопка «Изменить». Предназначена для перехода па страницу редактирования параметров резервирования выбранного интерфейса

Информация в таблице «Перечень интерфейсов» представлена со следующими параметрами:

1) «Интерфейсы»;

2) «IP-адрес»;

3) «Состояние».

После нажатия на кнопку «Изменить» откроется меню редактирования интерфейса (см. рис. 59). Данный блок позволяет добавить виртуальный IP-адрес резервируемого интерфейса и активировать его, выбрав чекбокс «Включить виртуальный ip-адрес».

Для применения новой настройки необходимо нажать кнопку «Сохранить».

Меню редактирования интерфейса

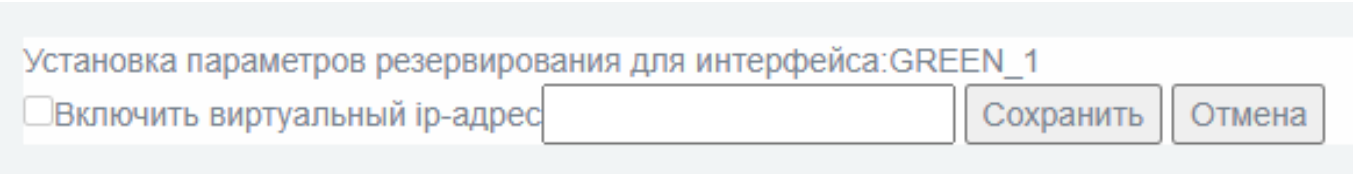

Рис. 59

4.4.3. Подраздел «Настройка адаптеров»

Подраздел «Настройка адаптеров» (см. рис. 60) предназначен для присвоения цветов существующим **физическим сетевым интерфейсам** (адаптерам) в соответствии с цветовой политикой, подробно описанной в подразделе «Настройка межсетевого экрана» руководства администратора НПЕШ.465614.005РА.

Подраздел «Настройка адаптеров»

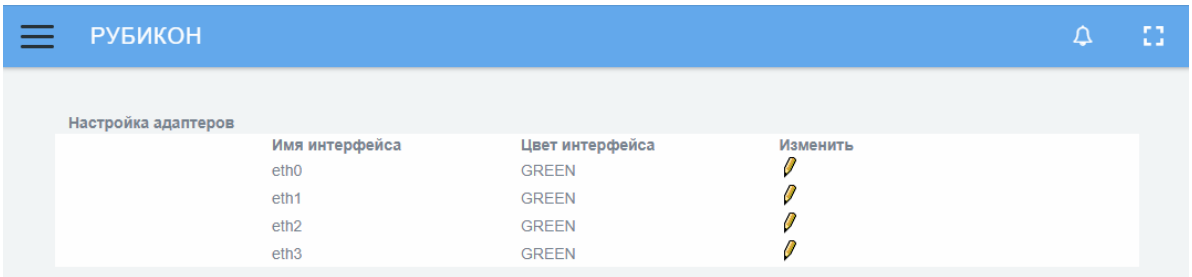

Рис. 60

Информация в таблице «Настройка адаптеров» представлена со следующими параметрами:

1) «Имя интерфейса»;

2) «Цвет интерфейса»;

3) кнопка «Изменить».

Кнопка «Изменить» ( ) позволяет редактировать выбранный адаптер в таблице «Настройка адаптеров» (см. рис. 61).

Редактирование таблицы «Настройка адаптера»

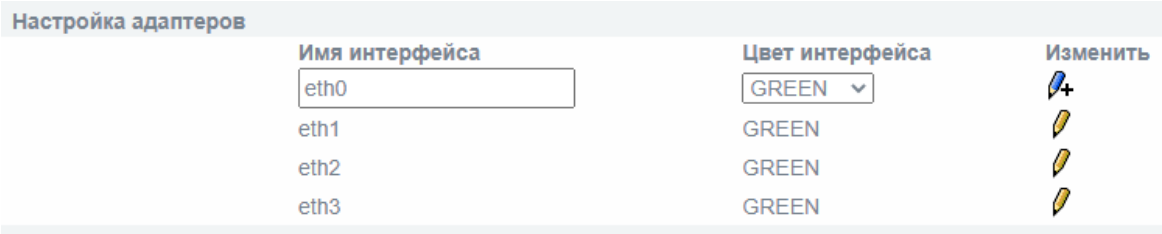

Рис. 61

Доступен к изменению параметр «Имя интерфейса» (в форме поля для ввода) и «Цвет интерфейса» (в форме выпадающего списка).

Для сохранения изменений настроек каждого адаптера необходимо нажимать кнопку «Сохранить» ( ).

4.4.4. Подраздел «Маршруты»

Подраздел «Маршруты» (см. рис. 62) предназначен для внесения элементов в таблицу маршрутизации изделия.

Подраздел «Маршруты»

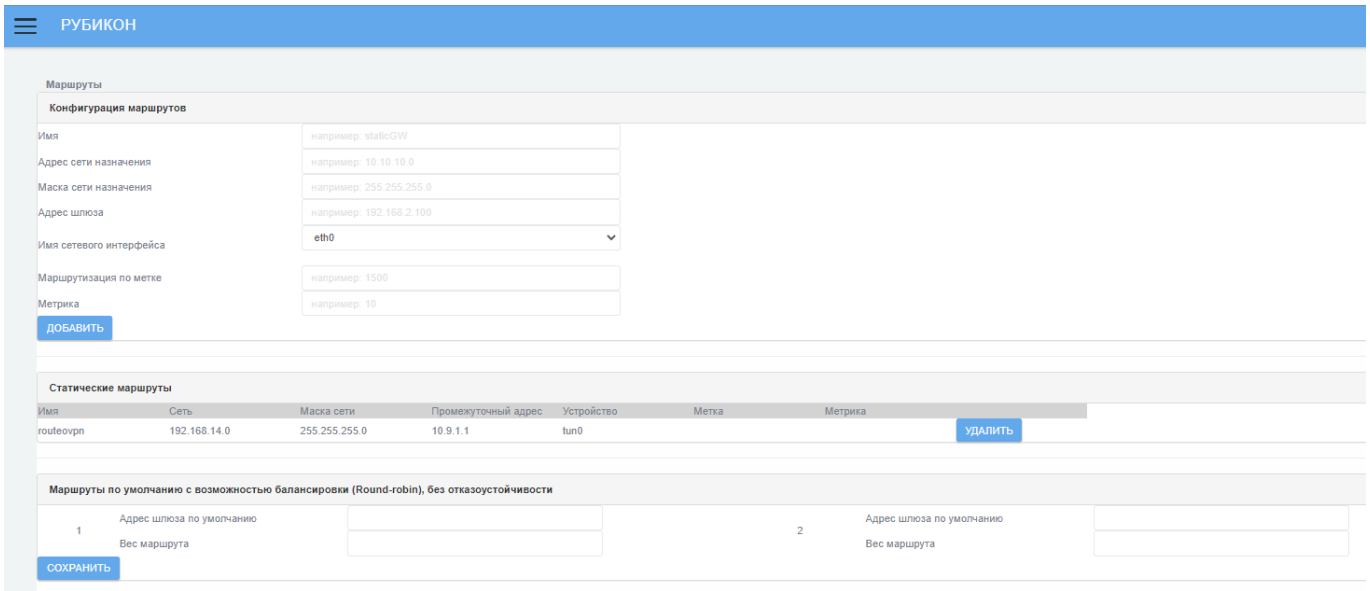

Рис. 62

В таблице 15 приведено описание элементов подраздела «Маршруты».

Таблица 15 – Описание элементов подраздела «Маршруты»

Элемент	Описание
Конфигурация маршрутов	
Поле «Имя»	Предназначено для указания имени сетевого маршрута. Имя должно состоять из латинских букв и цифр. Оно предназначено для удобства администратора и не влияет на работу межсетевого экрана (далее – МЭ)
Поле «Адрес сети назначения»	Предназначено для указания маршрутизируемой сети

Элемент	Описание
Поле «Маска сети назначения»	Предназначено для указания маски маршрутизируемой сети. Маска задается в полном десятичном виде
Поле «Адрес шлюза»	Предназначено для указания сетевого адреса первого шлюза, через который будет проложен маршрут
Выпадающий список «Имя сетевого интерфейса»	Предназначен для указания имени сетевого устройства, через которое будет проложен маршрут
Поле «Маршрутизация по метке»	Предназначено для указания метки, присваиваемой пакету межсетевым экраном для маршрутизации, управляемой межсетевым экраном
Поле «Метрика»	Предназначено для указания числового значения, влияющего на выбор маршрута в компьютерных сетях
Кнопка «Добавить»	Добавляет (сохраняет) указанные конфигурации в блоке
Статические маршруты	
Таблица «Статические маршруты»	Предназначена для отображения информации о таблице маршрутизации изделия
Кнопка «Удалить»	Предназначена для удаления выбранного маршрута из перечня статических маршрутов
Маршруты по умолчанию с возможностью балансировки (Round-robin), без отказоустойчивости	
Поле подблока 1 и 2 «Адрес шлюза по умолчанию»	Предназначено для ввода IP-адреса шлюза, используемого по умолчанию
Поле подблока 1 и 2 «Вес маршрута»	Предназначено для указания веса (приоритета выбора) маршрута
Примечание. При заполнении полей 1 «Адрес шлюза по умолчанию» и 2 «Адрес шлюза по умолчанию» необходимо заполнять поля 1 «Вес маршрута» и 2 «Вес маршрута». При заполнении только 1 адреса шлюза по умолчанию – вес маршрута указывать не следует.	

Таблица «Статические маршруты» с перечнем статических маршрутов представлена в блоке «Статические маршруты» (см. рис. 63).

Блок «Статические маршруты»

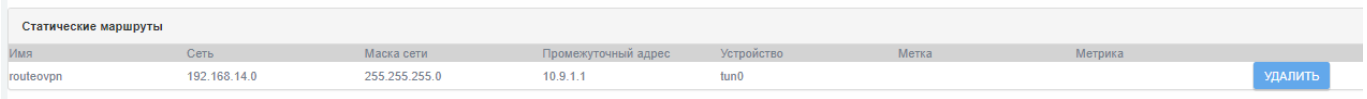

Рис. 63

Информация в таблице «Статические маршруты» представлена со следующими параметрами:

1) «Имя»;

2) «Сеть»;

3) «Маска сети»;

4) «Промежуточный адрес»;

5) «Устройство»;

6) «Метка»;

7) «Метрика».

Блок «Маршруты по умолчанию с возможностью балансировки (Round-robin), без отказоустойчивости» содержит описание маршрута, установленного по умолчанию (см. рис. 64).

Блок «Маршруты по умолчанию с возможностью балансировки (Round-robin), без отказоустойчивости»

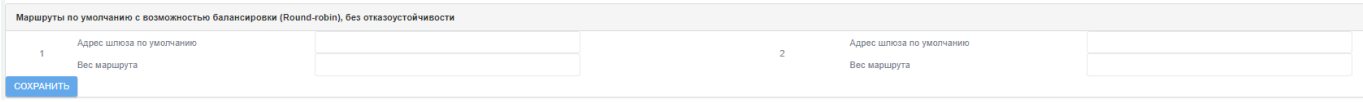

Рис. 64

4.4.5. Подраздел «Конфигурация ARP»

Подраздел «Конфигурация ARP» предназначен для конфигурации протокола ARP для определения MAC-адреса по известному IP-адресу (см. рис. 65).

Подраздел «Конфигурация ARP»

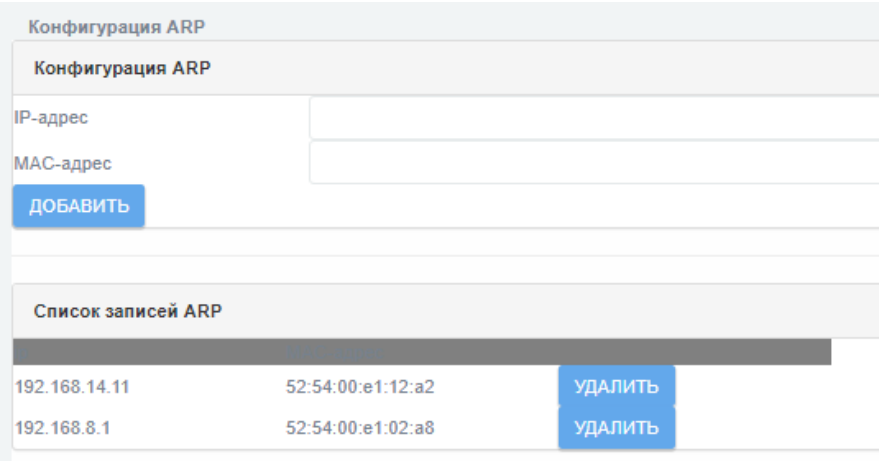

Рис. 65

В таблице 16 приведено описание элементов подраздела «Конфигурация ARP».

Таблица 16 – Описание элементов подраздела «Конфигурация ARP»

Элемент	Описание
Конфигурация ARP	
Поле «IP-адрес»	Предназначено для ввода IP-адреса
Поле «MAC-адрес»	Предназначено для ввода MAC-адреса
Кнопка «Добавить»	Предназначена для внесения записи о соответствии MAC-адреса и IP-адреса в таблицу ARP. После нажатия данной кнопки конфигурация ARP отображается в виде списка в нижней части окна (см. рис. 65)
Список записей ARP	
Таблица «Список записей ARP»	Предназначена для отображения пользовательских записей в ARP-таблице изделия
Кнопка «Удалить»	Предназначена для удаления выбранной пользовательской записи

Наличие записей в таблице ARP можно увидеть, перейдя на вкладку «Состояние» → «Состояние сети». В блоке информации «ARP таблица» отображаются соответствующие записи-сопоставления. Добавленная на вкладке «Сеть» → «Конфигурация ARP» запись элемента таблицы маркируется дополнительно флагом «M». Это показывает, что запись добавлена на постоянной основе (см. рис. 66).

Примечание. В случае ошибочного ввода параметров будет выдано сообщение о невозможности создания требуемой ARP-записи в таблице.

Блок информации «ARP таблица»

Address	HWtype	HWaddress	Flags Mask	Iface
192.168.1.25	ether	00:43:ab:cd:37:a0	CM	eth0
192.168.1.24		(incomplete)		eth0
192.168.1.101	ether	0a:00:27:00:00:00	C	eth0

Рис. 66

4.4.6. Подраздел «OSPF»

Подраздел «OSPF» (см. рис. 67) предназначен для управления службой динамической маршрутизации по протоколу OSPF.

Подраздел «OSPF»

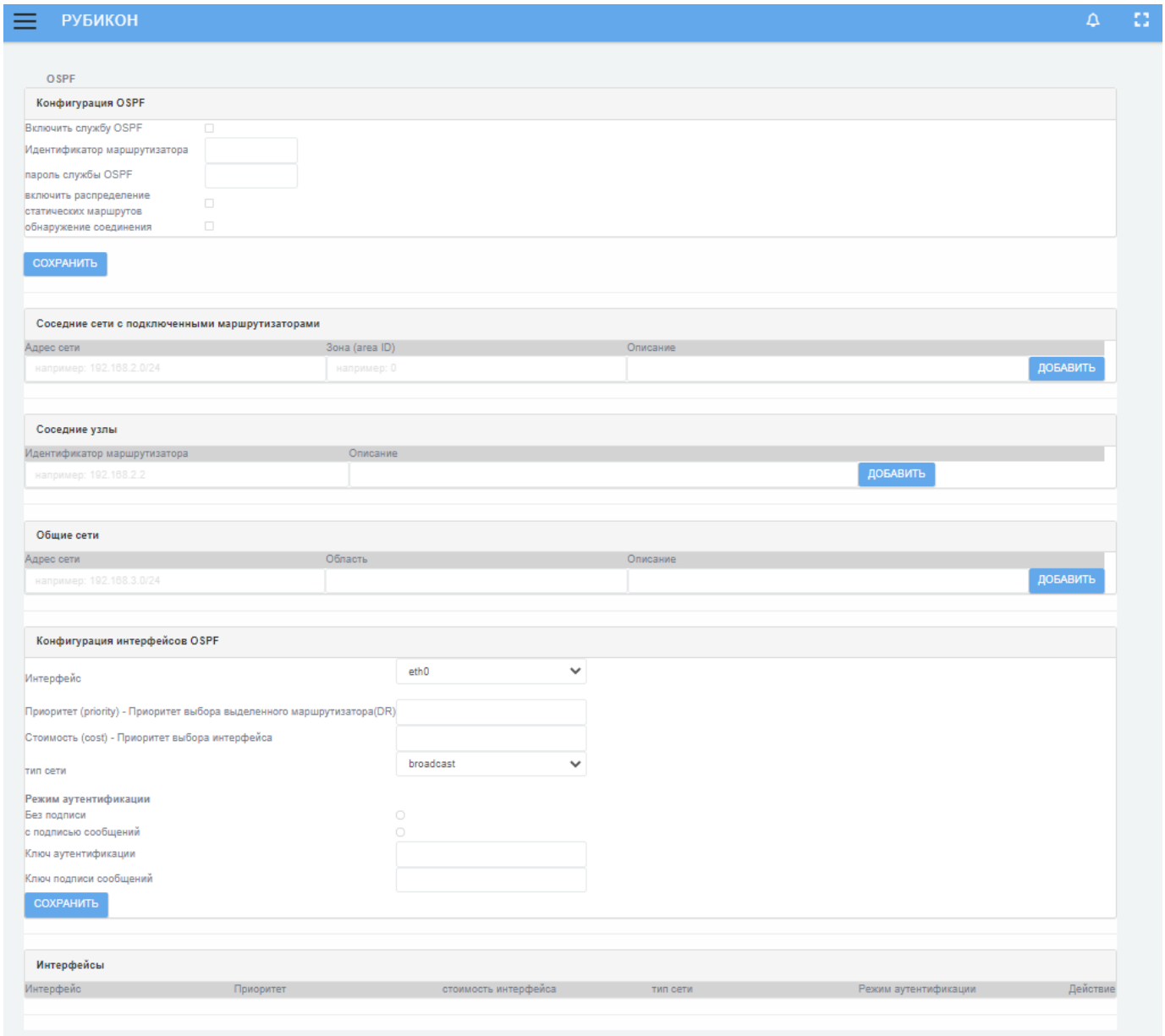

Рис. 67

Подраздел «OSPF» состоит из следующих блоков:

1) «Конфигурация OSPF» – задание параметров устройства (основного узла) в автономной системе OSPF;

2) «Соседние сети с подключенными маршрутизаторами» – задание сетей, в которые будут передаваться анонсы о маршрутах;

3) «Соседние узлы» – задание параметров соседних маршрутизаторов OSPF для взаимодействия с ними и вычисления эффективных маршрутов;

4) «Общие сети» – сети, информация о которых анонсируется по протоколу OSPF;

5) «Конфигурация интерфейсов OSPF» – настройка сетевых интерфейсов устройства, используемых для взаимодействия по протоколу OSPF;

6) «Интерфейсы» – сетевые интерфейсы, через которые будет производиться оповещение других узлов.

4.4.6.1. Блок «Конфигурация OSPF»

В таблице 17 приведено описание элементов блока «Конфигурация OSPF».

Таблица 17 – Описание элементов подраздела «Конфигурация OSPF»

Элемент	Описание
Чекбокс «Включить службу OSPF»	Предназначен для включения/отключения службы OSPF
Поле «Идентификатор маршрутизатора»	Предназначено для указания идентификатора маршрутизатора OSPF. Идентификатор маршрутизатора – идентификатор в сети, однозначно определяющих маршрутизатор OSPF. Допустимо в качестве идентификатора использовать корректный IP-адрес в формате последовательности четырех десятичных чисел, разделенных точками. Обычно, в качестве идентификатора используется наибольший IP-адрес среди интерфейсов маршрутизатора
Поле «Пароль службы OSPF»	Предназначено для указания пароля службы OSPF
Чекбокс «Включить распределение статических маршрутов»	Предназначен для включения/отключения распределения статических маршрутов
Чекбокс «Обнаружение соединения»	Предназначен включения/отключения использования режима отслеживания связи при работе службы OSPF

4.4.6.2. Блок «Соседние сети с подключенными маршрутизаторами»

Блок «Соседние сети с подключенными маршрутизаторами» представлен в виде полей для ввода, образующих таблицу, которая содержит список всех доступных сетей.

Таблица представлена со следующими доступными полями для ввода:

1) «Адрес сети» – предназначено для ввода IP-адреса сети;

2) «Зона (area ID)» – предназначено для ввода идентификатора зоны. Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса;

3) «Описание» – предназначено для ввода краткого описания сети.

Для добавления новой сети с введенными параметрами необходимо после заполнения полей таблицы нажать кнопку «Добавить».

4.4.6.3. Блок «Соседние узлы»

Блок «Соседние узлы» представлен в виде полей для ввода, образующих таблицу, которая содержит список всех доступных узлов.

Таблица представлена со следующими доступными полями для ввода:

1) «Идентификатор маршрутизатора» – предназначено для ввода IP-адреса маршрутизатора;

2) «Описание» – предназначено для ввода краткого описания узла сети.

Для добавления нового узла сети с введенными параметрами необходимо после заполнения полей таблицы нажать кнопку «Добавить».

4.4.6.4. Блок «Общие сети»

Блок «Общие сети» представлен в виде полей для ввода, образующих таблицу, которая содержит список всех общих сетей.

Таблица представлена со следующими доступными полями для ввода:

1) «Адрес сети» – предназначено для ввода IP-адреса сети;

2) «Область» – предназначено для ввода идентификатора зоны. Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса;

3) «Описание» – предназначено для ввода краткого описания сети.

Для добавления новой сети с введенными параметрами необходимо после заполнения полей таблицы нажать кнопку «Добавить».

4.4.6.5. Блок «Конфигурация интерфейсов OSPF»

Блок «Конфигурация интерфейсов OSPF» (см. рис. 68) содержит список всех интерфейсов.

Блок «Конфигурация интерфейсов OSPF»

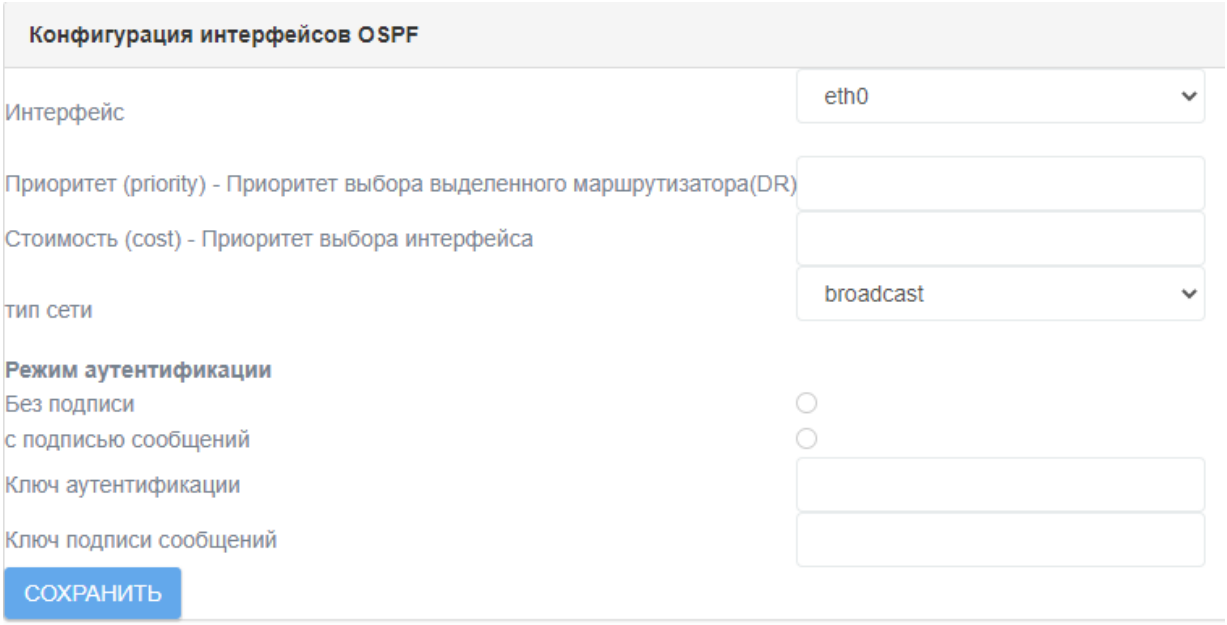

Рис. 68

В таблице 18 приведено описание элементов блока «Конфигурация интерфейсов OSPF».

Таблица 18 – Описание элементов блока «Конфигурация интерфейсов OSPF»

Элемент	Описание
Выпадающий список «Интерфейс»	Предназначен для выбора интерфейса для использования по протоколу OSPF

Элемент	Описание
Поле «Приоритет (priority) - Приоритет выбора выделенного маршрутизатора (DR)»	Предназначен для ввода номера приоритета выбора выделенного маршрутизатора. Диапазон значений: от 1 до 254
Поле «Стоимость (cost) - Приоритет выбора интерфейса»	Предназначен для ввода параметра определяющего предпочтения по прохождению трафика. В алгоритме OSPF предусматривается показатель стоимости использования маршрута через данный интерфейс. При сравнении двух маршрутов, будет выбран тот, для которого суммарная стоимость будет меньше. При этом не обязательно, что на данном маршрутизаторе лучший маршрут будет проходить через интерфейс с минимальной стоимостью. Допустимы целочисленные значения от 1 до 65535
Выпадающий список «Тип сети»	Предназначен для выбора одного из следующих параметров: – broadcast; – non-broadcast; – point-to-multipoint; – point-to-point
Режим аутентификации	
Чекбокс «Без подписи»	Предназначен для выбора метода аутентификации «Без подписи». Значение «Без подписи» устанавливается в случае отсутствия аутентификации
Чекбокс «С подписью сообщений»	Предназначен для выбора метода аутентификации «С подписью сообщений». Используется в случае аутентификации на основе MD5 HMAC. В случае выбора данного режима аутентификации необходимо задавать также параметр «Ключ подписи сообщений»
Поле «Ключ аутентификации»	Предназначено для ввода ключа, используемого для осуществления парольной аутентификации. Допустимыми значениями являются строки алфавитно-цифровых символов (латинский алфавит и цифры 0-9) длиной до 8 символов
Поле «Ключ подписи сообщений»	Предназначено для ввода ключа, используемого для защиты сообщений с помощью алгоритма MD5 HMAC. Допустимыми значениями являются строки алфавитно-цифровых символов (латинский алфавит и цифры 0-9) длиной не более 16 символов
Кнопка «Сохранить»	Предназначена для сохранения введенных изменений в конфигурации

4.4.6.6. Блок «Интерфейсы»

Таблица «Интерфейсы» с перечнем всех добавленных в данном подразделе интерфейсов представлена в блоке «Интерфейсы» (см. рис. 69).

Блок «Интерфейсы»

Интерфейсы

Интерфейс	Приоритет	стоимость интерфейса	тип сети	Режим аутентификации	Действие
eth3	5	20	non-broadcast	Без подписи	

Рис. 69

Информация в таблице «Интерфейсы» представлена со следующими параметрами:

1) «Интерфейс»;

2) «Приоритет»;

3) «Стоимость интерфейса»;

4) «Тип сети»;

5) «Режим аутентификации»;

6) «Действие».

В столбце «Действие» информационной таблицы «Интерфейсы» нажатие на кнопку «Удалить» ( ) позволяет удалить выбранный интерфейс.

4.4.7. Подраздел «BGP»

Подраздел «BGP» (см. рис. 70) предназначен для управления службой динамической маршрутизации по протоколу BGP.

Подраздел настройки службы динамической маршрутизации по протоколу BGP состоит из трех блоков:

1) «Конфигурация BGP» – задание параметров узла в автономной системе BGP;

2) «Общие сети» – назначение сетей, которые будут анонсироваться соседним узлам-маршрутизаторам BGP;

3) «Соседние узлы» – задание параметров соседних маршрутизаторов BGP для взаимодействия с ними и вычисления эффективных маршрутов.

Подраздел «BGP»

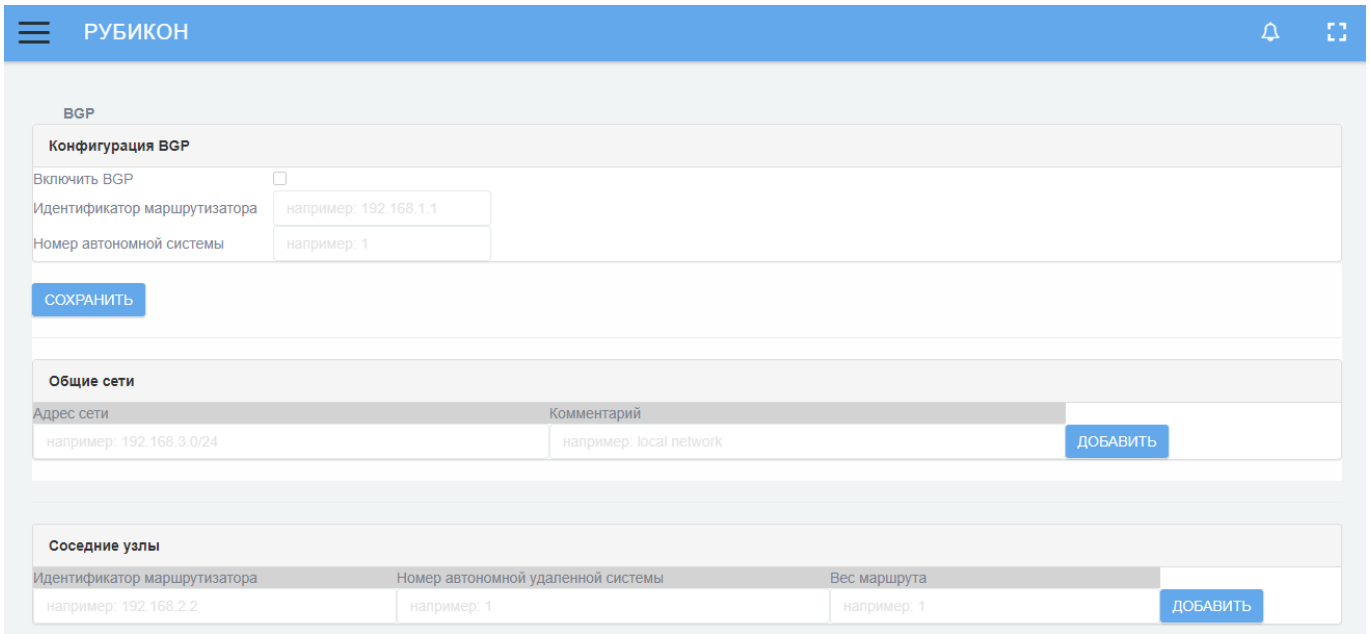

Рис. 70

4.4.7.1. Блок «Конфигурация BGP»

В таблице 19 приведено описание элементов подраздела «Конфигурация BGP».

Таблица 19 – Описание элементов подраздела «Конфигурация BGP»

Элемент	Описание
Чекбокс «Включить BGP»	Предназначен для включения/выключения службы BGP
Поле «Идентификатор маршрутизатора»	Предназначено для ввода идентификатора маршрутизатора BGP. Допустимо в качестве идентификатора использовать корректный IP-адрес в формате последовательности четырех десятичных чисел, разделенных точками. Обычно, в качестве идентификатора используется наибольший IP-адрес среди интерфейсов маршрутизатора
Поле «Номер автономной системы»	Предназначено для ввода номера автономной системы, которой принадлежит маршрутизатор (диапазон возможных значений равен 1 – 65535: для публичных номеров используется диапазон 1 – 64495, для приватных 64512 – 65535)
Кнопка «Сохранить»	Предназначена для сохранения внесенных изменений

4.4.7.2. Блок «Общие сети»

Блок «Общие сети» представлен в виде полей для ввода, образующих таблицу, которая содержит список всех добавленных в данном подразделе сетей.

Таблица представлена со следующими доступными полями для ввода:

1) «Адрес сети» – предназначено для ввода IP-адреса сети, маршрутная информация о которой будет распространяться;

2) «Комментарий» – предназначено для ввода описания сети.

Для добавления новой сети с введенными параметрами необходимо после корректного заполнения полей таблицы нажать кнопку «Добавить».

Добавленная сеть будет отображена в данной таблице (см. рис. 71), где вместо кнопки «Добавить» будет доступна кнопка «Удалить» ( ), нажатие которой позволит удалить добавленную ранее сеть.

Блок «Общие сети»

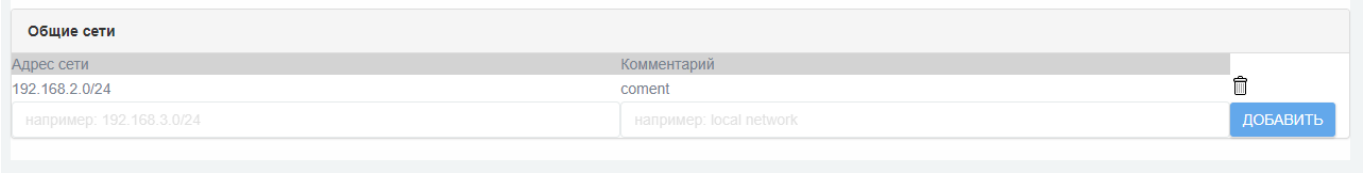

Рис. 71

4.4.7.3. Блок «Соседние узлы»

Блок «Соседние узлы» представлен в виде полей для ввода, образующих таблицу, которая содержит список всех добавленных в данном подразделе узлов.

Таблица представлена со следующими доступными полями для ввода:

1) «Идентификатор маршрутизатора» – предназначено для ввода идентификатора маршрутизатора, которому будут передаваться сообщения о маршрутах по протоколу BGP. Допустимо в качестве идентификатора использовать корректный IP-адрес в формате последовательности четырех десятичных чисел, разделенных точками. В общем случае в качестве идентификатора используется наибольший IP-адрес среди интерфейсов маршрутизатора;

2) «Номер автономной удаленной системы» – предназначено для ввода области, которой принадлежит соседний маршрутизатор BGP. Допустимы значения: от 1 до 65535. При этом значения от 64512 до 65535 считаются частными и не должны анонсироваться в глобальную сеть;

3) «Вес маршрута» – предназначено для ввода приоритета для маршрута. Вес маршрута – показатель, определяющий приоритет выбора маршрута через настраиваемый соседний маршрутизатор BGP. Чем выше вес маршрута, тем более предпочтительным является маршрут через данный соседний узел. Допустимыми значениями являются целые числа в диапазоне от 0 до 65535.

Для добавления нового узла с введенными параметрами необходимо после корректного заполнения полей таблицы нажать кнопку «Добавить».

Добавленный узел будет отображен в данной таблице, где вместо кнопки «Добавить» будет доступна кнопка «Удалить», нажатие которой позволит удалить добавленный ранее узел.

Примечание. В случае ввода и применения некорректных параметров, выводится сообщение об ошибке (см. рис. 72).

Сообщение об ошибке блока «Соседние узлы»

Рис. 72

4.4.8. Подраздел «VLANs»

Подраздел «VLANs» (см. рис. 73) предназначен для создания виртуальных локальных сетей (VLAN).

Подраздел «VLANs»

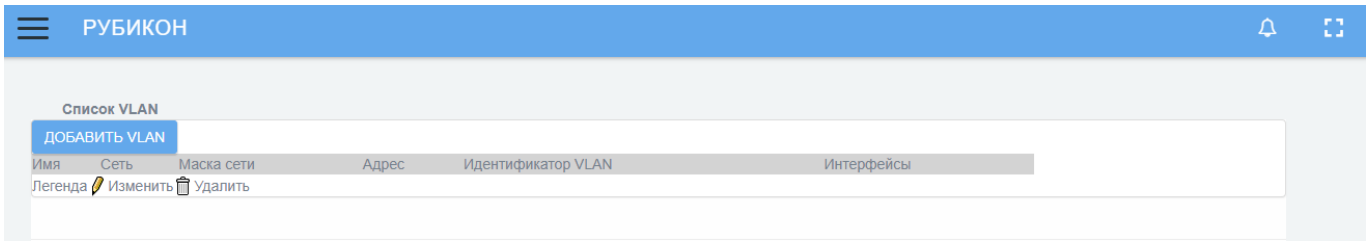

Рис. 73

Информация о перечне виртуальных сетевых интерфейсов представлена в виде таблицы «Список VLAN» со следующими параметрами:

1) «Имя»;

2) «Сеть»;

3) «Маска сети»;

4) «Адрес»;

5) «Идентификатор VLAN»;

6) «Интерфейсы».

Кнопка «Изменить» ( ) предназначена для перехода на страницу редактирования и изменения существующего в перечне виртуального сетевого интерфейса.

Кнопка «Удалить» ( ) предназначена для удаления из перечня выбранного виртуального сетевого интерфейса.

Кнопка «Добавить VLAN» позволяет перейти на страницу создания и настройки нового виртуального сетевого интерфейса (см. рис. 74). Данная страница предназначена для настройки виртуальных локальных сетей на канальном уровне модели OSI при создании логической топологии сети.

4.4.8.1. Страница создания и настройки нового виртуального сетевого интерфейса

Страница создания и настройки нового виртуального сетевого интерфейса

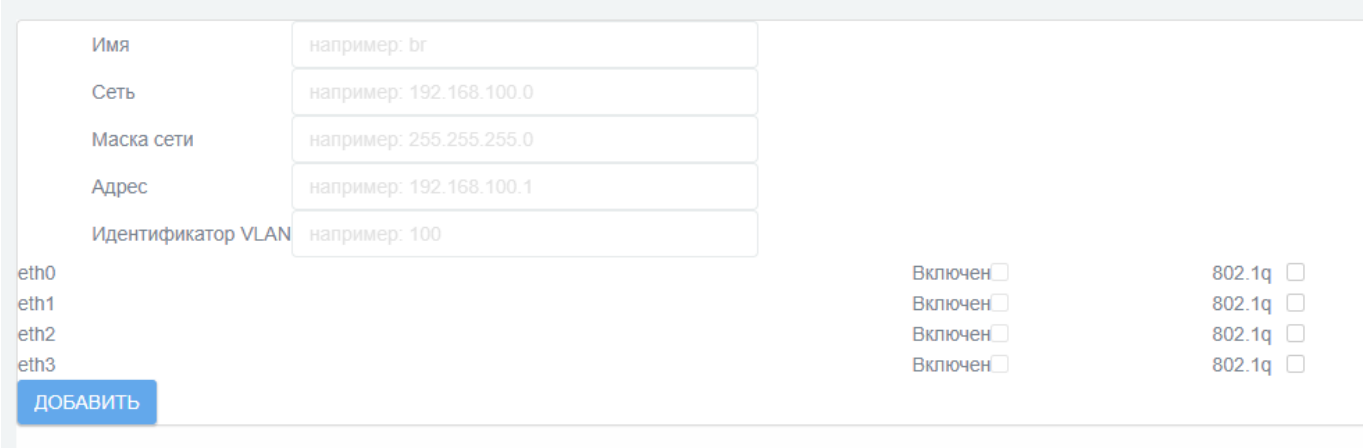

Рис. 74

Для создания и настройки нового виртуального сетевого интерфейса необходимо задать следующие параметры в полях:

1) «Имя» – имя виртуального сетевого адаптера, ассоциированного с виртуальной локальной сетью VLAN. Допускается имя из латинских букв верхнего и нижнего регистра и цифр от 0 до 9;

2) «Сеть» – IP-адрес виртуальной локальной сети. Допустим корректный IP-адрес сети, содержащий 0 в младших битах диапазона, покрываемого IP-маской;

3) «Маска сети» – IP-маска виртуальной локальной сети. Допустима корректная IP-маска в формате десятичной записи четырех байт маски, разделенных точками;

4) «Адрес» – адрес, который принимает сам комплекс «Рубикон» в настраиваемой виртуальной локальной сети VLAN. Допустим корректный IP-адрес, принадлежащий диапазону, определенному полем «Сеть» и «Маска сети»;

5) «Идентификатор VLAN» – идентификатор, присваиваемый виртуальной локальной сети VLAN согласно стандарту 802.1q (VLAN ID, VID). Допустимо целочисленное значение от 0 до 4095.

Также с помощью чекбоксов необходимо выбрать сетевые интерфейсы, которые будут использоваться при создании виртуальной сети VLAN.

При выборе используемых сетевых интерфейсов необходимо учитывать, что:

— настраиваемый сетевой интерфейс при создании виртуальной сети VLAN не будет иметь сетевого IP-адреса, поэтому **административный** интерфейс **нельзя** включать в список интерфейсов, использующихся при создании виртуальной сети VLAN;

— в том случае, если настраиваемый сетевой интерфейс используется при создании **нескольких** виртуальных сетей VLAN, то для этого сетевого интерфейса необходимо активировать чекбокс «**802.1q**» для применения данного протокола к интерфейсу.

Примечания:

1. В случае ввода некорректных параметров настройки виртуальной сети VLAN после нажатия на кнопку «Добавить» будет выведено сообщение об ошибке, а сама виртуальная сеть VLAN добавлена не будет.

2. Протокол 802.1q предполагает тегирование трафика для передачи информации о принадлежности сетевого пакета к VLAN по сетям стандарта IEEE 802.3ab Ethernet.

4.4.8.2. Страница редактирования интерфейса виртуальной локальной сети

Страница редактирования интерфейса виртуальной локальной сети (см. рис. 75) предназначена для внесения изменений в настройки интерфейса существующей виртуальной локальной сети.

Поля и параметры, доступные к редактированию интерфейса существующей виртуальной локальной сети аналогичны (кроме изменения поля «Имя») представленным на странице «Страница создания и настройки нового виртуального сетевого интерфейса» и подробно описаны в п. 4.4.8.1 настоящего документа.

Примечание. Недоступное для изменения поле «Имя» обозначено серым цветом.

Страница редактирования интерфейса виртуальной локальной сети

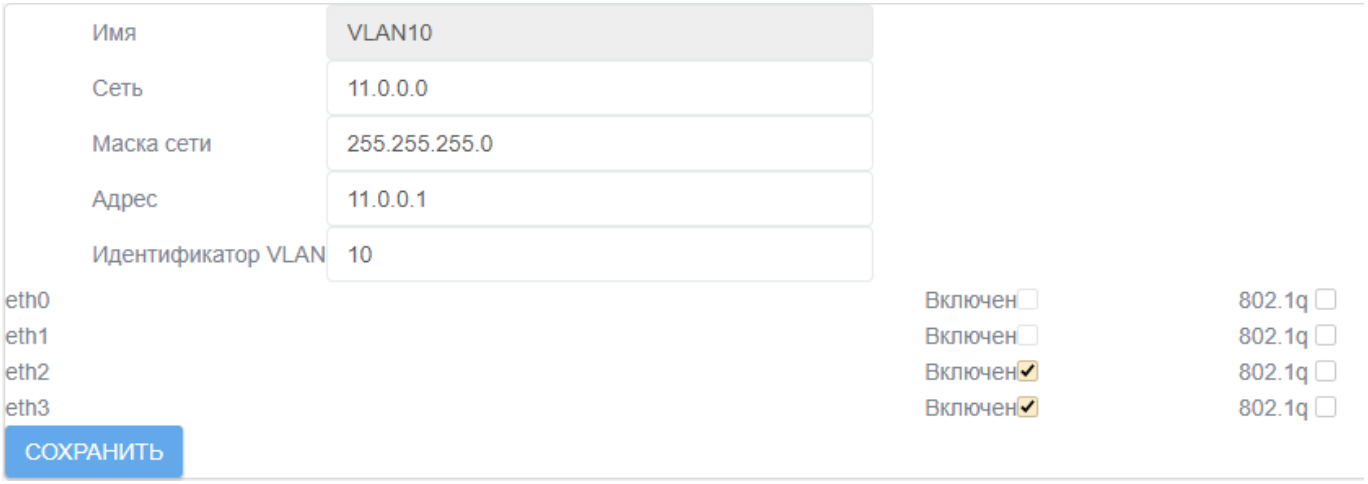

Рис. 75

4.4.9. Подраздел «Мосты»

Подраздел «Мосты» (см. рис. 76) позволяет объединить два или более сегментов сети Ethernet в одну L2 сеть.

Подраздел «Мосты»

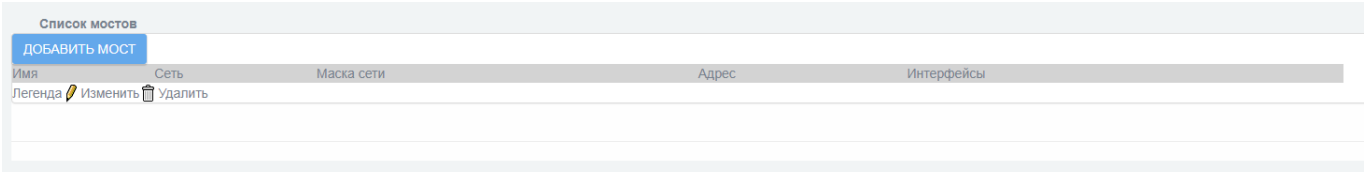

Рис. 76

Информация о перечне мостов представлена в виде таблицы «Список мостов» со следующими параметрами:

1) «Имя»;

2) «Сеть»;

3) «Маска сети»;

4) «Адрес»;

5) «Интерфейсы».

Кнопка «Изменить» ( ) предназначена для перехода на страницу редактирования и изменения, существующего в перечне мостов.

Кнопка «Удалить» ( ) предназначена для удаления из перечня выбранного моста.

Кнопка «Добавить мост» позволяет перейти на страницу создания и настройки нового моста (см. рис. 77).

Страница создания моста

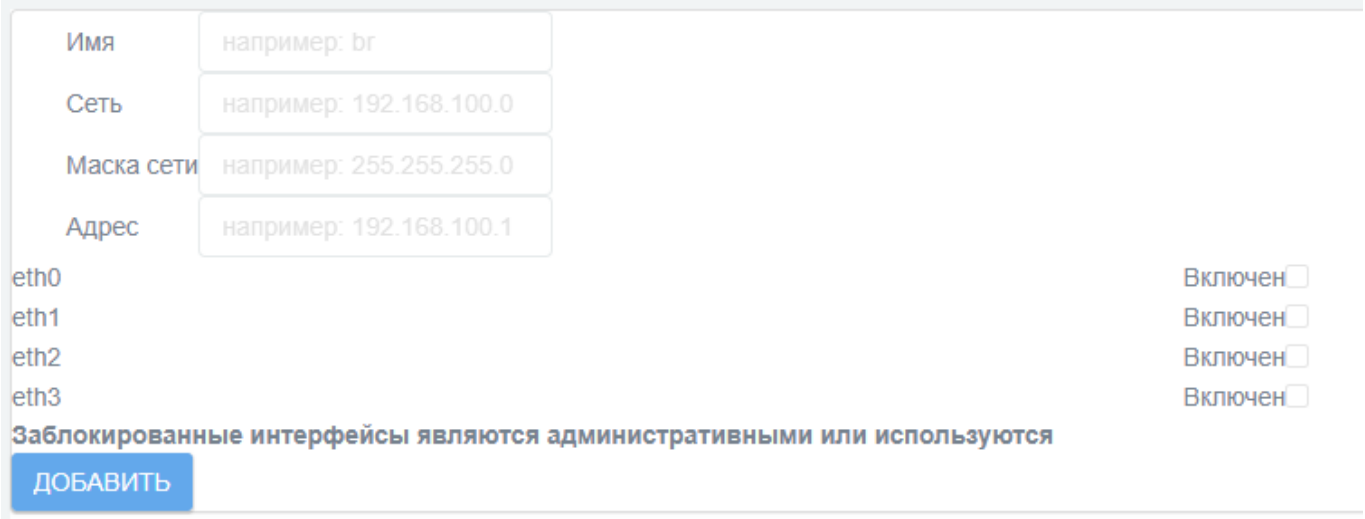

Рис. 77

По завершению настройки нового моста необходимо нажать кнопку «Добавить». При введении корректных настроек автоматически произойдет возврат на страницу подраздела «Мосты», новый мост будет добавлен в таблицу «Список мостов» и доступен для редактирования.

Примечание. На странице редактирования и изменения существующего в перечне моста доступное для изменения поле «Имя» обозначено серым цветом.

4.4.10. Подраздел «Объединение интерфейсов»

Подраздел «Объединение интерфейсов» (см. рис. 78) предназначен для задания конфигурации объединения интерфейсов.

Подраздел «Объединение интерфейсов»

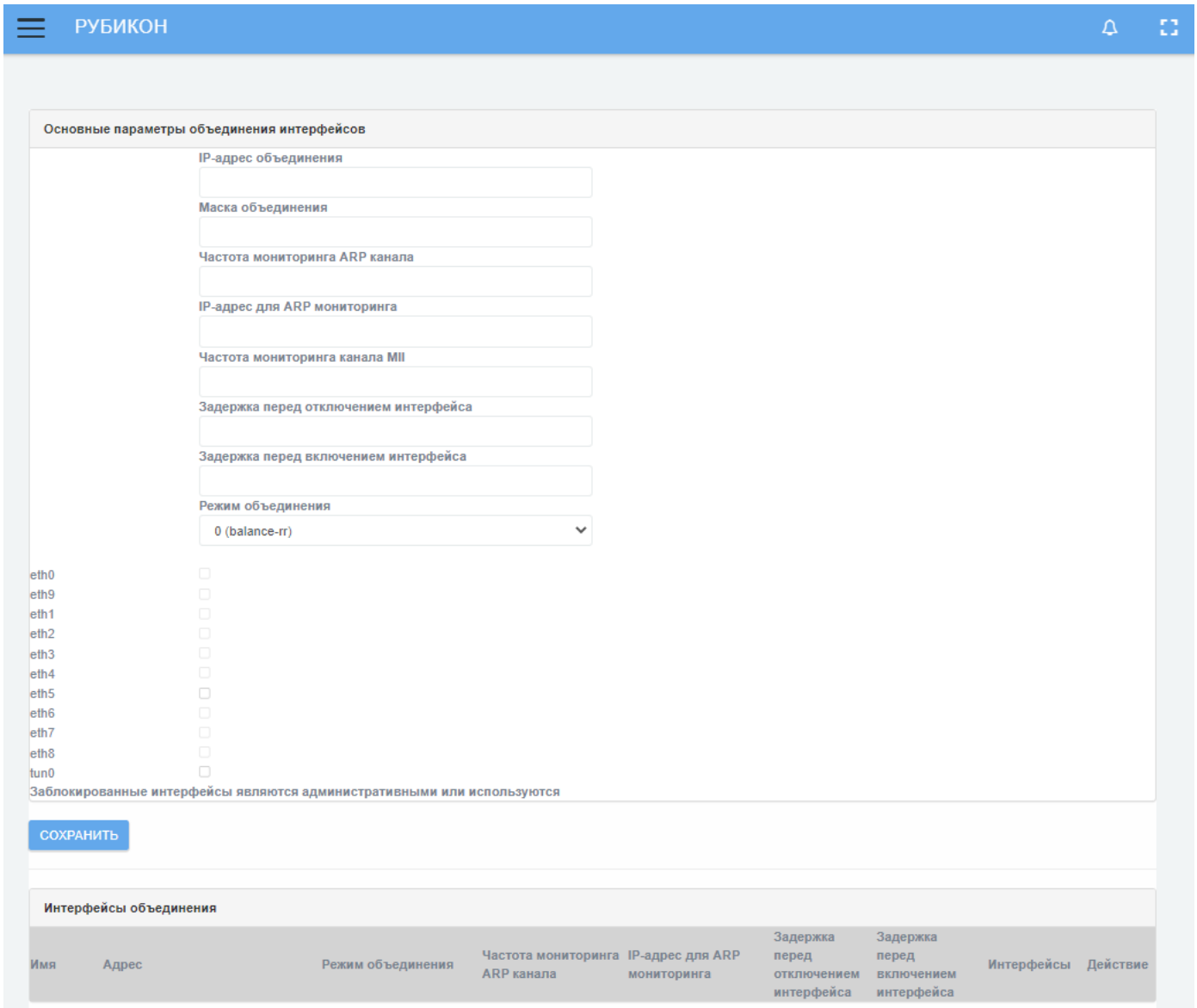

Рис. 78

В таблице 20 приведено описание элементов подраздела «Объединение интерфейсов».

Таблица 20 – Описание элементов подраздела «Объединение интерфейсов»

Элемент	Описание
Поле «IP-адрес объединения»	Предназначено для ввода общего IP-адреса для объединяемых интерфейсов. IP-адрес, который будет назначен виртуальному сетевому интерфейсу, объединяющему сетевые интерфейсы комплекса «Рубикон». Допустимо использовать корректный IP-адрес в формате последовательности четырех десятичных чисел, разделенных точками
Поле «Маска объединения»	Предназначено для ввода общей IP-маски для объединяемых интерфейсов. Маска, определяет диапазон адресов в подсети агрегированных интерфейсов в формате четырех десятичных чисел, разделенных точками
Поле «Частота мониторинга ARP канала»	Предназначено для ввода частоты мониторинга ARP канала (в миллисекундах). ARP мониторинг периодически проверяет на сетевых картах возможность приема и передачи трафика. Для проверки генерируются ARP запросы, отправляемые на адрес, указанный в поле «IP-адрес для ARP мониторинга». Выключен по умолчанию
Поле «IP-адрес для ARP мониторинга»	Предназначено для ввода IP-адреса для ARP мониторинга. Например, IP-адрес указывается не как число, а как строка в формате xxx.xxx.xxx.xxx (для IPv4). На эти адреса будут отправляться ARP запросы, для определения возможности приема-передачи через интерфейсы
Поле «Частота мониторинга канала MII»	Предназначено для ввода периодичности MII мониторинга (в миллисекундах). Определяет, как часто будет проверяться состояние линии на наличие отказов. Выключен по умолчанию
Поле «Задержка перед отключением интерфейса»	Предназначено для ввода времени задержки (в миллисекундах) перед отключением интерфейса, если произошел сбой соединения. Этот параметр активен только при заданном значении частоты MII мониторинга и значение параметра должно быть кратным значениям поля «Частота мониторинга канала MII»
Поле «Задержка перед включением интерфейса»	Предназначено для ввода времени задержки (в миллисекундах) перед тем, как установить соединение при обнаружении восстановления канала. Этот параметр активен только при заданном значении частоты MII мониторинге, значение параметра должно быть кратным значениям поля «Частота мониторинга канала MII»
Выпадающий список «Режим объединения»	Предназначен для выбора режима объединения, в котором будут согласованно работать выбранные интерфейсы. Доступен для выбора один из следующих режимов: – **«0» (balance-rr)** – режим балансировки (совместного использования интерфейсов с уравниванием пропускной способности), в котором сетевые пакеты поочередно отправляются через интерфейсы, включенные в объединение. Данный режим обеспечивает отказоустойчивость и балансировку нагрузки; – **«1» (active-backup)** – режим, при котором используется только один сетевой интерфейс (активный), а второй, резервный, подключается только при отсутствии передачи через первый. Данный режим обеспечивает отказоустойчивость

Элемент	Описание
Выпадающий список «Режим объединения»	– **«2» (balance-xor)** – режим балансировки (совместного использования интерфейсов с уравниванием пропускной способности), в котором решение о направлении сетевых пакетов через участвующих в объединении интерфейсы принимается на основании вычисления функции взятия остатка от деления на количество резервируемых интерфейсов от двоичной операции XOR MAC-адреса источника и MAC-адреса назначения. Данный режим обеспечивает отказоустойчивость и балансировку нагрузки; – **«3» (broadcast)** – режим, при котором во все сетевые интерфейсы, входящие в объединение, передаются одинаковые сетевые пакеты, что обеспечивает отказоустойчивость при возможном выходе из строя одного из каналов передачи; – **«4» (802.3ad)** – режим, при котором возможна организация резервирования каналов во взаимодействии с другим устройством «Рубикон». Сетевые пакеты передаются *через один сетевой интерфейс*, но после потери связи передача пакетов осуществляется через другой сетевой интерфейс. Данный режим обеспечивает балансировку нагрузки; – **«5» (balance-tlb)** – режим балансировки (совместного использования интерфейсов с уравниванием пропускной способности), в котором решение о направлении исходящих сетевых пакетов через участвующих в объединении интерфейсы принимается на основании текущей загрузки канала. Входящие сетевые пакеты приходят на текущую сетевую карту (первая по списку в колонке «Интерфейсы» таблицы «Интерфейсы объединения»). Если она выходит из строя, то другая сетевая карта (следующая по списку) устанавливает MAC-адрес вышедшей из строя; – **«6» (balance-alb)** – в отличии от предыдущего режима данный режим осуществляет балансировку входящих сетевых пакетов. Режим балансировки (совместного использования интерфейсов с уравниванием пропускной способности), в котором решение о направлении сетевых пакетов через участвующих в объединении интерфейсы принимается на основании текущей загрузки канала и ARP-ответов принимающего узла. Балансировка входящих сетевых пакетов распределяется между объединенными интерфейсами последовательно.
Чекбокс «**имя сетевого интерфейса*»*	Предназначен для выбора необходимых сетевых интерфейсов для дальнейшего объединения. Заблокированные интерфейсы являются административными или используются
Таблица «Интерфейсы объединения»	Предназначена для отображения созданных администратором интерфейсов в данном подразделе
Кнопка «Изменить»	Предназначена для перехода на страницу редактирования и изменения, существующего интерфейса
Кнопка «Удалить»	Предназначена для удаления из перечня созданных интерфейсов

4.5. Раздел «Службы»

Раздел «Службы» содержит следующие подразделы:

1) «Прокси»;

2) «FTP посредник»;

3) «Сервер DHCP»;

4) «Задать имена хостов»;

5) «Сервер времени»;

6) «Ограничение трафика»;

7) «Проверка доступности узлов».

4.5.1. Подраздел «Прокси»

Подраздел «Прокси» предназначен для перенаправления трафика прокси-сервера и его изменения.

Подраздел «Прокси» состоит из следующих блоков и секций:

1) блок «Настройки», который включает в себя:

— секцию «Общие параметры»;

— секцию «Прокси верхнего уровня»;

— секцию «Настройки журналирования».

2) блок «Расширенные настройки», который включает в себя:

— секцию «Управление кэшем»;

— секцию «Порты назначения»;

— секцию «Контроль доступа по адресу»;

— секцию «Классные расширения (CRE)»;

— секцию «Список URL фильтрации»;

— секцию «Ограничение по времени»;

— секцию «Лимиты передачи»;

— секцию «Регулирование закачки»;

— секцию «Фильтр MIME типов»;

— секцию «Веб-браузер»;

— секцию «Конфиденциальность»;

— секцию «Redirectors»;

— секцию «Метод аутентификации»;

— секцию «Включить взаимодействие с сервером ICAP»;

— секцию «Включить фильтрацию скриптов на дополнительном порту».

4.5.1.1. Блок «Настройки»

Блок «Настройки» (см. рис. 79) предназначен для настройки прокси-сервера.

Блок «Настройки»

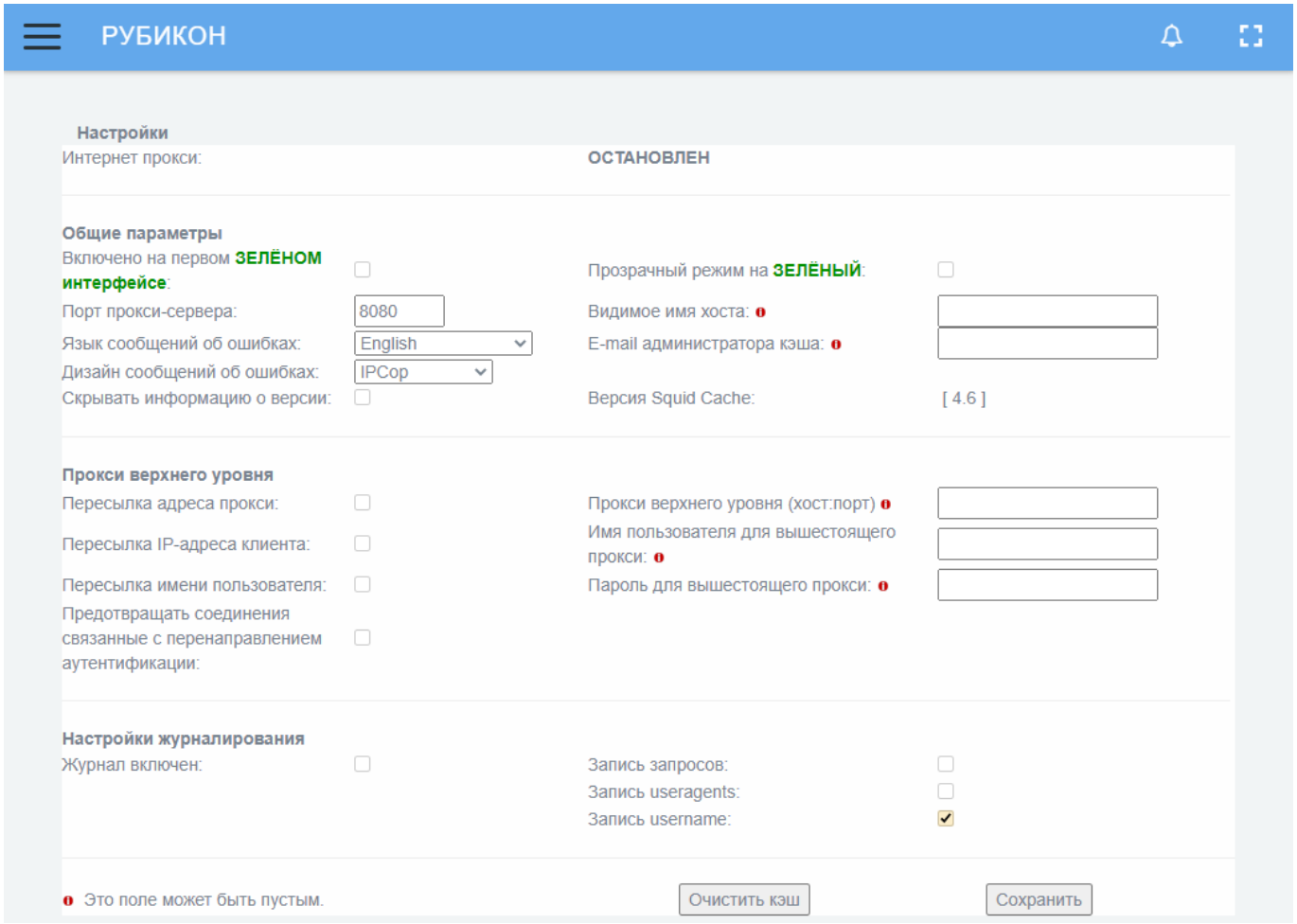

Рис. 79

В данном блоке присутствует информационное поле «Интернет прокси:» отображающее статус программного процесса прокси.

Данный процесс может находиться в состоянии:

— «остановлен»;

— «запущен».

В состоянии «запущен» дополнительно отображается объем занимаемой процессом памяти.

4.5.1.1.1. Секция «Общие параметры»

Секция «Общие параметры» (см. рис. 80) предназначена для ввода общих настроек прокси сервера.

Секция «Общие параметры»

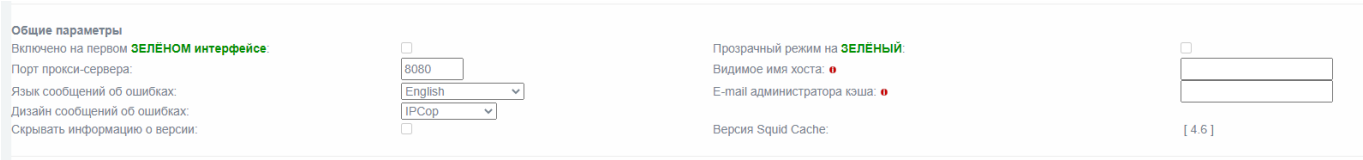

Рис. 80

В таблице 21 приведено описание элементов секции «Общие параметры».

Таблица 21 – Описание элементов секции «Общие параметры»

Элемент	Описание
Чекбокс «Включено на первом ЗЕЛЁНОМ интерфейсе»	Предназначен для включения/отключения службы прокси-сервера на первом зеленом интерфейсе
Поле «Порт прокси-сервера»	Предназначено для ввода номера сетевого порта, на котором работает служба прокси-сервера
Выпадающий список «Язык сообщений об ошибках»	Предназначен для выбора языка сообщений об ошибках
Выпадающий список «Дизайн сообщений об ошибках»	Предназначен для выбора одного из вариантов дизайна сообщений об ошибках: – IPCop; – Стандартный

Элемент	Описание
Чекбокс «Скрывать информацию о версии»	Предназначен для выбора включения/отключения отображения информации о версии прокси-сервера
Чекбокс «Прозрачный режим на ЗЕЛЁНЫЙ»	Предназначен для выбора включения/отключения службы прокси-сервера в прозрачном режиме. Это позволяет исключить необходимость настройки параметров прокси-сервера пользователем на стороне клиента
Поле «Видимое имя хоста»*	Предназначено для ввода имени узла прокси-сервера, которое будет передано клиенту при подключении
Поле «E-mail администратора кэша»*	Предназначено для ввода адреса электронной почты администратора механизма кэширования прокси-сервера
Информационное поле «Версия Squid Cache»	Предназначено для отображения информации о версии прокси-сервера
* – Поля, не обязательные к заполнению	

4.5.1.1.2. Секция «Прокси верхнего уровня»

Секция «Прокси верхнего уровня» (см. рис. 81) предназначена для настройки параметров верхнеуровневого прокси сервера.

Секция «Прокси верхнего уровня»

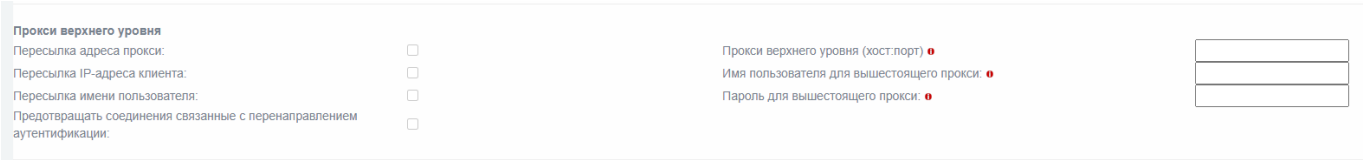

Рис. 81

В таблице 22 приведено описание элементов секции «Прокси верхнего уровня».

Таблица 22 – Описание элементов секции «Прокси верхнего уровня»

Элемент	Описание
Чекбокс «Пересылка адреса прокси»	Предназначен для выбора включения/отключения пересылки адреса прокси-серверу верхнего уровня
Чекбокс «Пересылка IP-адреса клиента»	Предназначен для выбора включения/отключения пересылки IP-адреса клиента прокси-серверу верхнего уровня
Чекбокс «Пересылка имени пользователя»	Предназначен для выбора включения/отключения необходимости пересылки имени пользователя прокси-серверу верхнего уровня

Элемент	Описание
Чекбокс «Предотвращать соединения связанные с перенаправлением аутентификации»	Предназначен для выбора включения/отключения предотвращения соединений, связанных с перенаправлением аутентификации
Поле «Прокси верхнего уровня (хост:порт)»*	Предназначено для ввода адреса и порта для прокси-сервера верхнего уровня
Поле «Имя пользователя для вышестоящего прокси»*	Предназначено для ввода имени пользователя для прокси-сервера верхнего уровня
Поле «Пароль для вышестоящего прокси»*	Предназначено для ввода пароля прокси-сервера верхнего уровня
* – Поля, не обязательные к заполнению	

4.5.1.1.3. Секция «Настройки журналирования»

Секция «Настройки журналирования» (см. рис. 82) предназначена для настройки параметров журналирования.

Секция «Настройки журналирования»

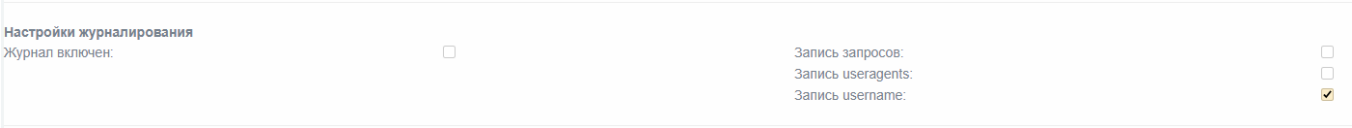

Рис. 82

В таблице 23 приведено описание элементов секции «Настройки журналирования».

Таблица 23 – Описание элементов секции «Настройки журналирования»

Элемент	Описание
Чекбокс «Журнал включен»	Предназначен для выбора включения/отключения журналирования событий прокси
Чекбокс «Запись запросов»	Предназначен для выбора включения/отключения записи запросов HTTP в журнал
Чекбокс «Запись useragents»	Предназначен для выбора включения/отключения записи параметра типа пользовательского приложения (параметр «useragent») в журнал
Чекбокс «Запись username»	Предназначен для выбора включения/отключения записи имени пользователя (параметр «username») в журнал
Кнопка «Очистить кэш»	Предназначена для очистки файла, создаваемого прокси-сервером
Кнопка «Сохранить»	Предназначена для сохранения введенных данных и параметров

4.5.1.2. Блок «Расширенные настройки»

Блок «Расширенные настройки» предназначен для настройки дополнительных параметров.

В конце данного блока присутствуют кнопки «Очистить кэш» и «Сохранить».

4.5.1.2.1. Секция «Управление кэшем»

Секция «Управление кэшем» (см. рис. 83) предназначена для настройки параметров кэширования.

Секция «Управление кэшем»

Рис. 83

В таблице 24 приведено описание элементов секции «Управление кэшем».

Таблица 24 – Описание элементов секции «Управление кэшем»

Элемент	Описание
Поле «Размер кэша в памяти (МБ)»	Предназначено для ввода размера кэша в памяти
Поле «Минимальный размер объекта (кБ)»	Предназначено для ввода минимального размера объекта
Выпадающий список «Количество субдиректорий 1-го уровня»	Предназначен для выбора одного из следующих параметров: – 16; – 32; – 64; – 128; – 256

Элемент	Описание
Выпадающий список «Стратегия использования памяти»	Предназначен для выбора одного из следующих параметров: – LRU; – heap LFUDA; – heap GDSF; – heap LRU
Выпадающий список «Стратегия замены в кэше»	Предназначен для выбора одного из следующих параметров: – LRU; – heap LFUDA; – heap GDSF; – heap LRU
Чекбокс «Включить автономный режим»	Предназначен для выбора включения/отключения автономного режима
Поле «Размер кэша на HDD (МБ)»	Предназначено для ввода размера кэша на жестком диске
Поле «Максимальный размер объекта (кБ)»	Предназначено для ввода максимального размера объекта
Поле «Не кэшировать эти домены (один в строке)»*	Предназначено для ввода перечня доменов вручную
* – Поля, не обязательные к заполнению	

4.5.1.2.2. Секция «Порты назначения»

Секция «Порты назначения» (см. рис. 84) предназначена для настройки параметров портов.

Секция «Порты назначения»

Рис. 84

В таблице 25 приведено описание элементов секции «Порты назначения».

Таблица 25 – Описание элементов секции «Порты назначения»

Элемент	Описание
Поле «Разрешенные стандартные порты (один в строке)»	Предназначено для ввода разрешенных стандартных портов
Поле «Разрешенные SSL порты (один в строке)»	Предназначено для ввода разрешенных SSL-портов

4.5.1.2.3. Секция «Контроль доступа по адресу»

Секция «Контроль доступа по адресу» (см. рис. 85) предназначена для настройки параметров доступа по заранее заданным адресам.

Секция «Контроль доступа по адресу»

Рис. 85

В таблице 26 приведено описание элементов секции «Контроль доступа по адресу».

Таблица 26 – Описание элементов секции «Контроль доступа по адресу»

Элемент	Описание
Поле «Разрешенные подсети (одна в строке)»	Предназначено для ввода разрешенных подсетей. Для всех перечисленных подсетей разрешен доступ к прокси-серверу
Поле «Неограниченные IP-адреса (один в строке)»*	Предназначено для ввода IP-адресов. Для всех клиентских IP-адресов этого списка будут действовать следующие ограничения: – ограничение времени; – предельные размеры для запросов на загрузку; – регулирование загрузки; – проверка браузера; – фильтр MIME типов; – аутентификация; – одновременный вход одного пользователя на разных электронно-вычислительных машинах (далее – ЭВМ) (доступно, если включена проверка подлинности)
Поле «Блокируемые IP-адреса (один в строке)»*	Предназначено для ввода IP-адресов, все запросы от которых будут заблокированы
Чекбокс «Запретить доступ через встроенный прокси»	Предназначен для выбора включения/отключения полного запрета доступа к прокси-серверу
Чекбокс «Запретить доступ через встроенный прокси к ЗЕЛЁНОЙ из других подсетей»	Предназначен для выбора включения/отключения запрета доступа через прокси к зеленым сетям из других подсетей
Поле «Неограниченные MAC-адреса (один в строке)»*	Предназначено для ввода MAC-адресов. Для всех MAC-адресов в этом списке будут действовать следующие ограничения: – ограничение времени; – предельные размеры для запросов на загрузку; – регулирование загрузки; – проверка браузера; – фильтр MIME типов; – аутентификация; – одновременный вход одного пользователя на разных ЭВМ (доступно, если включена проверка подлинности)
Поле «Блокируемые MAC-адреса (один в строке)»*	Предназначено для ввода MAC-адресов, все запросы от которых будут заблокированы
* – Поля, не обязательные к заполнению	

4.5.1.2.4. Секция «Классные расширения (CRE)

Секция «Классные расширения (CRE)» (см. рис. 86) предназначена для настройки параметров расширений групп классов по управлению.

Секция «Классные расширения (CRE)»

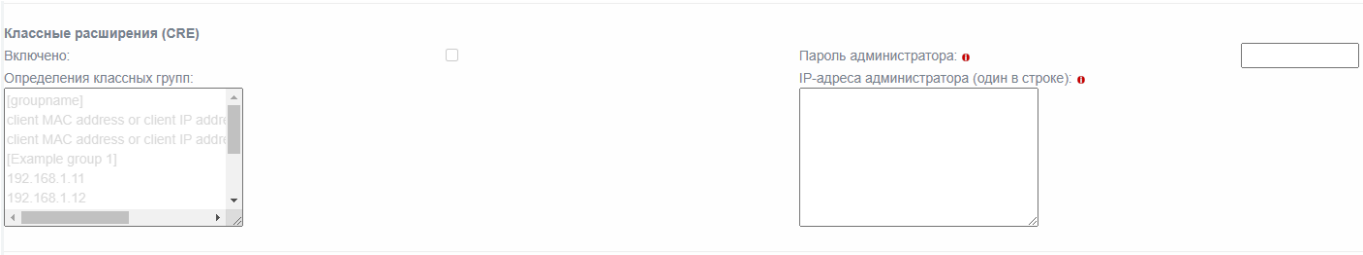

Рис. 86

В таблице 27 приведено описание элементов секции «Классные расширения (CRE)».

Таблица 27 – Описание элементов секции «Классные расширения (CRE)»

Элемент	Описание
Чекбокс «Включено»	Предназначен для выбора включения/отключения административного интерфейса управления веб-доступом
Поле «Определения классных групп»	Предназначено для ввода классных групп. Формат групп: [Название группы 1]; 192.168.1.11; 192.168.1.12; 192.168.1.13; [Название группы 2]; 192.168.1.21-192.168.1.25 [Название группы 3]; 192.168.1.32/255.255.255.240
Поле «Пароль администратора»*	Предназначено для ввода пароля для управления веб-доступом (если данный пароль установлен)
Поле «IP-адреса администратора (один в строке)»*	Предназначено для ввода IP-адресов, которые смогут управлять веб-доступом
* – Поля, не обязательные к заполнению	

4.5.1.2.5. Секция «Список URL фильтрации»

Секция «Список URL фильтрации» (см. рис. 87) дает возможность блокирования веб-запросов по ключевому слову в адресе с помощью задания «черных» и «белых» списков.

Секция «Список URL фильтрации»

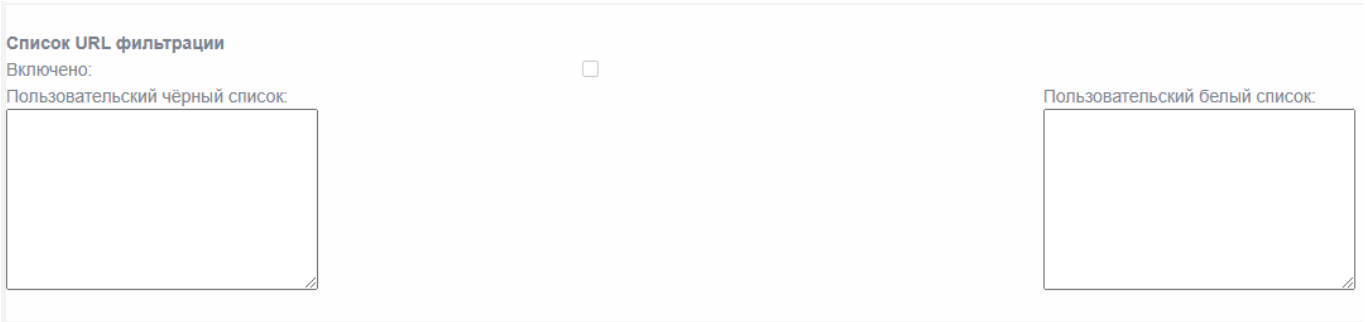

Рис. 87

В таблице 28 приведено описание элементов секции «Список URL фильтрации».

Таблица 28 – Описание элементов секции «Список URL фильтрации»

Элемент	Описание
Чекбокс «Включено»	Предназначен для выбора включения/отключения URL фильтрации
Поле «Пользовательский чёрный список»	Предназначено для ввода и создания «черного» списка
Поле «Пользовательский белый список»	Предназначено для ввода и создания «белого» списка

4.5.1.2.6. Секция «Ограничение по времени»

Секция «Ограничение по времени» (см. рис. 88) предназначена для настройки параметров ограничения времени.

Секция «Ограничение по времени»

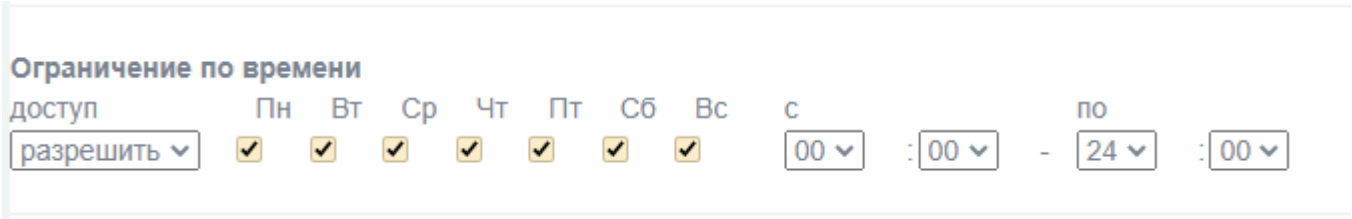

Рис. 88

В таблице 29 приведено описание элементов секции «Ограничение по времени».

Таблица 29 – Описание элементов секции «Ограничение по времени»

Элемент	Описание
Выпадающий список «Доступ»	Предназначен для выбора одного из следующих параметров: – разрешить; – запретить
Чекбоксы «Пн», «Вт», «Ср», «Чт», «Пт», «Сб», «Вс»	Предназначен для выбора дней недели, для которых будет действовать выбранное правило ограничения по времени
Выпадающие списки «с»	Предназначен для выбора начала ограничения по времени: – в первом списке – часов; – во втором списке – минут
Выпадающие списки «по»	Предназначен для выбора окончания ограничения по времени: – в первом списке – часов; – во втором списке – минут

4.5.1.2.7. Секция «Лимиты передачи»

Секция «Лимиты передачи» (см. рис. 89) предназначена для настройки параметров лимитов передачи.

Секция «Лимиты передачи»

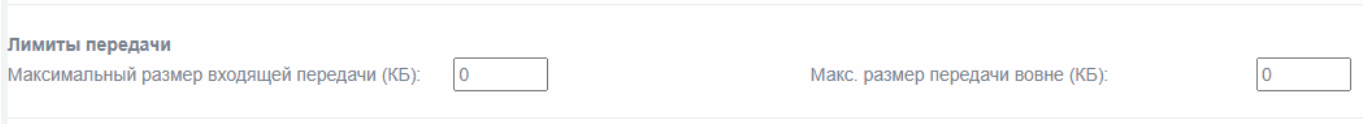

Рис. 89

В таблице 30 приведено описание элементов секции «Лимиты передачи».

Таблица 30 – Описание элементов секции «Лимиты передачи»

Элемент	Описание
Поле «Максимальный размер входящей передачи (КБ)»	Предназначено для ввода максимально разрешенного размера входящей передачи
Поле «Макс. размер передачи вовне (КБ)»	Предназначено для ввода максимально разрешенного размера передачи вовне

4.5.1.2.8. Секция «Регулирование закачки»

Секция «Регулирование закачки» (см. рис. 90) предназначена для регулирования параметров скорости и контента закачки.

Секция «Регулирование закачки»

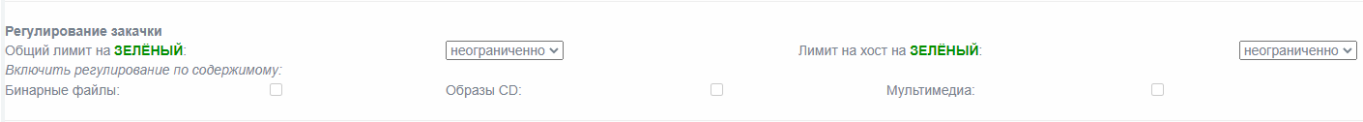

Рис. 90

В таблице 31 приведено описание элементов секции «Регулирование закачки».

Таблица 31 – Описание элементов секции «Регулирование закачки»

Элемент	Описание
Выпадающий список «Общий лимит на ЗЕЛЁНЫЙ»	Предназначен для выбора одного из следующих параметров: – 64 kBit/s; – 128 kBit/s; – 256 kBit/s; – 384 kBit/s; – 512 kBit/s; – 1024 kBit/s; – 2048 kBit/s; – 3072 kBit/s; – 5120 kBit/s; – 8192 kBit/s; – 10240 kBit/s; – неограниченно
Выпадающий список «Лимит на хост на ЗЕЛЁНЫЙ»	
Чекбоксы «Включить регулирование по содержимому»	Предназначены для выбора включения/отключения регулирования по определенным типам содержимого. Доступные для выбора варианты: – **бинарные файлы** (регулирование контента применяется к бинарным файлам: 7z, bz2, bin, cab, dmg, exe, gz, rar, sea, tar, tgz, zip); – **образы CD** (регулирование контента применяется к образам CD: b5t, bin, bwt, ccd, cdi, cue, flp, gho, img, iso, mds, nrg, pqi, raw, tib); – **мультимедиа** (регулирование контента применяется к мультимедийным файлам: aiff, asf, avi, divx, flv, mov, mp3, mp4, mpeg, qt, ram)

4.5.1.2.9. Секция «Фильтр MIME типов»

Секция «Фильтр MIME типов» (см рис. 91) предназначена для настройки параметров фильтра MIME типов.

Фильтр MIME включает фильтрацию по MIME типам и может быть настроен на блокирование содержимого в зависимости от его типа.

Секция «Фильтр MIME типов»

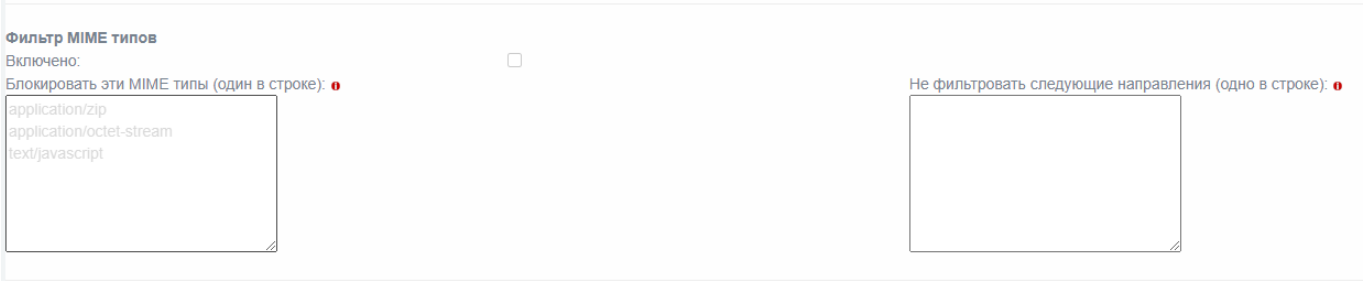

Рис. 91

В таблице 32 приведено описание элементов секции «Фильтр MIME типов».

Таблица 32 – Описание элементов секции «Фильтр MIME типов»

Элемент	Описание
Чекбокс «Включено»	Предназначен для выбора включения/отключения фильтра MIME типов. Если фильтр включен, проверяются все входящие заголовки MIME типов
Поле «Блокировать эти MIME типы (один в строке)»*	Предназначено для ввода MIME типов. Например: – video/mpeg – video/quicktime
Поле « Не фильтровать следующие направления (одно в строке)»*	Предназначено для ввода доменов, субдоменов, имен хостов, IP-адресов, URL
* – Поля, не обязательные к заполнению	

4.5.1.2.10. Секция «Веб-браузер»

Секция «Веб-браузер» (см. рис. 92) предназначена для настройки параметров проверки и разрешения использования веб-браузера.

Секция «Веб-браузер»

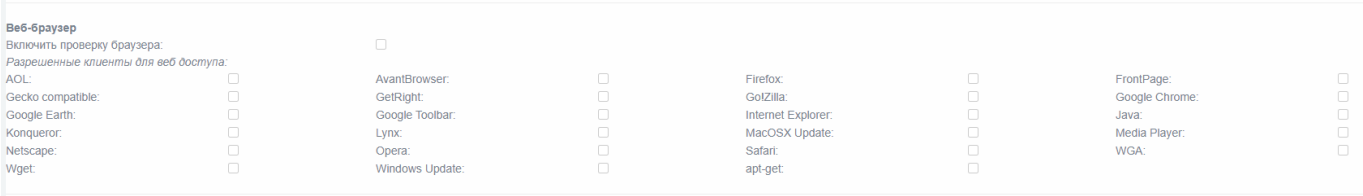

Рис. 92

В таблице 33 приведено описание элементов секции «Веб-браузер».

Таблица 33 – Описание элементов секции «Веб-браузер»

Элемент	Описание
Чекбокс «Включить проверку браузера»	Предназначен для выбора включения/отключения проверки веб-браузера на соответствие разрешенному типу
Список чекбоксов «Разрешенные клиенты для веб доступа»	Предназначены для выбора включения/отключения чекбоксов с типами веб-браузеров, разрешенных к использованию

4.5.1.2.11. Секция «Конфиденциальность»

Секция «Конфиденциальность» (см. рис. 93) предназначена для настройки параметров конфиденциальности.

Секция «Конфиденциальность»

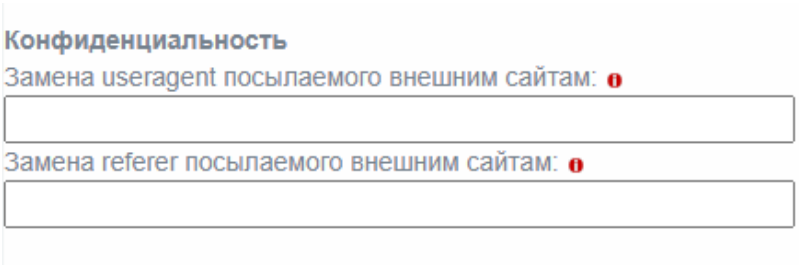

Рис. 93

В таблице 34 приведено описание элементов секции «Конфиденциальность».

Таблица 34 – Описание элементов секции «Конфиденциальность»

Элемент	Описание
Поле «Замена useragent посылаемого внешним сайтам»*	Предназначено для ввода замены параметра типа пользовательского приложения (параметр «useragent»), посылаемого внешним сайтам. По умолчанию параметр «useragent» используемый веб-браузером предоставляется на внешние веб-сервера. Некоторые динамические веб-сайты генерируют контент в зависимости от представленной параметр «useragent». Данная строка также записывается в лог-файлы веб-сервера
Поле «Замена referer посылаемого внешним сайтам»*	Предназначено для ввода строки-замены поля «referer» заголовков запроса клиента, пересылаемого серверу от пользователя. (Поле «referer» подставляется в заголовок и указывает URL, с которого пользователь осуществил переход к текущей странице пользователя. Текущая страница - та, от имени которой осуществлен обрабатываемый запрос). При получении запроса пользователя и включенном поле «Замена referer, посылаемого внешним сайтам» поле «referer» в заголовке запроса будет заменено, и измененный запрос будет перенаправлен серверу назначения
* – Поля, не обязательные к заполнению	

4.5.1.2.12. Секция «Redirectors»

Секция «Redirectors» (см. рис. 94) предназначена для настройки параметров перенаправления. «Redirectors» работают с прокси для фильтрации и перенаправления веб-трафика на основе правил, которые могут включать в себя «черные» и «белые» списки, временные ограничения.

Секция «Redirectors»

Рис. 94

В таблице 35 приведено описание элементов секции «Redirectors».

Таблица 35 – Описание элементов секции «Redirectors»

Элемент	Описание
Чекбокс «Включено»	Предназначен для выбора включения/отключения
Поле «Number of redirector processes»	Предназначено для увеличения или уменьшения количества активных процессов перенаправления. Количество процессов зависит от пропускной способности и числа одновременных пользователей. Значение по умолчанию «5»
Список чекбоксов «Available redirectors»	Список предназначен для отображения установленных активных модулей перенаправлений. Чекбокс (проставляется системой автоматически) справа от названия модуля – показывает состояние модуля (активен/не активен)

4.5.1.2.13. Секция «Метод аутентификации»

Секция «Метод аутентификации» (см. рис. 95) предназначена для настройки параметров метода аутентификации

Секция «Метод аутентификации»

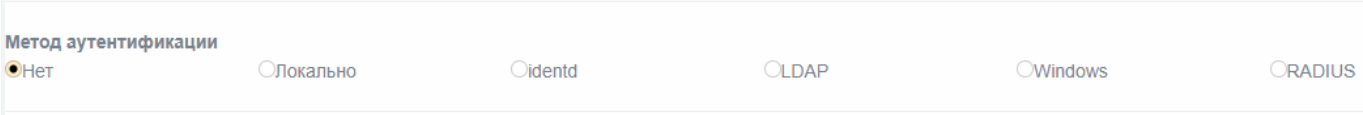

Рис. 95

В таблице 36 приведено описание элементов секции «Метод аутентификации».

Таблица 36 – Описание элементов секции «Метод аутентификации»

Элемент	Описание
Список чекбоксов «Метод аутентификации»	Список чекбоксов предназначен для выбора одного из нескольких методов аутентификации, указанных в списке: – «Нет»; – «Локально»; – «identd»; – «LDAP»; – «Windows»; – «RADIUS»

4.5.1.2.14. Секция «Взаимодействие с сервером ICAP»

Секция «Взаимодействие с сервером ICAP» (см. рис. 96) предназначена для настройки параметров взаимодействия с сервером ICAP.

Секция «Взаимодействие с сервером ICAP»

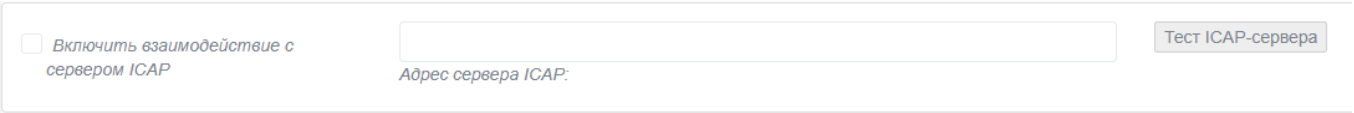

Рис. 96

В таблице 37 приведено описание элементов секции «Взаимодействие с сервером ICAP».

Таблица 37 – Описание элементов секции «Взаимодействие с сервером ICAP»

Элемент	Описание
Чекбокс «Включить взаимодействие с сервером ICAP»	Предназначен для выбора включения/отключения взаимодействия с сервером ICAP
Поле «Адрес сервера ICAP»	Предназначено для ввода адреса сервера ICAP
Кнопка «Тест ICAP-сервера»	Предназначена для выполнения тестирования внешнего средства защиты информации (Антивирус Касперского для шлюзов), взаимодействующего с межсетевым экраном по протоколу ICAP. При прохождении тестов пользователю выводится информация о результатах на странице «Прокси», а также делается запись в журнал

4.5.1.2.15. Секция «Фильтрация скриптов на дополнительном порту»

Секция «Фильтрация скриптов на дополнительном порту» (см. рис. 97) предназначена для настройки параметров фильтрации скриптов (разрешения или блокирования скриптов в ответах HTTP-сервера).

Секция «Фильтрация скриптов на дополнительном порту»

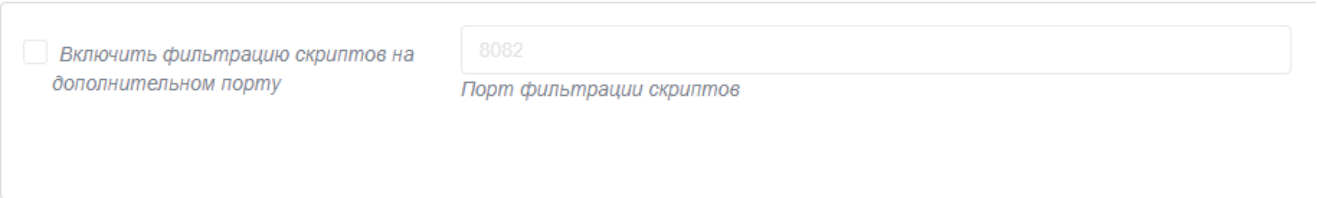

Рис. 97

В таблице 38 приведено описание элементов секции «Фильтрация скриптов на дополнительном порту».

Таблица 38 – Описание элементов секции «Фильтрация скриптов на дополнительном порту»

Элемент	Описание
Чекбокс «Включить фильтрацию скриптов на дополнительном порту»	Предназначен для выбора включения/отключения фильтрации скриптов
Поле «Порт фильтрации скриптов»	Предназначено для ввода порта фильтрации скриптов

4.5.2. Подраздел «FTP посредник»

Подраздел «FTP посредник» (см. рис. 98) предназначен для настройки FTP прокси.

Подраздел «FTP посредник»

Настройки FTP прокси

Включить FTP прокси
Порт
Блокировка последовательности FTP команд
СОХРАНИТЬ
Разрешить команды:
QUIT
REST
Запрещенные аргументы команды
RETR
Запрещенные аргументы команды
LIST
Запрещенные аргументы команды
USER
Запрещенные аргументы команды
PASV
NLST
Запрещенные аргументы команды
CDUP
STOU
ALLO
Запрещенные аргументы команды
MKD
Запрещенные аргументы команды
REIN
STRU
Запрещенные аргументы команды
RNFR
Запрещенные аргументы команды
ABOR
DELE
Запрещенные аргументы команды
MDTM
Запрещенные аргументы команды
CWD
PWD
STOR
Запрещенные аргументы команды
PORT
Запрещенные аргументы команды
PASS
Запрещенные аргументы команды
XPWD
SITE
Запрещенные аргументы команды
SMNT
Запрещенные аргументы команды
NOOP
APPE
Запрещенные аргументы команды
RMD
Запрещенные аргументы команды
SYST
TYPE
Запрещенные аргументы команды
MODE
Запрещенные аргументы команды
RNTO
Запрещенные аргументы команды
STAT
Запрещенные аргументы команды
SIZE
Запрещенные аргументы команды
СОХРАНИТЬ

Рис. 98

В таблице 39 приведено описание элементов подраздела «FTP посредник».

Таблица 39 – Описание элементов подраздела «FTP посредник»

Элемент	Описание
Чекбокс «Включить FTP прокси»	Предназначен для выбора включения/отключения FTP прокси
Поле «Порт»	Предназначено для ввода порта, на котором работает служба FTP прокси

Элемент	Описание
Поле «Блокировка последовательности FTP команд»	Предназначено для ввода последовательности FTP-команд, блокируемой службой FTP-прокси
Список чекбоксов «Разрешить команды»	Список предназначен для выбора необходимых FTP команд из списка. Доступны для выбора команды: – **QUIT** (завершить сеанс); – **CWD** (сменить директорию (аргумент – имя директории)); – **REST** (команда «перемотки» к определенной позиции в файле (аргумент – смещение в байтах)); – **PWD** (показать текущий рабочий каталог); – **RETR** (скачать файл. Сработает только после перехода в пассивный режим командой PASV (аргумент – имя файла)); – **STOR** (загрузить файл в пассивном режиме (аргумент – имя файла)); – **LIST** (вывести содержимое текущей или предоставленной директории. Команда поддерживается как относительный, так и абсолютный путь (аргумент – путь)); – **PORT** (перейти в активный режим передачи данных (аргумент – не требуется)); – **USER** (передать имя пользователя (аргумент – имя пользователя)); – **PASS** (передать пароль (аргумент – пароль)); – **PASV** (перейти в пассивный режим передачи данных (аргумент не требуется)); – **XPWD** (печать текущего рабочего каталога); – **NLST** (возвратить список файлов директории в более кратком формате, чем LIST. Только в режиме пассивного соединения (аргумент не требуется)); – **SITE** (изменение прав на файл); – **CDUP** (перейти в родительскую директорию); – **SMNT** (смонтировать указанную структуру файлов); – **NOOP** (нет операции); – **STOU** (хранить файл однозначно); – **APPE** (сообщить серверу и принять удаленный файл. Команда сработает только, если такого файла еще не существует в хранилище. Если файл существует, то будет возвращена ошибка (аргумент – имя файла)); – **ALLO** (вернуть ответ о наличии доступного места. Вне зависимости от аргумента ответ будет 202 OK (аргумент – размер в байтах)); – **RMD** (удалить директорию (аргумент – имя директории)); – **MKD** (создать директорию (аргумент – имя директории)); – **SYST** (отобразить операционную систему сервера); – **REIN** (инициализирует соединение); – **TYPE** (установить тип передачи файлов); – **STRU** (установить структуру передачи файлов);

Элемент	Описание
Список чекбоксов «Разрешить команды»	– **MODE** (активировать пассивный режим); – **RNFR** (выбрать файл для переименования (аргумент – имя файла)); – **RNTO** (задать новое имя файла. Только после того, как был выбран командой RNFR (аргумент – новое имя файла)); – **ABOR** (прервать передачу файла); – **STAT** (получить статистику соединения (аргумент не требуется)); – **DELE** (удалить файл (аргумент – имя файла)); – **SIZE** (получить размер файла (аргумент – имя файла)); – **MDTM** (получить дату и время изменения файла (аргумент – путь))
Поля «Запрещенные аргументы команды»	Предназначены для ввода запрещенных аргументов команды. Доступные поля находятся справа от команд, к которым они относятся

4.5.3. Подраздел «Сервер DHCP»

Подраздел «Сервер DHCP» (см. рис. 99) предназначен для настройки DHCP.

Подраздел «Сервер DHCP»

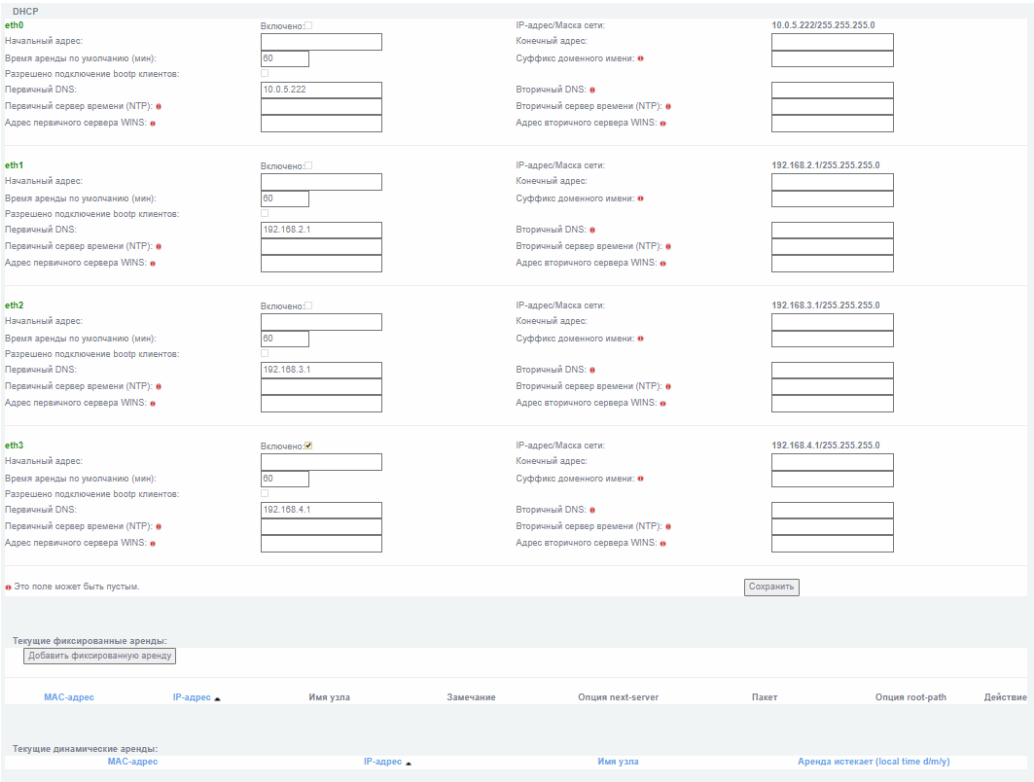

Рис. 99

Подраздел «Сервер DHCP» состоит из трех блоков:

1) «DHCP»;

2) «Текущие фиксированные аренды»;

3) «Текущие динамические аренды».

4.5.3.1. Блок «DHCP»

В таблице 40 приведено описание элементов блока «DHCP». Данный блок позволяет совершить настройку DHCP для «зеленых» и «синих» сетевых интерфейсов.

Таблица 40 – Описание элементов блока «DHCP»

Элемент	Описание
Чекбокс «Включено»	Предназначен для выбора включения/отключения сервера DHCP для выбранного сетевого интерфейса
Поле «Начальный адрес»	Предназначено для ввода начального адреса из диапазона адресов, выдаваемых DHCP-сервером
Поле «Время аренды по умолчанию (мин)»	Предназначено для ввода времени аренды IP-адреса. По истечении этого срока IP-адрес освобождается, если DHCP-клиент не прислал запроса на продление аренды
Чекбокс «Разрешено подключение bootp клиентов»	Предназначен для выбора включения/отключения возможности подключения клиентов по протоколу «bootp»
Поле «Первичный DNS»	Предназначено для ввода IP-адреса первичного DNS-сервера
Поле «Первичный сервер времени (NTP)»*	Предназначено для ввода IP-адреса первичного сервера времени (NTP)
Поле «Адрес первичного сервера WINS»*	Предназначено для ввода IP-адреса первичного сервера WINS
Информационное поле «IP-адрес/Маска сети»	Предназначено для вывода информации о IP-адресе и маске сети из текущих настроек выбранного сетевого интерфейса
Поле «Конечный адрес»	Предназначено для ввода конечного адреса из диапазона адресов, выдаваемых DHCP-сервером
Поле «Суффикс доменного имени»*	Предназначено для ввода суффикса доменного имени
Поле «Вторичный DNS»*	Предназначено для ввода IP-адреса вторичного (резервного) DNS-сервера
Поле «Вторичный сервер времени (NTP)»*	Предназначено для ввода IP-адреса вторичного (резервного) сервера времени (NTP)
Поле «Адрес вторичного сервера WINS»*	Предназначено для задания IP-адреса вторичного (резервного) сервера WINS
* – Поля, не обязательные к заполнению	

4.5.3.2. Блок «Текущие фиксированные аренды»

Блок «Текущие фиксированные аренды» (см. рис. 100) предназначен для отображения информации (в виде информационной таблицы) о используемых в текущий момент фиксированных арендах.

Блок «Текущие фиксированные аренды»

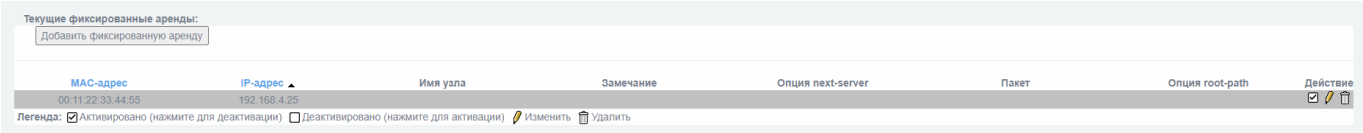

Рис. 100

Информация в информационной таблице «Текущие фиксированные аренды» представлена со следующими параметрами:

1) «MAC-адрес»;

2) «IP-адрес»;

3) «Имя узла»;

4) «Замечание»;

5) «Опция next-server»;

6) «Пакет»;

7) «Опция root-path»;

8) «Действие».

Чекбокс в столбце «Действие» необходим для активации (при проставленном флажке) выбранной фиксированной аренды или деактивации (при снятии флажка).

Кнопка «Изменить» ( ) предназначена для перехода на страницу редактирования и изменения существующего в перечне виртуального сетевого интерфейса.

Кнопка «Удалить» ( ) предназначена для удаления из перечня выбранного виртуального сетевого интерфейса.

Кнопка «Добавить фиксированную аренду» находится над информационной таблицей и позволяет открыть меню добавления фиксированной аренды (см. рис. 101).

4.5.3.2.1. Меню добавления фиксированной аренды

Меню добавления фиксированной аренды представлено на рисунке 101.

Меню добавления фиксированной аренды

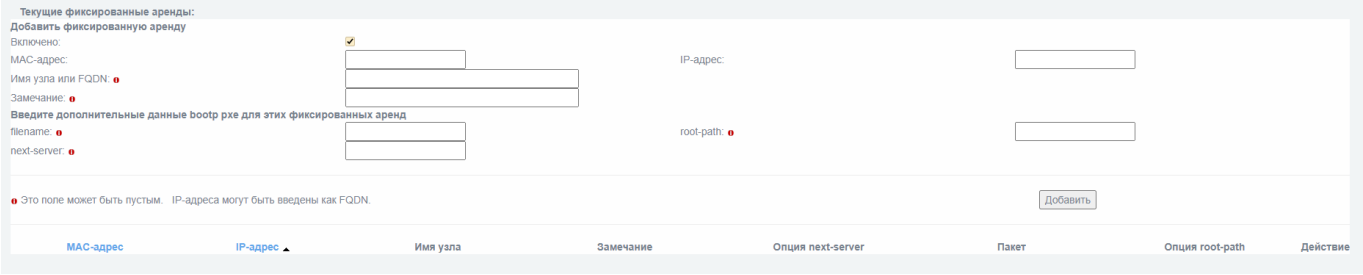

Рис. 101

В таблице 41 приведено описание элементов меню добавления фиксированной аренды.

Таблица 41 – Описание элементов меню добавления фиксированной аренды

Элемент	Описание
Чекбокс «Включено»	Предназначен для выбора включения/отключения фиксированной аренды IP адреса
Поле «MAC-адрес»	Предназначено для ввода MAC-адреса ЭВМ, которой назначается IP-адрес
Поле «Имя узла или FQDN»*	Предназначено для ввода имени узла или FQDN
Поле «Замечание»*	Предназначено для ввода замечаний к текущей настройке. Не влияет на работу DHCP-сервера
Поле «IP-адрес»	Предназначено для ввода назначаемого IP-адреса
Поле «filename»*	Предназначено для ввода дополнительных данных bootp pxe для этих фиксированных аренд, а именно **имени файла-образа** для загрузки по протоколу bootp
Поле «next-server»*	Предназначено для ввода дополнительные данные bootp pxe для этих фиксированных аренд, а именно **адреса сервера**, **содержащего файл-образ** для загрузки
Поле «root-path»*	Предназначено для ввода дополнительные данные bootp pxe для этих фиксированных аренд, а именно **пути загрузки для файла-образа**

Элемент	Описание
Кнопка «Добавить»	Предназначена для добавления новой фиксированной аренды с введенными настройками пользователя. Необходимо нажать после ввода всех необходимых параметров
* – Поля, не обязательные к заполнению. IP-адреса могут быть введены как FQDN	

4.5.3.3. Блок «Текущие динамические аренды»

Блок «Текущие динамические аренды» (см. рис. 102) предназначен для отображения информации (в виде информационной таблицы) о используемых в текущий момент динамических арендах.

Для отображения данного блока в подразделе необходимо активировать сервер DHCP хотя-бы для одного сетевого интерфейса (из необходимой подсети) и нажать кнопку «Добавить фиксированную аренду» (добавлять новую фиксированную аренду не обязательно). Информационная таблица «Текущие динамические аренды» появится под таблицей «Текущие фиксированные аренды» внизу экрана.

Блок «Текущие динамические аренды»


Текущие динамические аренды:

MAC-адрес	IP-адрес ▲	Имя узла	Аренда истекает (local time d/m/y)
52:54:00:e1:11:a2	192.168.14.231	pc-1	11/07/2022 10:14:06

Рис. 102

Информация в информационной таблице «Текущие динамические аренды» представлена со следующими параметрами:

1) «MAC-адрес»;

2) «IP-адрес»;

3) «Имя узла»;

4) «Аренда истекает (local time d/m/y)».

4.5.4. Подраздел «Задать имена хостов»

Подраздел «Задать имена хостов» (см. рис. 103) предназначен для настройки параметров сетевых узлов.

Подраздел «Задать имена хостов»

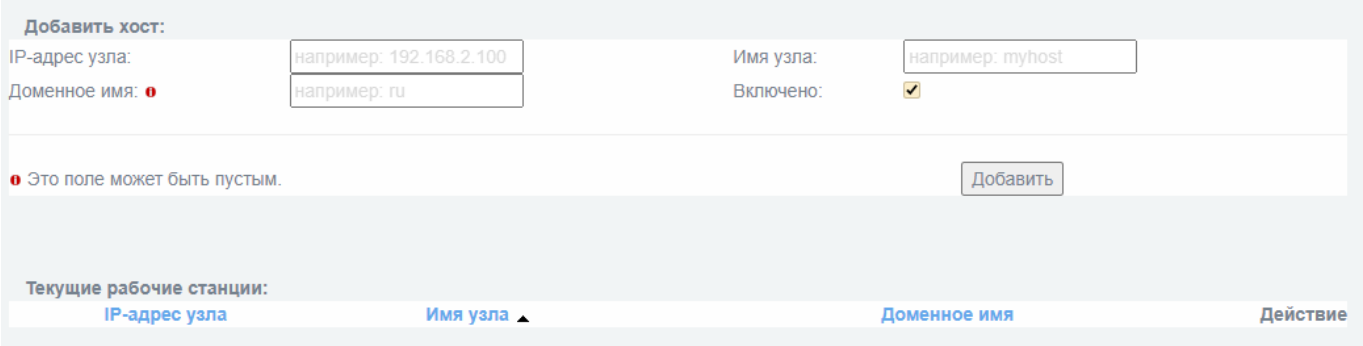

Рис. 103

В таблице 42 приведено описание элементов подраздела «Задать имена хостов».

Таблица 42 – Описание элементов подраздела «Задать имена хостов»

Элемент	Описание
Поле «IP-адрес узла»	Предназначено для ввода IP-адреса узла
Поле «Доменное имя»*	Предназначено для ввода доменного имени
Поле «Имя узла»	Предназначено для ввода имени узла
Чекбокс «Включено»	Предназначен для выбора включения/отключения хоста после добавления
Кнопка «Добавить»	Предназначена для сохранения введенной информации и добавления хоста
Информационная таблица «Текущие рабочие станции»	Предназначена для отображения добавленных администратором рабочих станций (хостов)
* – Поля, не обязательные к заполнению	

Информация в информационной таблице «Текущие рабочие станции» (см. рис. 104) представлена со следующими параметрами:

1) «IP-адрес узла»;

2) «Имя узла»;

3) «Доменное имя»;

4) «Действие».

Чекбокс в столбце «Действие» необходим для активации (при проставленном флажке) выбранной рабочей станции (хоста) или деактивации (при снятии флажка).

Кнопка «Изменить» ( ) предназначена для перехода на страницу редактирования и изменения существующей в перечне выбранной рабочей станции (хоста).

Кнопка «Удалить» ( ) предназначена для удаления из перечня выбранной рабочей станции (хоста).

Информационная таблица «Текущие рабочие станции»

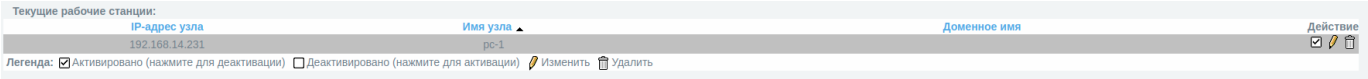

Рис. 104

4.5.5. Подраздел «Сервер времени»

Подраздел «Сервер времени» (см. рис. 105) предназначен для установки параметров времени.

Подраздел «Сервер времени»

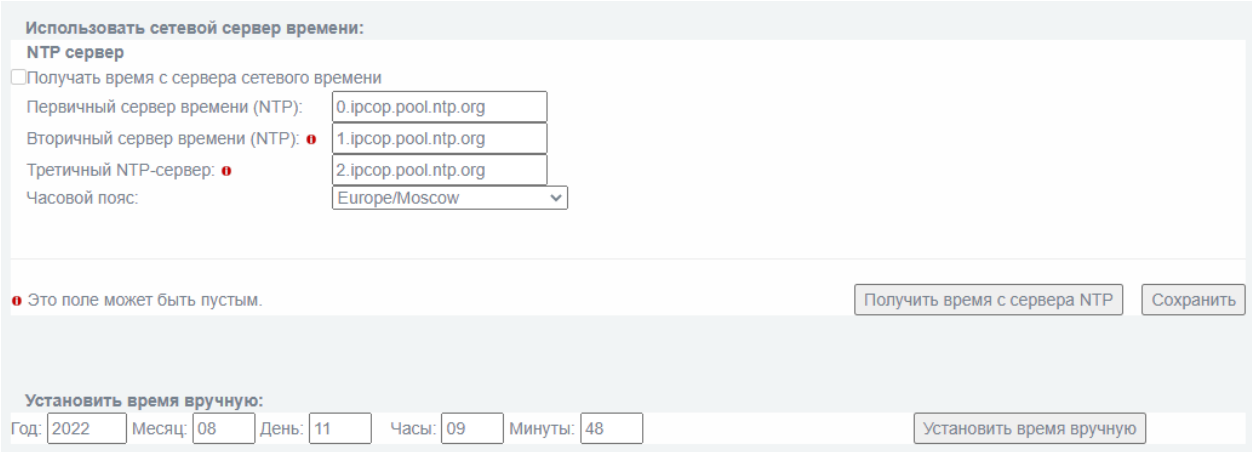

Рис. 105

Подраздел «Сервер времени» состоит из двух блоков:

1) «NTP сервер»;

2) «Установить время вручную».

4.5.5.1. Блок «NTP сервер»

Блок «NTP сервер» (см. рис. 106) предназначен для указания внешнего сервера времени.

Блок «NTP сервер»

Рис. 106

В таблице 43 приведено описание элементов блока «NTP сервер».

Таблица 43 – Описание элементов блока «NTP сервер»

Элемент	Описание
Чекбокс «Получать время с сервера сетевого времени»	Предназначен для выбора включения/отключения использования внешнего сервера времени
Поле «Первичный сервер времени (NTP)»	Предназначено для ввода адреса первичного сервера времени
Поле «Вторичный сервер времени (NTP)»*	Предназначено для ввода адреса вторичного сервера времени
Поле «Третичный NTP-сервер»*	Предназначено для ввода адреса третичного сервера времени
Выпадающий список «Часовой пояс»	Предназначен для выбора местонахождения изделия по континенту (стране) / городу
Кнопка «Получить время с сервера NTP»	Предназначена для обновления времени, полученного с указанных администратором серверов времени (NTP)
Кнопка «Сохранить»	Предназначена для сохранения введенной информации
* – Поля, не обязательные к заполнению	

4.5.5.2. Блок «Установить время вручную»

Блок «Установить время вручную» (см. рис. 107) предназначен для установки времени вручную администратором изделия.

Блок «Установить время вручную»

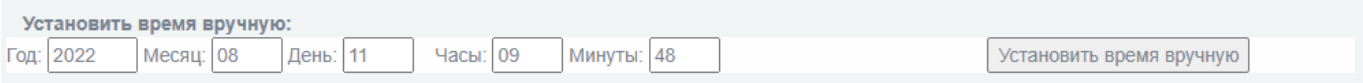

Рис. 107

В таблице 44 приведено описание элементов блока «Установить время вручную».

Таблица 44 – Описание элементов блока «Установить время вручную»

Элемент	Описание
Поле «Год»	Предназначено для ввода текущего года при ручном обновлении системного времени
Поле «Месяц»	Предназначено для ввода текущего месяца при ручном обновлении системного времени
Поле «День»	Предназначено для ввода текущего числа месяца при ручном обновлении системного времени
Поле «Часы»	Предназначено для ввода текущего часа при ручном обновлении системного времени
Поле «Минуты»	Предназначено для ввода текущих минут при ручном обновлении системного времени
Кнопка «Установить время вручную»	Предназначена для установки времени вручную если сервера времени (NTP) не доступны
Примечание – При изменении системного времени (в прошедшее время) пользователем вручную и включенном режиме «Подсчет трафика» необходимо нажать кнопку «Восстановление базы данных подсчета трафика» в подразделе «Настройки журналирования» раздела «Журналы»	

4.5.6. Подраздел «Ограничение Трафика»

Подраздел «Ограничение Трафика» (см. рис. 108) предназначен для ограничения трафика по определенным интерфейсам и для выставления приоритета трафика для служб.

Подраздел «Ограничение Трафика»

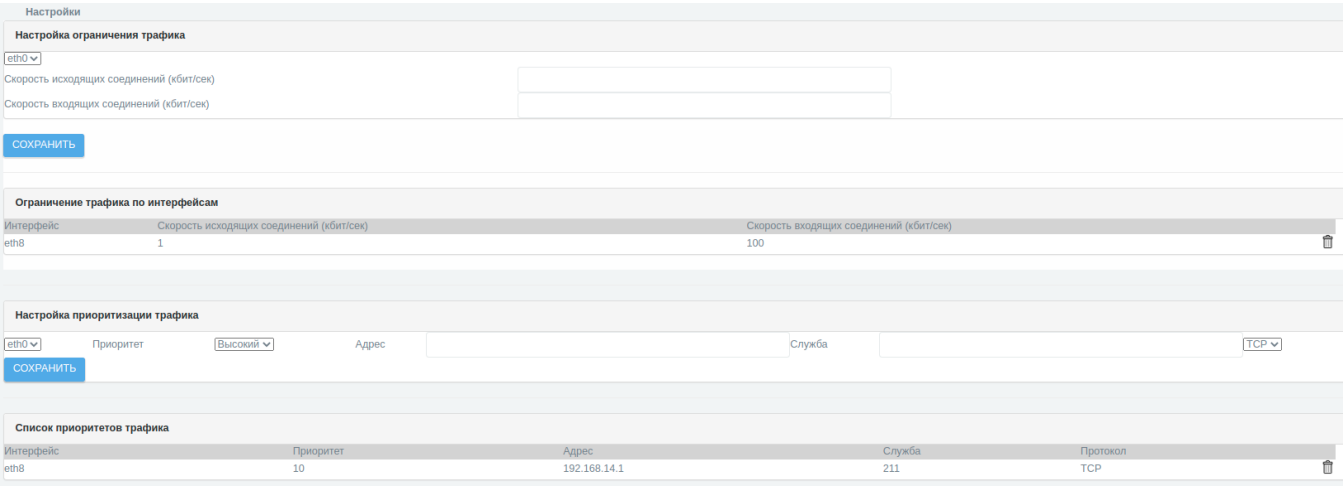

Рис. 108

Подраздел «Ограничение Трафика» состоит из следующих блоков:

1) «Настройка ограничения трафика»;

2) «Ограничение трафика по интерфейсам»;

3) «Настройка приоритизации трафика»;

4) «Список приоритетов трафика».

4.5.6.1. Блок «Настройка ограничения трафика»

Блок «Настройка ограничения трафика» (см. рис. 109) предназначен для настройки ограничения трафика по указанным интерфейсам.

Блок «Настройка ограничения трафика»

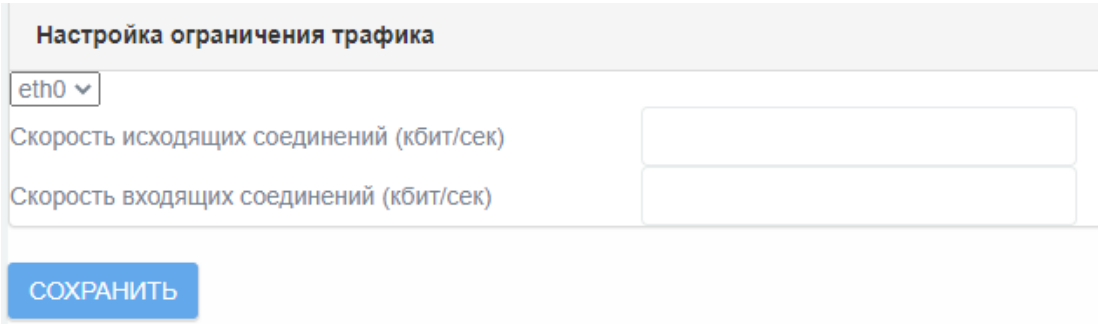

Рис. 109

В таблице 45 приведено описание элементов блока «Настройка ограничения трафика».

Таблица 45 – Описание элементов блока «Настройка ограничения трафика»

Элемент	Описание
Выпадающий список «Интерфейс»	Предназначен для выбора одного из доступных интерфейсов
Поле «Скорость исходящих соединений (кбит/сек)»	Предназначено для ввода и установки скорости исходящих соединений
Поле «Скорость входящих соединений (кбит/сек)»	Предназначено для ввода и установки скорости входящих соединений
Кнопка «Сохранить»	Предназначена для сохранения введенной информации

4.5.6.2. Блок «Ограничение трафика по интерфейсам»

Блок «Ограничение трафика по интерфейсам» (см. рис. 110) представляет собой информационную таблицу с настроенным ранее перечнем ограничений трафика.

Блок «Ограничение трафика по интерфейсам»

Рис. 110

Информация в информационной таблице «Ограничение трафика по интерфейсам» представлена со следующими параметрами:

1) «Интерфейс»;

2) «Скорость исходящих соединений (кбит/сек)»;

3) «Скорость входящих соединений (кбит/сек)».

Кнопка «Удалить» ( ) предназначена для удаления из перечня выбранного интерфейса.

4.5.6.3. Блок «Настройка приоритизации трафика»

Блок «Настройка приоритизации трафика» (см. рис. 111) предназначен для добавления приоритетов ограничений трафика по интерфейсам и протоколам.

Блок «Настройка приоритизации трафика»

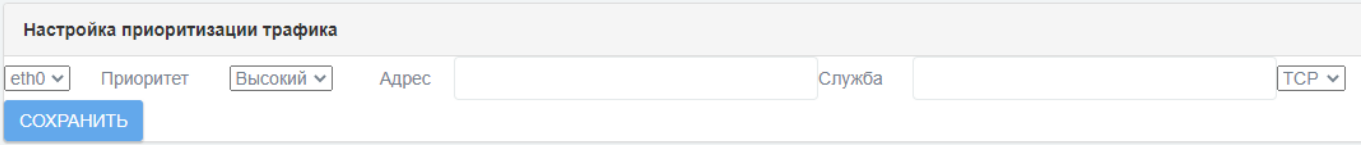

Рис. 111

В таблице 46 приведено описание элементов блока «Настройка ограничения трафика».

Таблица 46 – Описание элементов блока «Настройка приоритизации трафика»

Элемент	Описание
Выпадающий список «Интерфейс»	Предназначен для выбора одного из доступных интерфейсов
Выпадающий список «Приоритет»	Предназначено для выбора одного из следующих параметров: – «Высокий»; – «Средний»; – «Низкий»
Поле «Адрес»	Предназначено для ввода адреса выбираемой службы
Поле «Служба»	Предназначено для ввода имени выбираемой службы
Выпадающий список «Протокол»	Предназначено для выбора одного из следующих параметров: – «TCP»; – «UDP»
Кнопка «Сохранить»	Предназначена для сохранения введенной информации

4.5.6.4. Блок «Список приоритетов трафика»

Блок «Список приоритетов трафика» (см. рис. 112) представляет собой информационную таблицу с настроенным ранее перечнем приоритетов трафика.

Блок «Список приоритетов трафика»

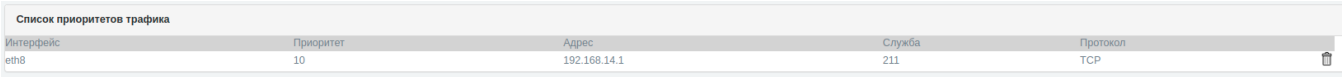

Рис. 112

Информация в информационной таблице «Список приоритетов трафика» представлена со следующими параметрами:

1) «Интерфейс»;

2) «Приоритет»;

3) «Адрес»;

4) «Служба»;

5) «Протокол».

Кнопка «Удалить» ( ) предназначена для удаления из перечня выбранного ограничения трафика.

4.5.7. Подраздел «Проверка доступности узлов»

Подраздел «Проверка доступности узлов» (см. рис. 113) осуществляет проверку сетевого соединения с удаленным узлом.

Подраздел «Проверка доступности узлов»

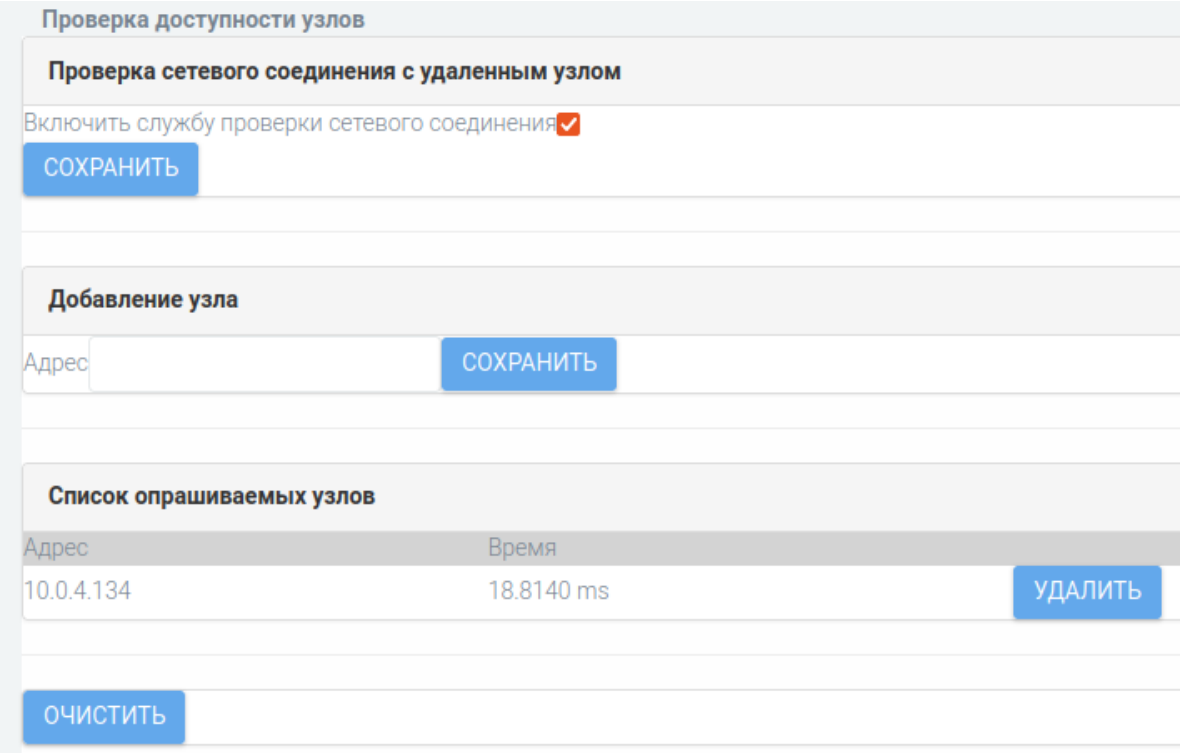

Рис. 113

В таблице 47 приведено описание элементов подраздела «Проверка доступности узлов».

Таблица 47 – Описание элементов подраздела «Проверка доступности узлов»

Элемент	Описание
Чекбокс «Включить службу проверки сетевого соединения»	Предназначен для выбора включения/отключения службы проверки сетевого соединения
Поле «Адрес»	Предназначено для ввода и добавления адреса узла
Информационная таблица «Список опрашиваемых узлов»	Предназначена для отображения адреса и времени отклика добавленных в список опрашиваемых узлов
Кнопка «Сохранить»	Предназначена для сохранения введенной информации
Кнопка «Удалить»	Предназначена для удаления выбранного узла информационной таблицы «Список опрашиваемых узлов» из списка опрашиваемых. Появляется после добавления опрашиваемого узла
Кнопка «Очистить»	Предназначена для сброса текущей информации о доступности узлов и производит дополнительный опрос времени отклика каждого из узлов в списке

4.6. Раздел «Система Обнаружения Вторжений»

Раздел «Система Обнаружения Вторжений» содержит следующие подразделы:

1) «Настройка правил СОВ»;
2) «Настройка обнаружения»;
3) «Обнаружение Атак»;
4) «Переменные СОВ».

4.6.1. Подраздел «Настройка правил СОВ»

Подраздел «Настройка правил СОВ» (см. рис. 114) предназначен для включения (отключения) срабатывания конкретного решающего правила.

Подраздел «Настройка правил СОВ»

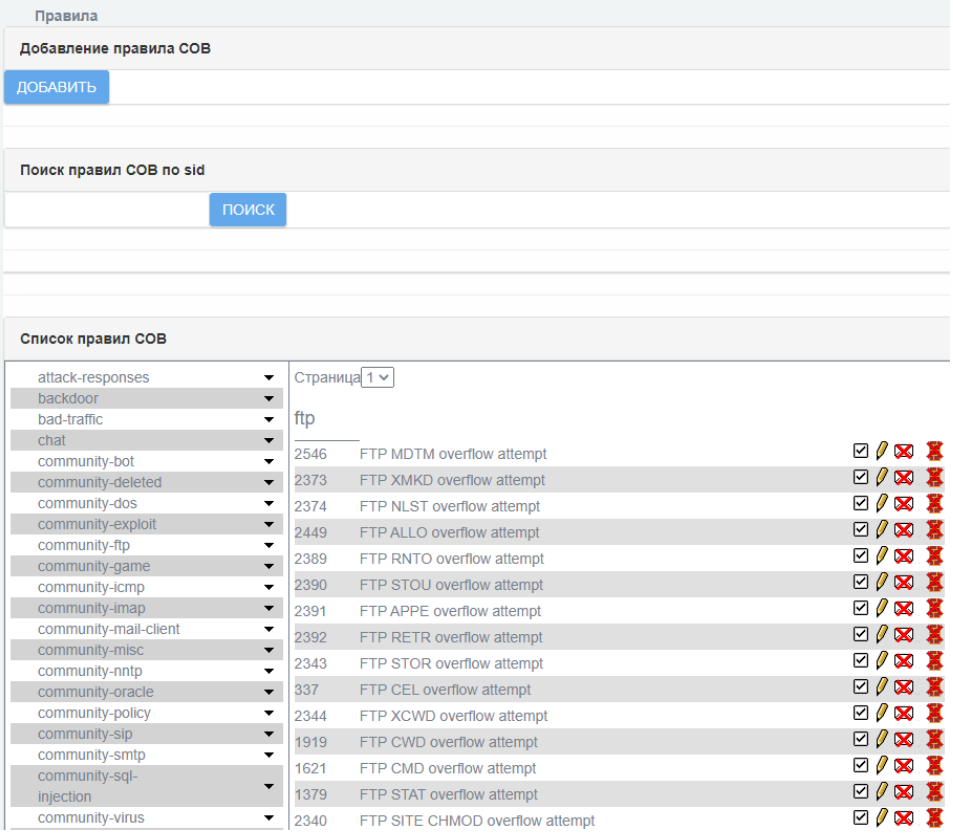

Рис. 114

Подраздел «Настройка правил СОВ» разделен на следующие блоки и страницы:

1) страница «Добавление правила СОВ»;

2) блок «Поиск правил СОВ по sid»;

3) блок «Список правил СОВ».

4.6.1.1. Страница «Добавление правила СОВ»

Страница «Добавление правила СОВ» (см. рис. 115) предназначена для настройки правил СОВ и добавления их в список правил СОВ.

Кнопка «Добавить» позволяет открыть данную страницу для добавления нового правила СОВ.

Страница «Добавление правила СОВ»

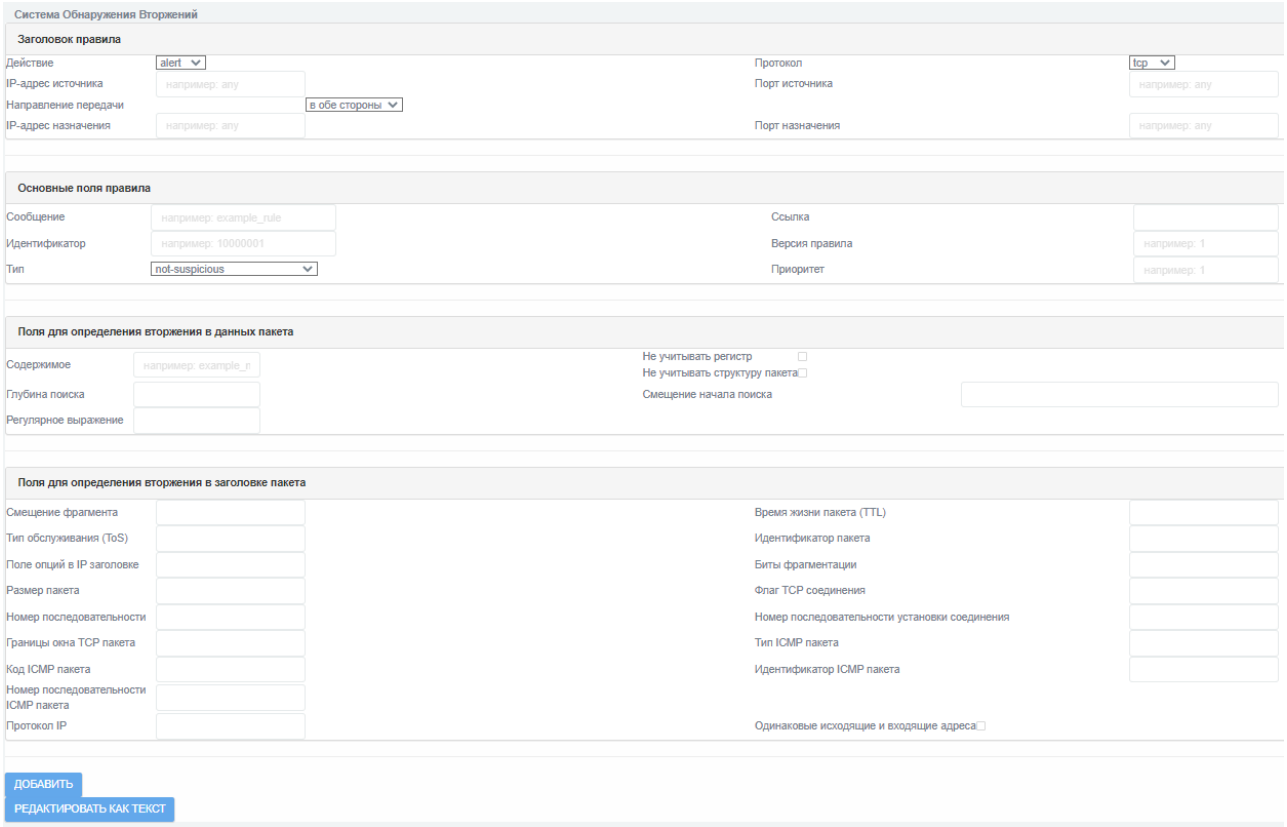

Рис. 115

Страница «Добавление правила СОВ» содержит следующие секции:

1) «Заголовок правила»;

2) «Основные поля правила»;

3) «Поля для определения вторжения в данных пакета»;

4) «Поля для определения вторжения в заголовке пакета».

4.6.1.1.1. Секция «Заголовок правила»

Секция «Заголовок правила» (см. рис. 116) предназначена для создания заголовка правила.

Секция «Заголовок правила»

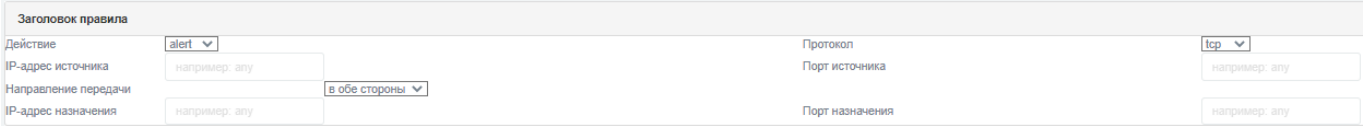

Рис. 116

В таблице 48 приведено описание элементов секции «Заголовок правила».

Таблица 48 – Описание элементов секции «Заголовок правила»

Элемент	Описание
Выпадающий список «Действие»	Предназначен для выбора дальнейшего действия изделия при срабатывании правила. Доступен для выбора один из следующих параметров: – **alert** (записывает информацию о срабатывании правила в журнал); – **pass** (игнорирует сетевой пакет); – **drop** (блокирует сетевой пакет и записывает информацию о срабатывании правила в журнал); – **reject** (блокирует сетевой пакет, записывает информацию о срабатывании правила в журнал и, затем отправляет сетевой пакет «TCP reset» (*при использовании протокола TCP*) или сетевой пакет «ICMP port unreachable» *(при использовании протокола UDP*)); – **sdrop** (блокирует пакет, но не записывает информацию о срабатывании правила в журнал)
Поле «IP-адрес источника»	Предназначено для ввода IP-адреса источника сетевого пакета
Выпадающий список «Направление передачи»	Предназначен для выбора направления передачи. Доступен для выбора один из следующих параметров: – в обе стороны; – в одну сторону
Поле «IP-адрес назначения»	Предназначено для ввода IP-адреса назначения сетевого пакета

Элемент	Описание
Выпадающий список «Протокол»	Предназначен для выбора используемого протокола для правила. Доступен для выбора один из следующих параметров: – tcp; – udp; – icmp; – ip
Поле «Порт источника»	Предназначено для ввода номера порта источника сетевого пакета
Поле «Порт назначения»	Предназначено для ввода номера порта назначения сетевого пакета

4.6.1.1.2. Секция «Основные поля правила»

Секция «Основные поля правила» (см. рис. 117Рис. 116) предназначена для заполнения основных полей правил.

Секция «Основные поля правила»

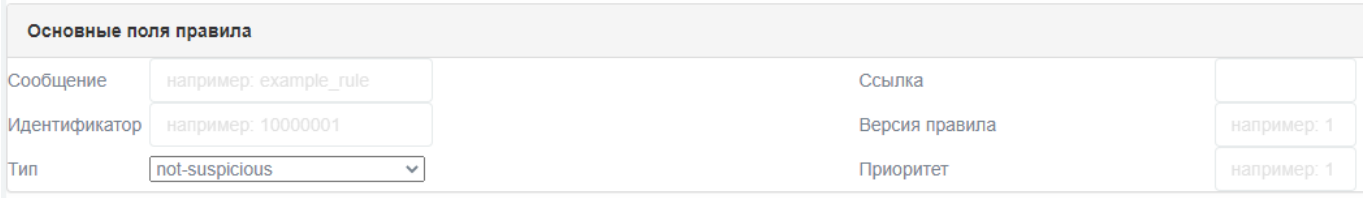

Рис. 117

В таблице 49 приведено описание элементов секции «Основные поля правила».

Таблица 49 – Описание элементов секции «Основные поля правила»

Элемент	Описание
Поле «Сообщение»	Предназначено для ввода имени / сообщения создаваемого правила
Поле «Идентификатор»*	Предназначено для ввода идентификатора правила. Необходимо указывать число больше 10000000
Выпадающий список «Тип»	Предназначен для выбора одного из доступных параметров типа для создаваемого правила
Поле «Ссылка»	Предназначено для ввода ссылки на информационные ресурсы, описывающие атаку, представленную данным правилом
Поле «Версия правила»	Предназначено для ввода версии правила

Элемент	Описание
Поле «Приоритет»	Предназначено для ввода приоритета правила
* – Элемент, обязательный к заполнению / выбору параметра	

4.6.1.1.3. Секция «Поля для определения вторжения в данных пакета»

Секция «Поля для определения вторжения в данных пакета» (см. рис. 118) предназначена для заполнения полей для определения вторжения в данных пакета.

Секция «Поля для определения вторжения в данных пакета»

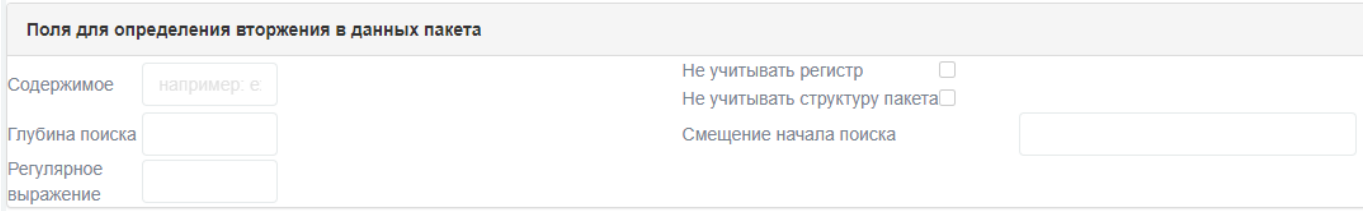

Рис. 118

В таблице 50 приведено описание элементов секции «Поля для определения вторжения в данных пакета».

Таблица 50 – Описание элементов секции «Поля для определения вторжения в данных пакета»

Элемент	Описание
Поле «Содержимое»	Предназначено для ввода содержимого пакета, определяющего срабатывание правила
Поле «Глубина поиска»	Предназначено для ввода длины последовательности относительно смещения, в которой осуществляется поиск требуемого содержимого
Поле «Регулярное выражение»	Предназначено для ввода регулярного выражения для поиска последовательности, определяющей срабатывание правила
Чекбокс «Не учитывать регистр»	Предназначен для выбора включения/отключения учета регистра в поле «Содержимое»
Чекбокс «Не учитывать структуру пакета»	Предназначен для выбора включения/отключения учета структуры пакета
Поле «Смещение начала поиска»	Предназначено для ввода смещения относительно начала пакета, от которого начинается поиск требуемого содержимого

4.6.1.1.4. Секция «Поля для определения вторжения в заголовке пакета»

Секция «Поля для определения вторжения в заголовке пакета» (см. рис. 119) предназначена для заполнения полей для определения вторжения в заголовке пакета.

Секция «Поля для определения вторжения в заголовке пакета»

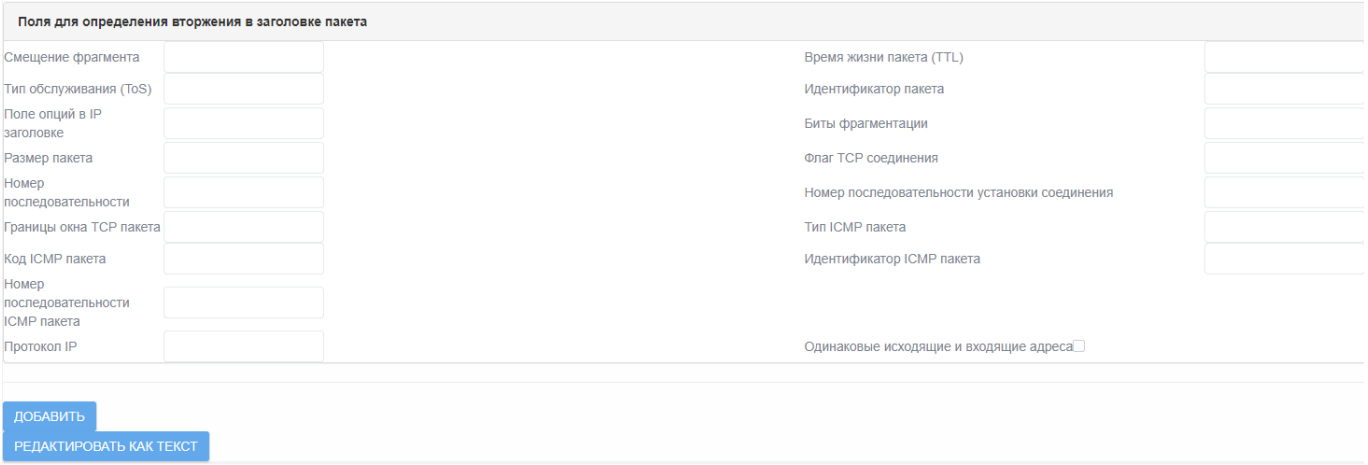

Рис. 119

В таблице 51 приведено описание элементов секции «Поля для определения вторжения в заголовке пакета».

Таблица 51 – Описание элементов секции «Поля для определения вторжения в заголовке пакета»

Элемент	Описание
Поле «Смещение фрагмента»	Предназначено для ввода значения смещения фрагмента
Поле «Тип обслуживания (ToS)»	Предназначено для ввода значения типа обслуживания (ToS)
Поле «Поле опций в IP заголовке»	Предназначено для ввода значения поля опций в IP заголовке пакета
Поле «Размер пакета»	Предназначено для ввода значения размера пакета
Поле «Номер последовательности»	Предназначено для ввода значения номера последовательности
Поле «Границы окна TCP пакета»	Предназначено для ввода значения границы окна TCP пакета
Поле «Код ICMP пакета»	Предназначено для ввода кода ICMP пакета

Элемент	Описание
Поле «Номер последовательности ICMP пакета»	Предназначено для ввода значения номера последовательности
Поле «Протокол IP»	Предназначено для ввода протокола IP
Поле «Время жизни пакета (TTL)»	Предназначено для ввода значения времени жизни пакета (TTL)
Поле «Идентификатор пакета»	Предназначено для ввода значения поля идентификатора пакета
Поле «Биты фрагментации»	Предназначено для ввода значения битов фрагментации
Поле «Флаг TCP соединения»	Предназначено для ввода значения флагов TCP соединения
Поле «Номер последовательности установки соединения»	Предназначено для ввода значения номера последовательности при установке соединения
Поле «Тип ICMP пакета»	Предназначено для ввода типа ICMP пакета
Поле «Идентификатор ICMP пакета»	Предназначено для ввода идентификатора ICMP пакета
Чекбокс «Одинаковые исходящие и входящие адреса»	Предназначен для выбора включения/отключения отслеживания одинаковых исходящих и входящих адресов
Кнопка «Добавить»	Предназначена для создания нового правила с заданными на данной странице параметрами
Кнопка «Редактировать как текст»	Предназначена для создания нового правила с дополнительными параметрами. Позволяет открыть страницу с возможностью строкового ввода параметров в синтаксисе правил «Snort»

4.6.1.2. Блок «Поиск правил СОВ по sid»

Блок «Поиск правил СОВ по sid» (см. рис. 120) предназначен для быстрого поиска в списке правил СОВ по номеру sid, который можно увидеть в журнале в случае атаки.

Блок «Поиск правил СОВ по sid»

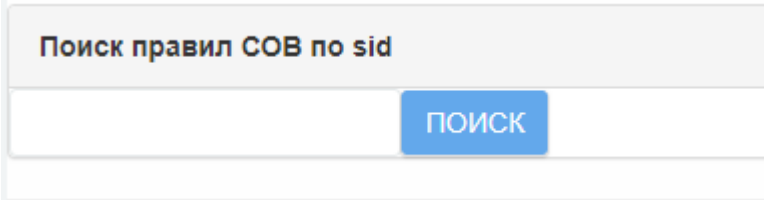

Рис. 120

На рисунках 121, 122, 123 показан пример поиска правила СОВ по известному номеру sid.

Ввод номера sid

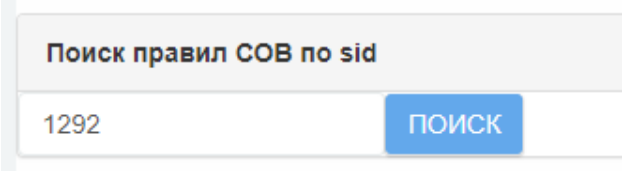

Рис. 121

Найденная поиском группа правил СОВ

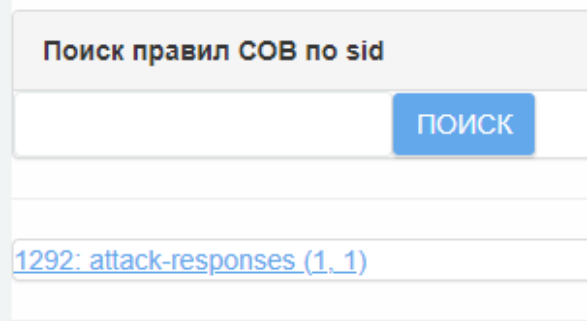

Рис. 122

Отображение в списке правил СОВ искомого правила

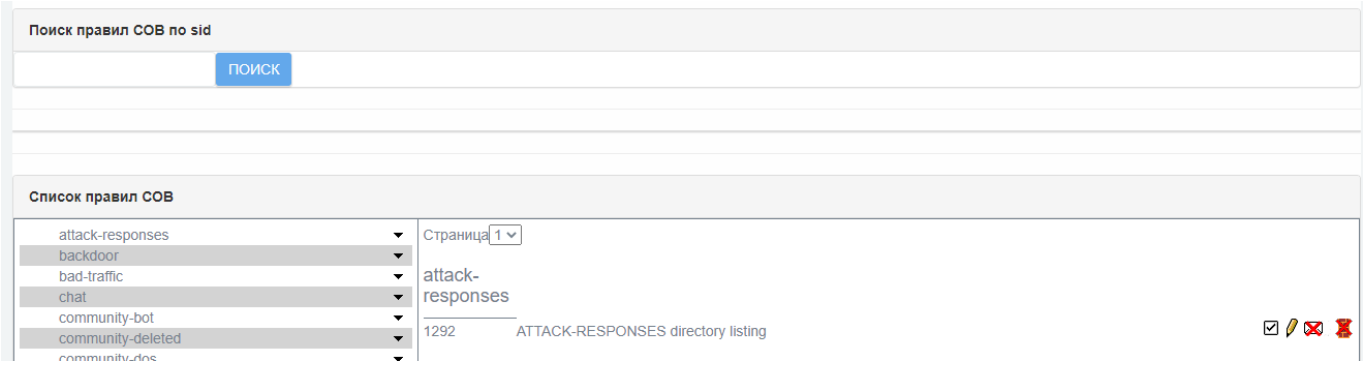

Рис. 123

Для того чтобы искомое правило отобразилось в списке правил СОВ необходимо нажать на найденное поиском правило (см. рис. 122) под строкой поиска.

4.6.1.3. Блок «Список правил СОВ»

Блок «Список правил СОВ» (см. рис. 124) содержит перечень правил СОВ с возможностью их редактирования.

Блок «Список правил СОВ»

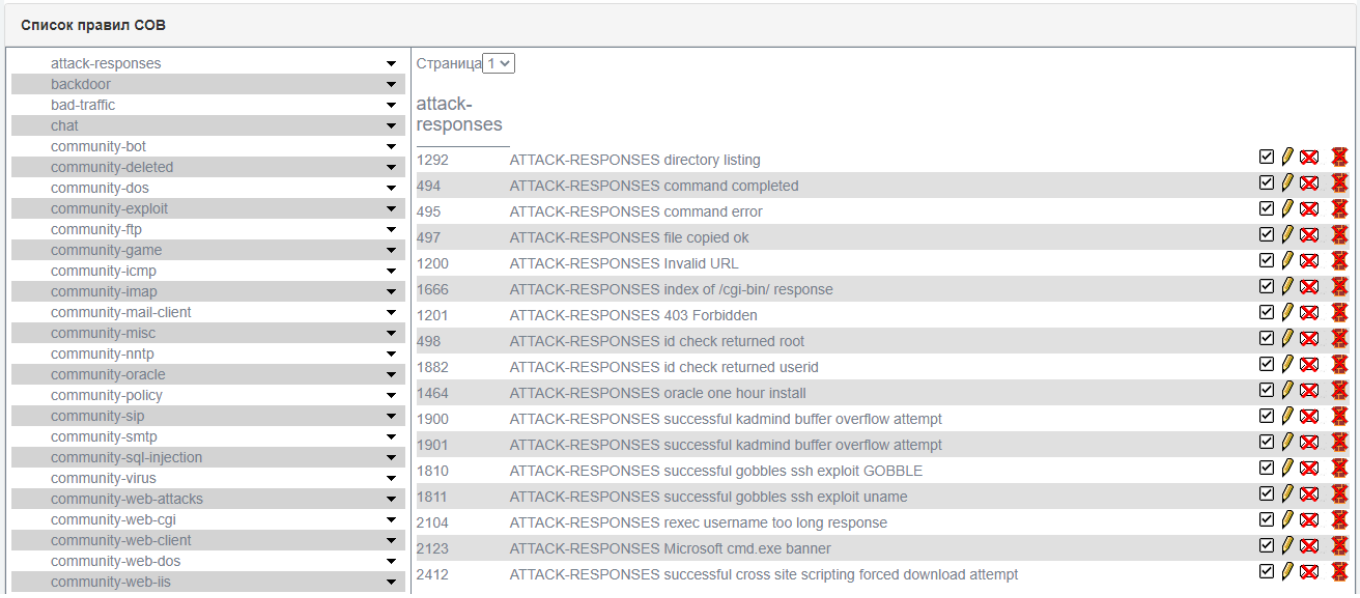

Рис. 124

В левом информационном поле содержится информация о группах правил СОВ. Пользовательские правила СОВ будут находиться в группе с названием «rubicon».

В таблице 52 приведено описание элементов блока «Список правил СОВ».

Таблица 52 – Описание элементов блока «Список правил СОВ»

Элемент	Описание
Кнопка « ▼ »	Предназначена для раскрытия однотипной группы правил

Элемент	Описание
Выпадающий список «Страница»	Предназначен для выбора номера просматриваемой страницы с правилами СОВ. Информационное поле, отображающее перечень правил СОВ, предоставляет возможность просматривать перечень до 150 правил на одной странице. Для дальнейшего просмотра перечня необходимо выбрать следующую страницу в данном списке
Чекбокс «**имя правила**»	Предназначен для выбора включения/отключения правила СОВ и позволяет пользователю включать или отключать выбранное правило, не удаляя его
Кнопка « »	Предназначена для редактирования правила. При нажатии открывается форма редактирования правил
Кнопка « »	Предназначена для включения/отключения уведомлений на почту о срабатывании правила
Кнопка « »	Предназначена для включения/отключения автоматического добавления правил сетевого экрана при срабатывании правила
Кнопка « »	Предназначена для удаления правила СОВ. Доступна **только** для пользовательских правил, **находящихся в группе «rubicon»** (см. п. 4.6.1.1 настоящего документа)

Под блоком «Список правил СОВ» представлена легенда (см. рис. 125) всех возможных действий с правилами в подразделе «Настройка правил СОВ».

Легенда подраздела «Настройка правил СОВ»

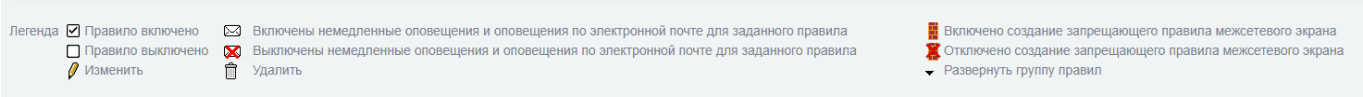

Рис. 125

4.6.1.3.1. Страница редактирования правил

Страница редактирования правил (см. рис. 126) предоставляет к настройке элементы, соответствующие описанным ранее в п. 4.6.1.1.1 настоящего документа.

Для всех правил, находящихся в группе «rubicon», доступны для изменения все поля правила СОВ. Для всех остальных групп – основные поля правила (выделены серым) для изменения недоступны.

Страница редактирования правил

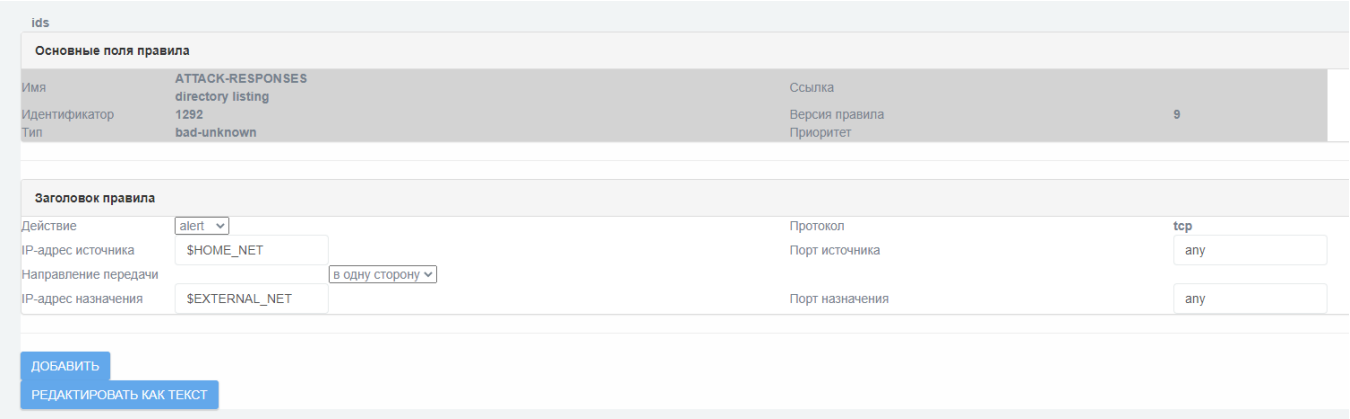

Рис. 126

4.6.2. Подраздел «Настройка обнаружения»

Подраздел «Настройка обнаружения» (см. рис. 127) предназначен для настройки параметров функции обнаружения сканирования.

Подраздел «Настройка обнаружения»

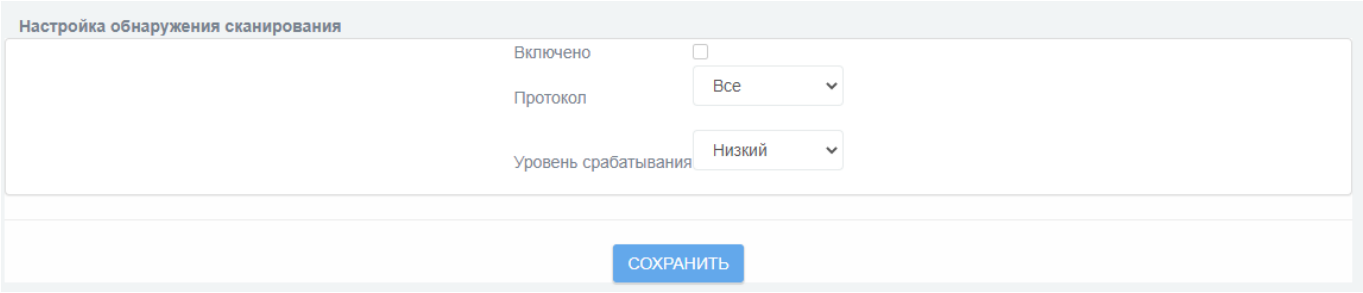

Рис. 127

В таблице 53 приведено описание элементов подраздела «Настройка обнаружения».

Таблица 53 – Описание элементов подраздела «Настройка обнаружения»

Элемент	Описание
Чекбокс «Включено»	Предназначен для выбора включения/отключения системы обнаружения сканирования

Элемент	Описание
Выпадающий список «Протокол»	Предназначен для выбора одного из доступных протоколов: – «Все»; – «TCP»; – «UDP»; – «ICMP»; – «Протокол IP»
Выпадающий список «Уровень срабатывания»	Предназначен для выбора одного из доступных уровней срабатывания: – «Низкий»; – «Средний»; – «Высокий»
Кнопка «Сохранить»	Предназначена для сохранения введенных ранее настроек

4.6.3. Подраздел «Обнаружение Атак»

Подраздел «Обнаружение Атак» (см. рис. 128) предназначен для установки параметров обнаружения атак и загрузки наборов правил.

Подраздел «Обнаружение Атак»

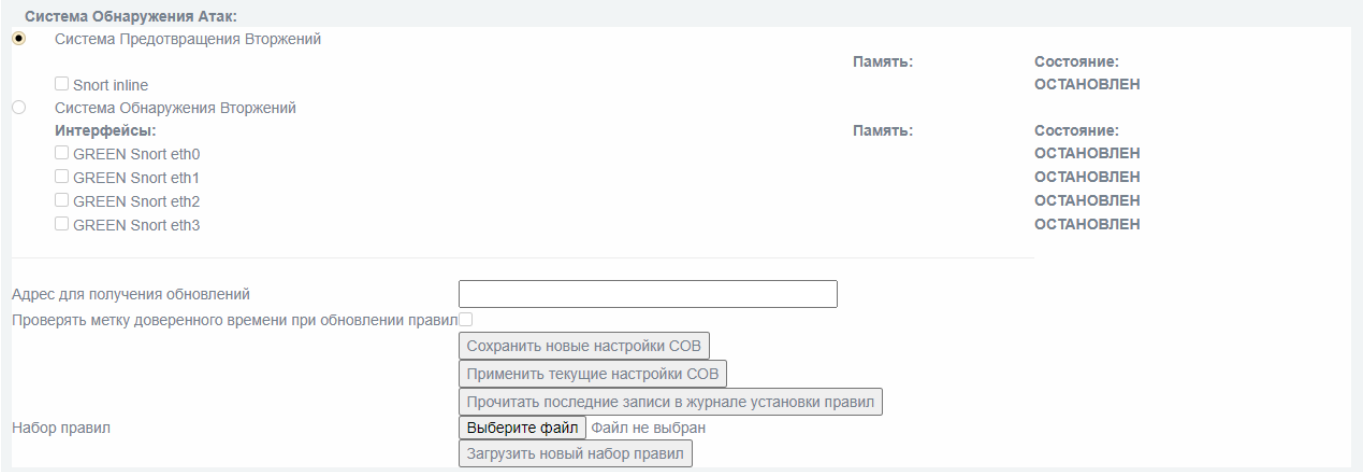

Рис. 128

В таблице 54 приведено описание элементов подраздела «Обнаружение Атак».

Таблица 54 – Описание элементов подраздела «Обнаружение Атак»

Элемент	Описание
Чекбокс «Система Предотвращения Вторжений»	Предназначен для выбора режима работы «Система Предотвращения Вторжений». Для активации работы режима необходимо включить службу «Snort inline»
Чекбокс «Snort inline»	Предназначен для выбора включения/отключения службы «Snort inline» и активации режима работы «Система Предотвращения Вторжений»
Информационное поле «Память»	Предназначен для отображения информации об оперативной памяти (в МБ), занимаемой процессом обнаружения вторжения (для перечисленных в подразделе режимов работы изделия)
Информационное поле «Состояние»	Предназначен для отображения информации о состоянии работы служб системы обнаружения атак
Чекбокс «Система Обнаружения Вторжений»	Предназначен для выбора режима работы «Система Обнаружения Вторжений». Для активации работы режима необходимо выбрать сетевой интерфейс, на котором она будет активирована.
Чекбокс «**имя интерфейса**»	Предназначен для выбора сетевого интерфейса и активации на нем службы обнаружения вторжений в режиме «Система Обнаружения Вторжений». *По умолчанию у сетевых интерфейсов, подключаемых к внутренней сети, все пакеты, маршрутизируемые между различными зелеными интерфейсами, не блокируются*
Поле «Адрес для получения обновлений»	Предназначено для ввода адреса для получения обновлений
Чекбокс «Проверять метку доверенного времени при обновлении правил»	Предназначен для выбора включения/отключения проверки метки доверенного времени при обновлении правил
Кнопка «Сохранить новые настройки СОВ»	Предназначена для сохранения настроек системы обнаружения вторжения. Внесенные изменения будут учтены при следующем запуске изделия или после нажатия кнопки «Применить текущие настройки СОВ»
Кнопка «Применить текущие настройки СОВ»	Предназначена для немедленного применения установленных параметров обнаружения атак. Нажатие этой кнопки приводит к полному перезапуску системы обнаружения вторжений на указанных ранее интерфейсах
Кнопка «Прочитать последние записи в журнале установки правил»	Предназначена для отображения последней записи в журнале установки правил
Кнопка «Выберите файл»	Предназначена для открытия системного окна ЭВМ для выбора загружаемого файла базы решающих правил
Кнопка «Загрузить новый набор правил»	Предназначена для загрузки нового набора базы решающих правил системы обнаружения вторжений из выбранного пользователем файла

4.6.4. Подраздел «Переменные СОВ»

Подраздел «Переменные СОВ» (см. рис. 129) предназначен для указания значений переменных в решающих правилах СОВ.

Подраздел «Переменные СОВ»

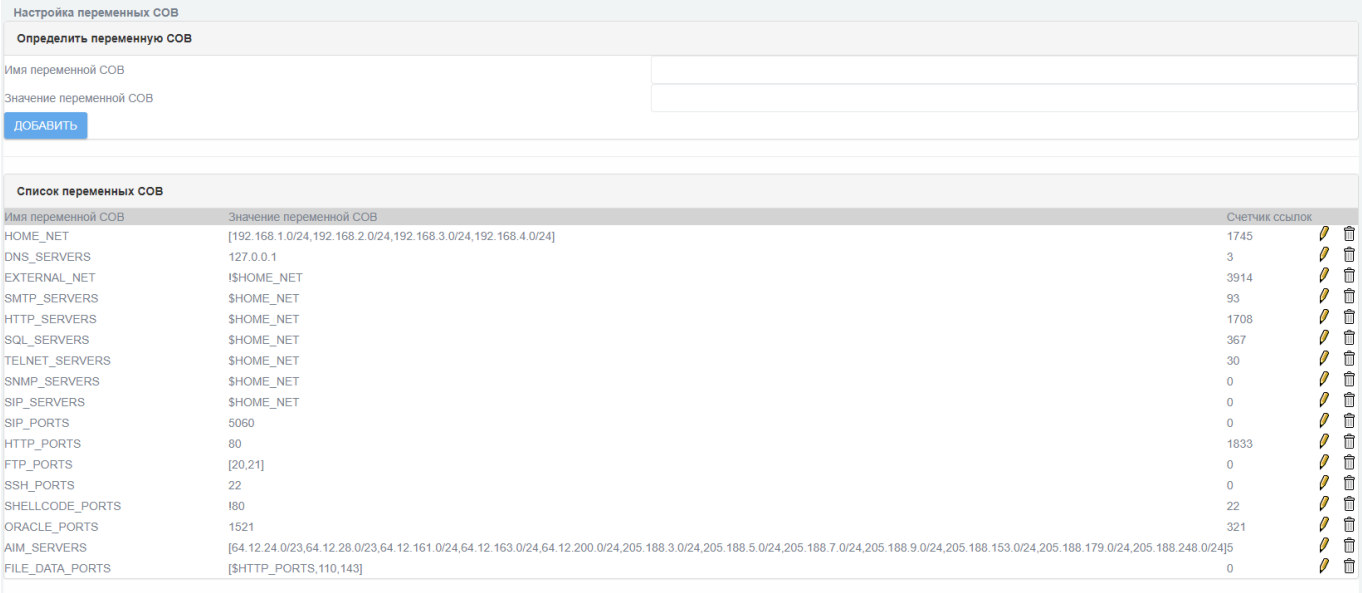

Рис. 129

Подраздел «Переменные СОВ» состоит из следующих блоков:

1) «Определить переменную СОВ»;

2) «Список переменных СОВ».

4.6.4.1. Блок «Определить переменную СОВ»

Блок «Определить переменную СОВ» (см. рис. 130) предназначен для добавления новой переменной СОВ.

Блок «Определить переменную СОВ»

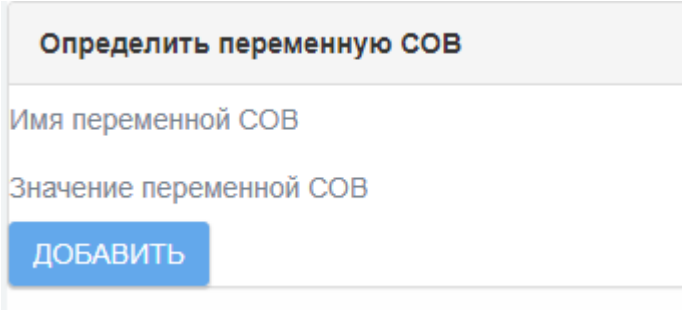

Рис. 130

В таблице 55 приведено описание элементов подраздела «Определить переменную СОВ».

Таблица 55 – Описание элементов блока «Определить переменную СОВ»

Элемент	Описание
Поле «Имя переменной СОВ»	Предназначено для ввода имени переменной СОВ
Поле «Значение переменной СОВ»	Предназначено для ввода сетевых объектов или сервисов. В значении переменной могут быть указаны **комбинации других переменных, IP-адресов и портов**. Допустимо пользоваться их перечислением через запятую (при этом содержание переменной нужно заключить в скобки), а также другими переменными (в формате $Имя_переменной)
Кнопка «Добавить»	Предназначена для сохранения и добавления переменной СОВ в список переменных СОВ

4.6.4.2. Блок «Список переменных СОВ»

Блок «Список переменных СОВ» (см. рис. 131) представлен в виде информационной таблицы.

Данный блок предназначен для отображения и редактирования списка переменных СОВ.

Блок «Список переменных СОВ»

Список переменных СОВ

Имя переменной СОВ	Значение переменной СОВ	Счетчик ссылок
HOME_NET	[192.168.1.0/24,192.168.2.0/24,192.168.3.0/24,192.168.4.0/24]	1745
DNS_SERVERS	127.0.0.1	3
EXTERNAL_NET	!$HOME_NET	3914
SMTP_SERVERS	$HOME_NET	93
HTTP_SERVERS	$HOME_NET	1708
SQL_SERVERS	$HOME_NET	367
TELNET_SERVERS	$HOME_NET	30
SNMP_SERVERS	$HOME_NET	0
SIP_SERVERS	$HOME_NET	0
SIP_PORTS	5060	0
HTTP_PORTS	80	1833
FTP_PORTS	[20,21]	0
SSH_PORTS	22	0
SHELLCODE_PORTS	!80	22
ORACLE_PORTS	1521	321
AIM_SERVERS	[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179.0/24,205.188.248.0/24]	5
FILE_DATA_PORTS	[$HTTP_PORTS,110,143]	0

Рис. 131

Столбец «Имя переменной СОВ» содержит перечень переменных, используемых в правилах СОВ. В столбце «Значения переменной СОВ» в соответствующих переменным строках отображаются их актуальные значения. В столбце «Счетчик ссылок» в соответствующих переменным строках содержится значение счетчика использования соответствующей переменной.

Для редактирования значения переменной СОВ необходимо нажать кнопку « » (изменить), после чего данные в поле «Значение переменной СОВ» подлежат редактированию (см. рис. 132). Для удаления переменной СОВ нажмите кнопку « ».

Редактирование переменной СОВ

Список переменных СОВ

Имя переменной СОВ	Значение переменной СОВ	Счетчик ссылок
HOME_NET	[192.168.1.0/24,192.168.2.0/24,192.168.3.0/24,192.168.4.0/24]	1745
DNS_SERVERS	127.0.0.1	3
EXTERNAL_NET	!$HOME_NET	3914
SMTP_SERVERS	$HOME_NET	93
HTTP_SERVERS	$HOME_NET	1708
SQL_SERVERS	$HOME_NET	367
TELNET_SERVERS	$HOME_NET	30
SNMP_SERVERS	$HOME_NET	0
SIP_SERVERS	$HOME_NET	0
SIP_PORTS	5060	0
HTTP_PORTS	80	1833
FTP_PORTS	[20,21]	0
SSH_PORTS	22	0
SHELLCODE_PORTS	!80	22
ORACLE_PORTS	1521	321
AIM_SERVERS	[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179.0/24,205.188.248.0/24]	5
FILE_DATA_PORTS	[$HTTP_PORTS,110,143]	0

Рис. 132

4.7. Раздел «Межсетевой экран»

Раздел «Межсетевой экран» содержит следующие подразделы:

1) «Настройки межсетевого экрана»;

2) «Доступ к Синему интерфейсу»;

3) «Службы»;

4) «Группы служб»;

5) «Адреса»;

6) «Группы адресов»;

7) «Интерфейсы по умолчанию»;

8) «Группы состояний»;

9) «Правила межсетевого экрана»;

10) «Конфигурация DMZ».

При настройке межсетевого экрана возникает необходимость использовать заранее предопределенные мнемонические обозначения параметров, например, определенных портов или адресов, связанных с конкретной сетью, либо их групп.

Администратор межсетевого экрана может вносить в изделие дополнительные записи для следующих элементов:

1) адреса;

2) службы;

3) группы адресов;

4) группы служб;

5) сетевые интерфейсы;

6) группы состояний.

4.7.1. Подраздел «Настройки межсетевого экрана»

Подраздел «Настройки межсетевого экрана» (см. рис. 133) предназначен для установки параметров администрирования межсетевого экрана. Общая настройка межсетевого экрана заключаются в настройке административного доступа к межсетевому экрану, выборе режимов его работы, а также в установке политик по умолчанию на интерфейсах.

Подраздел «Настройки межсетевого экрана»

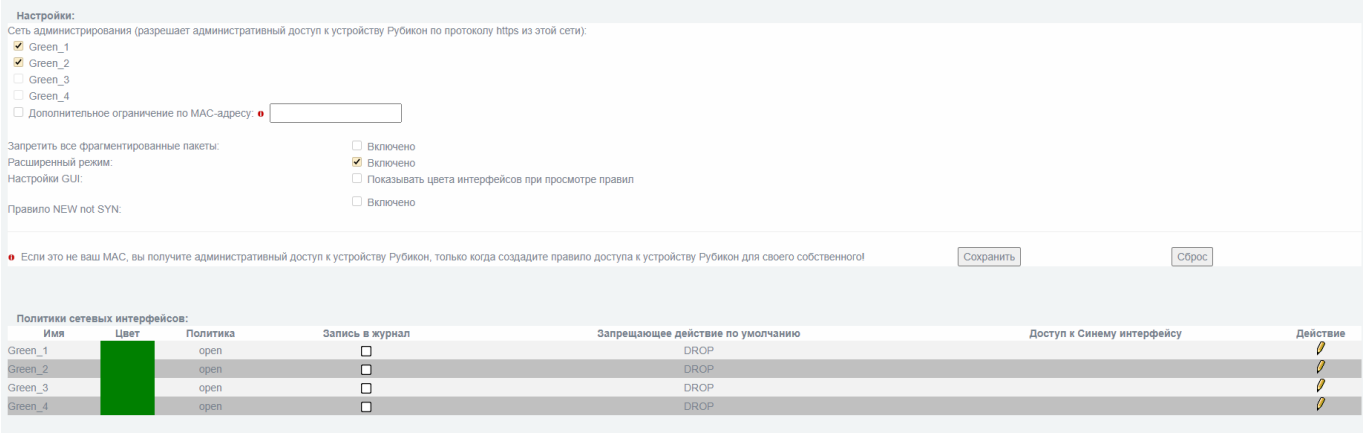

Рис. 133

Подраздел «Настройки межсетевого экрана» состоит из следующих блоков:

1) «Настройки»;

2) «Политики сетевых интерфейсов».

4.7.1.1. Блок «Настройки»

Блок «Настройки» (см. рис. 134) предназначен для ввода настроек межсетевого экрана.

Блок «Настройки»

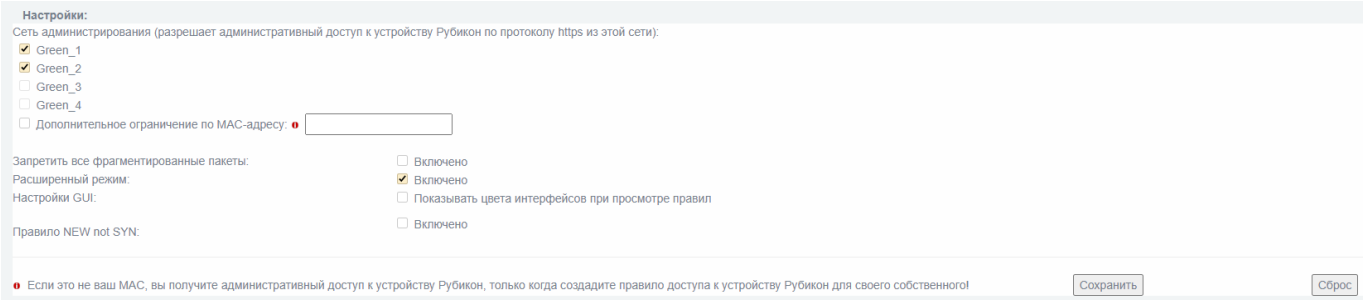

Рис. 134

В таблице 56 приведено описание элементов блока «Настройки».

Таблица 56 – Описание элементов блока «Настройки»

Элемент	Описание
Чекбоксы «Сеть администрирования *имя интерфейса*»	Предназначен для выбора включения/отключения разрешения административного доступа к изделию для доступных в перечне сетевых интерфейсов, подключаемых к внутренней сети по протоколу https из этой сети
Чекбокс «Дополнительное ограничение по MAC-адресу»	Предназначен для выбора включения/отключения функции ограничения по MAC-адресу ЭВМ, с которого возможно администрирование МЭ. MAC-адрес необходимо указывать в поле «Дополнительное ограничение по MAC-адресу». После активации данного чекбокса администрирование с других MAC-адресов будет **невозможно**. Примечание. Если это не ваш MAC-адрес, вы получите административный доступ к изделию, только тогда, когда будет **создано правило доступа** к изделию для собственного MAC-адреса ЭВМ администратора
Поле «Дополнительное ограничение по MAC-адресу»	Предназначено для ввода MAC-адреса ЭВМ, с которого возможно администрирование МЭ
Чекбокс «Запретить все фрагментированные пакеты»	Предназначен для выбора включения/отключения блокировки сетевых пакетов с флагом фрагментации в IP-заголовке
Чекбокс «Расширенный режим»	Предназначен для выбора включения/отключения
Чекбокс «Настройки GUI»	Предназначен для выбора включения/отключения цветной индикации интерфейсов при просмотре правил МЭ. Примечание. Активный чекбокс позволяет изделию показывать цвета интерфейсов при просмотре правил
Чекбокс «Правило NEW not SYN»	Предназначен для выбора включения/отключения блокировки SYN-пакетов по протоколу TCP для которых не было установлено соединение

Элемент	Описание
Кнопка «Сохранить»	Предназначена для сохранения введенных данных
Кнопка «Сброс»	Предназначена для отмены введенных настроек блока до состояния последней сохраненной конфигурации

4.7.1.2. Блок «Политики сетевых интерфейсов»

Блок «Политики сетевых интерфейсов» (см. рис. 135) содержит перечень текущих настроек политик сетевых интерфейсов.

Блок «Политики сетевых интерфейсов»

Рис. 135

Блок «Политики сетевых интерфейсов» представлен в виде таблицы, информация в которой представлена со следующими параметрами:

1) «Имя»;

2) «Цвет»;

3) «Политика;

4) «Запись в журнал»;

5) «Запрещающее действие по умолчанию»;

6) «Доступ к Синему интерфейсу»;

7) «Действие».

В таблице 57 приведено описание элементов блока «Политики сетевых интерфейсов».

Таблица 57 – Описание элементов блока «Политики сетевых интерфейсов»

Элемент	Описание
Чекбокс «Запись в журнал»	Предназначен для выбора включения/отключения записи о событиях в журнал

Элемент	Описание
Кнопка « »	Кнопка «Изменить». Предназначена для открытия страницы «Изменение настройки политики сетевых интерфейсов» для редактирования политики по умолчанию выбранного интерфейса

4.7.1.2.1. Страница «Изменение настройки политики сетевых интерфейсов»

Страница «Изменение настройки политики сетевых интерфейсов» (см. рис. 136) позволяет изменить политику по умолчанию выбранного сетевого интерфейса.

Подробная информация о настройке политики по умолчанию для сетевых интерфейсов указана в п. 2.3 руководства администратора НПЕШ.465614.005РА.

Страница «Изменение настройки политики сетевых интерфейсов»

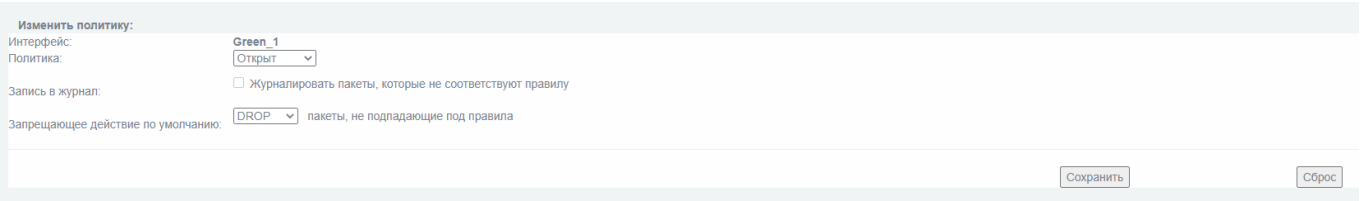

Рис. 136

В таблице 58 приведено описание доступных к изменению элементов страницы «Изменение настройки политики сетевых интерфейсов».

Таблица 58 – Описание элементов страницы «Изменение настройки политики сетевых интерфейсов»

Элемент	Описание
Информационное поле «Интерфейс»	Предназначено для отображения информации о наименовании выбранного для изменений сетевого интерфейса
Выпадающий список «Политика»	Предназначен для выбора одного из следующих параметров: – «Открыт»; – «Полуоткрыт»; – «Закрыт»
Чекбокс «Запись в журнал»	Предназначена для выбора включения/отключения журналирования пакетов, которые не соответствуют правилу

Элемент	Описание
Выпадающий список «Запрещающее действие по умолчанию»	Предназначен для выбора одного из следующих параметров: – «DROP»; – «REJECT»
Кнопка «Сохранить»	Предназначена для сохранения введенных данных
Кнопка «Сброс»	Предназначена для отмены введенных настроек страницы до состояния последней сохраненной конфигурации

4.7.2. Подраздел «Доступ к Синему интерфейсу»

Подраздел «Доступ к Синему интерфейсу» (см. рис. 137) предназначен для настройки доступа узлов (источников) к «синему» интерфейсу.

Подраздел «Доступ к Синему интерфейсу»

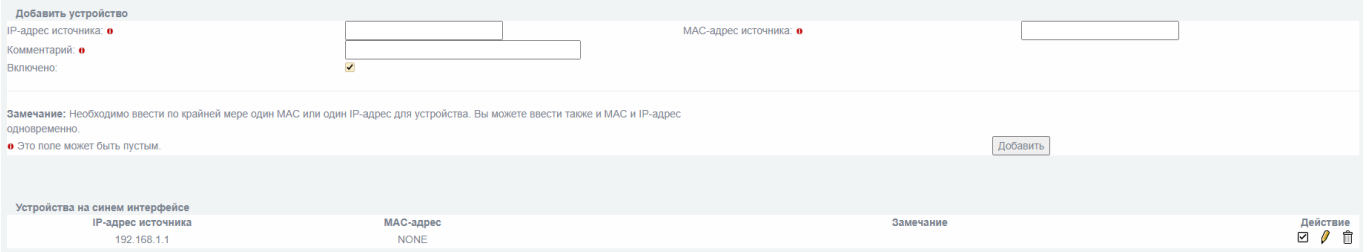

Рис. 137

В соответствии с цветовым профилем настроек МЭ узлы «синего» интерфейса могут иметь доступ в «зеленый» интерфейс только при наличии специальных разрешений. Такие разрешения необходимо устанавливать в данном подразделе меню изделия.

В таблице 59 приведено описание элементов подраздела «Доступ к Синему интерфейсу».

Таблица 59 – Описание элементов подраздела «Доступ к Синему интерфейсу»

Элемент	Описание
Поле «IP-адрес источника»*	Предназначено для ввода IP-адреса устройства
Поле «Комментарий»*	Предназначено для ввода описания

Элемент	Описание
Чекбокс «Включено»	Предназначена для выбора включения/отключения добавляемого устройства
Поле «MAC-адрес источника»*	Предназначено для ввода MAC-адрес источника
Кнопка «Добавить»	Предназначена для добавления нового устройства с заданными настройками.
Информационная таблица «Устройства на синем интерфейсе»	Предназначена для отображения добавленных пользователем устройств (сетевых узлов)
Чекбокс «Активация устройства»	Предназначена для выбора включения/отключения выбранного устройства
Кнопка « »	Кнопка «Изменить». Предназначена для открытия страницы «Изменение настройки устройства» для редактирования, где после внесения изменений необходимо нажать кнопку «Обновить»
Кнопка « »	Кнопка «Удалить». Предназначена для удаления сетевого узла из перечня устройств на «синем» интерфейсе
* – Поля, не обязательные к заполнению. Необходимо ввести по крайней мере один MAC или один IP-адрес для устройства. Вы можете ввести также и MAC и IP-адрес одновременно	

4.7.3. Подраздел «Службы»

Подраздел «Службы» (см. рис. 138) предназначена для внесения дополнительной службы или определенного порта для взаимодействия на транспортном уровне.

Подраздел «Службы»

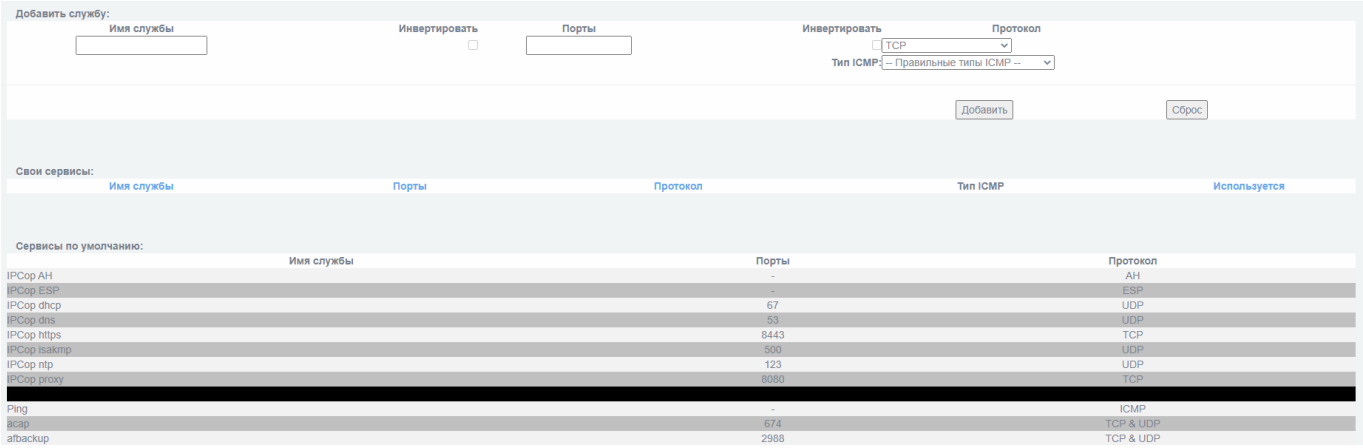

Рис. 138

Данный подраздел позволяет создавать новые сетевые службы для удобного задания правил МЭ, а также содержит список уже установленных служб.

МЭ содержит перечень основных служб и портов, которые используются в сети и зарегистрированы Центром назначения идентификаторов IANA. При возникновении необходимости использования дополнительной службы (порта) в целях фильтрации МЭ изделия необходимо добавить ее в список служб в интерфейсе управления.

В таблице 60 приведено описание элементов подраздела «Службы».

Таблица 60 – Описание элементов подраздела «Службы»

Элемент	Описание
Поле «Имя службы»	Предназначено для ввода имени службы. Допустимы символы латинского алфавита и цифры 0 – 9
Чекбокс «Инвертировать порты»*	Предназначена для выбора включения/отключения функции инвертирования порта, то есть всех портов кроме указанного
Поле «Порты»	Предназначено для ввода портов для службы. Допустимы числовые значения в диапазоне от 1 до 65535 или диапазон из значений номеров начального и конечного порта, разделенных знаком «-», которые будут указывать на транспортном уровне на порт (порты), используемые при взаимодействии. Данное поле заполняется в том случае, если служба предполагает порты транспортного уровня. *Например, служба OSPF не использует порты, поэтому заполнять это поле не требуется.* В случае, если требуется определить службу транспортного уровня, которая предполагает использование всех, кроме определенных портов, необходимо указать данные порты и активировать чекбокс «Инвертировать порты»
Чекбокс «Инвертировать Протокол»*	Предназначена для выбора включения/отключения функции инвертирования типа сообщения протокола ICMP, то есть всех типов сообщения ICMP кроме указанного
Выпадающий список «Протокол»	Предназначен для выбора одного из представленных в списке протоколов, который будет использовать служба
Выпадающий список «Тип ICMP»	Предназначен для выбора одного из представленных в списке типов ICMP
Кнопка «Добавить»	Предназначена для добавления новой службы с введенными настройками
Кнопка «Сброс»	Предназначена для отмены введенных настроек добавления службы. После нажатия перезагружает страницу и возвращает к подразделу «Службы». Не удаляет уже добавленные ранее службы
Информационная таблица «Свои сервисы»	Предназначена для отражения информации о сервисах, добавленных пользователем вручную
Кнопка « »	Кнопка «Изменить». Предназначена для редактирования служб, установленных пользователем вручную

Элемент	Описание
Кнопка « »	Кнопка «Удалить» в строке таблицы напротив определенной службы, установленной пользователем вручную, предназначена для удаления данной службы
Информационная таблица «Сервисы по умолчанию»	Предназначена для отражения информации о сервисах по умолчанию, имеющих специальное имя в изделии
Разделитель « » информационной таблицы	Предназначен для визуального отделения в таблице сервисов по умолчанию, имеющих специальное имя в изделии (часто используемые для доступа к изделию) от остальных именованных сетевых служб
* – Инвертированные поля отображаются в красных скобках со знаком «!»	

4.7.4. Подраздел «Группы служб»

Подраздел «Группы служб» (см. рис. 139) предназначен для группировки различных сетевых служб под одним обозначением для удобного задания правил МЭ.

Подраздел «Группы служб»

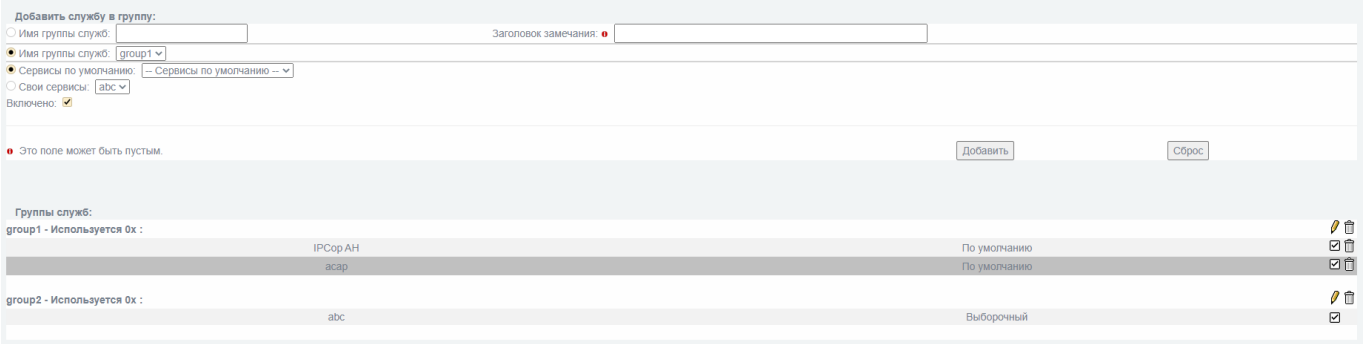

Рис. 139

В таблице 61 приведено описание элементов подраздела «Группы служб».

Таблица 61 – Описание элементов подраздела «Группы служб»

Элемент	Описание
Чекбокс «Имя группы служб»	Предназначен для выбора необходимости ввода нового имени группы служб. При отсутствии созданных групп выбор данного поля происходит автоматически
Поле «Имя группы служб»	Предназначено для ввода имени группируемых служб при активированном чекбоксе. Допустимы символы латинского алфавита и цифры 0 – 9

Элемент	Описание
Выпадающий список «Имя группы служб»	Предназначен для выбора одного из ранее введенных имен групп служб. Появляется если существует хотя бы одна ранее созданная пользователем группа
Поле «Заголовок замечания»	Предназначено для ввода примечаний к группе служб. Примечание. Данное поле не обязательно к заполнению
Чекбокс «Сервисы по умолчанию»	Предназначен для выбора добавления сервиса по умолчанию
Выпадающий список «Сервисы по умолчанию»	Предназначен для выбора одного из сервисов по умолчанию, имеющих специальное имя в изделии или именованных сетевых служб
Чекбокс «Свои сервисы»	Предназначен для выбора добавления сервиса из списка ранее добавленных пользователем вручную
Выпадающий список «Свои сервисы»	Предназначен для выбора одного из ранее добавленных пользователем вручную сервисов. Появляется если настроен хотя бы один сервис, добавленный пользователем вручную
Чекбокс «Включено»	Предназначен для выбора активации/деактивации созданной службы в выбранной группе. Примечание. Не активные службы не будут присутствовать в правилах МЭ при использовании выбранной группы
Кнопка «Добавить»	Предназначена для добавления службы в выбранную группу
Кнопка «Сброс»	Предназначена для отмены введенных настроек добавления службы. После нажатия перезагружает страницу. Не удаляет уже добавленные ранее службы
Информационная таблица «Группы служб»	Предназначена для отображения информации о группах служб, созданных пользователем вручную
Кнопка « »	Кнопка «Изменить». Предназначена для редактирования группы служб и открывает страницу «Изменение групп служб»
Кнопка « »	Кнопка «Удалить». Предназначена для удаления групп служб (кнопка в заголовке выбранной группы) и самих служб (кнопка справа от выбранной службы). Примечания: 1. Группу служб возможно удалить если она не используется изделием. Кнопка удаления группы служб присутствует только если данная группа не используется изделием. 2. Группа содержит хотя бы одну службу. Если в группе присутствует всего одна служба, то ее нельзя удалить отдельно – в таком случае необходимо удалять всю группу
Чекбокс «*имя службы*»	Предназначен для выбора активации/деактивации выбранной службы в группе. Примечание. Не активные службы не будут присутствовать в правилах МЭ при использовании выбранной группы

4.7.4.1. Страница «Изменение групп служб»

Страница «Изменение групп служб» (см. рис. 140) предназначена для изменения вручную добавленных пользователем групп служб.

Страница «Изменение групп служб»

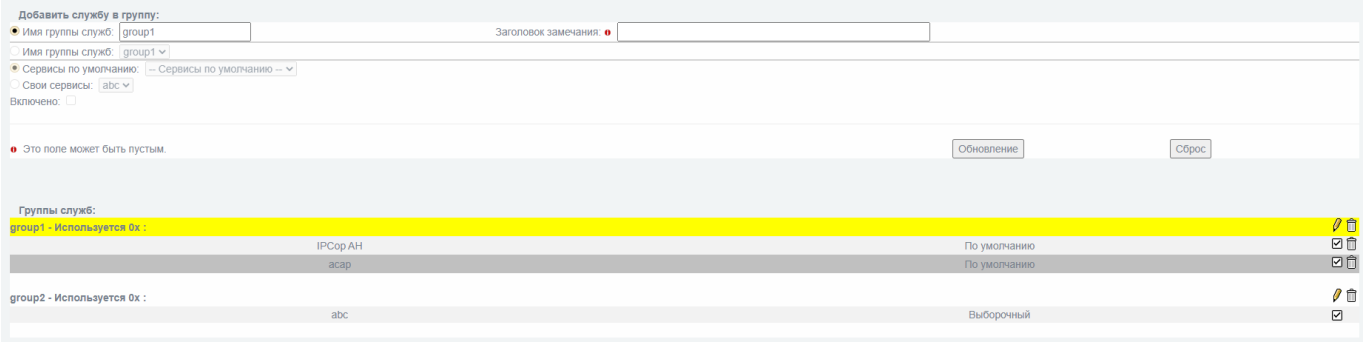

Рис. 140

В таблице 62 приведено описание доступных к изменению элементов страницы «Изменение групп служб».

Таблица 62 – Описание элементов страницы «Изменение групп служб»

Элемент	Описание
Поле «Имя группы служб»	Предназначено для редактирования имени выбранной группы
Поле «Заголовок замечания»	Предназначено для редактирования/добавления примечаний к группе служб. Примечание. Данное поле не обязательно к заполнению
Кнопка «Обновление»	Предназначена для сохранения и применения отредактированных настроек группы
Кнопка «Сброс»	Предназначена для отмены введенных настроек группы служб. После нажатия перезагружает страницу и возвращает к подразделу «Группы служб»

4.7.5. Подраздел «Адреса»

Подраздел «Адреса» (см. рис. 141) предназначен для предопределения адресов сетевых узлов для удобного указания правил МЭ.

Подраздел «Адреса»

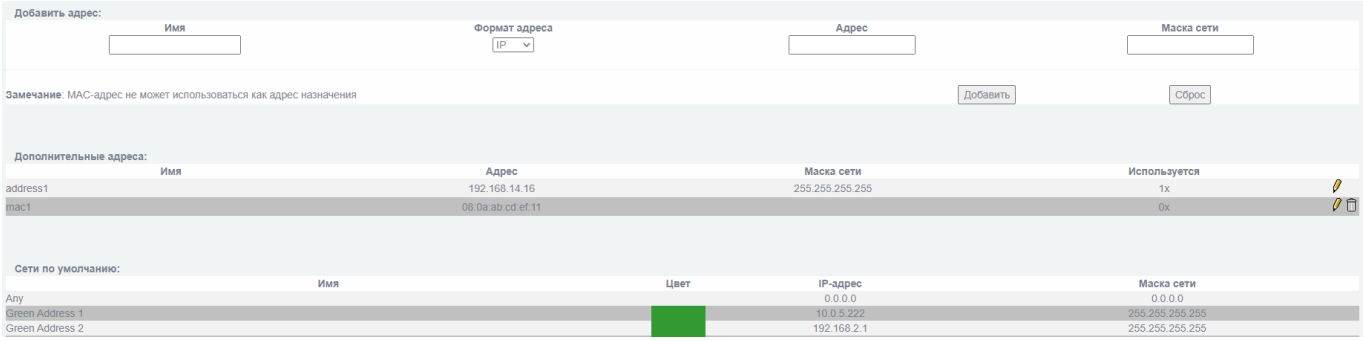

Рис. 141

В таблице 63 приведено описание элементов подраздела «Адреса».

Таблица 63 – Описание элементов подраздела «Адреса»

Элемент	Описание
Поле «Имя»	Предназначено для ввода имени (обозначения) адреса
Выпадающий список «Формат адреса»	Предназначено для выбора одного из форматов (типов) адреса для поля ввода «Адрес». Доступны варианты: **IP** или **MAC** (выбор MAC необходим для указания одиночного MAC-адреса сетевого устройства)
Поле «Адрес»	Предназначено для ввода адреса сетевого узла. Примечание. MAC-адрес не может использоваться как адрес назначения
Поле «Маска сети»	Предназначено для ввода маски сети в полном десятичном виде
Кнопка «Добавить»	Предназначена для добавления новой записи об адресе сетевого узла с введенными пользователем настройками
Кнопка «Сброс»	Предназначена для отмены введенных настроек новой записи об адресе сетевого узла. После нажатия перезагружает страницу
Информационная таблица «Дополнительные адреса»	Предназначена для отображения информации о дополнительных адресах сетевых узлов, созданных пользователем вручную
Кнопка « »	Кнопка «Изменить» в строке таблицы напротив определенного дополнительного адреса сетевого узла, добавленного пользователем вручную предназначена для редактирования данного адреса и открывает страницу «Изменение адреса»
Кнопка « »	Кнопка «Удалить» в строке таблицы напротив определенного дополнительного адреса сетевого узла, добавленного пользователем вручную, предназначена для удаления данного адреса. Примечание. Адрес сетевого узла возможно удалить если он не используется изделием. Кнопка удаления адреса сетевого узла присутствует только если данная группа не используется изделием.

Элемент	Описание
Информационная таблица «Сети по умолчанию»	Предназначена для отражения информации о сетях, связанных с сетевыми настройками изделия. Данные сети используются для удобства работы с настройками МЭ

4.7.5.1. Страница «Изменения адреса»

Страница «Изменения адреса» (см. рис. 142) позволяет редактировать настройки адреса выбранного сетевого узла.

Страница «Изменения адреса»

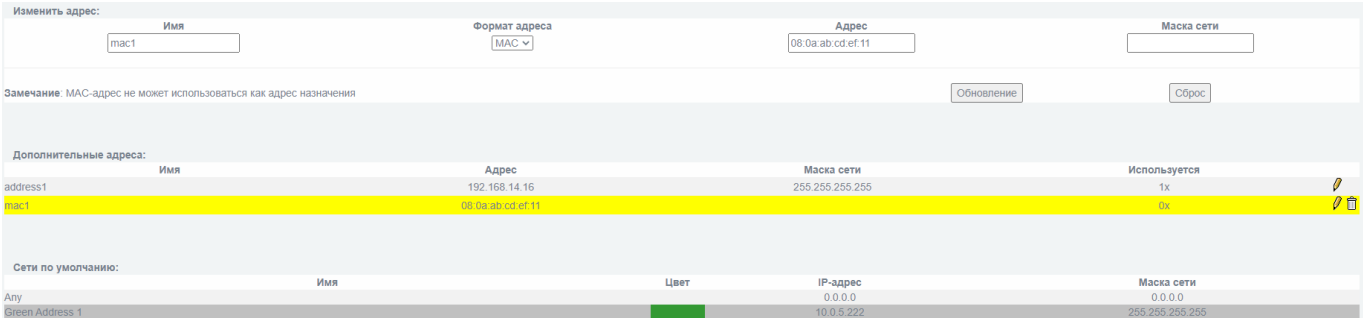

Рис. 142

В таблице 64 приведено описание элементов страницы «Изменения адреса».

Таблица 64 – Описание элементов страницы «Изменения адреса»

Элемент	Описание
Поле «Имя»	Предназначено для редактирования имени (обозначения) адреса
Выпадающий список «Формат адреса»	Предназначено для изменения выбора формата адреса для поля ввода «Адрес»
Поле «Адрес»	Предназначено для редактирования адреса сетевого узла
Поле «Маска сети»	Предназначено для редактирования маски сети сетевого узла
Кнопка «Обновление»	Предназначена для сохранения и применения отредактированных настроек адреса сетевого узла
Кнопка «Сброс»	Предназначена для отмены введенных настроек адреса сетевого узла. После нажатия перезагружает страницу и возвращает к подразделу «Адреса»

4.7.6. Подраздел «Группы адресов»

Подраздел «Группы адресов» (см. рис. 143) предназначен для группировки различных адресов сетевых узлов под одним обозначением для удобного задания правил МЭ.

Подраздел «Группы адресов»

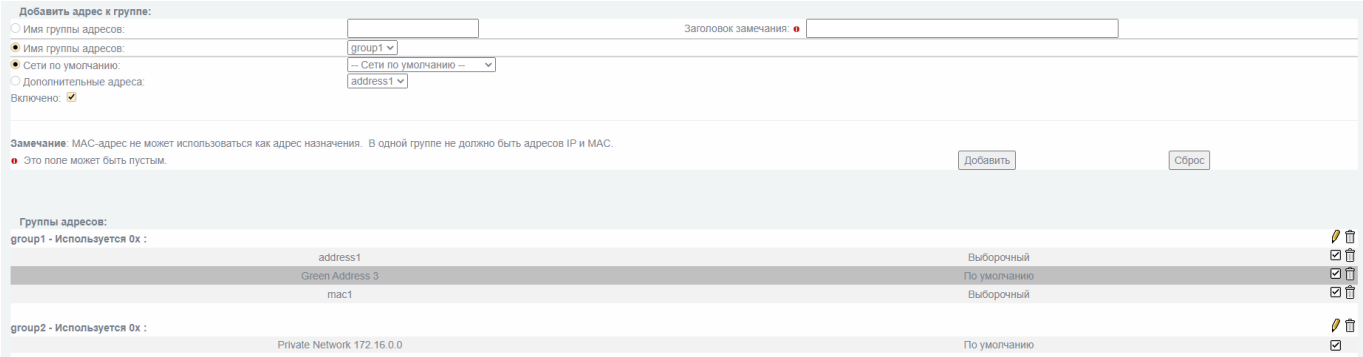

Рис. 143

В таблице 65 приведено описание элементов подраздела «Группы адресов».

Таблица 65 – Описание элементов подраздела «Группы адресов»

Элемент	Описание
Чекбокс «Имя группы адресов»	Предназначен для выбора необходимости ввода нового имени группы адресов. При отсутствии созданных групп выбор данного поля происходит автоматически
Поле «Имя группы адресов»	Предназначено для ввода имени группируемых адресов при активированном чекбоксе. Допустимы символы латинского алфавита и цифры 0 – 9
Выпадающий список «Имя группы адресов»	Предназначен для выбора одного из ранее введенных имен групп адресов. Появляется если существует хотя бы одна ранее созданная пользователем группа
Чекбокс «Сети по умолчанию»	Предназначен для выбора добавления сети по умолчанию
Выпадающий список «Сети по умолчанию»	Предназначен для выбора одной из сетей, связанных с сетевыми настройками изделия
Чекбокс «Дополнительные адреса»	Предназначен для выбора добавления адреса из списка ранее добавленных пользователем вручную
Выпадающий список «Дополнительные адреса»	Предназначен для выбора одного из ранее добавленных пользователем вручную адресов. Появляется если настроен хотя бы один адрес, добавленный пользователем вручную

Элемент	Описание
Чекбокс «Включено»	Предназначен для выбора активации/деактивации созданного адреса в выбранной группе. Примечание. Не активные адреса не будут присутствовать в правилах МЭ при использовании выбранной группы
Поле «Заголовок замечания»	Предназначено для ввода примечаний к группе адресов. Примечание. Данное поле не обязательно к заполнению
Кнопка «Добавить»	Предназначена для добавления адреса в выбранную группу
Кнопка «Сброс»	Предназначена для отмены введенных настроек добавления адреса. После нажатия перезагружает страницу. Не удаляет уже добавленные ранее адреса
Информационная таблица «Группы адресов»	Предназначена для отображения информации о группах адресов, созданных пользователем вручную
Кнопка « »	Кнопка «Изменить». Предназначена для редактирования группы адресов и открывает страницу «Изменение групп адресов»
Кнопка « »	Кнопка «Удалить». Предназначена для удаления групп адресов (кнопка в заголовке выбранной группы) и самих адресов (кнопка справа от выбранной службы). Примечания: 1. Группу адресов возможно удалить если она не используется изделием. Кнопка удаления группы адресов присутствует только если данная группа не используется изделием. 2. Группа содержит хотя бы один адрес. Если в группе присутствует всего один адрес, то его нельзя удалить отдельно – в таком случае необходимо удалять всю группу
Чекбокс «**имя адреса**»	Предназначен для выбора активации/деактивации выбранного адреса в группе. Примечание. Не активные адреса не будут присутствовать в правилах МЭ при использовании выбранной группы
Примечания: 1. MAC-адрес не может использоваться как адрес назначения. При создании и наполнении группы адресов необходимо учитывать ее последующее использование в правилах МЭ. MAC-адрес, в том числе в составе группы, не может быть использован для указания адреса назначения в правилах МЭ. 2. В одной группе не должно быть адресов IP и MAC	

4.7.6.1. Страница «Изменение групп адресов»

Страница «Изменение групп адресов» (см. рис. 144) позволяет редактировать настройки выбранной группы адресов.

Страница «Изменение групп адресов»

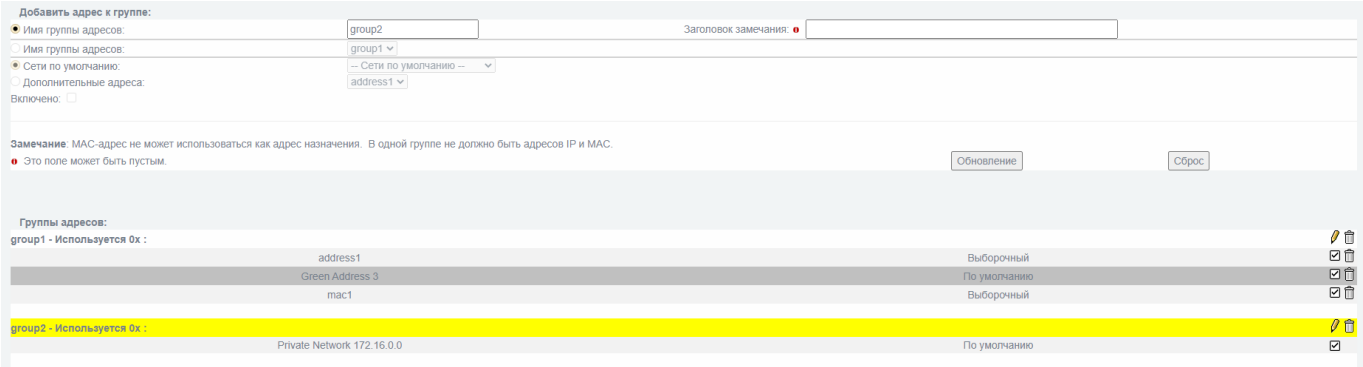

Рис. 144

В таблице 66 приведено описание элементов страницы «Изменение групп адресов».

Таблица 66 – Описание элементов страницы «Изменение групп адресов»

Элемент	Описание
Поле «Имя группы адресов»	Предназначено для редактирования имени группы адресов
Поле «Заголовок замечания»	Предназначено для редактирования примечаний к группе адресов. Примечание. Данное поле не обязательно к заполнению
Кнопка «Обновление»	Предназначена для сохранения и применения отредактированных настроек адреса сетевого узла
Кнопка «Сброс»	Предназначена для отмены введенных настроек группы служб. После нажатия перезагружает страницу и возвращает к подразделу «Адреса»

4.7.7. Подраздел «Интерфейсы по умолчанию»

Подраздел «Интерфейсы по умолчанию» (см. рис. 145) предназначен для регистрации в изделии виртуальных интерфейсов.

Подраздел «Интерфейсы по умолчанию»

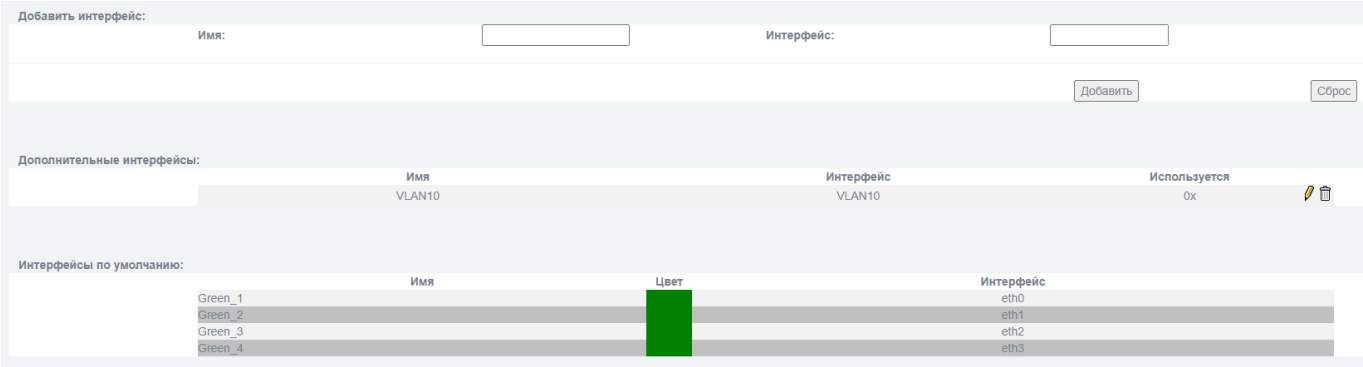

Рис. 145

Сетевые интерфейсы можно разбить на две группы:

1) физические – определяются исходя из наличия физических сетевых адаптеров;

2) виртуальные – назначаются на физических интерфейсах или объединяют их в виртуальные интерфейсы.

В качестве примера виртуальных интерфейсов можно выделить следующие:

1) туннели GRE;

2) туннели OpenVPN;

3) интерфейсы объединения;

4) интерфейсы моста;

5) интерфейсы VLAN.

Интерфейсы сетевых адаптеров могут напрямую участвовать в задании правил МЭ по именам соответствующим цветовым политикам («Green_1», «Blue_3» и т. д.).

Регистрация дополнительных интерфейсов осуществляется в данном подразделе меню изделия. При этом **МЭ должен быть переведен в расширенный режим** (в подразделе «Межсетевой Экран» → «Настройки межсетевого экрана»).

Подробнее информация о настройках физических и виртуальных интерфейсов представлена в подразделе «Настройка межсетевого экрана» руководства администратора НПЕШ.465614.005РА.

В таблице 67 приведено описание элементов подраздела «Интерфейсы по умолчанию».

Таблица 67 – Описание элементов подраздела «Интерфейсы по умолчанию»

Элемент	Описание
Поле «Имя»	Предназначено для ввода псевдонима для регистрируемого интерфейса. Псевдоним может совпадать с фактическим наименованием интерфейса
Поле «Интерфейс»	Предназначено для ввода фактического наименования существующего интерфейса для дальнейшей регистрации его в изделии
Кнопка «Добавить»	Предназначена для сохранения и добавления (регистрации) введенного интерфейса в информационную таблицу «Дополнительные интерфейсы»
Кнопка «Сброс»	Предназначена для отмены введенных настроек регистрации сетевого интерфейса. После нажатия перезагружает страницу
Информационная таблица «Дополнительные интерфейсы»	Предназначена для отображения информации о добавленных (зарегистрированных в изделии) вручную дополнительных интерфейсах
Кнопка « »	Кнопка «Изменить». Предназначена для редактирования выбранного дополнительного интерфейса и открывает страницу «Изменение интерфейсов по умолчанию»
Кнопка « »	Кнопка «Удалить». Предназначена для удаления выбранного дополнительного интерфейса. Примечание. Дополнительный интерфейс возможно удалить если он не используется изделием. Кнопка удаления дополнительного интерфейса присутствует только если данный интерфейс не используется изделием
Информационная таблица «Интерфейсы по умолчанию»	Предназначена для отображения списка физических сетевых интерфейсов

4.7.7.1. Страница «Изменение интерфейсов по умолчанию»

Страница «Изменение интерфейсов по умолчанию» (см. рис. 146) позволяет редактировать настройки выбранного интерфейса по умолчанию.

Страница «Изменение интерфейсов по умолчанию»

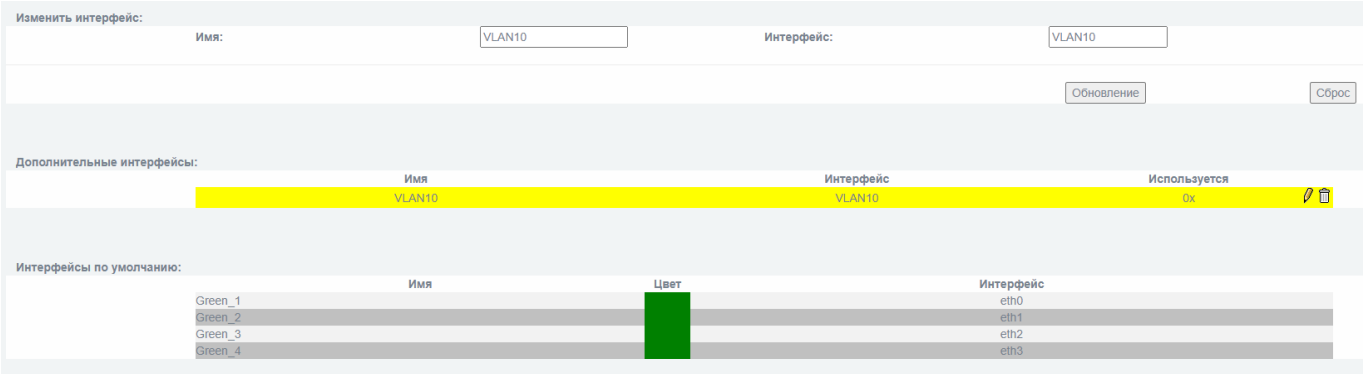

Рис. 146

В таблице 68 приведено описание элементов страницы «Изменение интерфейсов по умолчанию».

Таблица 68 – Описание элементов страницы «Изменение интерфейсов по умолчанию»

Элемент	Описание
Поле «Имя»	Предназначено для редактирования псевдонима для регистрируемого интерфейса. Псевдоним может совпадать с фактическим наименованием интерфейса. Примечание. Данное поле возможно редактировать если выбранный интерфейс не используется изделием в момент изменения
Поле «Интерфейс»	Предназначено для редактирования фактического наименования существующего сетевого интерфейса
Кнопка «Обновление»	Предназначена для сохранения и применения отредактированных настроек выбранного дополнительного сетевого интерфейса
Кнопка «Сброс»	Предназначена для отмены введенных настроек выбранного дополнительного сетевого интерфейса. После нажатия перезагружает страницу и возвращает к подразделу «Интерфейсы по умолчанию»

4.7.8. Подраздел «Группы состояний»

Подраздел «Группы состояний» (см. рис. 147) предназначен для создания и редактирования групп состояний сетевых соединений изделия.

Подраздел «Группы состояний»

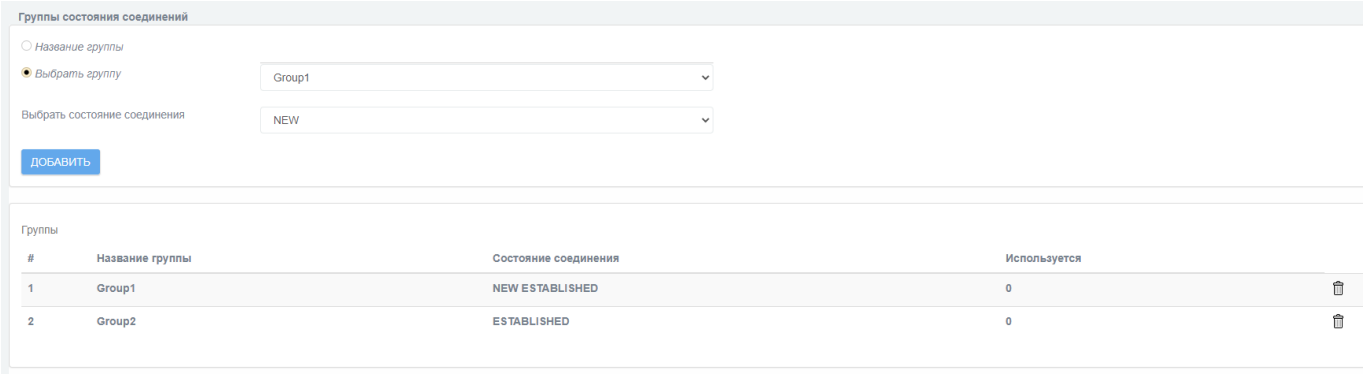

Рис. 147

В таблице 69 приведено описание элементов подраздела «Группы состояний».

Таблица 69 – Описание элементов подраздела «Группы состояний»

Элемент	Описание
Чекбокс «Название группы»	Предназначен для активации выбора ввода нового названия группы состояний
Поле «Название группы»	Предназначено для ввода вручную нового названия группы состояний
Чекбокс «Выбрать группу»	Предназначен для активации выбора уже существующей группы состояний
Выпадающий список «Выбрать группу»	Предназначен для выбора наименования одной из уже существующих групп состояний
Выпадающий список «Выбрать состояние соединения»	Предназначен для выбора одного из следующих вариантов состояния соединения для создаваемой группы: – «**NEW**» («Новое») – сетевой пакет, является пакетом установления соединения; – «**ESTABLISHED**» («Установленное») – анализируемый пакет принадлежит соединению, которое уже есть в списке установленных соединений; – «**RELATED**» («Связанное») – анализируемый сетевой пакет связан с установленным соединением. Например, при работе по протоколу FTP, сначала соединение устанавливается для порта с номером 21. По этому соединению передаются управляющие команды. А при необходимости передачи данных используется порт 20, но сетевые пакеты с данными связаны с соединением, установленным на порту 21; – «**INVALID**» («Ошибочное») – анализируемый сетевой пакет не может быть определен или не имеет определенного состояния, например, ошибка ICMP, которая не относится к какому-либо конкретному соединению

Элемент	Описание
Кнопка «Добавить»	Предназначена для сохранения и добавления новой группы состояний с введенными ранее настройками. Созданная группа состояний отобразится в информационной таблице «Группы»
Информационная таблица «Группы»	Предназначена для отображения информации о добавленных вручную группах состояний сетевых соединений изделия
Кнопка « »	Кнопка «Удалить». Предназначена для удаления выбранной группы состояний сетевых соединений. Примечания: 1. Группу состояний возможно удалить если она не используется изделием. Кнопка удаления группы состояний сетевых соединений присутствует только если данная группа не используется изделием. 2. При необходимости редактировать уже созданную группу состояний необходимо удалить выбранную группу и создать новую

Создаваемая пользователем группа состояний может содержать до четырех различных элементов (состояний соединения). Для добавления элемента в существующую группу состояний необходимо выбрать требуемое состояние и название группы, в которую необходимо его добавить. Созданная таким образом группа с указанным именем автоматически объединит выбранные состояния (см. рис. 148).

Группа с различными состояниями соединения

Группы

#	Название группы	Состояние соединения
1	Group1	NEW ESTABLISHED

Рис. 148

4.7.9. Подраздел «Правила межсетевого экрана»

Подраздел «Правила межсетевого экрана» (см. рис. 149) предназначен для отображения и установки новых правил МЭ.

Подраздел «Правила межсетевого экрана»

Добавить новое правило:

Другие из внутренней сети во внешнюю | Доступ к устройству Рубикон | Каналы (Pinholes) | Перенаправление портов | Прокси | Доступ извне | L2 | СОВ

Текущие правила:

L2:

#	Сеть Интерфейс	Источник	Журнал:	Сеть Интерфейс	Назначение	Замечание	Действие

Другие из внутренней сети во внешнюю:

#	Сеть Интерфейс	Источник	Журнал:	Сеть Интерфейс	Назначение	Замечание	Действие
1	Green_1	Green Network 1		Any	Any : afs3-vlserver		
2	Green_1	Green Network 1		Any	Any		

Доступ к устройству Рубикон:

#	Сеть Интерфейс	Источник	Журнал:	Назначение	Замечание	Действие
1	Green_1	Green Network 1		IPCop : Ping		

Каналы (Pinholes):

#	Сеть Интерфейс	Источник	Журнал:	Сеть Интерфейс	Назначение	Замечание	Действие
1	Blue_1	Blue Network 1		Green_1	Green Network 1 : Ping		

Доступ извне:

#	Сеть Интерфейс	Источник	Журнал:	Назначение	Замечание	Действие
1	VLAN10	Any		IPCop : IPCop dhcp		

Система Обнаружения Вторжений:

#	Сеть Интерфейс	Источник	Журнал:	Назначение	Замечание	Действие

Настройка перенаправления портов:

#	Сеть Интерфейс	Источник	Внешний адрес назначения Rubicon	Журнал:	Сеть Интерфейс	Внутренний адрес назначения	Замечание	Действие
1	Any	Any	-- : asp		Green_1	address1 : bgp		

Прокси:

#	Сеть Интерфейс	Источник	Внешний адрес назначения Rubicon	Журнал:	Сеть Интерфейс	Внутренний адрес назначения	Замечание	Действие
1	Red_1	Any	-- : afs3-rmtsys		Red	: http		

Легенда: Запись в журнал Активировано (нажмите для деактивации) | Запись в журнал Деактивировано (нажмите для активации) | Стандартное правило принятия | Запрещающее правило | Правило журналирования, только запись в журнал | Расширенное правило принятия, открывает Ваш МЭ
Активировано (нажмите для деактивации) | Деактивировано (нажмите для активации) | Изменить | Скопировать правило | Удалить | Вверх
Вниз | Все зеленые, VPN, синие, оранжевые красные интерфейсы | Все синие, оранжевые, красные интерфейсы | Все оранжевые, красные интерфейсы | Все красные интерфейсы

Рис. 149

Подраздел «Правила межсетевого экрана» состоит из следующих страниц и блоков:

1) страница «Другие из внутренней сети во внешнюю»;

2) страница «Доступ к устройству Рубикон»;

3) страница «Каналы»;

4) страница «Перенаправление портов»;

5) страница «Прокси»;

6) страница «Доступ извне»;

7) страница «L2»;

8) страница «СОВ»;

9) блок «Текущие правила».

4.7.9.1. Страница «Другие из внутренней сети во внешнюю»

Страница «Другие из внутренней сети во внешнюю» (см. рис. 150) открывается после нажатия одноименной кнопки, находящейся в верхней части экрана подраздела «Правила межсетевого экрана».

Страница «Другие из внутренней сети во внешнюю»

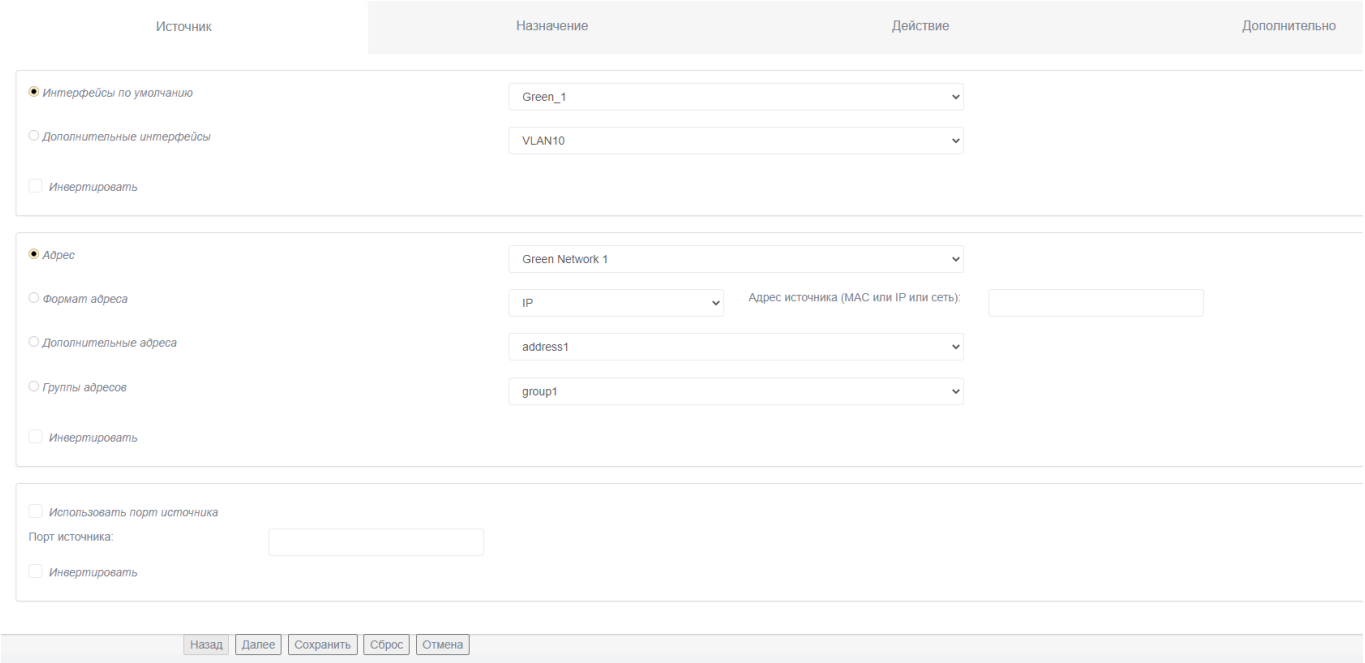

Рис. 150

Страница «Другие из внутренней сети во внешнюю» предназначена для добавления правил фильтрации сетевых пакетов, для которых адрес источника и адрес назначения маршрутизируются из одного **физического** сетевого интерфейса в другой.

Страница «Другие из внутренней сети во внешнюю» состоит из следующих вкладок:

1) «Источник»;

2) «Назначение»;

3) «Действие»;

4) «Дополнительно».

На данной странице присутствуют также следующие элементы навигационного меню:

1) кнопка «Назад» – предназначена для перехода на предыдущую вкладку страницы;

2) кнопка «Далее» – предназначена для перехода на следующую вкладку страницы;

3) кнопка «Сохранить» – предназначена для сохранения введенной информации;

4) кнопка «Сброс» – предназначена для очищения заполнения всей формы активной вкладки;

5) кнопка «Отмена» – предназначена для возврата в подраздел «Правила межсетевого экрана» без сохранения введенных данных на странице.

4.7.9.1.1. Вкладка «Источник»

Вкладка «Источник» (см. рис. 151) предназначена для настройки параметров фильтрации по данным об источнике сетевого пакета в правиле МЭ.

Вкладка «Источник»

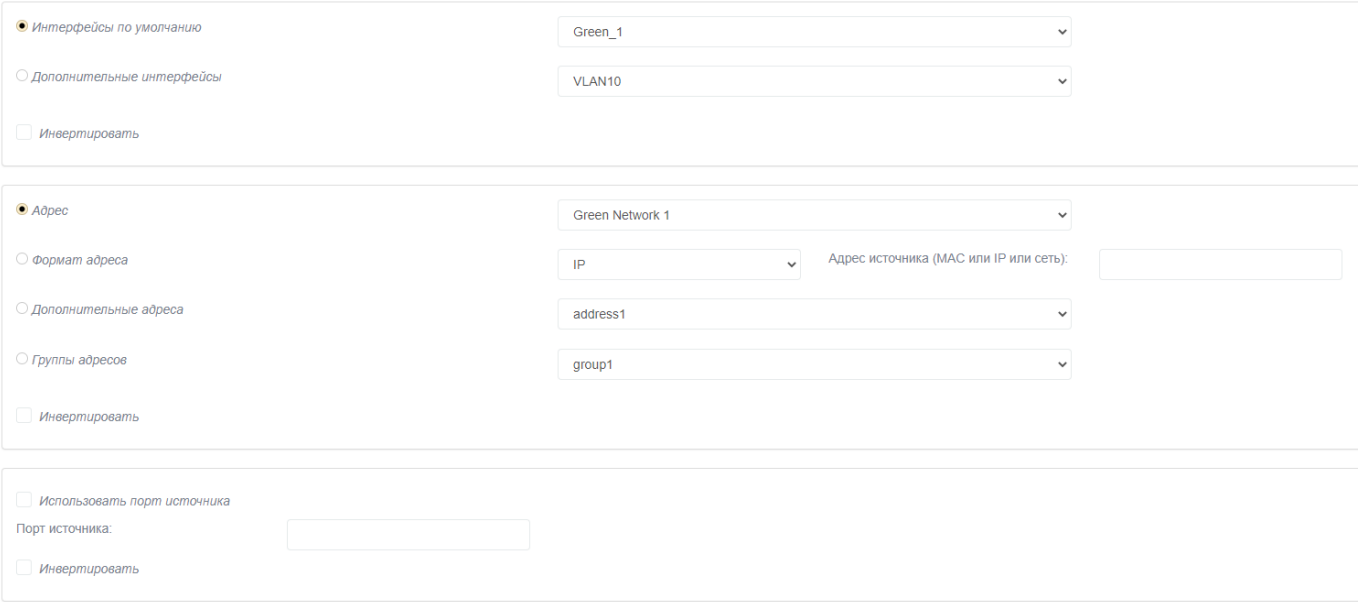

Рис. 151

В таблице 70 приведено описание элементов вкладки «Источник».

Таблица 70 – Описание элементов вкладки «Источник»

Элемент	Описание
Чекбокс «Интерфейсы по умолчанию»	Предназначен для активации выбора физического интерфейса изделия
Выпадающий список «Интерфейсы по умолчанию»	Предназначен для выбора одного из перечня доступных физических интерфейсов изделия
Чекбокс «Дополнительные интерфейсы»*	Предназначен для активации выбора виртуального интерфейса изделия, определяемого пользователем
Выпадающий список «Дополнительные интерфейсы»*	Предназначен для выбора одного из перечня доступных виртуальных (зарегистрированных пользователем вручную) интерфейсов изделия
Чекбокс «Инвертировать»*	Предназначен для выбора включения/отключения функции инвертирования сетевого интерфейса, то есть всех сетевых интерфейсов кроме указанного
Чекбокс «Адрес»	Предназначен для активации выбора адреса источника из перечня доступных адресов
Выпадающий список «Адрес»	Предназначен для выбора одного из перечня доступных адресов источника
Чекбокс «Формат адреса»	Предназначен для активации выбора ввода адреса источника вручную с указанием его типа (MAC, IP или сеть)

Элемент	Описание
Выпадающий список «Формат адреса»	Предназначен для выбора одного из следующих типов адресов источника: – «IP»; – «MAC»
Поле «Адрес источника (MAC или IP или сеть)»	Предназначено для ввода адреса источника обрабатываемых пакетов в формате MAC или IP или сеть. Для работы данного параметра необходимо активировать чекбокс «Формат адреса»
Чекбокс «Дополнительные адреса»	Предназначен для активации выбора дополнительных адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Дополнительные адреса»	Предназначен для выбора одного дополнительного адреса из перечня (созданных ранее пользователем вручную) дополнительных сетевых узлов
Чекбокс «Группы адресов»	Предназначен для активации выбора группы адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Группы адресов»	Предназначен для выбора одной группы из перечня (созданных ранее пользователем вручную) групп адресов
Чекбокс «Инвертировать»*	Предназначен для выбора включения/отключения функции инвертирования адреса сетевого узла, то есть всех адресов сетевых узлов кроме указанного
Чекбокс «Использовать порт источника»*	Предназначен для выбора включения/отключения использования порта, указанного пользователем вручную
Поле «Порт источника»*	Предназначено для ввода порта, с которого поступают сетевые пакеты
Чекбокс «Инвертировать»*	Предназначен для выбора включения/отключения функции инвертирования порта, с которого поступают сетевые пакеты, то есть всех портов кроме указанного
* – Элемент интерфейса, доступный только в «Расширенном режиме»	

4.7.9.1.2. Вкладка «Назначение»

Вкладка «Назначение» (см. рис. 152) предназначена для настройки параметров фильтрации по данным о назначении в сетевом пакете в правиле МЭ.

Вкладка «Назначение»

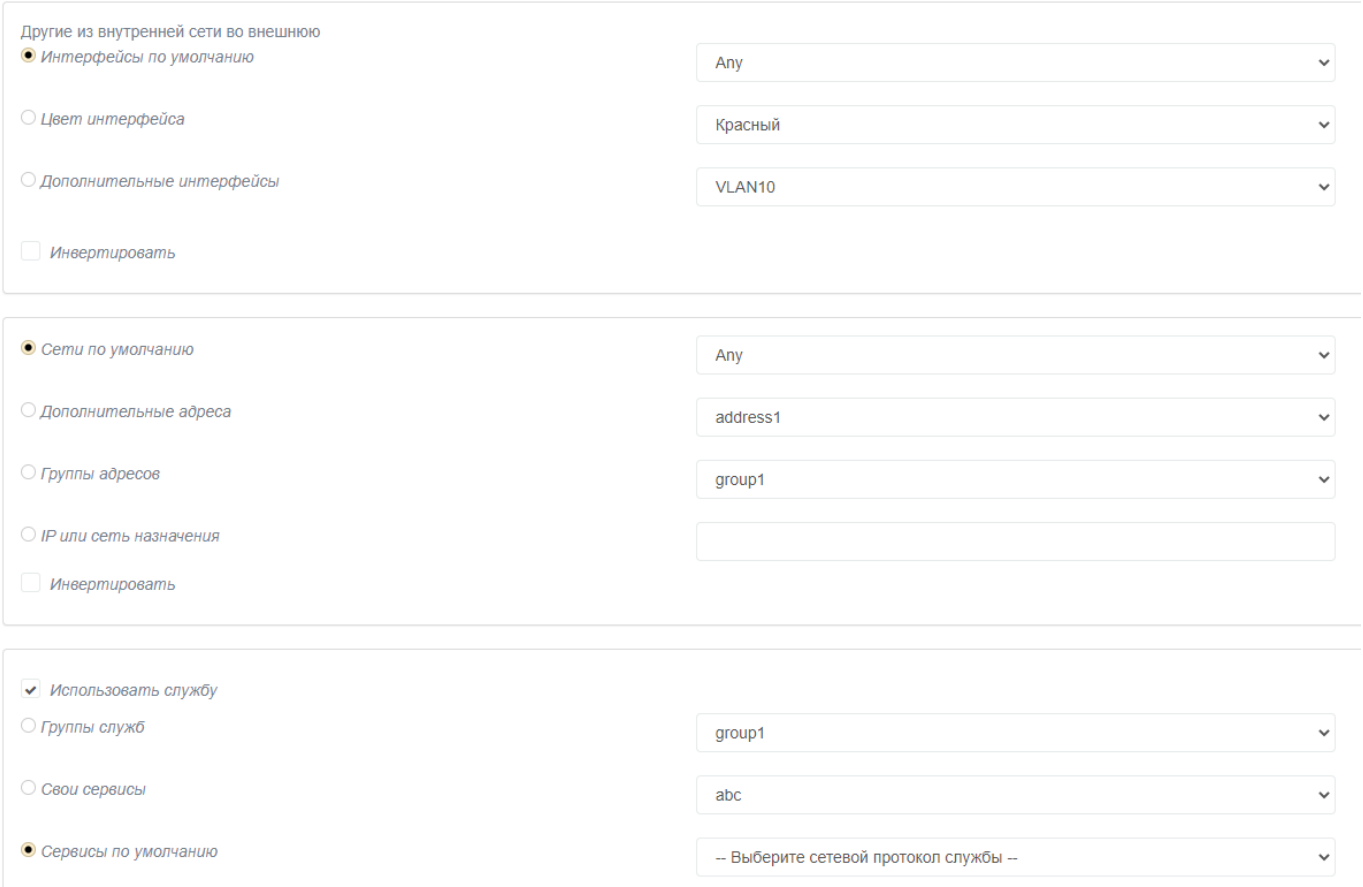

Рис. 152

В таблице 71 приведено описание элементов вкладки «Назначение».

Таблица 71 – Описание элементов вкладки «Назначение»

Элемент	Описание
Чекбокс «Интерфейсы по умолчанию»	Предназначен для активации выбора интерфейсов по умолчанию
Выпадающий список «Интерфейсы по умолчанию»	Предназначен для выбора одного из доступных в перечне физических сетевых интерфейсов изделия
Чекбокс «Цвет интерфейса»	Предназначен для активации выбора цветовой политики сетевого интерфейса изделия
Выпадающий список «Цвет интерфейса»	Предназначен для выбора одной из следующих цветовых политик: – «Зеленый/VPN»; – «Синий»; – «Оранжевый»; – «Красный».

Элемент	Описание
Чекбокс «Дополнительные интерфейсы»*	Предназначен для активации выбора виртуального интерфейса изделия, определяемого пользователем
Выпадающий список «Дополнительные интерфейсы»*	Предназначен для выбора одного из перечня доступных виртуальных (зарегистрированных пользователем вручную) интерфейсов изделия
Чекбокс «Инвертировать»*	Предназначен для выбора включения/отключения функции инвертирования сетевого интерфейса, то есть всех сетевых интерфейсов кроме указанного
Чекбокс «Сети по умолчанию»	Предназначен для выбора добавления сети по умолчанию
Выпадающий список «Сети по умолчанию»	Предназначен для выбора одной из сетей, связанных с сетевыми настройками изделия
Чекбокс «Дополнительные адреса»	Предназначен для активации выбора дополнительных адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Дополнительные адреса»	Предназначен для выбора одного дополнительного адреса из перечня (созданных ранее пользователем вручную) дополнительных сетевых узлов
Чекбокс «Группы адресов»	Предназначен для активации выбора группы адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Группы адресов»	Предназначен для выбора одной группы из перечня (созданных ранее пользователем вручную) групп адресов
Чекбокс «IP или сеть назначения»	Предназначен для активации выбора адреса назначения с указанным вручную пользователем IP или сетью
Поле «IP или сеть назначения»	Предназначен для ввода IP-адреса или сети для узла назначения (целевого узла обрабатываемого пакета)
Чекбокс «Инвертировать»*	Предназначен для выбора включения/отключения функции инвертирования адреса сетевого узла, то есть всех адресов сетевых узлов кроме указанного
Чекбокс «Использовать службу»	Предназначен для выбора включения/отключения использования выбранной пользователем службы или сервиса
Чекбокс «Группы служб»	Предназначен для активации выбора использования групп служб, созданных ранее вручную пользователем
Выпадающий список «Группы служб»	Предназначен для выбора одной группы из перечня созданных ранее вручную пользователем
Чекбокс «Свои сервисы»	Предназначен для активации выбора использования сервиса, созданного ранее вручную пользователем
Выпадающий список «Свои сервисы»	Предназначен для выбора одного сервиса из перечня ранее добавленных вручную пользователем
Чекбокс «Сервисы по умолчанию»	Предназначен для активации выбора использования сетевого протокола службы, имеющей специальное имя в изделии
Выпадающий список «Сервисы по умолчанию»	Предназначен для выбора одной из сетевых протоколов службы, из перечня имеющих специальное имя в изделии
* – Элемент интерфейса, доступный только в «Расширенном режиме»	

4.7.9.1.3. Вкладка «Действие»

Вкладка «Действие» (см. рис. 153) предназначена для настройки действий по фильтрации при срабатывании правил.

Вкладка «Действие»

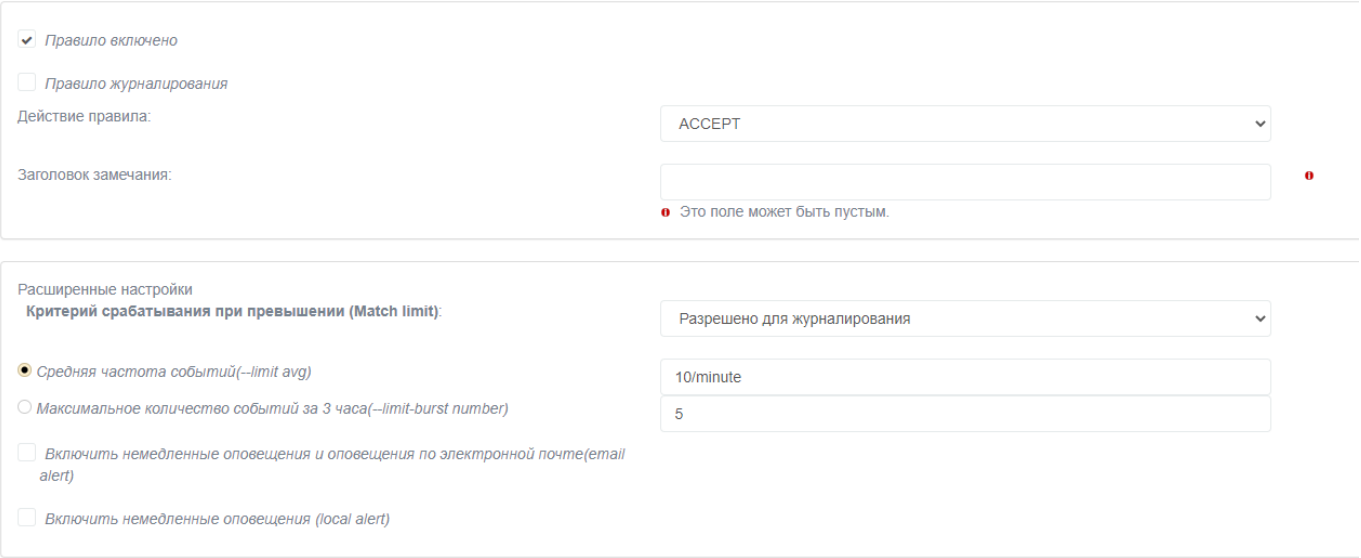

Рис. 153

В таблице 72 приведено описание элементов вкладки «Действие».

Таблица 72 – Описание элементов вкладки «Действие»

Элемент	Описание
Чекбокс «Правило включено»	Предназначен для выбора включения/отключения правила и выбранных действий, при его срабатывании
Чекбокс «Правило журналирования»	Предназначен для выбора включения/отключения правила журналирования прохождения пакетов по настраиваемому правилу
Выпадающий список «Действие правила»	Предназначен для выбора одного из следующих действий при срабатывании правила: – «ACCEPT»; – «DROP»; – «REJECT»; – «Только запись в журнал»; – «Система Обнаружения Вторжений»
Поле «Заголовок замечания»	Предназначено для ввода примечаний к настраиваемому правилу. Примечание. Данное поле не обязательно к заполнению

Элемент	Описание
Выпадающий список «Критерий срабатывания при превышении (Match limit)»*	Предназначен для выбора одного из доступных в перечне расширенных настроек действия при срабатывании правил: – «Возможность отключена»; – «Разрешено для журналирования»; – «Разрешено для политики принятия или сбрасывания»; – «Разрешено для политик обоих видов»
Чекбокс «Средняя частота событий (--limit avg)»*	Предназначен для активации выбора использования функции ограничения записи событий в журнал по средней частоте событий
Поле «Средняя частота событий (--limit avg)»*	Предназначено для ввода средней частоты событий. Необходимо указывать в формате: **число событий/единица времени**
Чекбокс «Максимальное количество событий за 3 часа (--limit-burst number)»*	Предназначен для активации выбора использования функции ограничения записи событий в журнал по максимальному количеству событий
Поле «Максимальное количество событий за 3 часа (--limit-burst number)»*	Предназначено для ввода максимального количество событий за 3 часа, записываемых в журнал. Данный параметр будет определять пик «разовой» доставки пакетов. Значение по умолчанию «5»
Чекбокс «Включить немедленные оповещения и оповещения по электронной почте (email alert)»*	Предназначен для выбора включения/отключения функции получения оповещения о сработавшем правиле на электронную почту
Чекбокс «Включить немедленные оповещения (local alert)»*	Предназначен для выбора включения/отключения функции оповещения в всплывающем окне уведомлений изделия «»
* – Элемент интерфейса, доступный только в «Расширенном режиме»	

4.7.9.1.4. Вкладка «Дополнительно»

Вкладка «Дополнительно» (см. рис. 154) предназначена для настройки дополнительных параметров фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам.

При срабатывании правила возможно присвоение числовой метки, применяемой для дальнейшей обработки сетевого пакета в целях маршрутизации.

Примечание – Данная вкладка доступна только в расширенном режиме (включить расширенный режим можно в разделе «Межсетевой Экран» → «Настройки межсетевого экрана» активировав чекбокс «Расширенный режим»)

Вкладка «Дополнительно»

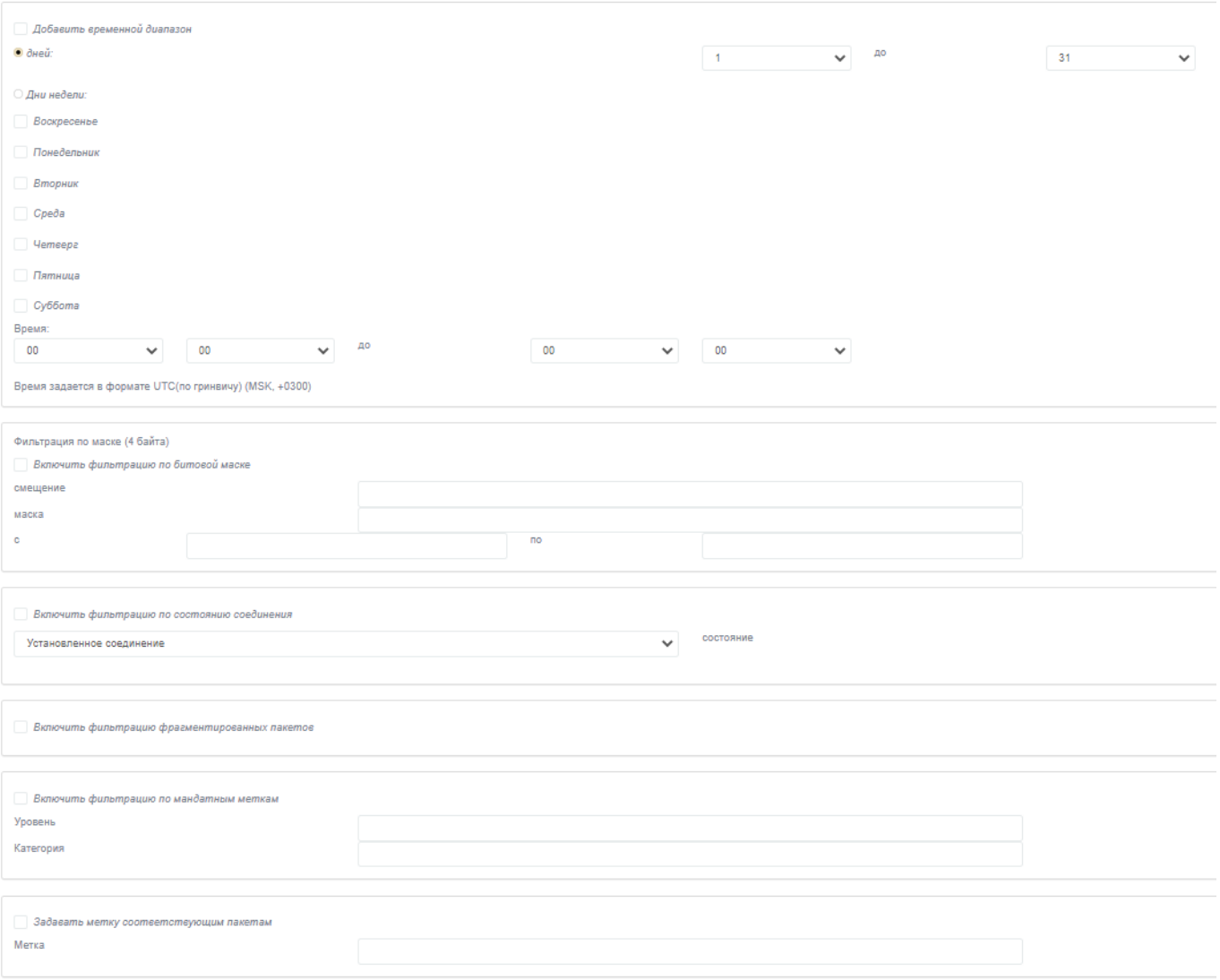

Рис. 154

В таблице 73 приведено описание элементов вкладки «Дополнительно».

Таблица 73 – Описание элементов вкладки «Дополнительно»

Элемент	Описание
Чекбокс «Добавить временной диапазон»	Предназначен для активации выбора использования функции добавления временного диапазона для правил фильтрации сетевых пакетов
Чекбокс «дней»	Предназначен для активации временного диапазона в днях, указанных в выпадающих полях «дней»

Элемент	Описание
Выпадающие поля «дней»	Предназначены для выбора временного диапазона в днях месяца. Начало временного диапазона (первый день) необходимо выбрать в первом списке, а окончание временного диапазона (последний день) во втором выпадающем списке (справа от надписи «до»)
Чекбокс «Дни недели»	Предназначен для активации выбора использования правила фильтрации сетевых пакетов в соответствии с выбранными днями недели и времени, указанному в выпадающих списках «Часы» и «Минуты»
Чекбоксы «Воскресенье», «Понедельник», «Вторник», «Среда», «Четверг», «Пятница», «Суббота»	Предназначены для выбора дней недели, по которым будет использоваться правило фильтрации сетевых пакетов
Выпадающие списки «Часы»*	Предназначены для выбора часов, по которым будет использоваться правило фильтрации сетевых пакетов. Начало часового диапазона необходимо выбрать в первом списке, а окончание – в третьем выпадающем списке (первый справа от надписи «до»)
Выпадающие списки «Минуты»*	Предназначены для выбора минут, по которым будет использоваться правило фильтрации сетевых пакетов. Начало минутного диапазона необходимо выбрать во втором списке, а окончание – в четвертом выпадающем списке (второй справа от надписи «до»)
Чекбокс «Включить фильтрацию по битовой маске»	Предназначен для активации функции фильтрации по битовой маске (4 байта)
Поле «смещение»	Предназначено для ввода величины смещения окна поиска 32-х битного фрагмента относительно начала пакета в байтах
Поле «маска»	Предназначено для ввода маски, накладываемой на данные сетевого пакета по выбранному смещению
Поле «с»	Предназначено для ввода минимального значения 32-х битного фрагмента данных
Поле «по»	Предназначено для ввода максимального значения 32-х битного фрагмента данных
Чекбокс «Включить фильтрацию по состоянию соединения»	Предназначен для активации выбора использования функции фильтрации по состоянию соединения или созданной ранее пользователем вручную группой состояний
Выпадающий список «Состояние соединения»	Предназначен для выбора одного из следующих состояний соединений: – «Установленное соединение»; – «Новое соединение»; – «**Наименование пользовательской группы состояний соединений**». Примечание. Строки выпадающего списка «Состояние соединения» – **«Установленное соединение»** и **«Новое соединение»**, являются **зарезервированными** и отвечают состояниям **«NEW»** и **«ESTABLISHED»** соответственно

Элемент	Описание
Чекбокс «Включить фильтрацию фрагментированных пакетов»	Предназначен для активации выбора использования функции фильтрации фрагментированных пакетов
Чекбокс «Включить фильтрацию по мандатным меткам»	Предназначен для активации выбора использования функции фильтрации по мандатным меткам. При активации данной функции созданное правило МЭ проверяет наличие мандатной метки согласно ГОСТ Р 58256 (RFC 1108)
Поле «Уровень»	Предназначено для ввода значения уровня данных (согласно ГОСТ Р 58256). Задается в **десятичном** формате 0, 1, 2 и т. д.
Поле «Категория»	Предназначено для ввода и описания категории, к которой относятся данные (согласно ГОСТ Р 58256). Задается в формате **последовательности 0 и 1** (пример: 1, 10, 11 и т. д.)
Чекбокс «Задавать метку соответствующим пакетам»	Предназначен для активации выбора использования функции задания метки соответствующим пакетам. При активации данной функции сетевые пакеты, попадающие под правило МЭ, будут промаркированы метками для обработки в изделии. Данный механизм используется для статической маршрутизации по меткам
Поле «Метка»	Предназначено для ввода и задания метки, начиная с **1002** (например, 1002, 1003, 1004 и т. д.)
* – Время задается в формате UTC (по Гринвичу) (MSK, +0300)	

4.7.9.2. Страница «Доступ к устройству Рубикон»

Страница «Доступ к устройству Рубикон» (см. рис. 155) открывается после нажатия одноименной кнопки, находящейся в верхней части экрана подраздела «Правила межсетевого экрана».

Страница «Доступ к устройству Рубикон»

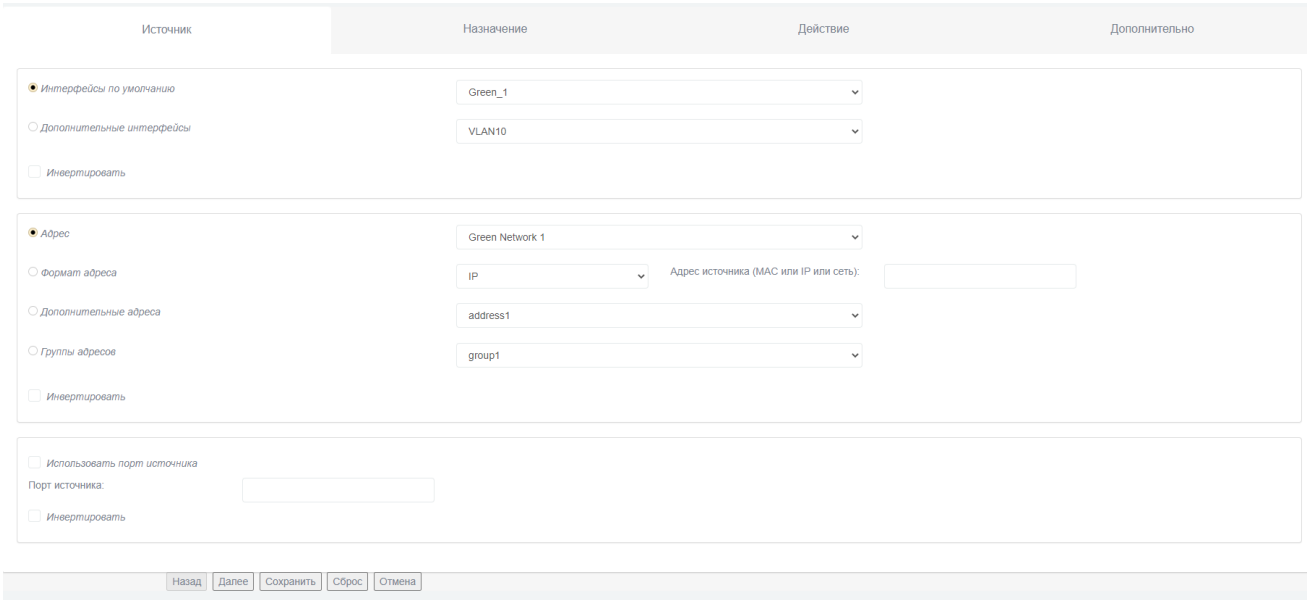

Рис. 155

Страница «Доступ к устройству Рубикон» предназначена для перехода к странице добавления правил фильтрации сетевых пакетов, для которых адресом назначения является адрес (или псевдоним адреса) сетевого интерфейса МЭ (например, для настройки административного доступа из «зеленой» или из «синей» подсети, или для разрешения пакетов инициализации интерфейса для протокола GRE).

Страница «Доступ к устройству Рубикон» состоит из следующих вкладок:

1) «Источник»;

2) «Назначение»;

3) «Действие»;

4) «Дополнительно».

На данной странице присутствуют также следующие элементы навигационного меню:

1) кнопка «Назад» – предназначена для перехода на предыдущую вкладку страницы;

2) кнопка «Далее» – предназначена для перехода на следующую вкладку страницы;

3) кнопка «Сохранить» – предназначена для сохранения введенной информации;

4) кнопка «Сброс» – предназначена для очищения заполнения всей формы активной вкладки;

5) кнопка «Отмена» – предназначена для возврата в подраздел «Правила межсетевого экрана» без сохранения введенных данных на странице.

4.7.9.2.1. Вкладка «Источник»

Вкладка «Источник» на странице «Доступ к устройству Рубикон» предназначена для настройки параметров фильтрации по данным об источнике сетевого пакета в правиле МЭ и описана подробно в п. 4.7.9.1.1 настоящего документа.

4.7.9.2.2. Вкладка «Назначения»

Вкладка «Назначения» на странице «Доступ к устройству Рубикон» (см. рис. 156) предназначена для настройки параметров фильтрации по данным о назначении в сетевом пакете в правиле МЭ. Адресом назначения всегда является адрес (или псевдоним адреса) сетевого интерфейса МЭ.

Вкладка «Назначения»

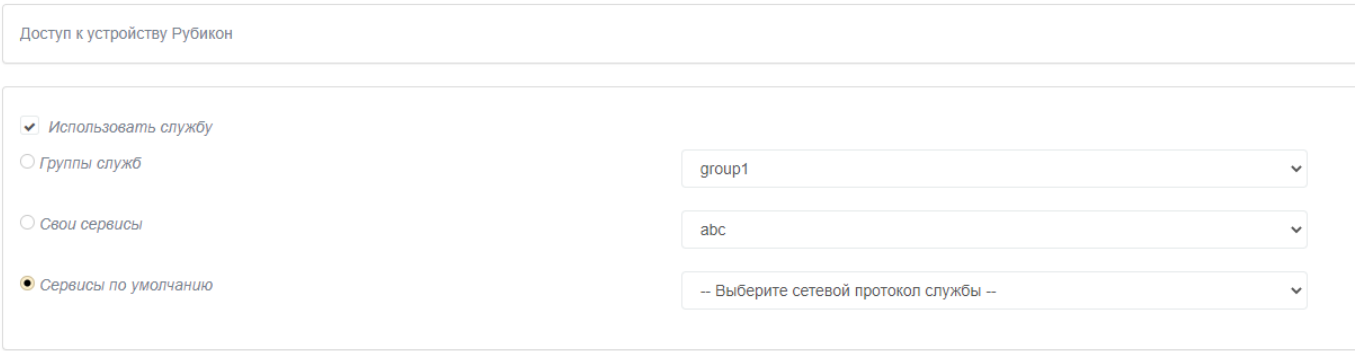

Рис. 156

В таблице 74 приведено описание элементов вкладки «Назначение» на странице «Доступ к устройству Рубикон».

Таблица 74 – Описание элементов вкладки «Назначение» на странице «Доступ к устройству Рубикон»

Элемент	Описание
Чекбокс «Использовать службу»	Предназначен для выбора включения/отключения использования выбранной пользователем службы или сервиса
Чекбокс «Группы служб»	Предназначен для активации выбора использования групп служб, созданных ранее вручную пользователем
Выпадающий список «Группы служб»	Предназначен для выбора одной группы из перечня созданных ранее вручную пользователем
Чекбокс «Свои сервисы»	Предназначен для активации выбора использования сервиса, созданного ранее вручную пользователем
Выпадающий список «Свои сервисы»	Предназначен для выбора одного сервиса из перечня ранее добавленных вручную пользователем
Чекбокс «Сервисы по умолчанию»	Предназначен для активации выбора использования сетевого протокола службы, имеющей специальное имя в изделии
Выпадающий список «Сервисы по умолчанию»	Предназначен для выбора одной из сетевых протоколов службы, из перечня имеющих специальное имя в изделии

4.7.9.2.3. Вкладка «Действие»

Вкладка «Действие» предназначена для настройки действий по фильтрации при срабатывании правил и описана подробно в п. 4.7.9.1.3 настоящего документа.

4.7.9.2.4. Вкладка «Дополнительно»

Вкладка «Дополнительно» предназначена для настройки дополнительных параметров фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам и описана подробно в п. 4.7.9.1.4 настоящего документа.

Примечание. В данной вкладке, в отличии от описанной ранее в п. 4.7.9.1.4 настоящего документа, отсутствует возможность задания метки соответствующим пакетам.

4.7.9.3. Страница «Каналы (Pinholes)»

Страница «Каналы (Pinholes)» (см. рис. 157) открывается после нажатия одноименной кнопки, находящейся в верхней части экрана подраздела «Правила межсетевого экрана». Данная кнопка станет видимой и доступной в подразделе только если в изделии присутствует (создан) «синий» сетевой интерфейс.

Страница «Каналы (Pinholes)»

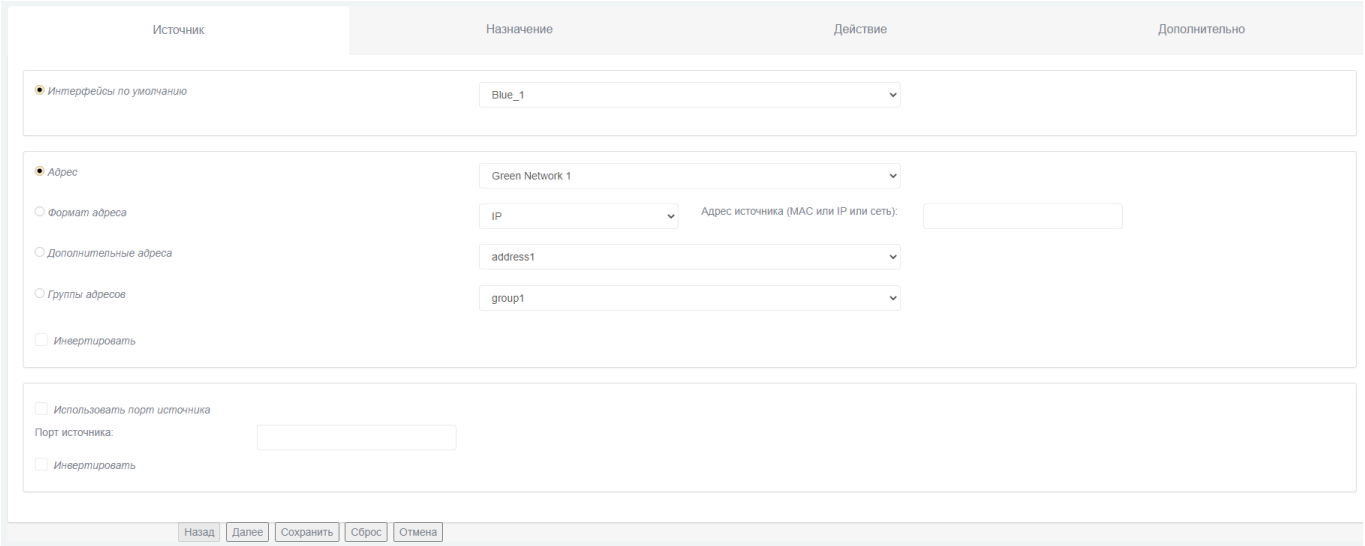

Рис. 157

Страница «Каналы (Pinholes)» предназначена для настройки параметров фильтрации пакетов от выделенных узлов «синей» или «оранжевой» сети к узлам «зеленой» сети.

Страница «Каналы (Pinholes)» состоит из следующих вкладок:

1) «Источник»;

2) «Назначение»;

3) «Действие»;

4) «Дополнительно».

На данной странице присутствуют также следующие элементы навигационного меню:

1) кнопка «Назад» – предназначена для перехода на предыдущую вкладку страницы;

2) кнопка «Далее» – предназначена для перехода на следующую вкладку страницы;

3) кнопка «Сохранить» – предназначена для сохранения введенной информации;

4) кнопка «Сброс» – предназначена для очищения заполнения всей формы активной вкладки;

5) кнопка «Отмена» – предназначена для возврата в подраздел «Правила межсетевого экрана» без сохранения введенных данных на странице.

4.7.9.3.1. Вкладка «Источник»

Вкладка «Источник» на странице «Каналы (Pinholes)» (см. рис. 158) предназначена для настройки параметров фильтрации по данным об источнике сетевого пакета в правиле МЭ.

Вкладка «Источник»

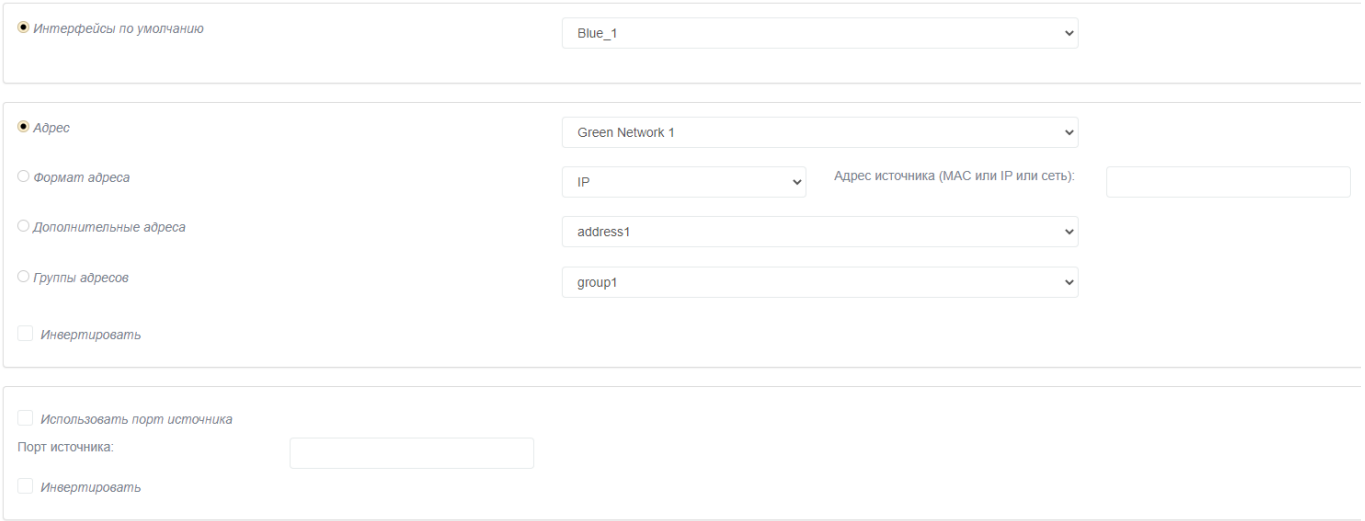

Рис. 158

В таблице 75 приведено описание элементов вкладки «Источник» на странице «Каналы (Pinholes)».

Таблица 75 – Описание элементов вкладки «Источник» на странице «Каналы (Pinholes)»

Элемент	Описание
Чекбокс «Интерфейсы по умолчанию»	Предназначен для активации выбора физического интерфейса изделия
Выпадающий список «Интерфейсы по умолчанию»	Предназначен для выбора одного из перечня доступных физических интерфейсов изделия (доступны для выбора только «синие» и «оранжевые» сетевые интерфейсы)
Чекбокс «Адрес»	Предназначен для активации выбора адреса источника из перечня доступных адресов
Выпадающий список «Адрес»	Предназначен для выбора одного из перечня доступных адресов источника
Чекбокс «Формат адреса»	Предназначен для активации выбора ввода адреса источника вручную с указанием его типа (MAC, IP или сеть)
Выпадающий список «Формат адреса»	Предназначен для выбора одного из следующих типов адресов источника: – «IP»; – «MAC»
Поле «Адрес источника (MAC или IP или сеть)»	Предназначено для ввода адреса источника обрабатываемых пакетов в формате MAC или IP или сеть. Для работы данного параметра необходимо активировать чекбокс «Формат адреса»
Чекбокс «Дополнительные адреса»	Предназначен для активации выбора дополнительных адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Дополнительные адреса»	Предназначен для выбора одного дополнительного адреса из перечня (созданных ранее пользователем вручную) дополнительных сетевых узлов
Чекбокс «Группы адресов»	Предназначен для активации выбора группы адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Группы адресов»	Предназначен для выбора одной группы из перечня (созданных ранее пользователем вручную) групп адресов
Чекбокс «Инвертировать»*	Предназначен для выбора включения/отключения функции инвертирования адреса сетевого узла, то есть всех адресов сетевых узлов кроме указанного
Чекбокс «Использовать порт источника»*	Предназначен для выбора включения/отключения использования порта, указанного пользователем вручную
Поле «Порт источника»*	Предназначено для ввода порта, с которого поступают сетевые пакеты
Чекбокс «Инвертировать»*	Предназначен для выбора включения/отключения функции инвертирования порта, с которого поступают сетевые пакеты, то есть всех портов кроме указанного
* – Элемент интерфейса, доступный только в «Расширенном режиме»	

4.7.9.3.2. Вкладка «Назначение»

Вкладка «Назначение» на странице «Каналы (Pinholes)» (см. рис. 159) предназначена для настройки параметров фильтрации по данным о назначении в сетевом пакете в правиле МЭ.

Вкладка «Назначение»

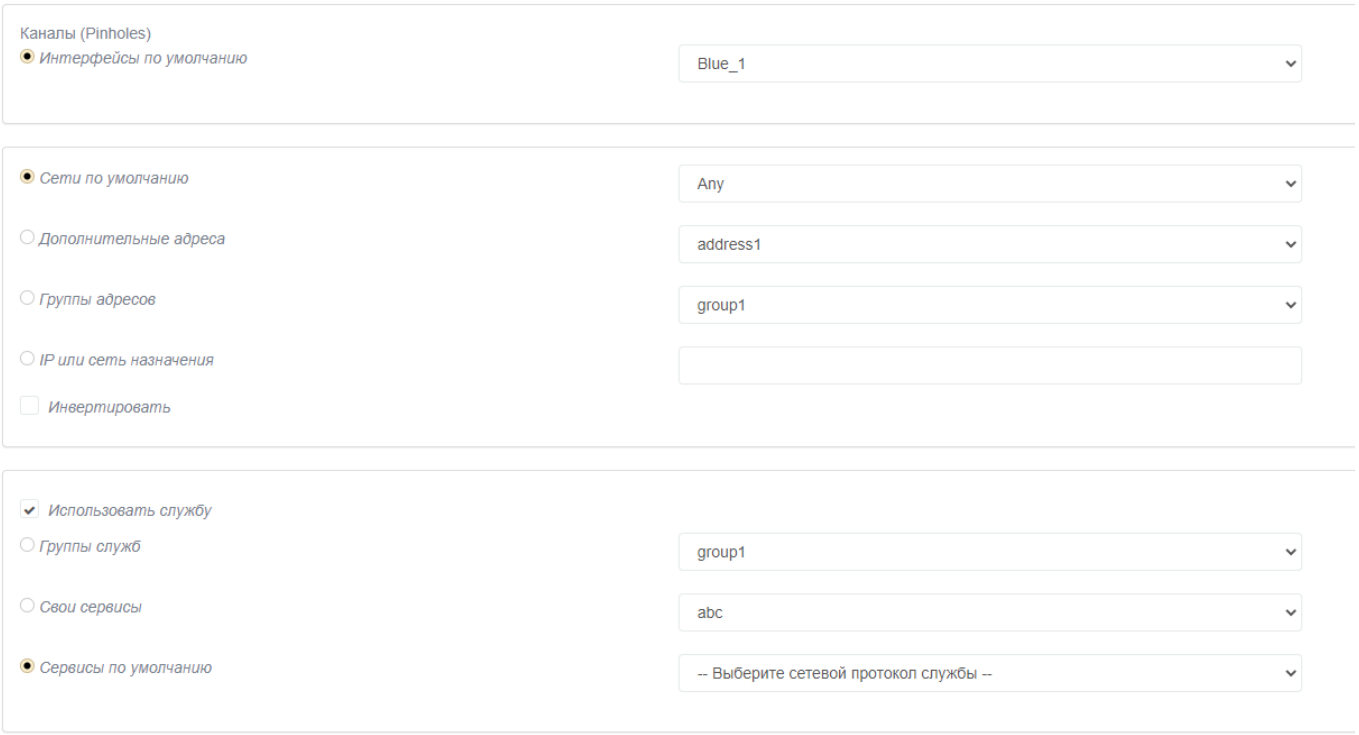

Рис. 159

В таблице 76 приведено описание элементов вкладки «Назначение» на странице «Каналы (Pinholes)».

Таблица 76 – Описание элементов вкладки «Назначение» на странице «Каналы (Pinholes)»

Элемент	Описание
Чекбокс «Интерфейсы по умолчанию»	Предназначен для активации выбора интерфейсов по умолчанию
Выпадающий список «Интерфейсы по умолчанию»	Предназначен для выбора одного из доступных в перечне физических сетевых интерфейсов изделия (доступны для выбора только «синие» и «зеленые» сетевые интерфейсы)

Элемент	Описание
Чекбокс «Сети по умолчанию»	Предназначен для выбора добавления сети по умолчанию
Выпадающий список «Сети по умолчанию»	Предназначен для выбора одной из сетей, связанных с сетевыми настройками изделия
Чекбокс «Дополнительные адреса»	Предназначен для активации выбора дополнительных адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Дополнительные адреса»	Предназначен для выбора одного дополнительного адреса из перечня (созданных ранее пользователем вручную) дополнительных сетевых узлов
Чекбокс «Группы адресов»	Предназначен для активации выбора группы адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Группы адресов»	Предназначен для выбора одной группы из перечня (созданных ранее пользователем вручную) групп адресов
Чекбокс «IP или сеть назначения»	Предназначен для активации выбора адреса назначения с указанным вручную пользователем IP или сетью
Поле «IP или сеть назначения»	Предназначен для ввода IP-адреса или сети для узла назначения (целевого узла обрабатываемого пакета)
Чекбокс «Инвертировать»*	Предназначен для выбора включения/отключения функции инвертирования адреса сетевого узла, то есть всех адресов сетевых узлов кроме указанного
Чекбокс «Использовать службу»	Предназначен для выбора включения/отключения использования выбранной пользователем службы или сервиса
Чекбокс «Группы служб»	Предназначен для активации выбора использования групп служб, созданных ранее вручную пользователем
Выпадающий список «Группы служб»	Предназначен для выбора одной группы из перечня созданных ранее вручную пользователем
Чекбокс «Свои сервисы»	Предназначен для активации выбора использования сервиса, созданного ранее вручную пользователем
Выпадающий список «Свои сервисы»	Предназначен для выбора одного сервиса из перечня ранее добавленных вручную пользователем
Чекбокс «Сервисы по умолчанию»	Предназначен для активации выбора использования сетевого протокола службы, имеющей специальное имя в изделии
Выпадающий список «Сервисы по умолчанию»	Предназначен для выбора одной из сетевых протоколов службы, из перечня имеющих специальное имя в изделии
* – Элемент интерфейса, доступный только в «Расширенном режиме»	

4.7.9.3.3. Вкладка «Действие»

Вкладка «Действие» на странице «Каналы (Pinholes)» (см. рис. 160) на странице «Каналы (Pinholes)» предназначена для настройки действий по фильтрации при срабатывании правил.

Вкладка «Действие»

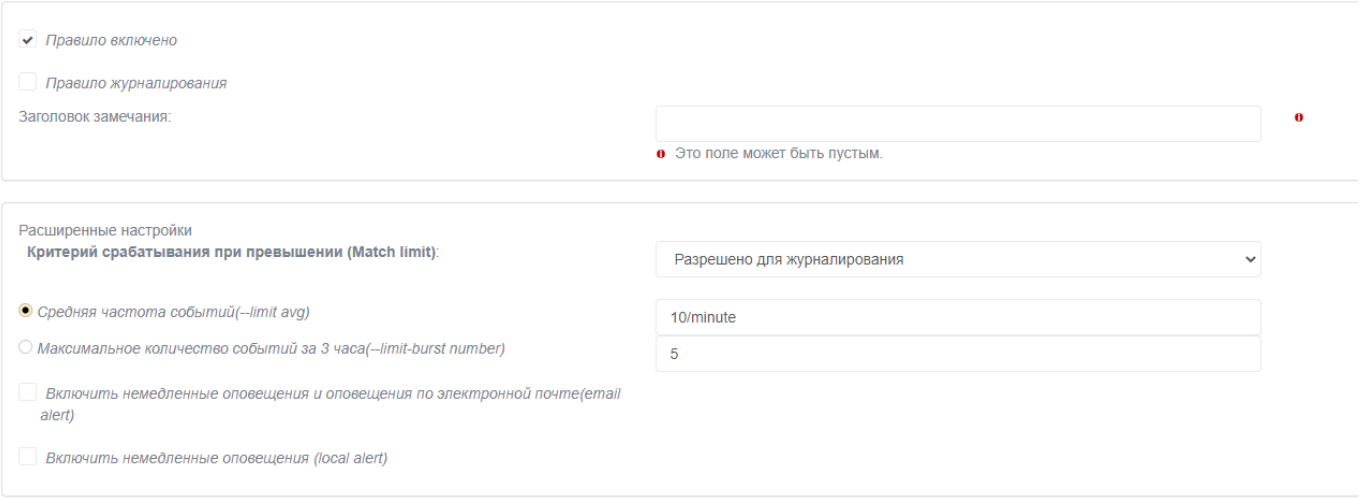

Рис. 160

В таблице 77 приведено описание элементов вкладки «Действие» на странице «Каналы (Pinholes)».

Таблица 77 – Описание элементов вкладки «Действие» на странице «Каналы (Pinholes)»

Элемент	Описание
Чекбокс «Правило включено»	Предназначен для выбора включения/отключения правила и выбранных действий, при его срабатывании
Чекбокс «Правило журналирования»	Предназначен для выбора включения/отключения правила журналирования прохождения пакетов по настраиваемому правилу
Поле «Заголовок замечания»	Предназначено для ввода примечаний к настраиваемому правилу. Примечание. Данное поле не обязательно к заполнению
Выпадающий список «Критерий срабатывания при превышении (Match limit)»*	Предназначен для выбора одного из доступных в перечне расширенных настроек действия при срабатывании правил: – «Возможность отключена»; – «Разрешено для журналирования»; – «Разрешено для политики принятия или сбрасывания»; – «Разрешено для политик обоих видов»
Чекбокс «Средняя частота событий (--limit avg)»*	Предназначен для активации выбора использования функции ограничения записи событий в журнал по средней частоте событий
Поле «Средняя частота событий (--limit avg)»*	Предназначено для ввода средней частоты событий. Необходимо указывать в формате: **число событий/единица времени**
Чекбокс «Максимальное количество событий за 3 часа (--limit-burst number)»*	Предназначен для активации выбора использования функции ограничения записи событий в журнал по максимальному количеству событий

Элемент	Описание
Поле «Максимальное количество событий за 3 часа (--limit-burst number)»*	Предназначено для ввода максимального количество событий за 3 часа, записываемых в журнал. Данный параметр будет определять пик «разовой» доставки пакетов. Значение по умолчанию «5»
Чекбокс «Включить немедленные оповещения и оповещения по электронной почте (email alert)»*	Предназначен для выбора включения/отключения функции получения оповещения о сработавшем правиле на электронную почту
Чекбокс «Включить немедленные оповещения (local alert)»*	Предназначен для выбора включения/отключения функции оповещения в всплывающем окне уведомлений изделия «»
* – Элемент интерфейса, доступный только в «Расширенном режиме»	

4.7.9.3.4. Вкладка «Дополнительно»

Вкладка «Дополнительно» предназначена для настройки дополнительных параметров фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам и описана подробно в п. 4.7.9.1.4 настоящего документа.

Примечание. В данной вкладке, в отличии от описанной ранее в п. 4.7.9.1.4 настоящего документа, отсутствует возможность задания метки соответствующим пакетам.

4.7.9.4. Страница «Перенаправление портов»

Страница «Перенаправление портов» (см. рис. 161) открывается после нажатия одноименной кнопки, находящейся в верхней части экрана подраздела «Правила межсетевого экрана».

Страница «Перенаправление портов»

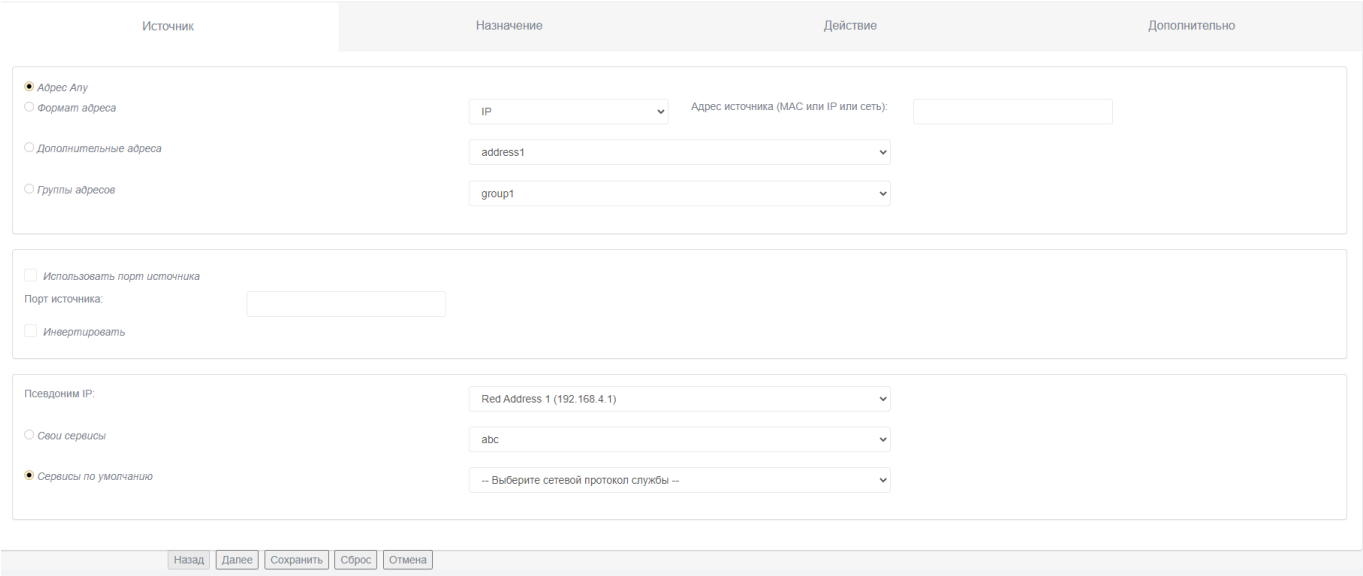

Рис. 161

Страница «Перенаправление портов» предназначена для настройки параметров фильтрации сетевых пакетов, для которых физический адрес и порт назначения подставляется при получении МЭ пакета с определенными администратором параметрами назначения. Например, для организации доступа к серверам в демилитаризованной зоне (далее – ДМЗ).

Страница «Перенаправление портов» состоит из следующих вкладок:

1) «Источник»;

2) «Назначение»;

3) «Действие»;

4) «Дополнительно».

На данной странице присутствуют также следующие элементы навигационного меню:

1) кнопка «Назад» – предназначена для перехода на предыдущую вкладку страницы;

2) кнопка «Далее» – предназначена для перехода на следующую вкладку страницы;

3) кнопка «Сохранить» – предназначена для сохранения введенной информации;

4) кнопка «Сброс» – предназначена для очищения заполнения всей формы активной вкладки;

5) кнопка «Отмена» – предназначена для возврата в подраздел «Правила межсетевого экрана» без сохранения введенных данных на странице.

4.7.9.4.1. Вкладка «Источник»

Вкладка «Источник» на странице «Перенаправление портов» (см. рис. 162) предназначена для настройки параметров фильтрации по данным об источнике сетевого пакета в правиле МЭ.

Вкладка «Источник»

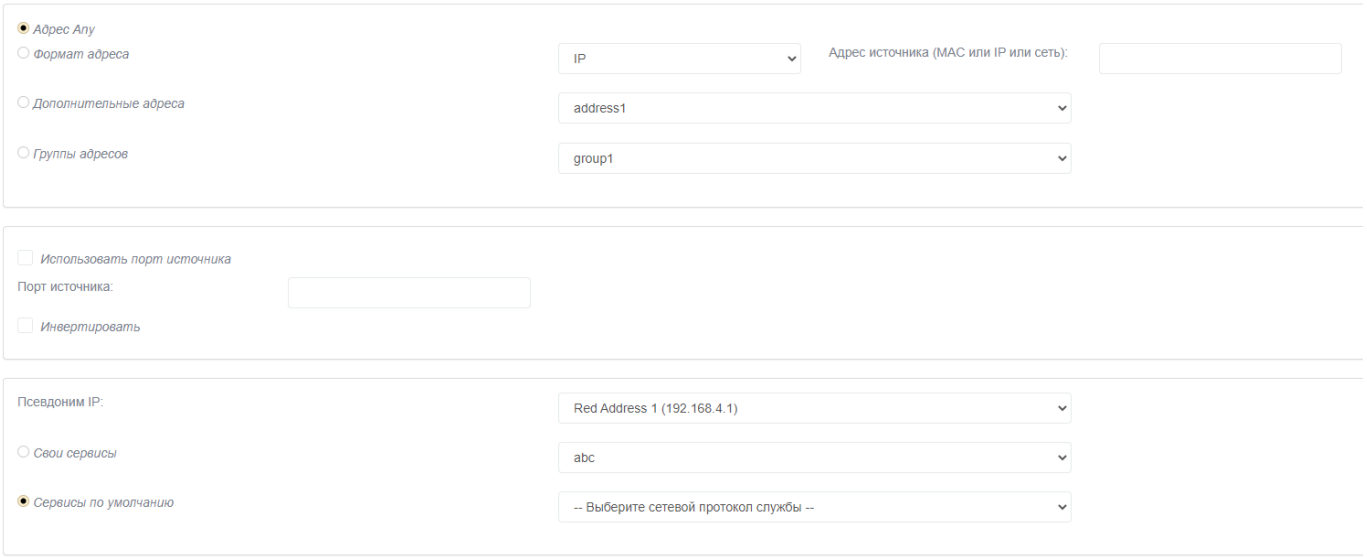

Рис. 162

В таблице 78 приведено описание элементов вкладки «Источник» на странице «Перенаправление портов».

Таблица 78 – Описание элементов вкладки «Источник» на странице «Перенаправление портов»

Элемент	Описание
Чекбокс «Адрес Any»	Предназначен для активации выбора всех возможных адресов источника

Элемент	Описание
Чекбокс «Формат адреса»	Предназначен для активации выбора ввода адреса источника вручную с указанием его типа (MAC, IP или сеть)
Выпадающий список «Формат адреса»	Предназначен для выбора одного из следующих типов адресов источника: – «IP»; – «MAC»
Поле «Адрес источника (MAC или IP или сеть)»	Предназначено для ввода адреса источника обрабатываемых пакетов в формате MAC или IP или сеть. Для работы данного параметра необходимо активировать чекбокс «Формат адреса»
Чекбокс «Дополнительные адреса»	Предназначен для активации выбора дополнительных адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Дополнительные адреса»	Предназначен для выбора одного дополнительного адреса из перечня (созданных ранее пользователем вручную) дополнительных сетевых узлов
Чекбокс «Группы адресов»	Предназначен для активации выбора группы адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Группы адресов»	Предназначен для выбора одной группы из перечня (созданных ранее пользователем вручную) групп адресов
Чекбокс «Использовать порт источника»	Предназначен для выбора включения/отключения использования порта, указанного пользователем вручную
Поле «Порт источника»	Предназначено для ввода порта, с которого поступают сетевые пакеты
Чекбокс «Инвертировать»	Предназначен для выбора включения/отключения функции инвертирования порта, с которого поступают сетевые пакеты, то есть всех портов кроме указанного
Выпадающий список «Псевдоним IP»	Предназначен для выбора псевдонима интерфейса или «красного» сетевого интерфейса. Обязательный параметр для выбора. Примечание. Данный адрес является одним из параметров принятия решения о преобразовании адреса и порта назначения, позволяя разделить запросы к узлам внутренней сети
Чекбокс «Свои сервисы»	Предназначен для активации выбора использования сервиса, созданного ранее вручную пользователем
Выпадающий список «Свои сервисы»	Предназначен для выбора одного сервиса из перечня ранее добавленных вручную пользователем
Чекбокс «Сервисы по умолчанию»	Предназначен для активации выбора использования сетевого протокола службы, имеющей специальное имя в изделии
Выпадающий список «Сервисы по умолчанию»	Предназначен для выбора одной из сетевых протоколов службы, из перечня имеющих специальное имя в изделии

4.7.9.4.2. Вкладка «Назначения»

Вкладка «Назначения» на странице «Перенаправление портов» (см. рис. 163) предназначена для настройки параметров фильтрации по данным о назначении в сетевом пакете в правиле МЭ.

Вкладка «Назначение»

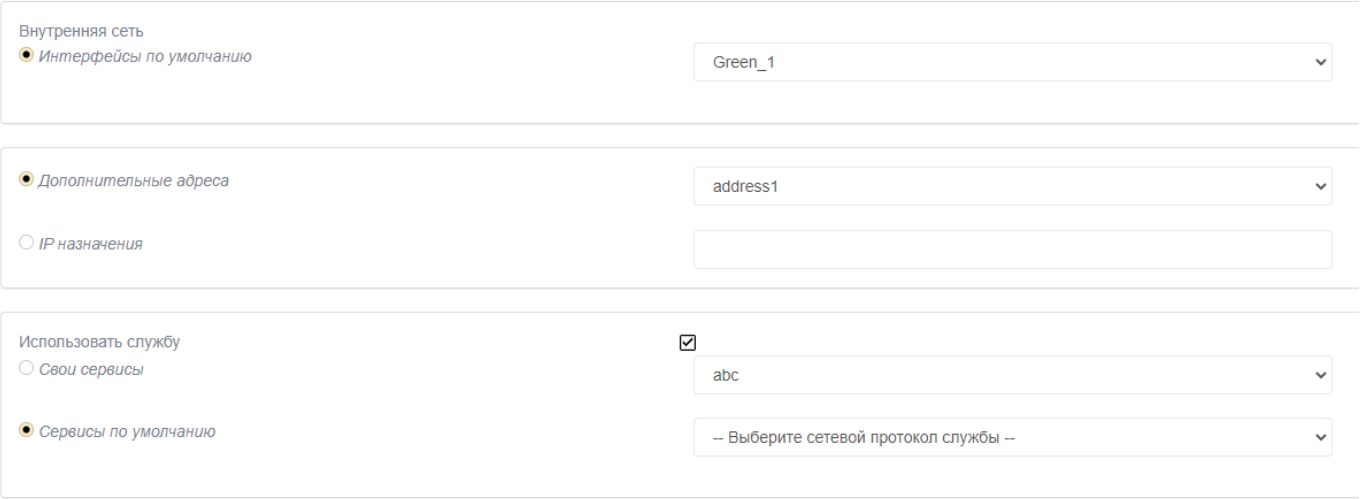

Рис. 163

В таблице 79 приведено описание элементов вкладки «Назначение» на странице «Перенаправление портов».

Таблица 79 – Описание элементов вкладки «Назначение» на странице «Перенаправление портов»

Элемент	Описание
Чекбокс «Интерфейсы по умолчанию»	Предназначен для активации выбора интерфейсов по умолчанию
Выпадающий список «Интерфейсы по умолчанию»	Предназначен для выбора одного из доступных в перечне физических сетевых интерфейсов изделия
Чекбокс «Дополнительные адреса»	Предназначен для активации выбора дополнительных адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Дополнительные адреса»	Предназначен для выбора одного дополнительного адреса из перечня (созданных ранее пользователем вручную) дополнительных сетевых узлов
Чекбокс «IP назначения»	Предназначен для активации выбора адреса назначения с указанным вручную пользователем IP или сетью
Поле «IP назначения»	Предназначен для ввода IP-адреса или сети для узла назначения (целевого узла обрабатываемого пакета)
Чекбокс «Использовать службу»	Предназначен для выбора включения/отключения использования выбранной пользователем службы или сервиса. Примечание. Данная служба является одним из параметров принятия решения о преобразовании порта назначения, позволяя разделить запросы к узлам внутренней сети. Необходимо выбрать дополнительно один из чекбоксов: «Свои сервисы» или «Сервисы по умолчанию»

Элемент	Описание
Чекбокс «Свои сервисы»	Предназначен для активации выбора использования сервиса, созданного ранее вручную пользователем
Выпадающий список «Свои сервисы»	Предназначен для выбора одного сервиса из перечня ранее добавленных вручную пользователем
Чекбокс «Сервисы по умолчанию»	Предназначен для активации выбора использования сетевого протокола службы, имеющей специальное имя в изделии
Выпадающий список «Сервисы по умолчанию»	Предназначен для выбора одной из сетевых протоколов службы, из перечня имеющих специальное имя в изделии

4.7.9.4.3. Вкладка «Действие»

Вкладка «Действие» предназначена для настройки действий по фильтрации при срабатывании правил и описана подробно в п. 4.7.9.1.3 настоящего документа.

4.7.9.4.4. Вкладка «Дополнительно»

Вкладка «Дополнительно» предназначена для настройки дополнительных параметров фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам и описана подробно в п. 4.7.9.1.4 настоящего документа.

Примечание. В данной вкладке, в отличии от описанной ранее в п. 4.7.9.1.4 настоящего документа, отсутствует возможность задания метки соответствующим пакетам.

4.7.9.5. Страница «Прокси»

Страница «Прокси» (см. рис. 164) открывается после нажатия одноименной кнопки, находящейся в верхней части экрана подраздела «Правила межсетевого экрана».

Страница «Прокси»

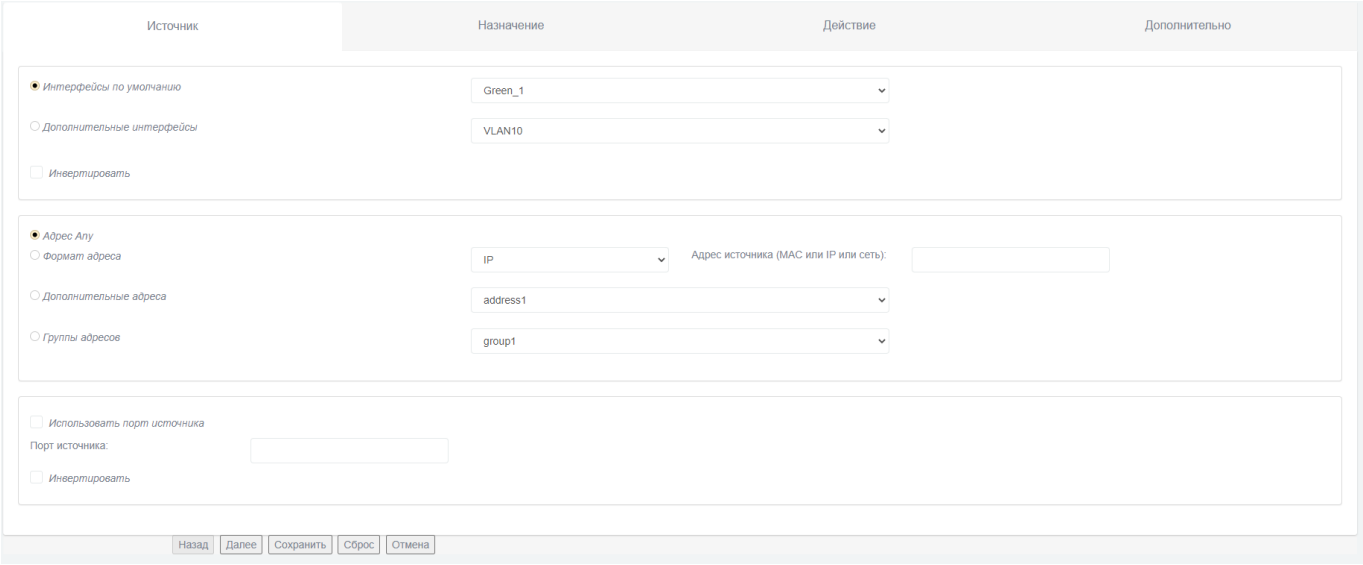

Рис. 164

Страница «Прокси» предназначена для ассоциации трафика, поступающего на определенный порт, с одним из обрабатываемых типов (HTTP, FTP). Обработка этого трафика осуществляется с помощью программы-посредника.

Страница «Прокси» состоит из следующих вкладок:

1) «Источник»;

2) «Назначение»;

3) «Действие»;

4) «Дополнительно».

На данной странице присутствуют также следующие элементы навигационного меню:

1) кнопка «Назад» – предназначена для перехода на предыдущую вкладку страницы;

2) кнопка «Далее» – предназначена для перехода на следующую вкладку страницы;

3) кнопка «Сохранить» – предназначена для сохранения введенной информации;

4) кнопка «Сброс» – предназначена для очищения заполнения всей формы активной вкладки;

5) кнопка «Отмена» – предназначена для возврата в подраздел «Правила межсетевого экрана» без сохранения введенных данных на странице.

4.7.9.5.1. Вкладка «Источник»

Вкладка «Источник» на странице «Прокси» (см. рис. 165) предназначена для настройки параметров фильтрации по данным об источнике сетевого пакета в правиле МЭ.

Вкладка «Источник»

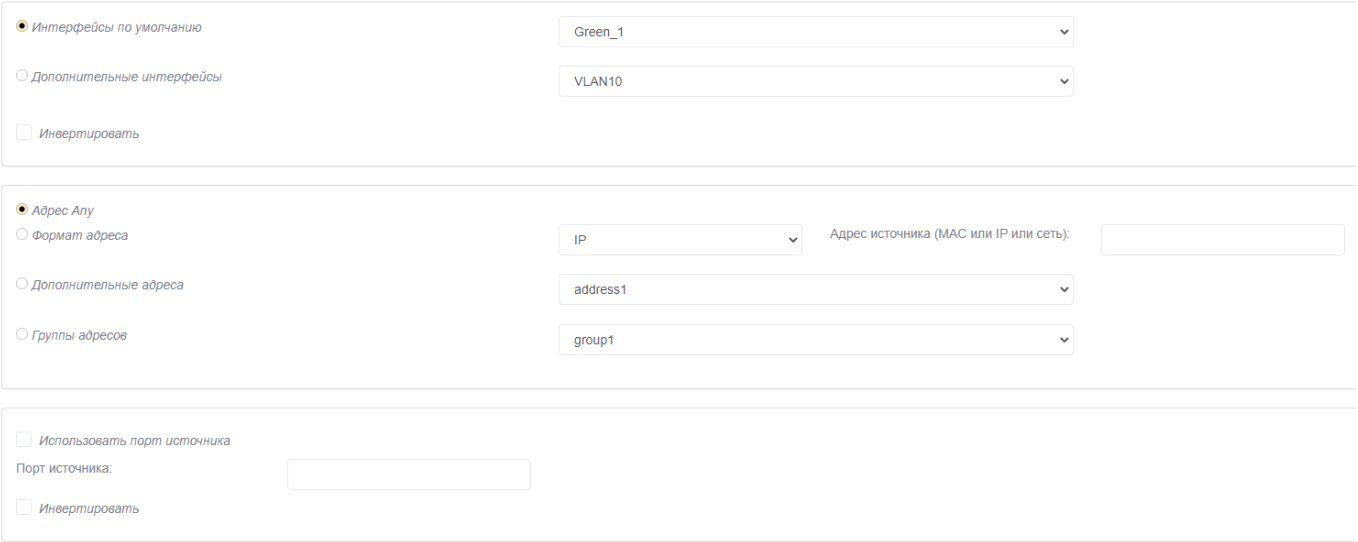

Рис. 165

В таблице 80 приведено описание элементов вкладки «Источник» на странице «Прокси».

Таблица 80 – Описание элементов вкладки «Источник» на странице «Прокси»

Элемент	Описание
Чекбокс «Интерфейсы по умолчанию»	Предназначен для активации выбора физических интерфейсов изделия
Выпадающий список «Интерфейсы по умолчанию»	Предназначен для выбора одного из перечня доступных физических интерфейсов изделия
Чекбокс «Дополнительные интерфейсы»*	Предназначен для активации выбора виртуального интерфейса изделия, определяемого пользователем

Элемент	Описание
Выпадающий список «Дополнительные интерфейсы»*	Предназначен для выбора одного из перечня доступных виртуальных (зарегистрированных пользователем вручную) интерфейсов изделия
Чекбокс «Инвертировать»*	Предназначен для выбора включения/отключения функции инвертирования сетевого интерфейса, то есть всех сетевых интерфейсов кроме указанного
Чекбокс «Адрес Any»	Предназначен для активации выбора всех возможных адресов источника
Чекбокс «Формат адреса»	Предназначен для активации выбора ввода адреса источника вручную с указанием его типа (MAC, IP или сеть)
Выпадающий список «Формат адреса»	Предназначен для выбора одного из следующих типов адресов источника: – «IP»; – «MAC»
Поле «Адрес источника (MAC или IP или сеть)»	Предназначено для ввода адреса источника обрабатываемых пакетов в формате MAC или IP или сеть. Для работы данного параметра необходимо активировать чекбокс «Формат адреса»
Чекбокс «Дополнительные адреса»	Предназначен для активации выбора дополнительных адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Дополнительные адреса»	Предназначен для выбора одного дополнительного адреса из перечня (созданных ранее пользователем вручную) дополнительных сетевых узлов
Чекбокс «Группы адресов»	Предназначен для активации выбора группы адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Группы адресов»	Предназначен для выбора одной группы из перечня (созданных ранее пользователем вручную) групп адресов
Чекбокс «Использовать порт источника»	Предназначен для выбора включения/отключения использования порта, указанного пользователем вручную
Поле «Порт источника»	Предназначено для ввода порта, с которого поступают сетевые пакеты
Чекбокс «Инвертировать»	Предназначен для выбора включения/отключения функции инвертирования порта, с которого поступают сетевые пакеты, то есть всех портов кроме указанного
* – Элемент интерфейса, доступный только в «Расширенном режиме»	

4.7.9.5.2. Вкладка «Назначение»

Вкладка «Назначение» на странице «Прокси» (см. рис. 166) предназначена для настройки параметров фильтрации по данным о назначении в сетевом пакете в правиле МЭ.

Вкладка «Назначение»

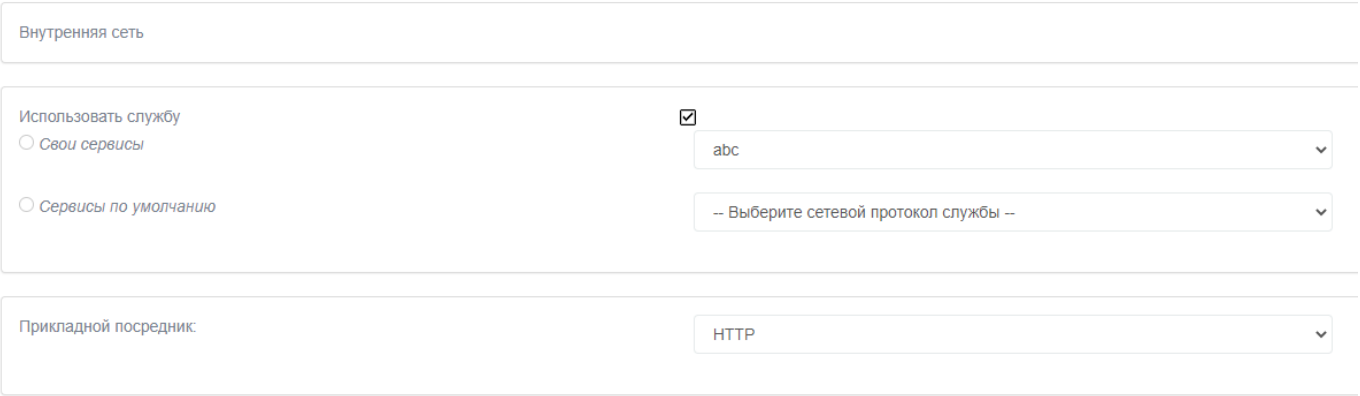

Рис. 166

В таблице 81 приведено описание элементов вкладки «Назначение» на странице «Прокси».

Таблица 81 – Описание элементов вкладки «Назначение» на странице «Прокси»

Элемент	Описание
Чекбокс «Использовать службу»	Предназначен для выбора включения/отключения использования выбранной пользователем службы или сервиса. Примечание. Данная служба является одним из параметров принятия решения о преобразовании порта назначения для ассоциации трафика, поступающего на определенный порт, с одним из обрабатываемых типов (HTTP, FTP). Необходимо выбрать дополнительно один из чекбоксов: «Свои сервисы» или «Сервисы по умолчанию»
Чекбокс «Свои сервисы»	Предназначен для активации выбора использования сервиса, созданного ранее вручную пользователем
Выпадающий список «Свои сервисы»	Предназначен для выбора одного сервиса из перечня ранее добавленных вручную пользователем
Чекбокс «Сервисы по умолчанию»	Предназначен для активации выбора использования сетевого протокола службы, имеющей специальное имя в изделии
Выпадающий список «Сервисы по умолчанию»	Предназначен для выбора одной из сетевых протоколов службы, из перечня имеющих специальное имя в изделии
Выпадающий список «Прикладной посредник»	Предназначен для выбора прикладного протокола для ассоциации и обработки трафика, определенного пользователем. Доступны для выбора следующие варианты: – «HTTP»; – «FTP»

4.7.9.5.3. Вкладка «Действие»

Вкладка «Действие» предназначена для настройки действий по фильтрации при срабатывании правил и описана подробно в п. 4.7.9.1.3 настоящего документа.

4.7.9.5.4. Вкладка «Дополнительно»

Вкладка «Дополнительно» предназначена для настройки дополнительных параметров фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам и описана подробно в п. 4.7.9.1.4 настоящего документа.

Примечание. В данной вкладке, в отличии от описанной ранее в п. 4.7.9.1.4 настоящего документа, отсутствует возможность задания метки соответствующим пакетам.

4.7.9.6. Страница «Доступ извне»

Страница «Доступ извне» (см. рис. 167) открывается после нажатия одноименной кнопки, находящейся в верхней части экрана подраздела «Правила межсетевого экрана».

Страница «Доступ извне»

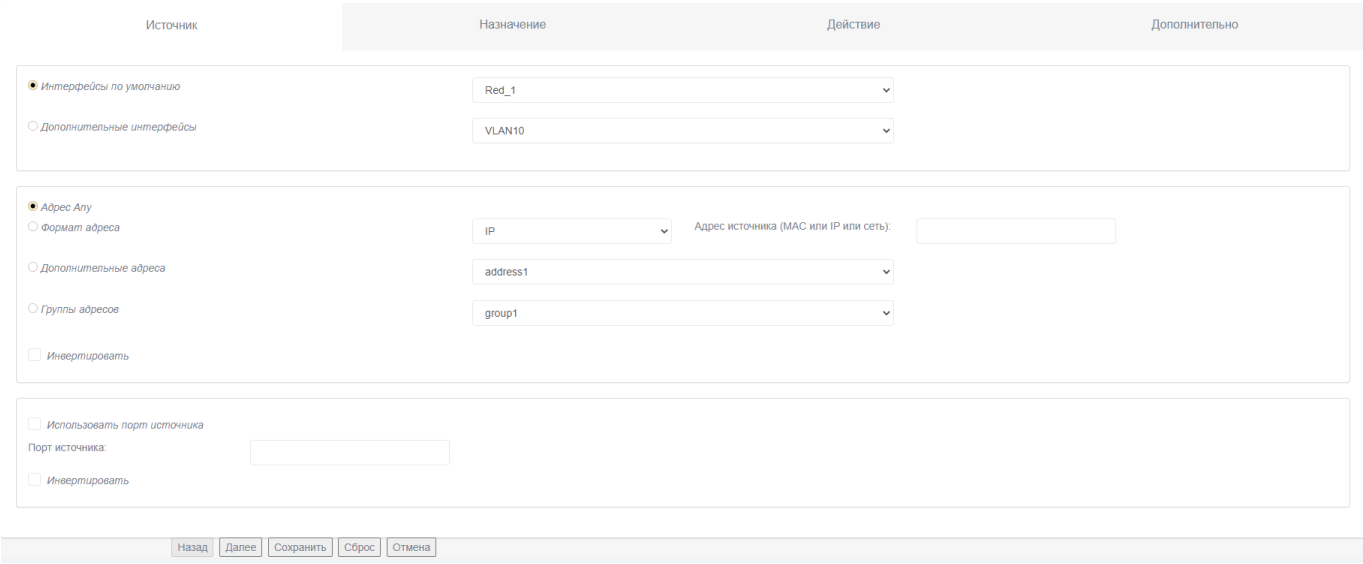

Рис. 167

Страница «Доступ извне» предназначена для создания правил организации административного доступа к МЭ из «красной» сети.

Страница «Доступ извне» состоит из следующих вкладок:

1) «Источник»;

2) «Назначение»;

3) «Действие»;

4) «Дополнительно».

На данной странице присутствуют также следующие элементы навигационного меню:

1) кнопка «Назад» – предназначена для перехода на предыдущую вкладку страницы;

2) кнопка «Далее» – предназначена для перехода на следующую вкладку страницы;

3) кнопка «Сохранить» – предназначена для сохранения введенной информации;

4) кнопка «Сброс» – предназначена для очищения заполнения всей формы активной вкладки;

5) кнопка «Отмена» – предназначена для возврата в подраздел «Правила межсетевого экрана» без сохранения введенных данных на странице.

4.7.9.6.1. Вкладка «Источник»

Вкладка «Источник» на странице «Доступ извне» (см. рис. 168) предназначена для настройки параметров фильтрации по данным об источнике сетевого пакета в правиле МЭ.

Вкладка «Источник»

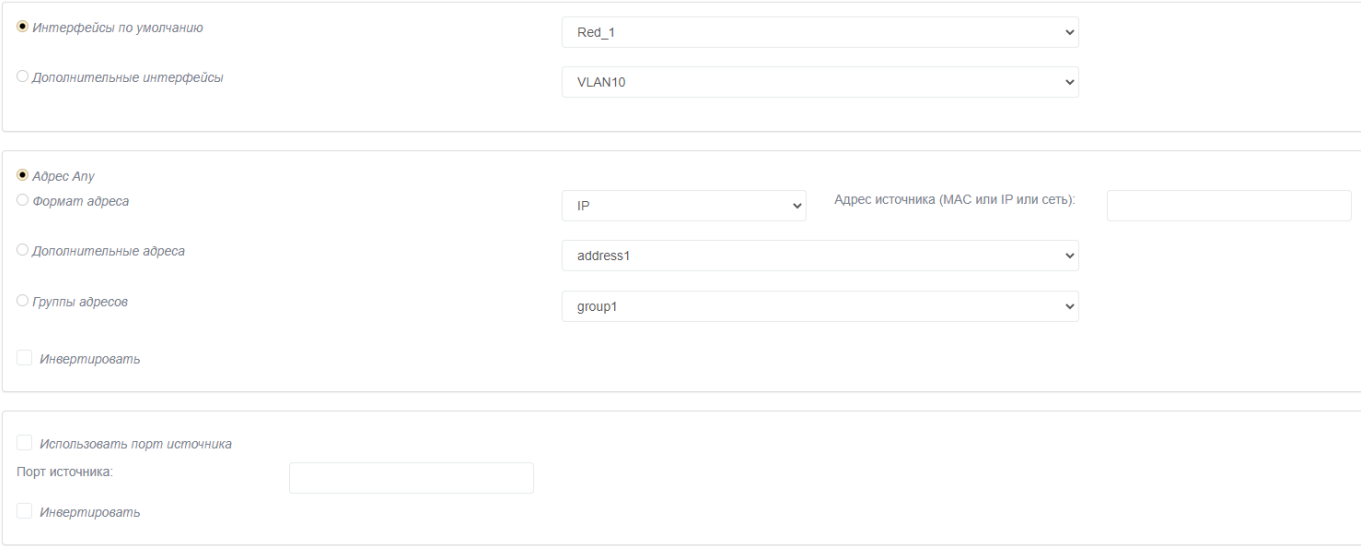

Рис. 168

В таблице 82 приведено описание элементов вкладки «Источник» на странице «Доступ извне».

Таблица 82 – Описание элементов вкладки «Источник» на странице «Доступ извне»

Элемент	Описание
Чекбокс «Интерфейсы по умолчанию»	Предназначен для активации выбора физических интерфейсов изделия
Выпадающий список «Интерфейсы по умолчанию»	Предназначен для выбора одного из перечня доступных физических интерфейсов изделия
Чекбокс «Дополнительные интерфейсы»*	Предназначен для активации выбора виртуального интерфейса изделия, определяемого пользователем
Выпадающий список «Дополнительные интерфейсы»*	Предназначен для выбора одного из перечня доступных виртуальных (зарегистрированных пользователем вручную) интерфейсов изделия
Чекбокс «Адрес Any»	Предназначен для активации выбора всех возможных адресов источника
Чекбокс «Формат адреса»	Предназначен для активации выбора ввода адреса источника вручную с указанием его типа (MAC, IP или сеть)
Выпадающий список «Формат адреса»	Предназначен для выбора одного из следующих типов адресов источника: – «IP»; – «MAC»
Поле «Адрес источника (MAC или IP или сеть)»	Предназначено для ввода адреса источника обрабатываемых пакетов в формате MAC или IP или сеть. Для работы данного параметра необходимо активировать чекбокс «Формат адреса»

Элемент	Описание
Чекбокс «Дополнительные адреса»	Предназначен для активации выбора дополнительных адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Дополнительные адреса»	Предназначен для выбора одного дополнительного адреса из перечня (созданных ранее пользователем вручную) дополнительных сетевых узлов
Чекбокс «Группы адресов»	Предназначен для активации выбора группы адресов сетевых узлов из созданных ранее пользователем вручную
Выпадающий список «Группы адресов»	Предназначен для выбора одной группы из перечня (созданных ранее пользователем вручную) групп адресов
Чекбокс «Инвертировать»*	Предназначен для выбора включения/отключения функции инвертирования адреса сетевого узла, то есть всех адресов сетевых узлов кроме указанного
Чекбокс «Использовать порт источника»*	Предназначен для выбора включения/отключения использования порта, указанного пользователем вручную
Поле «Порт источника»*	Предназначено для ввода порта, с которого поступают сетевые пакеты
Чекбокс «Инвертировать»*	Предназначен для выбора включения/отключения функции инвертирования порта, с которого поступают сетевые пакеты, то есть всех портов кроме указанного
* – Элемент интерфейса, доступный только в «Расширенном режиме»	

4.7.9.6.2. Вкладка «Назначение»

Вкладка «Назначение» предназначена для настройки параметров фильтрации по данным о назначении в сетевом пакете в правиле МЭ. Адресом назначения всегда является адрес (или псевдоним адреса) сетевого интерфейса МЭ.

Данная вкладка описана подробно в п. 4.7.9.2.2 настоящего документа.

4.7.9.6.3. Вкладка «Действие»

Вкладка «Действие» предназначена для настройки действий по фильтрации при срабатывании правил и описана подробно в п. 4.7.9.1.3 настоящего документа.

Примечание. В данной вкладке, в отличии от описанной ранее в п. 4.7.9.1.3 настоящего документа, отсутствует поле «Действие правила».

4.7.9.6.4. Вкладка «Дополнительно»

Вкладка «Дополнительно» предназначена для настройки дополнительных параметров фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам и описана подробно в п. 4.7.9.1.4 настоящего документа.

Примечание. В данной вкладке, в отличии от описанной ранее в п. 4.7.9.1.4 настоящего документа, отсутствует возможность задания метки соответствующим пакетам.

4.7.9.7. Страница «L2»

Страница «L2» (см. рис. 169) открывается после нажатия одноименной кнопки, находящейся в верхней части экрана подраздела «Правила межсетевого экрана».

Страница «L2»

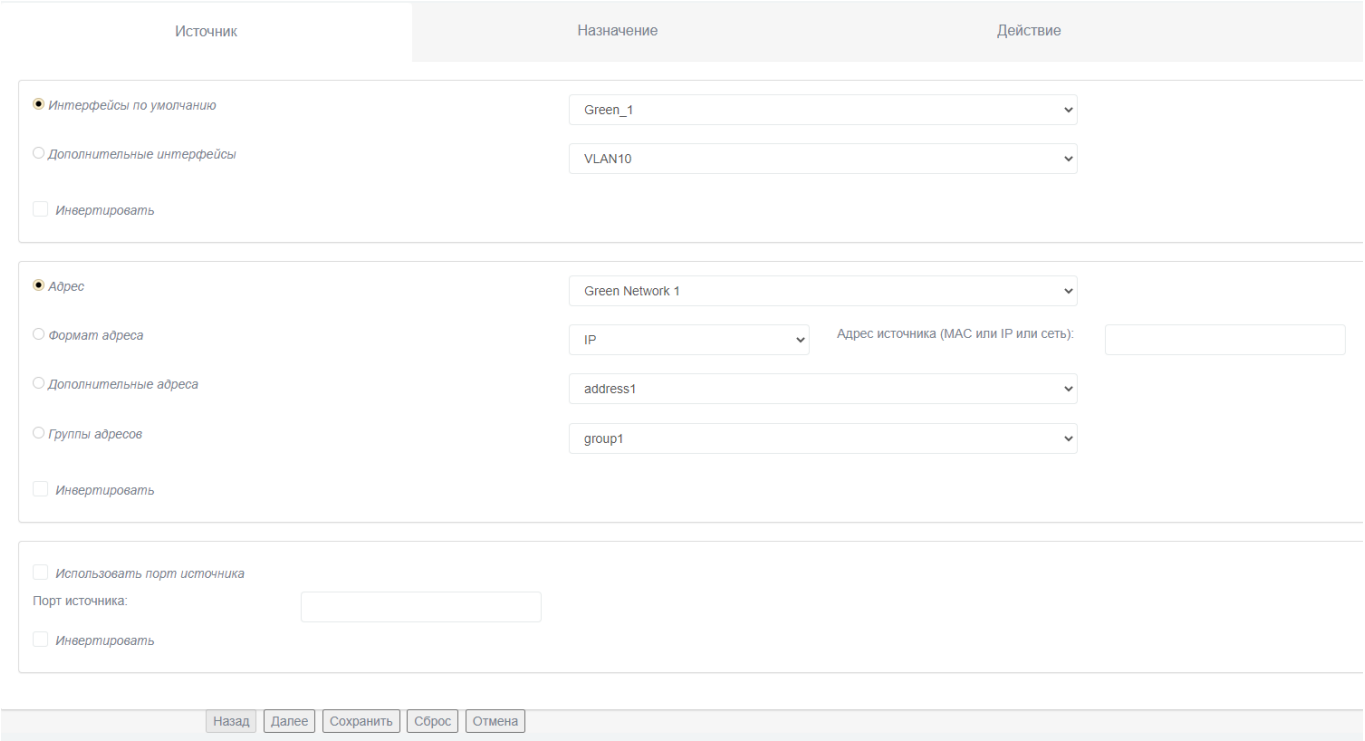

Рис. 169

Страница «L2» предназначена для создания правил фильтрации МЭ на канальном уровне (L2).

Страница «L2» состоит из следующих вкладок:

1) «Источник»;

2) «Назначение»;

3) «Действие».

На данной странице присутствуют также следующие элементы навигационного меню:

1) кнопка «Назад» – предназначена для перехода на предыдущую вкладку страницы;

2) кнопка «Далее» – предназначена для перехода на следующую вкладку страницы;

3) кнопка «Сохранить» – предназначена для сохранения введенной информации;

4) кнопка «Сброс» – предназначена для очищения заполнения всей формы активной вкладки;

5) кнопка «Отмена» – предназначена для возврата в подраздел «Правила межсетевого экрана» без сохранения введенных данных на странице.

4.7.9.7.1. Вкладка «Источник»

Вкладка «Источник» предназначена для настройки параметров фильтрации по данным об источнике сетевого пакета в правиле МЭ и описана подробно в п. 4.7.9.1.1 настоящего документа.

4.7.9.7.2. Вкладка «Назначение»

Вкладка «Назначение» предназначена для настройки параметров фильтрации по данным о назначении в сетевом пакете в правиле МЭ и описана подробно в п. 4.7.9.1.2 настоящего документа.

Примечание. В данной вкладке, в отличии от описанной ранее в п. 4.7.9.1.2 настоящего документа, отсутствует возможность выбора использования группы служб.

4.7.9.7.3. Вкладка «Действие»

Вкладка «Действие» предназначена для настройки действий по фильтрации при срабатывании правил и описана подробно в п. 4.7.9.1.3 настоящего документа.

4.7.9.8. Страница «СОВ»

Страница «СОВ» (см. рис. 170) открывается после нажатия одноименной кнопки, находящейся в верхней части экрана подраздела «Правила межсетевого экрана».

Страница «СОВ»

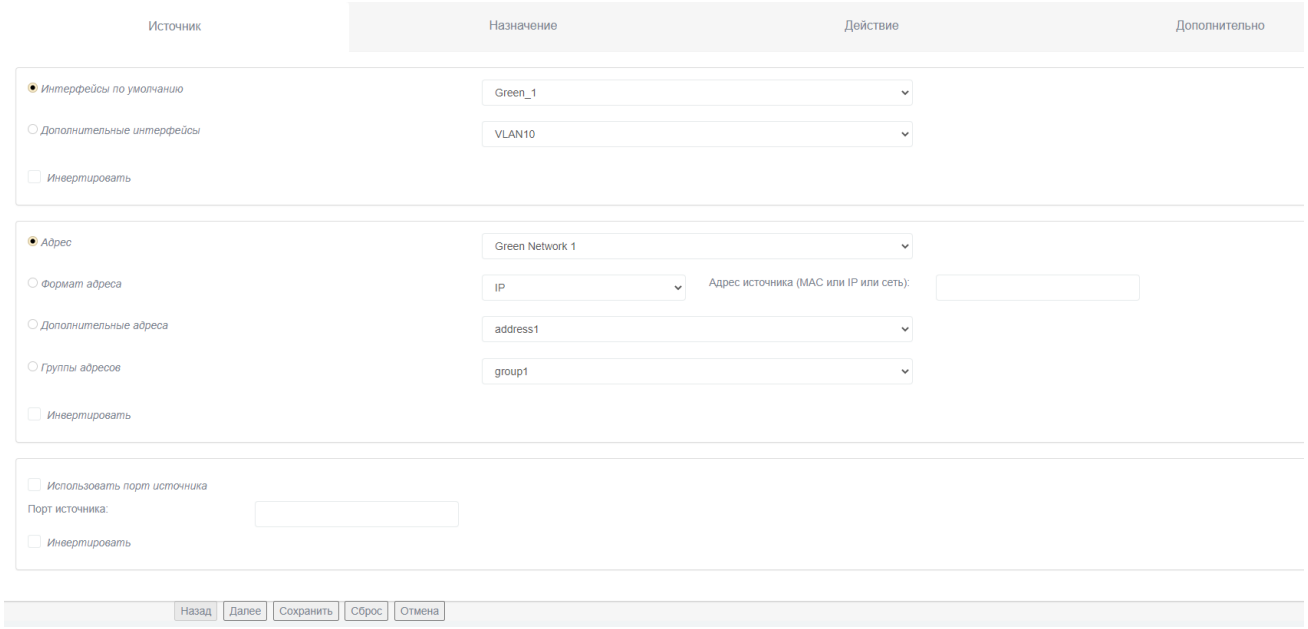

Рис. 170

Страница «СОВ» предназначена для создания правил фильтрации МЭ по перенаправлению сетевых пакетов в СОВ.

Страница «СОВ» состоит из следующих вкладок:

1) «Источник»;

2) «Назначение»;

3) «Действие»;

4) «Дополнительно».

На данной странице присутствуют также следующие элементы навигационного меню:

5) кнопка «Назад» – предназначена для перехода на предыдущую вкладку страницы;

6) кнопка «Далее» – предназначена для перехода на следующую вкладку страницы;

7) кнопка «Сохранить» – предназначена для сохранения введенной информации;

8) кнопка «Сброс» – предназначена для очищения заполнения всей формы активной вкладки;

9) кнопка «Отмена» – предназначена для возврата в подраздел «Правила межсетевого экрана» без сохранения введенных данных на странице.

4.7.9.8.1. Вкладка «Источник»

Вкладка «Источник» предназначена для настройки параметров фильтрации по данным об источнике сетевого пакета в правиле МЭ и описана подробно в п. 4.7.9.1.1 настоящего документа.

4.7.9.8.2. Вкладка «Назначение»

Вкладка «Назначение» предназначена для настройки параметров фильтрации по данным о назначении в сетевом пакете в правиле МЭ и описана подробно в п. 4.7.9.2.2 настоящего документа.

4.7.9.8.3. Вкладка «Действие»

Вкладка «Действие» (см. рис. 171) на странице «СОВ» предназначена для настройки действий по фильтрации при срабатывании правил.

Вкладка «Действие»

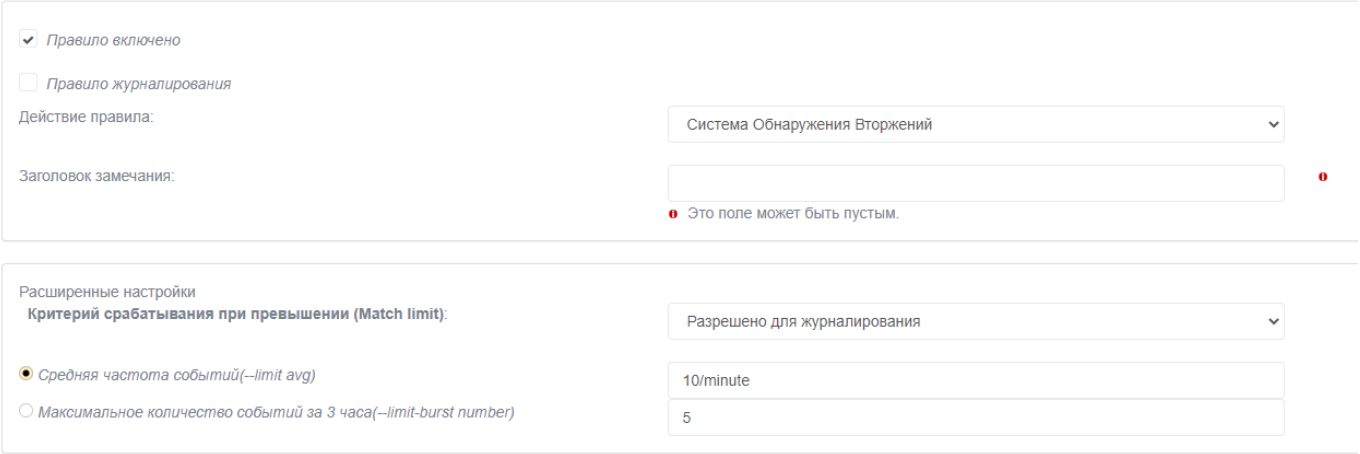

Рис. 171

В таблице 83 приведено описание элементов вкладки «Действие» на странице «СОВ».

Таблица 83 – Описание элементов вкладки «Действие» на странице «СОВ»

Элемент	Описание
Чекбокс «Правило включено»	Предназначен для выбора включения/отключения правила и выбранных действий, при его срабатывании
Чекбокс «Правило журналирования»	Предназначен для выбора включения/отключения правила журналирования прохождения пакетов по настраиваемому правилу
Выпадающий список «Действие правила»	Предназначен для декларирования действий правил по пересылке пакетов в СОВ
Поле «Заголовок замечания»	Предназначено для ввода примечаний к настраиваемому правилу. Примечание. Данное поле не обязательно к заполнению
Выпадающий список «Критерий срабатывания при превышении (Match limit)»*	Предназначен для выбора одного из доступных в перечне расширенных настроек действия при срабатывании правил: – «Возможность отключена»; – «Разрешено для журналирования»; – «Разрешено для политики принятия или сбрасывания»; – «Разрешено для политик обоих видов»
Чекбокс «Средняя частота событий (--limit avg)»*	Предназначен для активации выбора использования функции ограничения записи событий в журнал по средней частоте событий
Поле «Средняя частота событий (--limit avg)»*	Предназначено для ввода средней частоты событий. Необходимо указывать в формате: **число событий/единица времени**
Чекбокс «Максимальное количество событий за 3 часа (--limit-burst number)»*	Предназначен для активации выбора использования функции ограничения записи событий в журнал по максимальному количеству событий

Элемент	Описание
Поле «Максимальное количество событий за 3 часа (--limit-burst number)»*	Предназначено для ввода максимального количество событий за 3 часа, записываемых в журнал. Данный параметр будет определять пик «разовой» доставки пакетов. Значение по умолчанию «5»
* – Элемент интерфейса, доступный только в «Расширенном режиме»	

4.7.9.8.4. Вкладка «Дополнительно»

Вкладка «Дополнительно» предназначена для настройки дополнительных параметров фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам и описана подробно в п. 4.7.9.1.4 настоящего документа.

Примечание. В данной вкладке, в отличии от описанной ранее в п. 4.7.9.1.4 настоящего документа, отсутствует возможность задания метки соответствующим пакетам.

4.7.9.9. Блок «Текущие правила»

Блок «Текущие правила» (см. рис. 172) представляет собой перечень информационных таблиц, отображающих установленные на изделии правила МЭ в соответствии с описанными в подразделе «Правила межсетевого экрана» страницами.

Соответствие информационных таблиц и страниц определяется по имени страницы и заголовка таблицы.

Блок «Текущие правила»

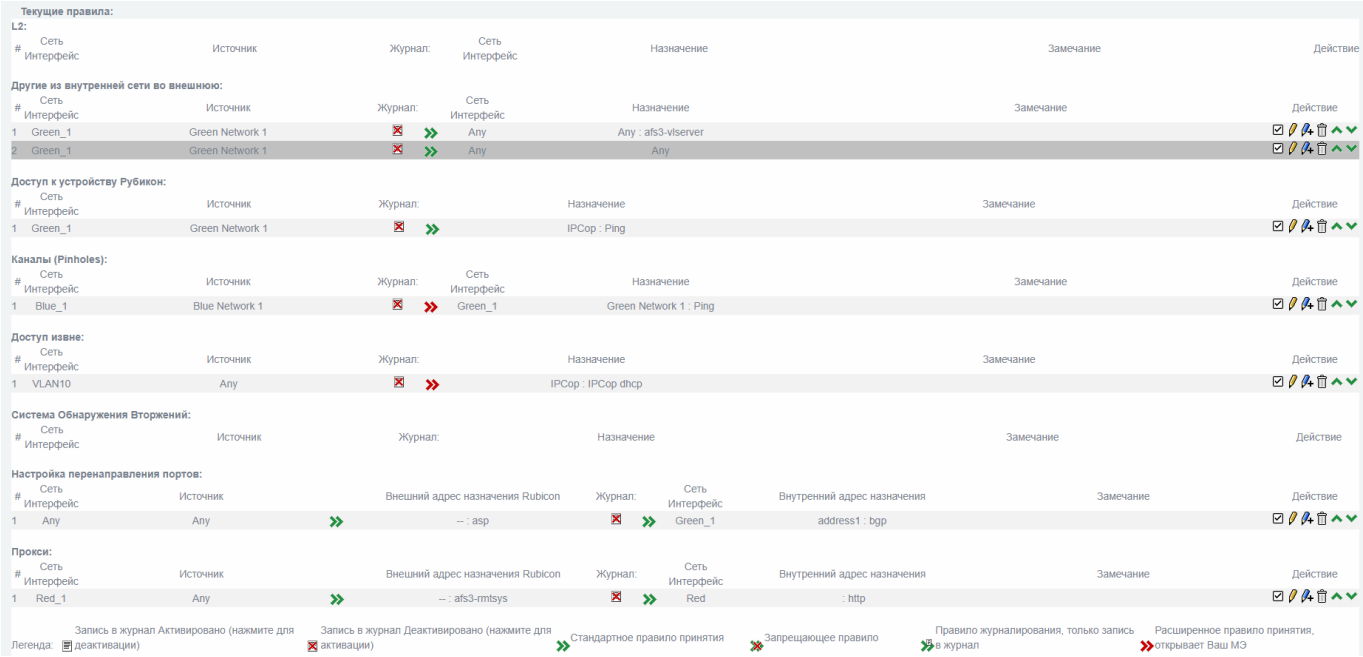

Рис. 172

В таблице 84 приведено описание элементов блока «Текущие правила».

Таблица 84 – Описание элементов блока «Текущие правила»

Элемент	Описание
Информационная таблица «L2»	Предназначена для отображения списка правил фильтрации МЭ на канальном уровне (L2)
Информационная таблица «Другие из внутренней сети во внешнюю»	Предназначена для отображения списка правил фильтрации сетевых пакетов, для которых адрес источника и адрес назначения маршрутизируются из одного физического сетевого интерфейса в другой
Информационная таблица «Доступ к устройству Рубикон»	Предназначена для отображения списка правил фильтрации сетевых пакетов, для которых адресом назначения является адрес (или псевдоним адреса) сетевого интерфейса МЭ
Информационная таблица «Каналы (Pinholes)»	Предназначена для отображения списка правил фильтрации пакетов от выделенных узлов «синей» или «оранжевой» сети к узлам «зеленой» сети
Информационная таблица «Доступ извне»	Предназначена для отображения списка правил организации административного доступа к МЭ из «красной» сети
Информационная таблица «Система Обнаружения Вторжений»	Предназначена для отображения списка правил фильтрации МЭ по перенаправлению сетевых пакетов в СОВ

Элемент	Описание
Информационная таблица «Настройка перенаправления портов»	Предназначена для отображения списка правил фильтрации сетевых пакетов, для которых физический адрес и порт назначения подставляется при получении МЭ пакета с определенными администратором параметрами назначения
Информационная таблица «Прокси»	Предназначена для отображения списка правил ассоциации трафика, поступающего на определенный порт, с одним из обрабатываемых типов (HTTP, FTP)

В конце блока «Текущие правила» представлена легенда (см. рис. 173), действующая для всех представленных информационных таблиц в блоке.

Легенда блока «Текущие правила»

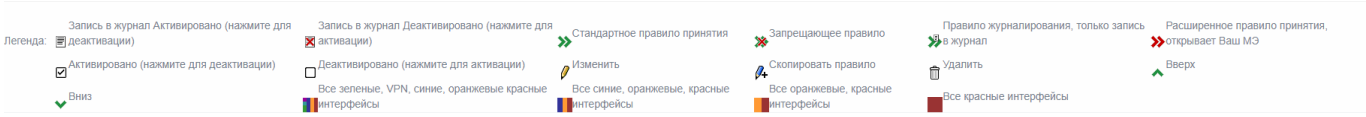

Рис. 173

4.7.10. Подраздел «Конфигурация DMZ»

Подраздел «Конфигурация DMZ» (см. рис. 174) предназначен для создания правил ДМЗ для МЭ.

Примечание. Создание правил ДМЗ при конфигурации **без** добавленных вручную маршрутов (включая маршруты по умолчанию).

Подраздел «Конфигурация DMZ»

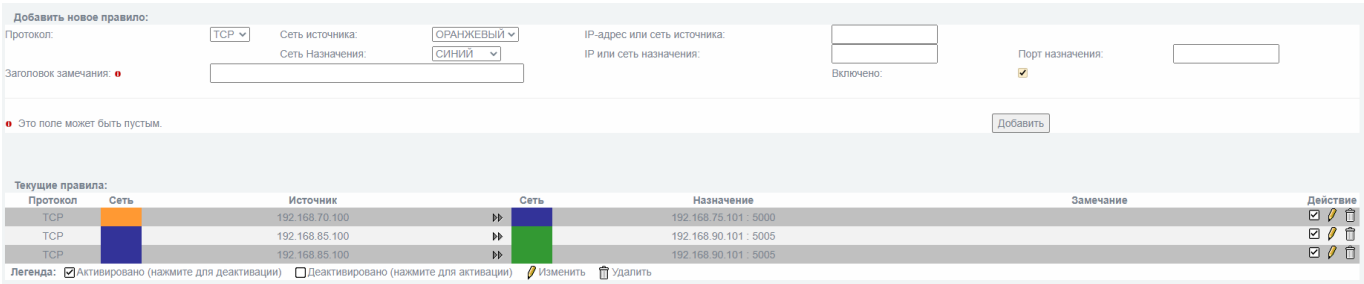

Рис. 174

В таблице 85 приведено описание элементов подраздела «Конфигурация DMZ».

Таблица 85 – Описание элементов подраздела «Конфигурация DMZ»

Элемент	Описание
Выпадающий список «Протокол»	Предназначен для выбора одного из представленных в списке протоколов, который будет использовать новое правило ДМЗ
Поле «Заголовок замечания»	Предназначено для ввода заголовка примечаний к новому правилу ДМЗ, который будет помещен в строку журналирования по данному правилу. Примечание. Данное поле не обязательно к заполнению
Выпадающий список «Сеть источника»	Предназначен для выбора из списка одного интерфейса сети источника пакета из ранее добавленных сетевых интерфейсов (доступны для выбора только «синие» и «оранжевые» сетевые интерфейсы)
Выпадающий список «Сеть Назначения»	Предназначен для выбора из списка одного интерфейса сети назначения пакета из ранее добавленных сетевых интерфейсов (доступны для выбора только «синие» и «зеленые» сетевые интерфейсы)
Поле «IP-адрес или сеть источника»	Предназначено для ввода IP-адреса или сети источника пакета
Поле «IP или сеть назначения»	Предназначено для ввода IP-адреса или сети назначения пакета
Чекбокс «Включено»	Предназначен для выбора включения/отключения нового правила ДМЗ
Поле «Порт назначения»	Предназначено для ввода порта назначения пакета
Кнопка «Добавить»	Предназначена для сохранения введенной информации и добавляет в изделие новое правило в список текущих правил ДМЗ
Информационная таблица «Текущие правила»	Предназначена для отображения и взаимодействия пользователя с добавленными ранее вручную правилами ДМЗ
Информационный знак «»	Предназначен для указания пользователю в строке таблицы направления сетевых пакетов в текущем правиле ДМЗ
Чекбокс «Действие»	Предназначен для выбора включения/отключения выбранного правила ДМЗ без его удаления из изделия
Кнопка «»	Кнопка «Изменить». Предназначена для редактирования выбранного правила ДМЗ и открывает страницу «Изменение текущего правила ДМЗ»
Кнопка «»	Кнопка «Удалить». Предназначена для удаления выбранного правила ДМЗ

Под информационной таблицей представлена легенда (см. рис. 175) всех возможных действий с текущими правилами ДМЗ в данном подразделе.

Легенда информационной таблицы «Текущие правила»

Рис. 175

4.7.10.1. Страница «Изменение текущего правила ДМЗ»

Страница «Изменение текущего правила ДМЗ» (см. рис. 176) позволяет редактировать настройки выбранного правила ДМЗ.

Страница «Изменение текущего правила ДМЗ»

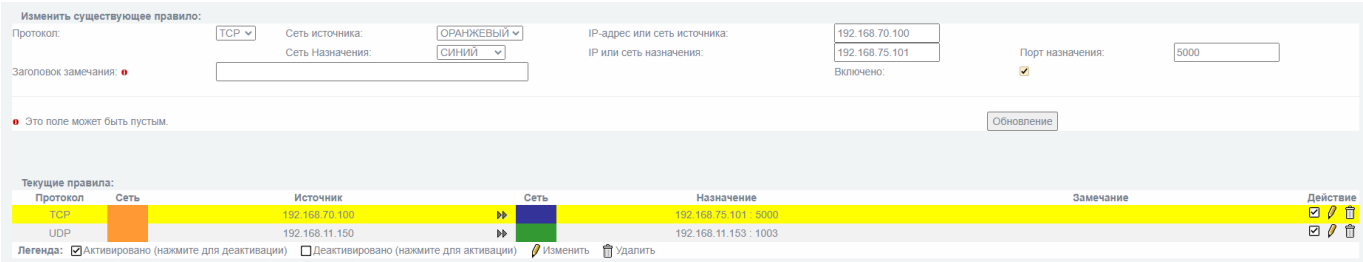

Рис. 176

В таблице 85 приведено описание элементов страницы «Изменение текущего правила ДМЗ».

Элементы данной страницы аналогичны представленным в подразделе «Конфигурация DMZ», что позволяет редактировать любой ранее сделанный выбор пользователя относительно настройки правил ДМЗ.

4.8. Раздел «VPN»

Раздел «VPN» содержит следующие подразделы:

1) «Настройка IPSec»;
2) «Настройка VPN»;
3) «GRE»;
4) «Выпуск сертификатов».

4.8.1. Подраздел «Настройка IPSec»

Подраздел «Настройка IPSec» (см. рис. 177) предназначен для организации сетевого туннеля и настройки взаимодействия по протоколу «IPSec».

Подраздел «Настройка IPSec»

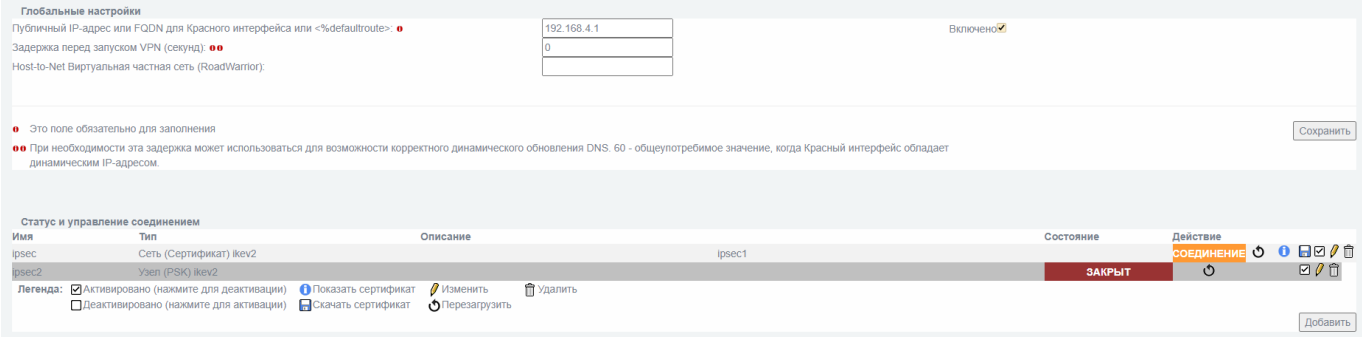

Рис. 177

Подраздел «Настройка IPSec» состоит из следующих блоков:

1) «Глобальные настройки»;

2) «Статус и управление соединением».

4.8.1.1. Блок «Глобальные настройки»

Блок «Глобальные настройки» (см. рис. 178) предназначен для настройки общих (для всех соединений) параметров службы создания туннеля «IPSec».

Блок «Глобальные настройки»

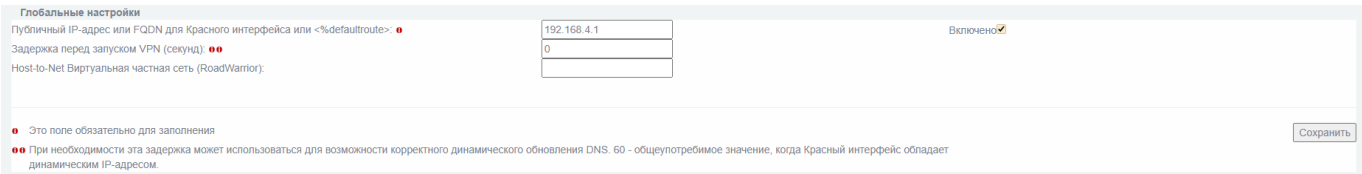

Рис. 178

В таблице 86 приведено описание элементов блока «Глобальные настройки».

Таблица 86 – Описание элементов блока «Глобальные настройки»

Элемент	Описание
Поле «Публичный IP-адрес или FQDN для Красного интерфейса или <%defaultroute>»[1]	Предназначено для ввода внешнего IP-адреса или FQDN сетевого интерфейса, использующегося для установления туннеля IPSec (параметр <%defaultroute> протокола «IPSec»). Данное поле применяется к интерфейсу, для которого определен маршрут по умолчанию
Поле «Задержка перед запуском VPN (секунд)»[2]	Предназначено для ввода времени задержки в секундах перед началом процесса организации туннеля при старте подсистемы захвата и разбора пакетов
Поле «Host-to-Net Виртуальная частная сеть (RoadWarrior)»	Предназначено для ввода IP-адреса сети. Данный адрес указывается при организации туннеля IPSec, при котором туннель создается между отдельным узлом и устройством, осуществляющим маршрутизацию между несколькими сетями
Чекбокс «Включено»	Предназначен для включения/выключения службы создания туннеля «IPSec»
Кнопка «Сохранить»	Предназначена для сохранения введенной информации и настроек
Примечания: 1. Данное поле обязательно к заполнению. 2. При необходимости эта задержка может использоваться для возможности корректного динамического обновления DNS. 60 – общеупотребимое значение, когда «красный» интерфейс обладает динамическим IP-адресом	

4.8.1.2. Блок «Статус и управление соединением»

Блок «Статус и управление соединением» (см. рис. 179) предназначен для отображения статуса и управления созданных вручную пользователем соединений, а также создания новых.

Блок «Статус и управление соединением»

Рис. 179

В таблице 87 приведено описание элементов блока «Статус и управление соединением».

Таблица 87 – Описание элементов блока «Статус и управление соединением»

Элемент	Описание
Информационная таблица «Статус и управление соединением»	Предназначена для отображения и взаимодействия пользователя с добавленными ранее вручную соединениями
Кнопка « »	Кнопка «Перезагрузить». Предназначена для перезагрузки выбранного соединения или сертификата
Кнопка « »	Кнопка «Показать сертификат». Предназначена для отображения информации о назначенном данному соединению сертификате. Информация будет представлена в открывшейся странице. Для возврата на предыдущую страницу необходимо нажать кнопку «Назад» (появится внизу страницы)
Кнопка « »	Кнопка «Скачать сертификат». Предназначена для скачивания сертификата на ЭВМ администратора
Чекбокс «Действие»	Предназначен для выбора включения/отключения соединения (в данной строке таблицы) без его удаления из изделия
Кнопка « »	Кнопка «Изменить». Предназначена для редактирования настроек выбранного соединения и открывает страницу «Изменение настроек соединения»
Кнопка « »	Предназначена для удаления выбранного соединения
Кнопка «Добавить»	Предназначена для настройки и добавления нового соединения. Открывает окно «Создание нового соединения»

Под информационной таблицей «Статус и управление соединением» представлена легенда (см. рис. 180) всех возможных действий с добавленными вручную пользователем соединениями в данном подразделе.

Легенда информационной таблицы «Статус и управление соединением»

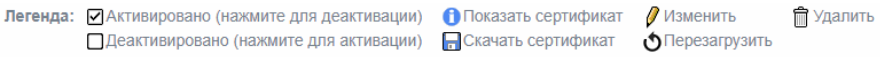

Рис. 180

4.8.1.2.1. Окно «Создание нового соединения»

Окно «Создание нового соединения» представляет собой совокупность страниц с настройками (см. рис. 181 и рис. 182) и предназначена для создания и настройки нового соединения.

Страница «Создание нового соединения № 1»

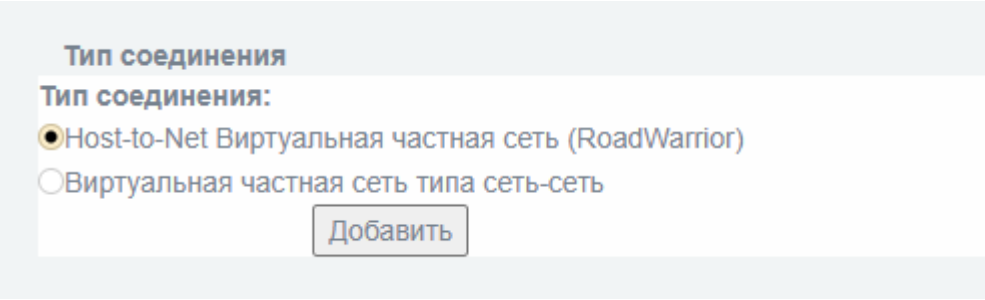

Рис. 181

Страница «Создание нового соединения № 1» (см. рис. 181) представляет собой список чекбоксов для выбора одного из типов создаваемого соединения.

Пользователю для выбора доступны следующие варианты:

1) «Host-to-Net Виртуальная частная сеть (RoadWarrior)»;

2) «Виртуальная частная сеть типа сеть-сеть».

После активации (выбора) необходимого чекбокса следует нажать кнопку «Добавить» для перехода к следующей странице создания нового соединения.

Страница «Создание нового соединения № 2» (см. рис. 182) предназначена для настройки создаваемого соединения.

Страница «Создание нового соединения № 2»

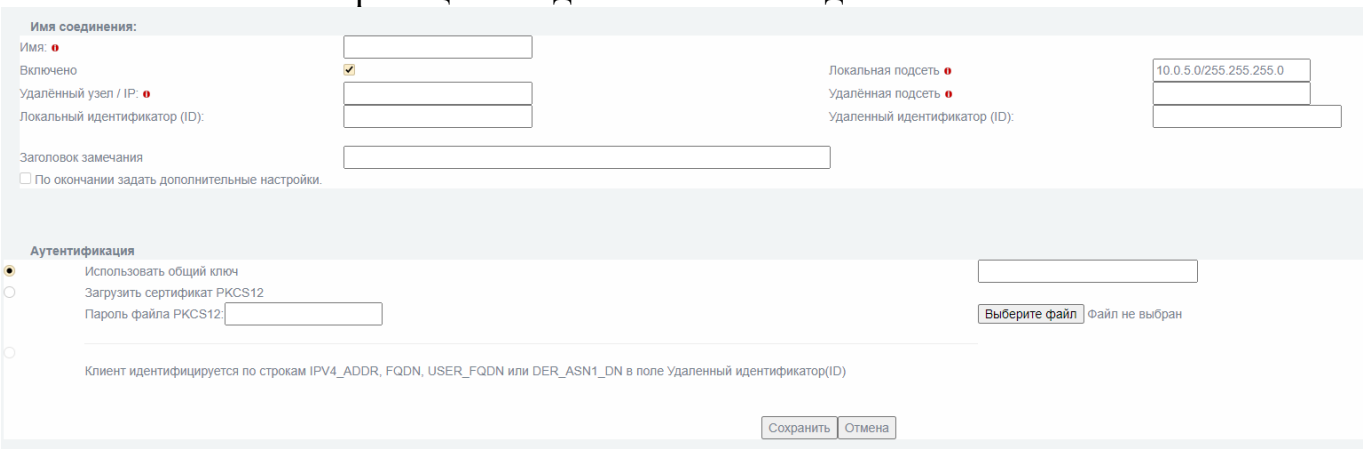

Рис. 182

В таблице 88 приведено описание элементов страницы «Создание нового соединения № 2».

Таблица 88 – Описание элементов страницы «Создание нового соединения № 2»

Элемент	Описание
Поле «Имя»[1, 2]	Предназначено для ввода имени создаваемого соединения (туннеля)
Чекбокс «Включено»	Предназначен для выбора включения/отключения нового соединения
Поле «Удаленный узел / IP»	Предназначено для ввода IP-адреса удаленного узла для его участия в организации туннеля «IPSec»
Поле «Локальный идентификатор (ID)»	Предназначено для ввода идентификатора локального узла
Поле «Заголовок замечания»	Предназначено для ввода примечаний к настраиваемому соединению
Чекбокс «По окончании задать дополнительные настройки»	Предназначен для выбора включения/отключения дополнительных настроек алгоритмов организации туннеля «IPSec» после заполнения основной информации о настройках туннеля, а также открывает страницу «Дополнительные настройки по окончании»
Поле «Локальная подсеть»[1, 2]	Предназначено для ввода IP-адреса локальной подсети, которая взаимодействует через туннель «IPSec»
Поле «Удалённая подсеть»[2]	Предназначено для ввода IP-адреса удаленной подсети, которая взаимодействует через туннель «IPSec». Примечание. Данное поле активно **только** в режиме «Виртуальная частная сеть типа сеть-сеть»
Поле «Удаленный идентификатор (ID)»	Предназначено для ввода идентификатора удаленного узла
Чекбокс «Использовать общий ключ»	Предназначен для включения/отключения возможности использования общего PSK-ключа
Поле «Использовать общий ключ»	Предназначено для ввода (установки) общего PSK-ключа для организации туннеля «IPSec»
Чекбокс «Загрузить сертификат PKCS12»	Предназначено для выбора включения/отключения функции организации туннеля с использованием аутентификации с помощью сертификата
Кнопка «Выберите файл»	Предназначена для выбора файла для загрузки сертификата PKCS12 в изделие
Поле «Пароль файла PKCS12»	Предназначено для ввода пароля для файла сертификата PKCS12
Чекбокс «Клиент идентифицируется по строкам IPV4_ADDR, FQDN, USER_FQDN или DER_ASN1_DN в поле «Удаленный идентификатор (ID)»	Предназначен для выбора включения/отключения аутентификации клиента по IP-адресу, доменному имени или полю «Remote ID» в сертификате. Примечание. Возможность активации данного чекбокса появляется **только** при наличии корневого сертификата, выпущенного в подразделе «VPN» → «Выпуск сертификатов»
Кнопка «Сохранить»	Предназначена для сохранения введенной информации и настроек

Элемент	Описание
Кнопка «Отмена»	Предназначена для возврата в подраздел «Настройка IPSec» без сохранения введенных данных на странице
Примечания: 1. Данное поле обязательно к заполнению в режиме «Host-to-Net Виртуальная частная сеть (RoadWarrior)». 2. Данное поле обязательно к заполнению в режиме «Виртуальная частная сеть типа сеть-сеть»	

4.8.1.2.2. Страница «Дополнительные настройки по окончании»

Страница «Дополнительные настройки по окончании» (см. рис. 183) предназначена для выбора настроек протоколов шифрования, ключевого обмена, а также действий при обнаружении неработающих узлов.

Данная страница настроек для соединения открывается автоматически при создании нового соединения и активации чекбокса «По окончании задать дополнительные настройки» или при изменении выбранного соединения после нажатия кнопки «Специальный».

Страница «Дополнительные настройки по окончании»

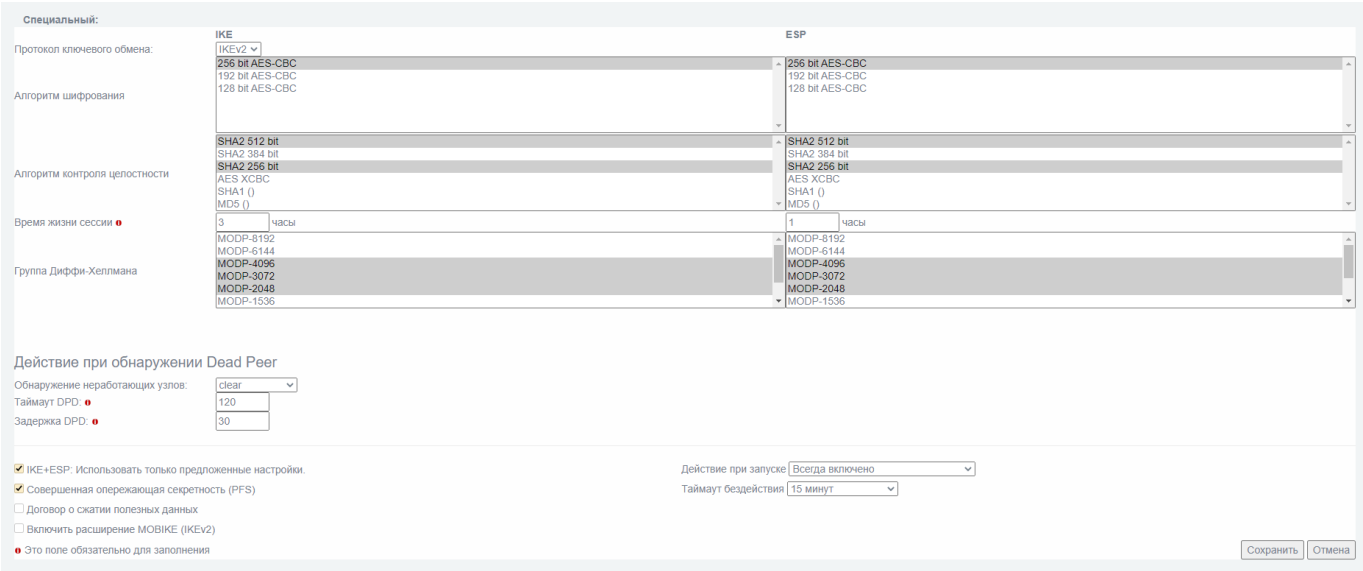

Рис. 183

На данной странице настройка протоколов «IKE» и «ESP» представлена отдельными столбцами, но с одинаковыми построчными параметрами.

При настройке необходимо выбирать параметры и для протокола «IKE» и для «ESP». Цветом в перечнях выделены «установленные» параметры (цвет может меняться в зависимости от используемого браузера). Также в данных перечнях доступен множественный выбор (см. рис. 184).

Перечни параметров для настройки протоколов «IKE» и «ESP»

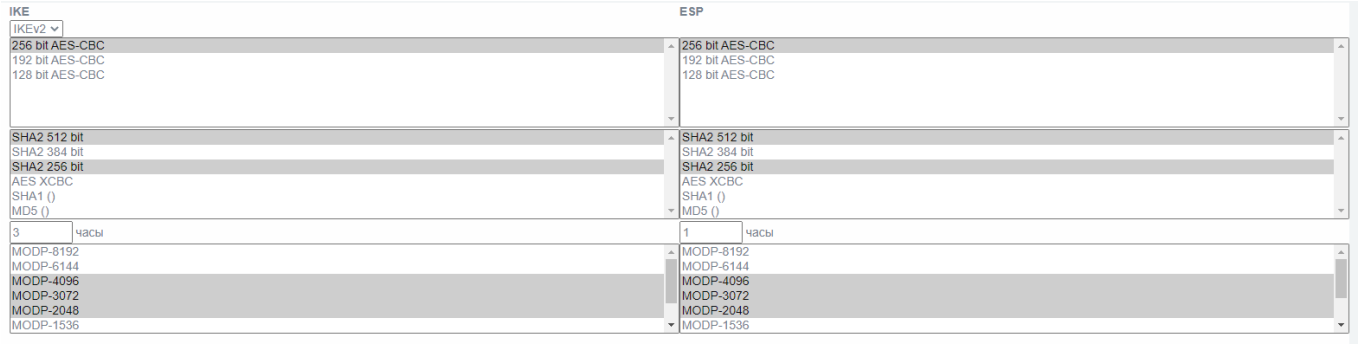

Рис. 184

Пример. Для множественного выбора из представленных перечней (пример актуален при использовании браузера «Яндекс») необходимо, удерживая левую кнопку «Ctrl» клавиатуры, выбрать нажатиями мышки необходимое из перечней.

В таблице 89 приведено описание элементов страницы «Дополнительные настройки по окончании».

Таблица 89 – Описание элементов страницы «Дополнительные настройки по окончании»

Элемент	Описание
Выпадающий список «Протокол ключевого обмена»[1]	Предназначен для выбора одного из следующих версий «IKE», разрешенных для VPN-туннеля: – «IKEv1»; – «IKEv2»
Перечень для выбора «Алгоритм шифрования»[1, 2]	Предназначен для выбора одного или нескольких алгоритмов шифрования из представленных в перечне
Перечень для выбора «Алгоритм контроля целостности»[1, 2]	Предназначен для выбора одного или нескольких алгоритмов контроля целостности

Элемент	Описание
Поле «Время жизни сессии»[1, 2 ,3]	Предназначено для ввода времени существования сессии (в часах)
Перечень для выбора «Группа Диффи-Хеллмана»[1, 2]	Предназначен для выбора одной или нескольких групп «Диффи-Хеллмана»
Выпадающий список «Обнаружение неработающих узлов»	Предназначен для выбора одного из представленных в списке варианта действий изделия при обнаружении неработающих узлов. Доступны для выбора следующие варианты: – «-отключено-»; – «clear» (остановка туннеля и очистка маршрутов); – «hold» (не предпринимаются никакие действия); – «restart» (перезапуск протокола ключевого обмена). По умолчанию: «clear»
Поле «Таймаут DPD»[3]	Предназначено для ввода времени ожидания (в секундах) ответа на запрос функции обнаружения неработающих узлов «Dead Peer Detection» (далее – DPD). По умолчанию: 120 секунд
Поле «Задержка DPD»	Предназначено для ввода периода времени (в секундах) между запросами функции «DPD». По умолчанию: 30 секунд
Чекбокс «IKE+ESP: использовать только предложенные настройки»	Предназначено для включения/отключения использования только предложенных настроек для протоколов «IKE» и «ESP»
Чекбокс «Совершенная опережающая секретность (PFS)»	Предназначен для выбора включения/отключения опции «Perfect forward secrecy» (далее – PFS) в протоколе «IPsec»
Чекбокс «Договор о сжатии полезных данных»	Предназначен для выбора включения/отключения функции сжатия полезных данных
Чекбокс «Включить расширение MOBIKE (IKEv2)»	Предназначен для выбора включения/отключения расширения протокола «IKEv2» для мобильных подключений «MOBIKE»
Выпадающий список «Действие при запуске»	Предназначен для выбора одного из следующих параметров: – «Установить соединение по запросу»; – «Всегда включено». По умолчанию: «Всегда включено»
Выпадающий список «Таймаут бездействия»	Предназначен для выбора одного из следующих параметров: – «-Без ограничений-»; – «5 минут»; – «10 минут»; – «15 минут»; – «30 минут»; – «1 час»; – «12 часов»; – «24 часа». По умолчанию: «15 минут»
Кнопка «Сохранить»	Предназначена для сохранения введенной информации и настроек

Элемент	Описание
Кнопка «Отмена»	Предназначена для возврата в подраздел «Настройка IPSec» без сохранения введенных данных на странице
Примечания: 1. Параметр для настройки протокола «IKE». 2. Параметр для настройки протокола «ESP». 3. Поля, обязательные к заполнению	

4.8.1.2.3. Страница «Изменение настроек соединения»

Страница «Изменение настроек соединения» (см. рис. 185) предназначена для редактирования настроек, созданных вручную пользователем соединений.

Страница «Изменение настроек соединения»

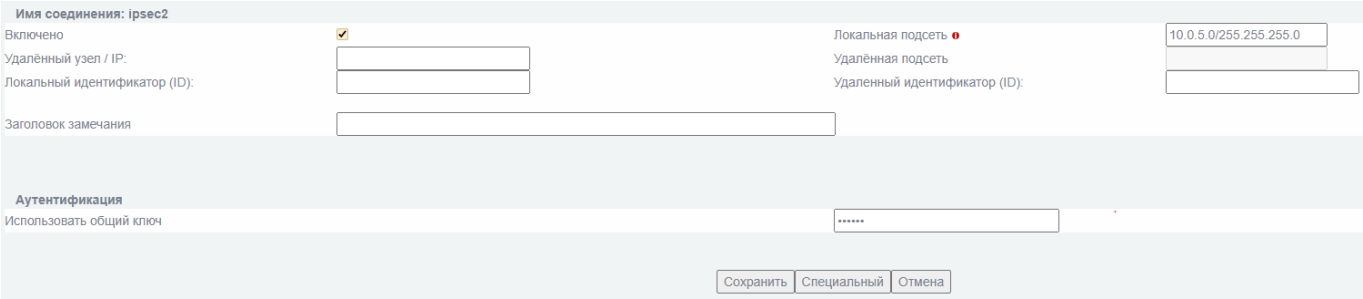

Рис. 185

В таблице 90 приведено описание элементов страницы «Изменение настроек соединения».

Таблица 90 – Описание элементов страницы «Изменение настроек соединения»

Элемент	Описание
Информационное поле «Имя соединения»	Предназначено для отображения информации о имени (обозначении) соединения, выбранного для изменения
Чекбокс «Включено»	Предназначен для выбора включения/отключения выбранного соединения
Поле «Удаленный узел/IP»	Предназначено для редактирования IP-адреса удаленного узла для его участия в организации туннеля «IPSec»
Поле «Локальный идентификатор (ID)»	Предназначено для редактирования идентификатора локального узла
Поле «Заголовок замечания»	Предназначено для ввода примечаний к настраиваемому соединению

Элемент	Описание
Поле «Локальная подсеть»	Предназначено для редактирования IP-адреса локальной подсети, которая взаимодействует через туннель «IPSec»
Поле «Удаленная подсеть»	Предназначено для редактирования IP-адреса удаленной подсети, которая взаимодействует через туннель «IPSec». Примечание. Данное поле активно **только** в режиме «Виртуальная частная сеть типа сеть-сеть»
Поле «Удаленный идентификатор (ID)»	Предназначено для редактирования идентификатора удаленного узла
Поле «Использовать общий ключ»	Предназначено для редактирования общего PSK-ключа для организации туннеля «IPSec»
Кнопка «Сохранить»	Предназначена для сохранения введенной информации и настроек
Кнопка «Специальный»	Предназначена для редактирования дополнительных настроек алгоритмов организации туннеля «IPSec», а также открывает страницу «Дополнительные настройки по окончании» (п. 4.8.1.2.2)
Кнопка «Отмена»	Предназначена для возврата в подраздел «Настройка IPSec» без сохранения введенных данных на странице

4.8.2. Подраздел «Настройка VPN»

Подраздел «Настройка VPN» (см. рис. 186) предназначен для создания и настройки экземпляров серверов и клиентов VPN.

Подраздел «Настройка VPN»

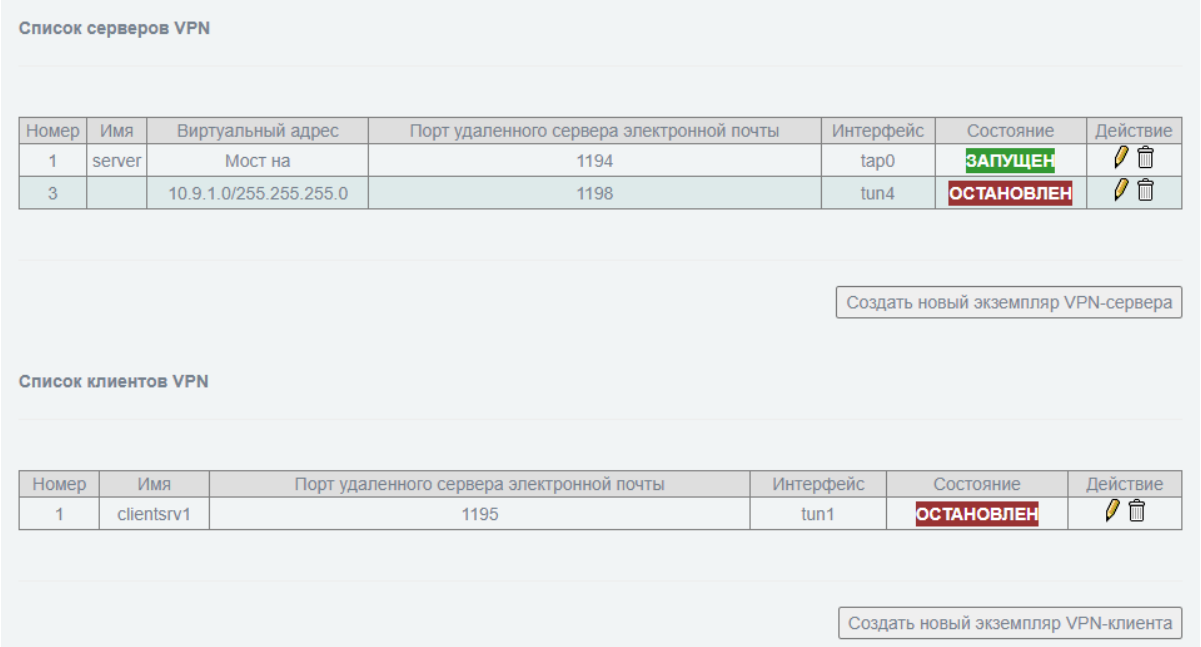

Рис. 186

Подраздел «Настройка VPN» состоит из следующих блоков и страниц:

1) блок «Список серверов VPN»;

2) страница «Настройка сервера VPN»;

3) страница «Добавление локальной подсети»;

4) страница «Добавление сети клиента»;

5) страница «Изменить выбранный экземпляр VPN-клиента»;

6) страница «Управление сертификатами»;

7) блок «Список клиентов VPN»;

8) страница «Настройка клиента VPN»;

9) страница «Изменить выбранный экземпляр VPN-клиента»;

10) страница «Удаленный узел».

4.8.2.1. Блок «Список серверов VPN»

Блок «Список серверов VPN» (см. рис. 187) предназначен для отображения, создания и редактирования созданных пользователем VPN-серверов.

Блок «Список серверов VPN»

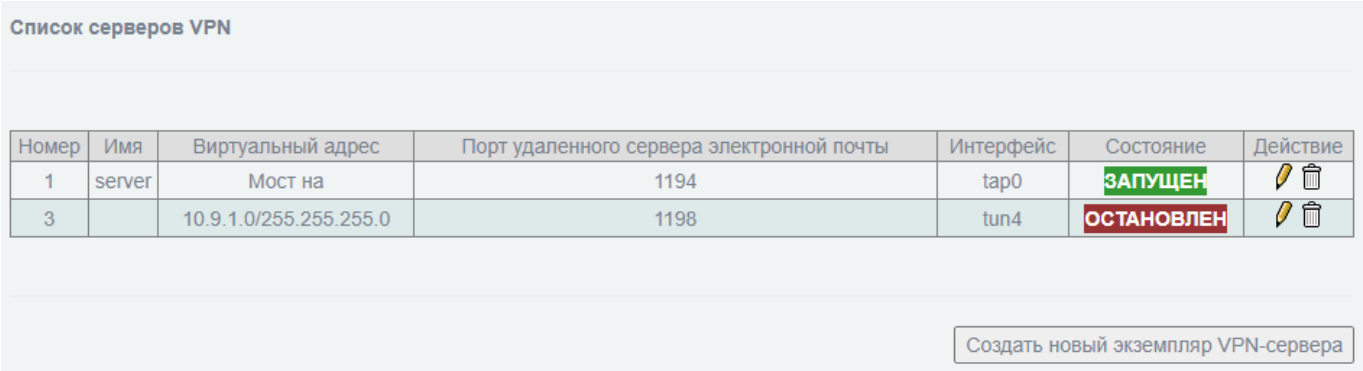

Рис. 187

В таблице 91 приведено описание элементов блока «Список серверов VPN».

Таблица 91 – Описание элементов блока «Список серверов VPN»

Элемент	Описание
Информационная таблица «Список серверов VPN»	Предназначена для отображения добавленных ранее вручную VPN-серверов и взаимодействия с ними пользователя
Кнопка « »	Кнопка «Изменить». Предназначена для редактирования добавленного ранее вручную VPN-сервера и открывает страницу «Изменить выбранный экземпляр VPN-сервера»
Кнопка « »	Кнопка «Удалить». Предназначена для удаления добавленного ранее вручную VPN-сервера из информационной таблицы «Список серверов VPN»
Кнопка «Создать новый экземпляр VPN-сервера»	Предназначена для создания нового VPN-сервера с заданными пользователем параметрами и открывает страницу «Настройка сервера VPN»

4.8.2.2. Страница «Настройка сервера VPN»

Страница «Настройка сервера VPN» (см. рис. 188) предназначена для создания нового VPN-сервера с заданными пользователем параметрами.

Страница «Настройка сервера VPN»

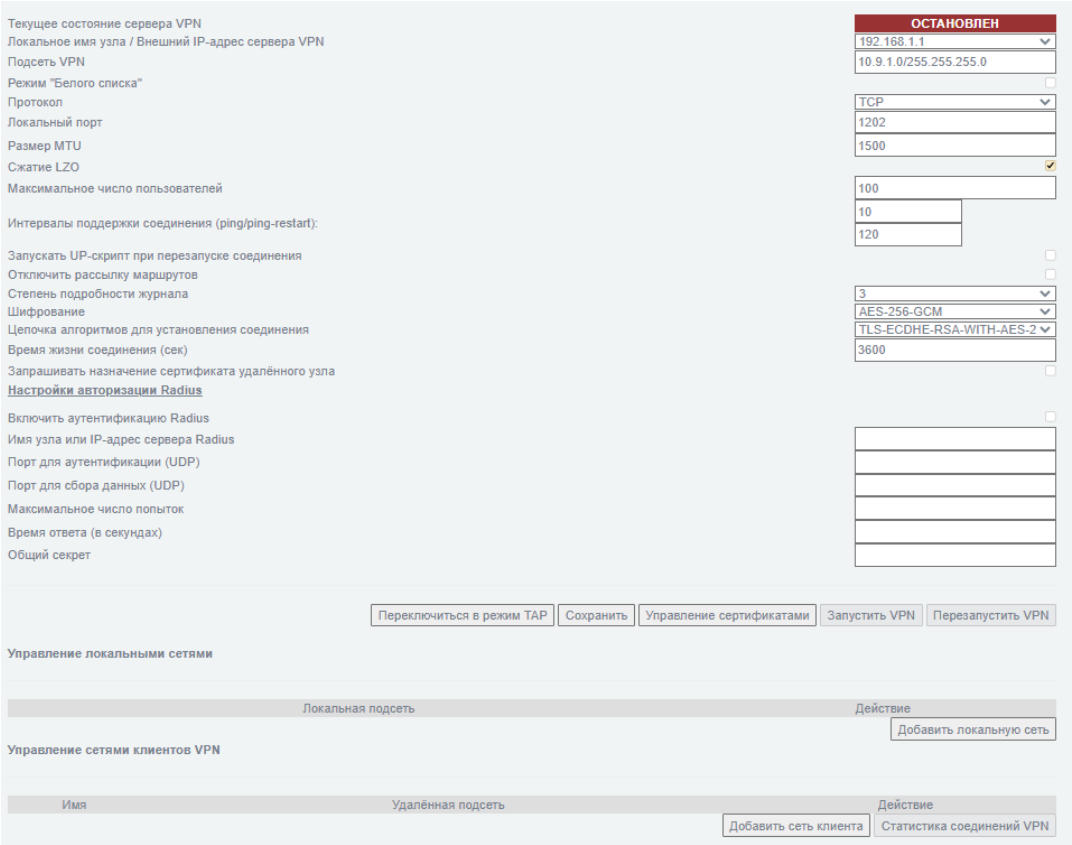

Рис. 188

Настроить VPN-сервер возможно в следующих режимах:

1) «TAP» – обеспечивает сетевую коммутацию на уровне L2;

2) «TUN» – обеспечивает сетевую коммутацию на уровне L3.

В таблице 92 приведено описание элементов страницы «Настройка сервера VPN».

Описание элементов данной страницы представлено с учетом активированного расширенного режима работы изделия.

Примечание. Включение расширенного режима предусмотрено в разделе «Межсетевой экран», посредством выбора чекбокса «Расширенный режим» в поле «Настройки» подраздела «Настройки межсетевого экрана».

Таблица 92 – Описание элементов страницы «Настройка сервера VPN»

Элемент	Описание
Информационное поле «Текущее состояние сервера VPN»[1, 2]	Предназначено для отображения состояния (статуса) сервера VPN. Доступны для отображения статусы: – «ОСТАНОВЛЕН»; – «ЗАПУЩЕН»
Выпадающий список «Локальное имя узла / Внешний IP-адрес сервера VPN»[1, 2]	Предназначен для выбора из представленных в списке внешних IP-адресов или всех имен сетевых интерфейсов сервера VPN
Поля «Адрес/маска (необязательно)»[2]	Предназначены для ввода следующих данных: – верхнее поле – внешний IP-адрес «моста»; – нижнее поле – внешняя маска «моста»
Поля «Диапазон IP-адресов для VPN-клиентов (от..до, необязательно)»[2]	Предназначены для ввода диапазона IP-адресов для VPN-клиентов (в верхнем поле начало диапазона, в нижнем – окончание)
Поле «Подсеть VPN»[1]	Предназначено для ввода подсети, которая будет использоваться в туннеле VPN
Чекбокс «Режим «Белого списка»[1]	Предназначен для включения режима «Белого списка», когда к соединению через туннель VPN допускаются только клиенты из разрешенных сетей (присутствующих в списке «Управление сетями клиентов VPN»)
Выпадающий список «Протокол»[1, 2]	Предназначен для выбора протокола, используемого для VPN-сервера. Доступны для выбора следующие параметры: – «TCP»; – «UDP»
Поле «Локальный порт»[1, 2]	Предназначено для ввода информации о локальном порте, на который приходят запросы на установление VPN-соединения

Элемент	Описание
Поле «Размер MTU»[1, 2]	Предназначено для ввода максимального размера пакета для настраиваемого сервера VPN
Чекбокс «Сжатие LZO»[1, 2]	Предназначен для выбора включения/отключения использования алгоритма сжатия данных без потерь при передаче информации
Поле «Максимальное число пользователей»[1, 2]	Предназначено для ввода максимального числа пользователей сервера VPN
Поля «Интервалы поддержки соединения (ping/ping-restart)»[1, 2]	Предназначены для ввода интервалов поддержки соединения (в секундах) в следующем формате: – верхнее поле – время, через которое отправляется ping-запрос; – нижнее поле – временной интервал между выполнениями команды «ping» сервера VPN в режиме ожидания его возможного перезапуска при обнаружении отсутствия откликов на ping-запрос
Чекбокс «Запускать UP-скрипт при перезапуске соединения»[1, 2]	Предназначен для выбора включения/выключения запуска внутреннего скрипта обработки ситуации перезапуска соединения
Чекбокс «Отключить рассылку маршрутов»[1, 2]	Предназначен для выбора включения/выключения необходимости рассылки маршрутов сетей, настроенных в сервисе VPN
Выпадающий список «Степень подробности журнала»[1, 2]	Предназначен для выбора одной из представленных степеней подробности записи событий в журнал. Доступны варианты выбора: от 0 до 11, где 0 – минимальная степень записи, а 11 – максимальная
Выпадающий список «Шифрование»[1, 2]	Предназначен для выбора алгоритма шифрования, применяемого для передачи данных в соединении, формируемым сервером VPN
Выпадающий список «Цепочка алгоритмов для установления соединения»[1, 2]	Предназначен для выбора одной из представленных в списке цепочки (блока) алгоритмов, применяемых при установлении соединения VPN
Поле «Время жизни соединения (сек)»[1, 2]	Предназначено для установки пользователем промежутка времени до автоматического разрыва установленного соединения в случае отсутствия активного обмена информацией
Чекбокс «Запрашивать назначение сертификата удалённого узла»[1, 2]	Предназначен для выбора включения/отключения функции запроса назначения сертификата удаленного узла (необходимо для проверки информации в поле назначения сертификата)
Чекбокс «Включить аутентификацию Radius»[1, 2]	Предназначен для выбора включения/отключения проверки подлинности с помощью протокола для авторизации, аутентификации и учёта «Radius» в случае наличия в сети сервера Radius
Поле «Имя узла или IP-адрес сервера Radius»[1, 2]	Предназначено для ввода имени узла или IP-адреса сервера Radius для подключения к нему
Поле «Порт для аутентификации (UDP)»[1, 2]	Предназначено для ввода порта для аутентификации (UDP) сервера Radius для подключения к нему
Поле «Порт для сбора данных (UDP)»[1, 2]	Предназначено для ввода порта для сбора данных (UDP) сервера Radius для подключения к нему
Поле «Максимальное число попыток»[1, 2]	Предназначено для ввода максимального числа попыток подключения к серверу Radius в рамках запроса на подключение
Поле «Время ответа (в секундах)»[1, 2]	Предназначено для ввода максимального времени ответа от сервера при подключении к серверу Radius в рамках запроса на подключение
Поле «Общий секрет»[1, 2]	Предназначено для ввода случайной строки, которая распределяется между клиентом и сервером защищенным образом

Элемент	Описание
Кнопка «Переключиться в режим TAP / TUN»	Предназначена для переключения пользователем сервера из режима «TAP» в режим «TUN» и наоборот
Кнопка «Сохранить»	Предназначена для сохранения введенных настроек сервера VPN
Кнопка «Управление сертификатами»	Предназначена для открытия и настройки страницы «Управление сертификатами»
Кнопка «Запустить VPN»	Предназначена для перезапуска сервера VPN с указанными пользователем настройками. Примечание. Данная кнопка доступна **только** после загрузки сертификата на странице «Управление сертификатами»
Кнопка «Перезапустить VPN»	Предназначена для запуска сервера VPN с указанными пользователем настройками. Примечание. Данная кнопка доступна **только** после загрузки сертификата на странице «Управление сертификатами»
Информационная таблица «Управление локальными сетями»	Предназначена для отражения информации и возможности взаимодействия с локальными сетями, к которым открыт доступ через соединение VPN со стороны клиентов VPN
Кнопка «Добавить локальную подсеть»	Предназначена для добавления новой локальной подсети пользователем и открытия страницы «Добавление локальной подсети»
Информационная таблица «Управление сетями клиентов VPN»	Предназначена для отражения информации и возможности взаимодействия с сетями клиентов VPN, к которым открыт доступ через соединение VPN
Чекбокс «Действие»	Предназначен для выбора включения/отключения определенной сети
Кнопка « »	Кнопка «Изменить». Предназначена для изменения выбранной сети
Кнопка « »	Кнопка «Удалить». Предназначена для удаления выбранной сети
Кнопка «Добавить сеть клиента»[1]	Предназначена для добавления новой сети клиента пользователем и открытия страницы «Добавление сети клиента»
Кнопка «Статистика соединений VPN»	Предназначена для открытия страницы «Статистика соединений VPN» и просмотра представленной там одноименной информационной таблицы со статистикой VPN-соединений. Для возврата на страницу «Настройка сервера VPN» необходимо нажать кнопку « ». Примечание. Данная кнопка доступна **только** тогда, когда были загружены сертификаты на странице «Управление сертификатами» и данный сервер VPN был запущен.
Примечания: 1. Элемент страницы доступен для работы VPN-сервера режиме «TUN». 2. Элемент страницы доступен для работы VPN-сервера режиме «TAP»	

4.8.2.3. Страница «Добавление локальной подсети»

Страница «Добавление локальной подсети» (см. рис. 189) предназначена для добавления новой локальной подсети пользователем.

Для добавления локальной подсети следует ввести IP-адрес/маску подсети и нажать кнопку «Добавить локальную сеть».

Кнопка «Отмена» предназначена для возврата пользователя на страницу «Настройка сервера VPN» без сохранения введенных данных.

Страница «Добавление локальной подсети»

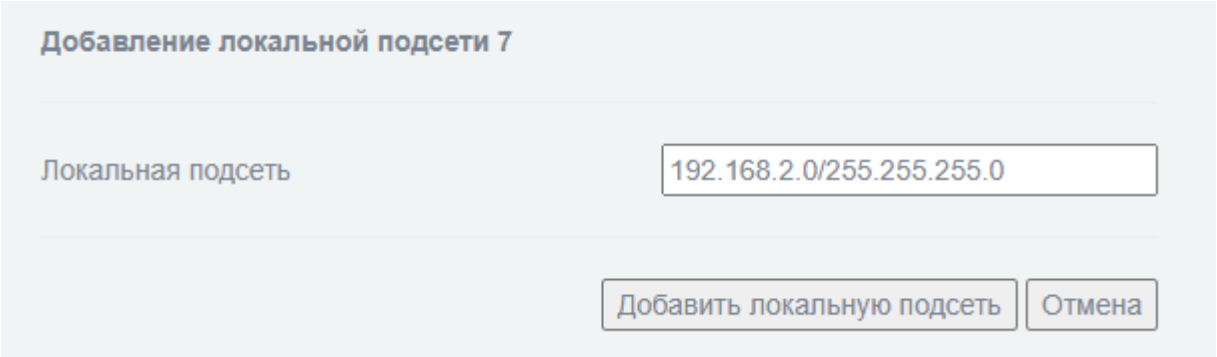

Рис. 189

4.8.2.4. Страница «Добавление сети клиента»

Страница «Добавление сети клиента» (см. рис. 190) предназначена для добавления новой сети клиента пользователем.

Для добавления новой сети клиента следует ввести имя клиента (имя клиента **должно совпадать** с именем, указанным в сертификате), IP-адрес/маску клиентской подсети и нажать кнопку «Добавить сеть клиента».

Страница «Добавление сети клиента»

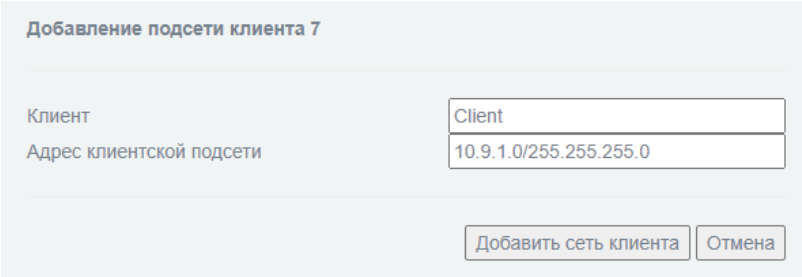

Рис. 190

4.8.2.5. Страница «Изменить выбранный экземпляр VPN-сервера»

Страница «Изменить выбранный экземпляр VPN-сервера» предназначена для редактирования добавленных ранее пользователем вручную настроек VPN-серверов и аналогична странице, описанной подробно в п. 4.8.2.2 настоящего документа.

4.8.2.6. Страница «Управление сертификатами»

Страница «Управление сертификатами» (см. рис. 191) предназначена для предоставления пользователю возможности загрузить новый сертификат удостоверяющего центра, сгенерировать запрос на сертификат или загрузить новый список отозванных сертификатов.

Данная страница позволяет активировать необходимый пользователю чекбокс и нажать кнопку «Далее» для перехода к дальнейшей работе с сертификатами.

Кнопка «Отмена» предназначена для возврата пользователя на страницу «Настройка сервера VPN» без сохранения введенных данных.

Страница «Управление сертификатами»

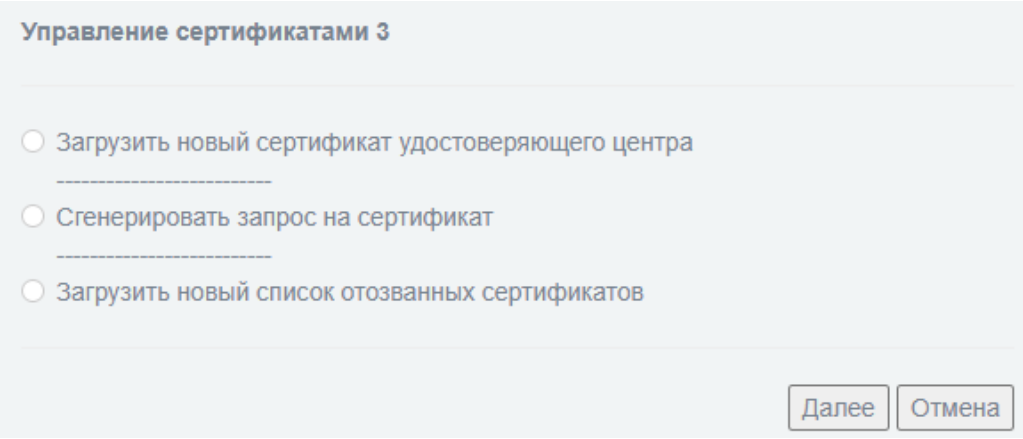

Рис. 191

4.8.2.6.1. Страница «Загрузить новый сертификат удостоверяющего центра»

Чекбокс «Загрузить новый сертификат удостоверяющего центра» предназначен для открытия страницы «Загрузка нового сертификата удостоверяющего центра» (см. рис. 192).

Страница «Загрузка нового сертификата удостоверяющего центра»

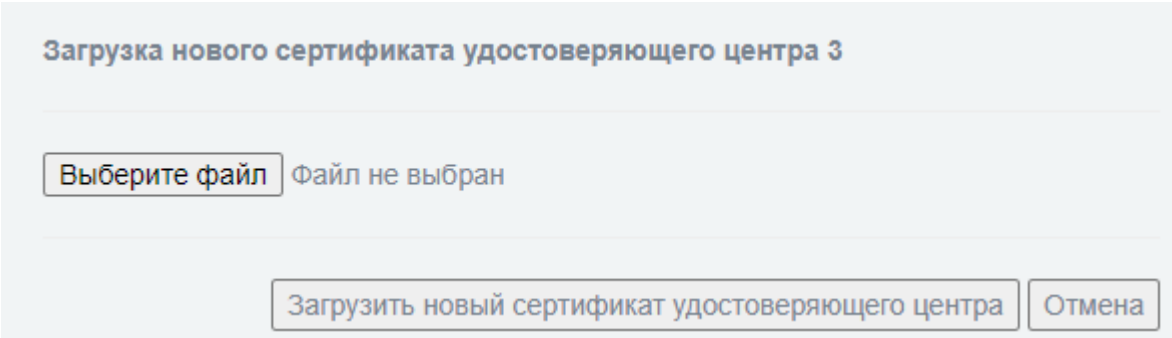

Рис. 192

На данной странице необходимо выбрать на ЭВМ администратора файл сертификата (предварительно полученный в удостоверяющем центре) используя кнопку «Выберите файл».

Выбранный сертификат следует загрузить в изделие нажав кнопку «Загрузить новый сертификат удостоверяющего центра».

Для отмены загрузки нового сертификата и возврата на страницу «Настройка сервера VPN» необходимо нажать кнопку «Отмена».

4.8.2.6.2. Страница «Сгенерировать запрос на сертификат»

Чекбокс «Сгенерировать запрос на сертификат» предназначен для открытия страницы «Сгенерировать запрос на сертификат» (см. рис. 193).

Данная страница позволяет сформировать запрос на выдачу сертификата удостоверяющим центром путем заполнения пользователем формы для дальнейшей отправки в удостоверяющий центр.

Страница «Сгенерировать запрос на сертификат»

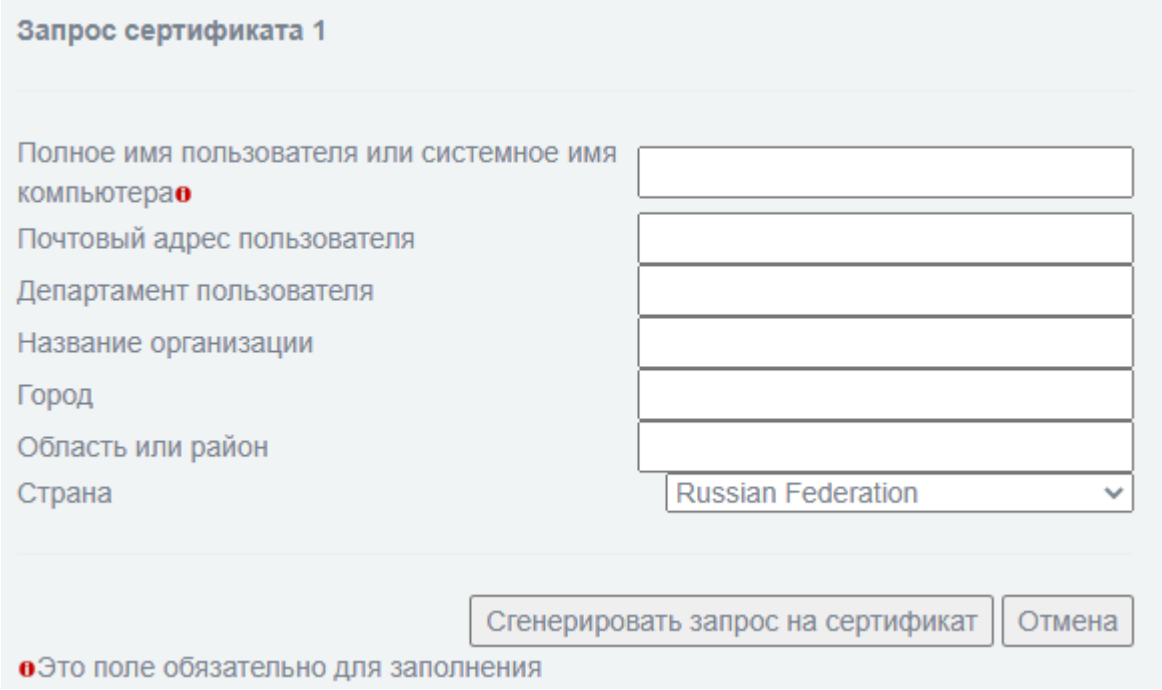

Рис. 193

В таблице 93 приведено описание элементов формы для заполнения пользователем.

Таблица 93 – Описание элементов формы для заполнения пользователем

Элемент	Описание
Поле «Полное имя пользователя или системное имя компьютера»	Предназначено для ввода полного имени пользователя или системного имени ЭВМ. Примечание. Данное поле обязательно к заполнению
Поле «Почтовый адрес пользователя»	Предназначено для ввода почтового адреса пользователя
Поле «Департамент пользователя»	Предназначено для ввода отдела пользователя в организации
Поле «Название организации»	Предназначено для ввода названия организации пользователя
Поле «Город»	Предназначено для ввода города пользователя
Поле «Область или район»	Предназначено для области или района пользователя
Выпадающий список «Страна»	Предназначен для выбора одной из представленной в списке страны пользователя
Примечание – Указанные поля таблицы должны соответствовать атрибутам в уникальном имени (DN) сертификата	

После заполнения формы запроса на сертификат далее необходимо нажать кнопку «Сгенерировать запрос на сертификат».

Нажатие на кнопку «Сгенерировать запрос на сертификат» открывает страницу «Обработка запроса на сертификат» (см. рис. 194), в которой можно скачать экземпляр запроса на сертификат, выбрать файл сертификата на ЭВМ и загрузить его в изделие.

Страница «Обработка запроса на сертификат»

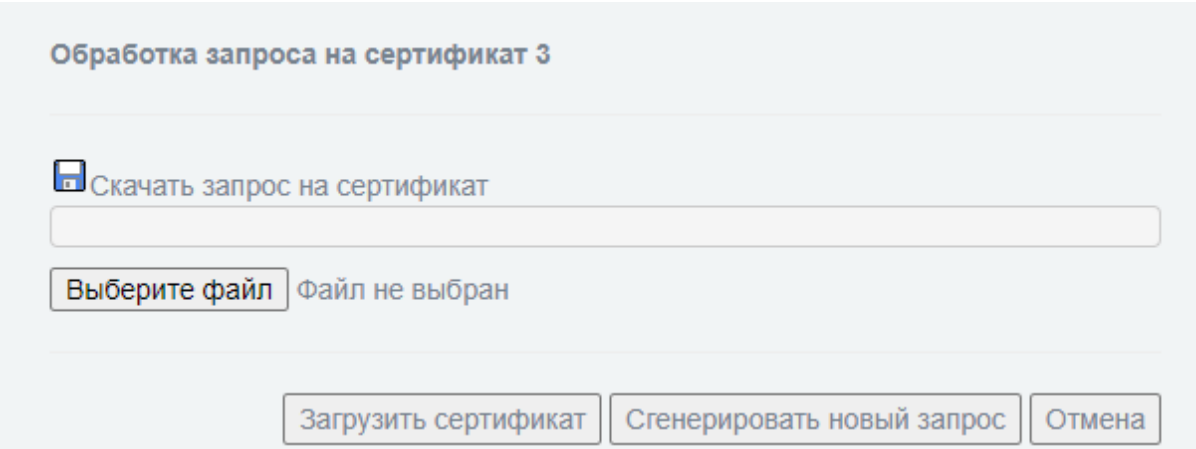

Рис. 194

Кнопка «Сгенерировать новый запрос» предназначена для возврата пользователя к странице «Сгенерировать запрос на сертификат».

Кнопка «Отмена» предназначена для возврата пользователя к странице «Настройка сервера VPN».

После генерации первого запроса на сертификат – страница «Управление сертификатами» изменится на представленную на рисунке 195 (пока сгенерированный запрос не будет обработан).

Измененная страница «Управление сертификатами»

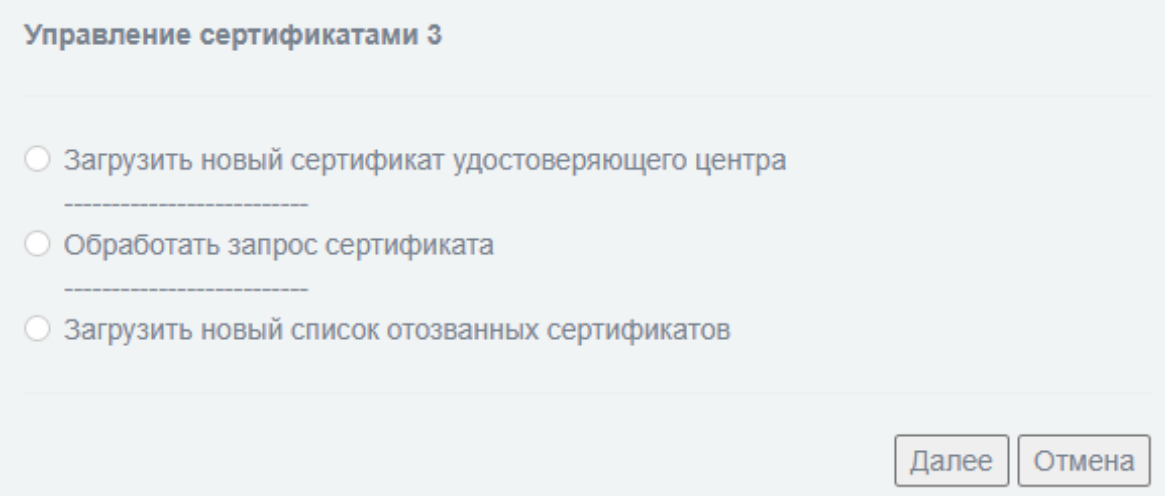

Рис. 195

4.8.2.6.3. Страница «Загрузить новый список отозванных сертификатов»

Чекбокс «Загрузить новый список отозванных сертификатов» предназначен для открытия страницы «Загрузить новый список отозванных сертификатов» (см. рис. 196).

Данная страница позволяет пользователю выбрать файл нового списка отозванных сертификатов и загрузить его в изделие.

Страница «Загрузить новый список отозванных сертификатов»

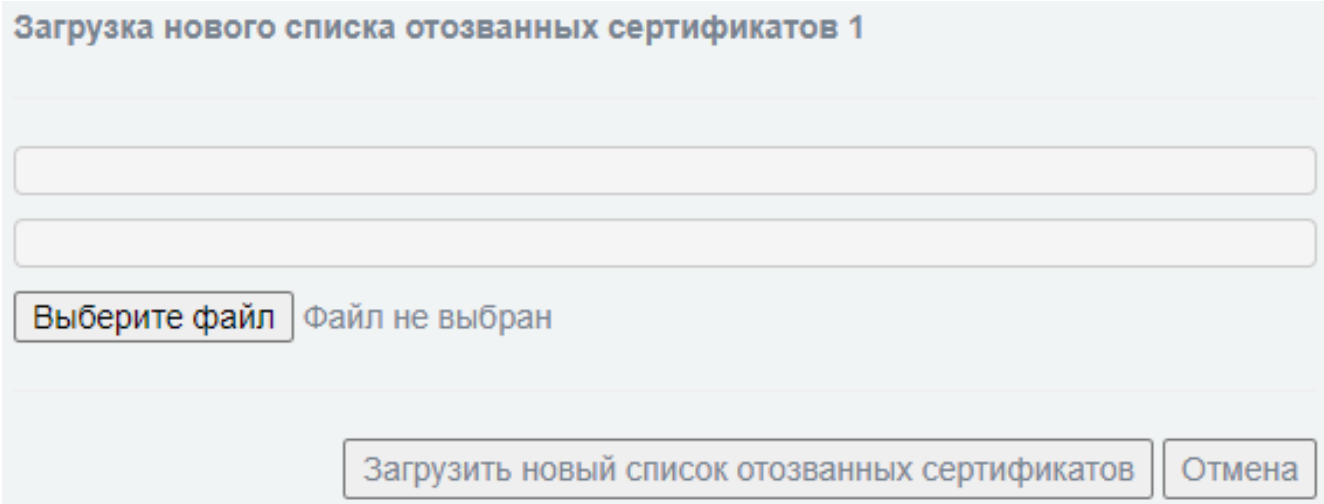

Рис. 196

На данной странице необходимо выбрать на ЭВМ файл нового списка отозванных сертификатов используя кнопку «Выберите файл».

Выбранный файл следует загрузить в изделие нажав кнопку «Загрузить новый список отозванных сертификатов».

Для отмены загрузки нового списка отозванных сертификатов и возврата на страницу «Настройка сервера VPN» необходимо нажать кнопку «Отмена».

4.8.2.7. Блок «Список клиентов VPN»

Блок «Список клиентов VPN» (см. рис. 197) предназначен для отображения, создания и редактирования созданных пользователем VPN-клиентов.

Блок «Список клиентов VPN»

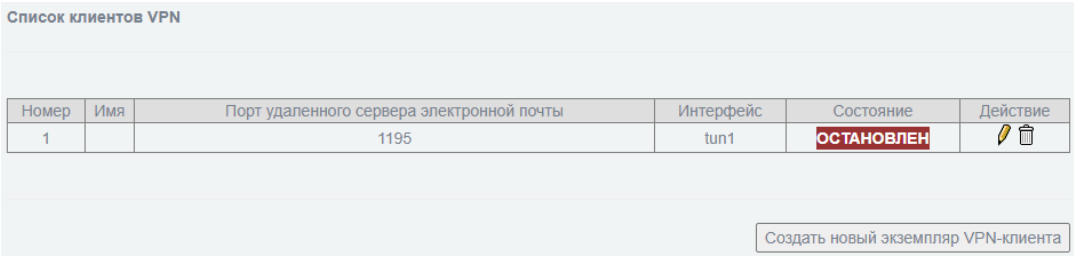

Рис. 197

В таблице 94 приведено описание элементов блока «Список клиентов VPN».

Таблица 94 – Описание элементов блока «Список клиентов VPN»

Элемент	Описание
Информационная таблица «Список клиентов VPN»	Предназначена для отображения добавленных ранее вручную VPN-клиентов и взаимодействия с ними пользователя
Кнопка « »	Кнопка «Изменить». Предназначена для редактирования добавленных ранее вручную VPN-клиентов и открывает страницу «Изменить выбранный экземпляр VPN-клиента»
Кнопка « »	Кнопка «Удалить». Предназначена для удаления добавленных ранее вручную VPN-клиентов из информационной таблицы «Список клиентов VPN»
Кнопка «Создать новый экземпляр VPN-клиента»	Предназначена для создания нового VPN-клиента с заданными пользователем параметрами и открывает страницу «Настройка клиента VPN»

4.8.2.8. Страница «Настройка клиента VPN»

Страница «Настройка клиента VPN» (см. рис. 198) предназначена для создания нового клиента VPN с заданными пользователем параметрами.

Страница «Настройка клиента VPN»

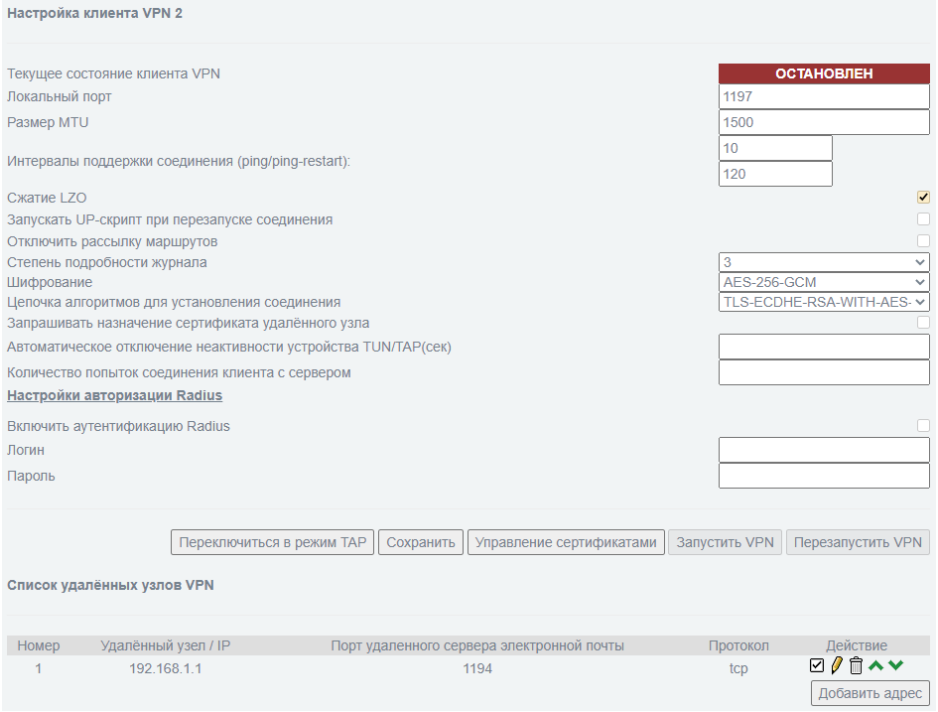

Рис. 198

Настроить клиента VPN возможно в следующих режимах:

3) «TAP» – обеспечивает сетевую коммутацию на уровне L2;

4) «TUN» – обеспечивает сетевую коммутацию на уровне L3.

В таблице 95 приведено описание элементов страницы «Настройка клиента VPN».

Описание элементов данной страницы представлено с учетом активированного расширенного режима работы изделия.

Примечание. Включение расширенного режима предусмотрено в разделе «Межсетевой экран», посредством выбора чекбокса «Расширенный режим» в поле «Настройки» подраздела «Настройки межсетевого экрана».

Таблица 95 – Описание элементов страницы «Настройка клиента VPN»

Элемент	Описание
Информационное поле «Текущее состояние клиента VPN»[1, 2]	Предназначено для отображения состояния (статуса) клиента VPN. Доступны для отображения статусы: – «ОСТАНОВЛЕН»; – «ЗАПУЩЕН»; – «СОЕДИНЕНИЕ»
Поля «Адрес/маска (необязательно)»[2]	Предназначены для ввода следующих данных: – верхнее поле – внешний IP-адрес «моста»; – нижнее поле – внешняя маска «моста»
Поле «Локальный порт»[1, 2]	Предназначено для ввода информации о локальном порте, на который приходят запросы на установление VPN-соединения
Поле «Размер MTU»[1, 2]	Предназначено для ввода максимального размера пакета для настраиваемого клиента VPN
Поля «Интервалы поддержки соединения (ping/ping-restart)»[1, 2]	Предназначены для ввода интервалов поддержки соединения (в секундах) в следующем формате: – верхнее поле – время, через которое отправляется ping-запрос; – нижнее поле – временной интервал между выполнениями команды «ping» сервера VPN в режиме ожидания его возможного перезапуска при обнаружении отсутствия откликов на ping-запрос
Чекбокс «Сжатие LZO»[1, 2]	Предназначен для выбора включения/отключения использования алгоритма сжатия данных без потерь при передаче информации
Чекбокс «Запускать UP-скрипт при перезапуске соединения»[1, 2]	Предназначен для выбора включения/выключения запуска внутреннего скрипта обработки ситуации перезапуска соединения
Чекбокс «Отключить рассылку маршрутов»[1, 2]	Предназначен для выбора включения/выключения необходимости рассылки маршрутов сетей, настроенных в сервисе VPN

Элемент	Описание
Выпадающий список «Степень подробности журнала»[1, 2]	Предназначен для выбора одной из представленных степеней подробности записи событий в журнал. Доступны варианты выбора: от 0 до 11, где 0 – минимальная степень записи, а 11 – максимальная
Выпадающий список «Шифрование»[1, 2]	Предназначен для выбора алгоритма шифрования, применяемого для передачи данных в создаваемом клиенте VPN
Выпадающий список «Цепочка алгоритмов для установления соединения»[1, 2]	Предназначен для выбора одной из представленных в списке цепочки (блока) алгоритмов, применяемых при установлении соединения VPN
Чекбокс «Запрашивать назначение сертификата удалённого узла»[1, 2]	Предназначен для выбора включения/отключения функции запроса назначения сертификата удаленного узла (необходимо для проверки информации в поле назначения сертификата)
Поле «Автоматическое отключение неактивности устройства TUN/TAP (сек)»	Предназначено для ввода временного диапазона, при котором клиент отсоединится от сервера, когда канал между сервером и клиентом установлен, но по нему ничего не передается
Поле «Количество попыток соединения клиента с сервером»	Предназначено для ввода количества попыток, после которых клиент перестанет соединяться с сервером
Чекбокс «Включить аутентификацию Radius»[1, 2]	Предназначен для выбора включения/отключения проверки подлинности с помощью протокола для авторизации, аутентификации и учёта «Radius» в случае наличия в сети сервера Radius
Поле «Логин»	Предназначено для ввода имени учетной записи пользователя
Поле «Пароль»	Предназначено для ввода пароля учетной записи пользователя
Кнопка «Переключиться в режим TAP / TUN»	Предназначена для переключения пользователем клиента из режима «TAP» в режим «TUN» и наоборот
Кнопка «Сохранить»	Предназначена для сохранения введенных настроек клиента VPN
Кнопка «Управление сертификатами»	Предназначена для открытия и настройки страницы «Управление сертификатами»
Кнопка «Запустить VPN»	Предназначена для перезапуска клиента VPN с указанными пользователем настройками. Примечание. Данная кнопка доступна **только** после загрузки сертификата на странице «Управление сертификатами»
Кнопка «Перезапустить VPN»	Предназначена для запуска клиента VPN с указанными пользователем настройками. Примечание. Данная кнопка доступна **только** после загрузки сертификата на странице «Управление сертификатами»
Информационная таблица «Список удаленных узлов VPN»	Предназначена для отражения информации и возможности взаимодействия со списком удаленных узлов VPN
Чекбокс «Действие»	Предназначен для выбора включения/отключения определенного удаленного узла VPN
Кнопка «  »	Кнопка «Повышение приоритета». Предназначена для поднятия выбранного узла в списке и соответственно повышения приоритета подключения выбранного удаленного узла

Элемент	Описание
Кнопка « »	Кнопка «Понижение приоритета». Предназначена для снижения выбранного узла в списке и соответственно понижения приоритета подключения выбранного удаленного узла
Кнопка « »	Кнопка «Изменить». Предназначена для изменения выбранного удаленного узла VPN
Кнопка « »	Кнопка «Удалить». Предназначена для удаления выбранного удаленного узла VPN
Кнопка «Добавить адрес»	Предназначена для добавления нового удаленного узла VPN пользователем и открытия страницы «Удаленный узел»
Примечания: 1. Элемент страницы доступен для работы VPN-сервера режиме «TUN». 2. Элемент страницы доступен для работы VPN-сервера режиме «TAP»	

Страница «Управление сертификатами» предназначена для предоставления пользователю возможности загрузить новый сертификат удостоверяющего центра, сгенерировать запрос на сертификат или загрузить новый список отозванных сертификатов и аналогична странице, описанной подробно в п. 4.8.2.6 настоящего документа.

4.8.2.9. Страница «Изменить выбранный экземпляр VPN-клиента»

Страница «Изменить выбранный экземпляр VPN-клиента» предназначена для редактирования добавленных ранее пользователем вручную настроек VPN-клиентов и аналогична странице, описанной подробно в п. 4.8.2.8 настоящего документа.

4.8.2.10. Страница «Удаленный узел»

Страница «Удаленный узел» (см. рис. 199) предназначена для добавления нового удаленного узла VPN.

Для добавления нового удаленного узла VPN следует ввести удаленный адрес/IP узла, порт удаленного сервера электронной почты, сетевой протокол удаленного узла и нажать кнопку «Сохранить параметры удаленного узла».

Страница «Удаленный узел»

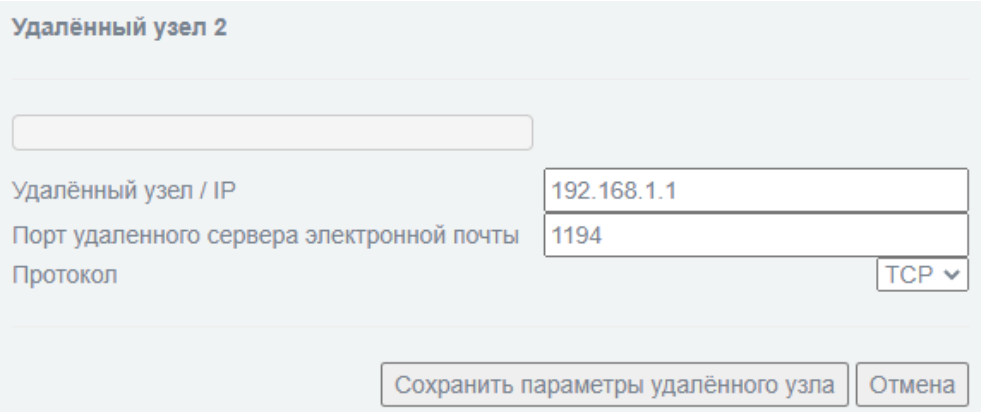

Рис. 199

4.8.3. Подраздел «GRE»

Подраздел «GRE» (см. рис. 200) предназначен для создания GRE-туннелей.

Подраздел «GRE»

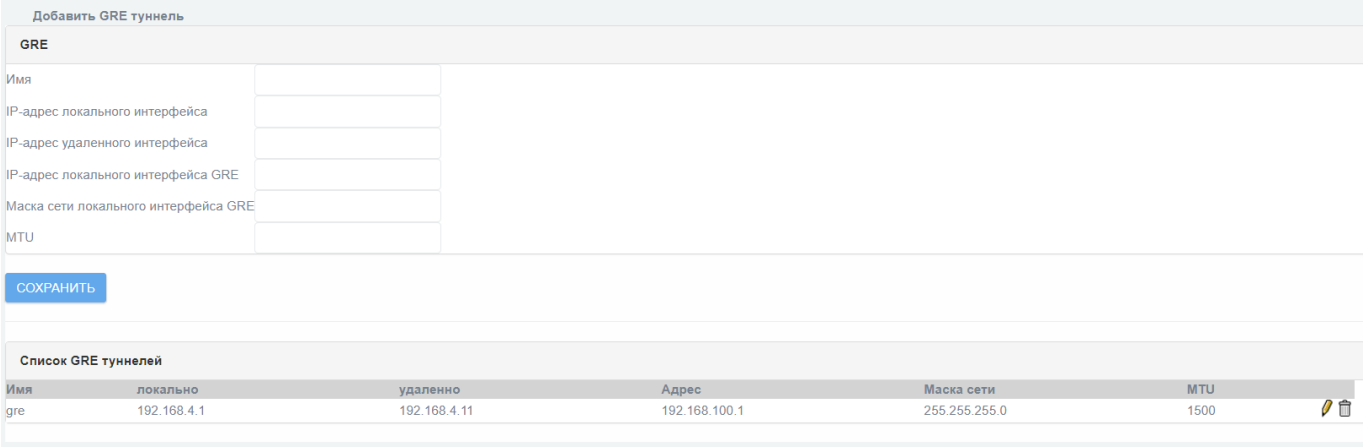

Рис. 200

В таблице 96 приведено описание элементов подраздела «GRE».

Таблица 96 – Описание элементов подраздела «GRE»

Элемент	Описание
Поле «Имя»	Предназначено для ввода имени нового GRE-туннеля
Поле «IP-адрес локального интерфейса»	Предназначено для ввода локального IP-адреса устройства, от которого будет устанавливаться GRE-туннель
Поле «IP-адрес удаленного интерфейса»	Предназначено для ввода IP-адреса удаленного устройства, с которым будет устанавливаться GRE-туннель
Поле «IP-адрес локального интерфейса GRE»	Предназначено для ввода виртуального локального IP-адреса GRE-туннеля
Поле «Маска сети локального интерфейса GRE»	Предназначено для ввода IP-маски для локального адреса GRE-туннеля
Поле «MTU»	Предназначено для ввода максимального размера пакета для GRE-туннеля
Кнопка «Сохранить»	Предназначена для сохранения введенной информации и настроек
Информационная таблица «Список GRE туннелей»	Предназначена для отражения информации и возможности взаимодействия со списком GRE-туннелей
Кнопка « »	Кнопка «Изменить». Предназначена для изменения выбранного GRE-туннеля и открывает страницу «Изменить выбранный GRE-туннель»
Кнопка « »	Кнопка «Удалить». Предназначена для удаления выбранного GRE-туннеля

4.8.3.1. Страница «Изменить выбранный GRE-туннель»

Страница «Изменить выбранный GRE-туннель» предназначена для редактирования настроек одного из добавленных ранее пользователем вручную GRE-туннелей.

Поля, доступные к изменению аналогичны представленным на странице Подраздел «GRE» и описаны подробно в п. 4.8.3 настоящего документа.

Для применения внесенных изменений в настройки выбранного GRE-туннеля необходимо нажать кнопку «Сохранить».

4.8.4. Подраздел «Выпуск сертификатов»

Подраздел «Выпуск сертификатов» (см. рис. 201) предназначен для предназначен для управления сертификатами.

Подраздел «Выпуск сертификатов»

Рис. 201

Подраздел «Выпуск сертификатов» состоит из следующих блоков:

1) «Удостоверяющий центр»;

2) «Запросы на выдачу сертификата»;

3) «Выданные сертификаты».

4.8.4.1. Блок «Удостоверяющий центр»

Блок «Удостоверяющий центр» (см. рис. 202) предназначен для операций с корневым сертификатом удостоверяющего центра (далее – УЦ). Содержит информацию о сертификате и кнопки для управления УЦ.

Блок «Удостоверяющий центр»

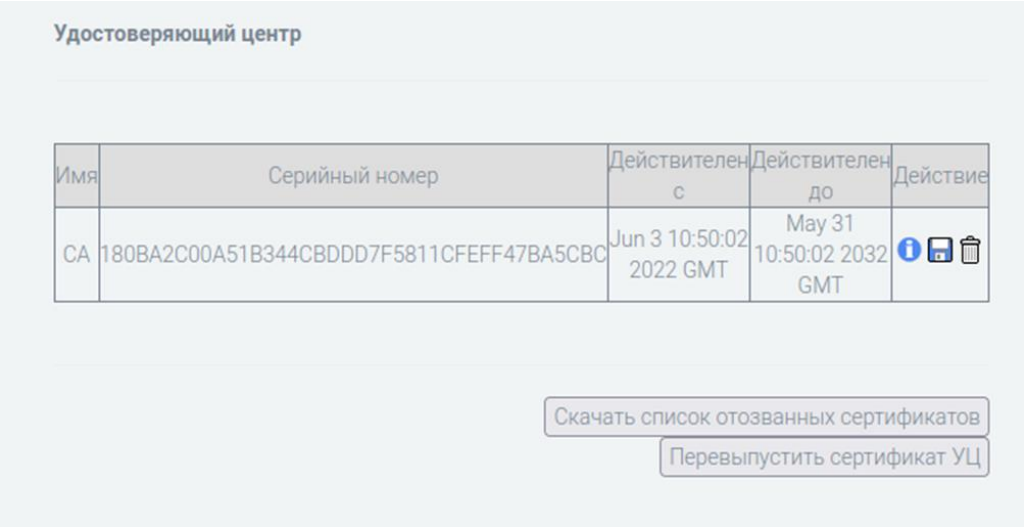

Рис. 202

Информация о сертификате представляет собой таблицу, в которой указаны данные об основных полях сертификата УЦ, и действия, которые могут быть выполнены с этим сертификатом.

Информация в информационной таблице «Удостоверяющий центр» представлена со следующими параметрами:

1) «Имя»;

2) «Серийный номер»;

3) «Действителен с»;

4) «Действителен до»;

5) «Действие».

В столбце «Действие» информационной таблицы «Удостоверяющий центр» в соответствующих отдельному сертификату строках содержатся следующие кнопки взаимодействия с выбранным сертификатом:

1) кнопка «» – кнопка «Информация» предназначена для отображения полной информации о корневом сертификате;

2) кнопка «» – кнопка «Скачать» предназначена для сохранения корневого сертификата на ЭВМ администратора;

3) кнопка «🗑» – кнопка «Удалить» предназначена для удаления корневого сертификата.

В данном блоке так же присутствуют кнопки «Скачать список отозванных сертификатов» и «Сгенерировать новый сертификат».

Кнопка «Скачать список отозванных сертификатов» становится доступна для нажатия после добавления хотя-бы одного сертификата и предназначена для скачивания CRL-списка удаленных ранее (отозванных) сертификатов в формате «.pem».

Кнопка «Сгенерировать новый сертификат» предназначена для открытия страницы «Сертификат Удостоверяющего Центра» для выпуска нового самоподписанного сертификата удостоверяющего центра.

4.8.4.1.1. Страница «Сертификат Удостоверяющего Центра»

Страница «Сертификат Удостоверяющего Центра» (см. рис. 203) предназначена для выпуска нового сертификата удостоверяющего центра.

Страница «Сертификат Удостоверяющего Центра»

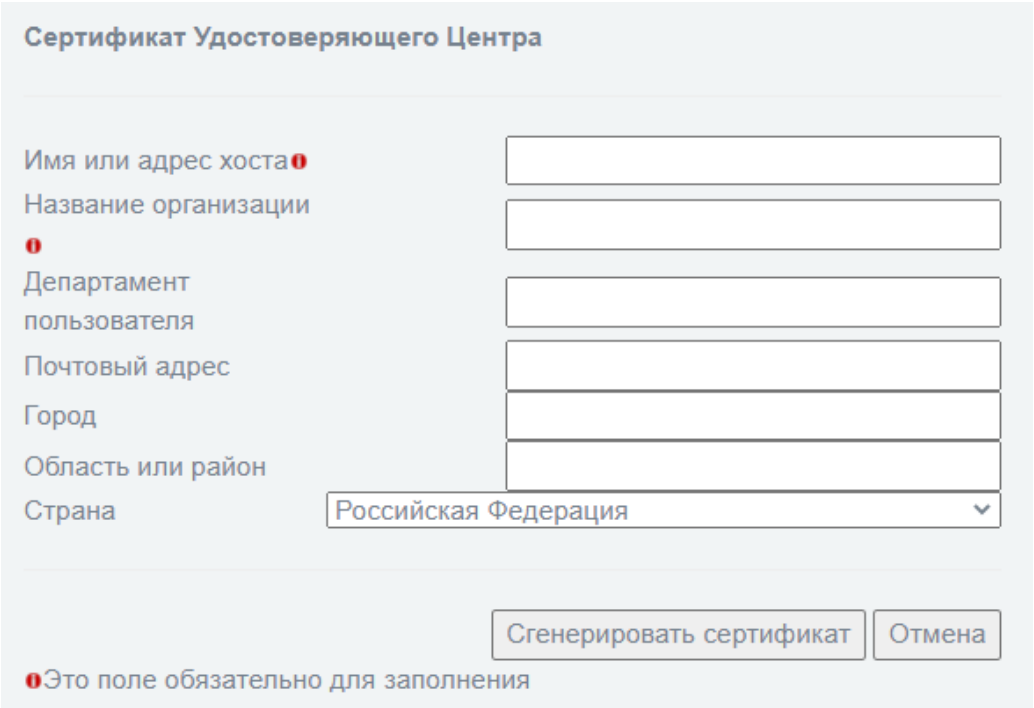

Рис. 203

В таблице 97 приведено описание элементов страницы «Сертификат Удостоверяющего Центра».

Таблица 97 – Описание элементов страницы «Сертификат Удостоверяющего Центра»

Элемент	Описание
Поле «Имя или адрес хоста»*	Предназначено для ввода имени или адреса сетевого узла. Соответствует атрибуту «CN» в уникальном имени (DN) сертификата
Поле «Название организации»*	Предназначено для ввода названия организации. Соответствует атрибуту «O» в уникальном имени (DN) сертификата
Поле «Департамент пользователя»	Предназначено для ввода названия департамента пользователя организации. Соответствует атрибуту «OU» в уникальном имени (DN) сертификата
Поле «Почтовый адрес»	Предназначено для ввода почтового адреса пользователя организации. Соответствует атрибуту «emailAddress» в уникальном имени (DN) сертификата
Поле «Город»	Предназначено для ввода города размещения пользователя. Соответствует атрибуту «L» в уникальном имени (DN) сертификата
Поле «Область или район»	Предназначено для ввода области или района размещения пользователя. Соответствует атрибуту «S» в уникальном имени (DN) сертификата
Выпадающий список «Страна»	Предназначен для выбора одной из представленной в списке страны размещения пользователя. Соответствует атрибуту «C» в уникальном имени (DN) сертификата
Кнопка «Сгенерировать сертификат»	Предназначена для формирования корневого сертификата УЦ по заданным пользователем данным
Кнопка «Отмена»	Предназначена для возврата в подраздел «Выпуск сертификатов» без выдачи сертификата и сохранения введенных данных на странице
* – Данное поле обязательно к заполнению. Информация в данных полях должна быть уникальна для сертификатов удостоверяющего центра	

После выпуска нового сертификата удостоверяющего центра в информационной таблице «Удостоверяющий центр» появится информация о сертификате: имя сертификата, серийный номер, дата выпуска, дата истечения срока и действия, которые возможны для работы с сертификатом (см. рис. 202).

4.8.4.2. Блок «Запросы на выдачу сертификата»

Блок «Запросы на выдачу сертификата» (см. рис. 204) предназначен для обработки запросов на выдачу сертификатов и представлен в виде одноименной информационной таблицы.

Для обработки запроса необходимо файл запроса поместить в информационную таблицу «Запросы на выдачу сертификата» с помощью кнопок «Выберите файл» и «Загрузить запрос сертификата» (см. рис. 205).

Блок «Запросы на выдачу сертификата»

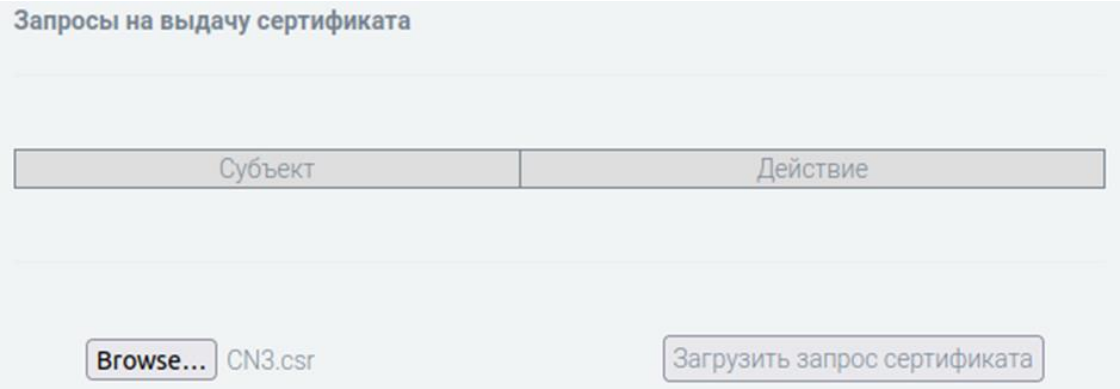

Рис. 204

Заполненная информационная таблица «Запросы на выдачу сертификата»

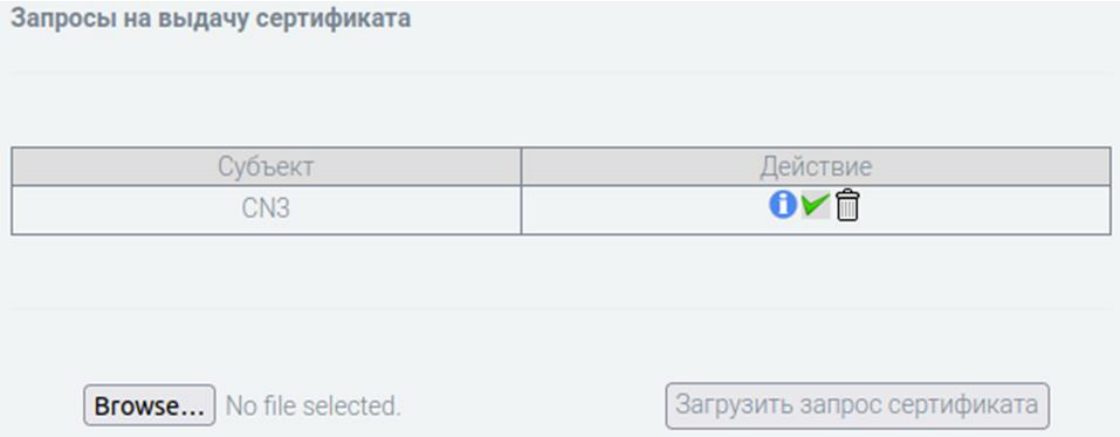

Рис. 205

В таблице 98 приведено описание элементов блока «Запросы на выдачу сертификата».

Таблица 98 – Описание элементов блока «Запросы на выдачу сертификата»

Элемент	Описание
Кнопка «Выберите файл»	Предназначена для выбора файла запроса на выдачу сертификата
Кнопка «Загрузить запрос сертификата»	Предназначена для помещения запроса на выдачу сертификата в информационную таблицу «Запросы на выдачу сертификата» для последующей его подписи
	Кнопка «Информация». Предназначена для отображения информации о запросе на выдачу сертификата
	Кнопка «Запрос на получение сертификата». Предназначена для формирования сертификата, подписанного удостоверяющим центром. Примечание. При нажатии на данную кнопку запрос на получение сертификата проверяется, и на его основе удостоверяющим центром производится выпуск сертификата клиента с параметрами, указанными в запросе. Информация о сертификате помещается в информационную таблицу «Выданные сертификаты»
	Предназначена для удаления запроса на выдачу сертификата

4.8.4.3. Блок «Выданные сертификаты»

Блок «Выданные сертификаты» (см. рис. 206) предназначен для отображения информации в виде одноименной информационной таблицы о выданных сертификатах и выполнения операций с сертификатами, выданными удостоверяющим центром на основании запросов на получение сертификатов.

Информационная таблица содержит следующую информацию: имя сертификата, серийный номер, даты начала и окончания действия, а также возможные операции (действия) с конкретным выданным сертификатом. Кнопки просмотра данных о выданном сертификате, сохранения сертификата на ЭВМ администратора, удаления сертификата содержатся в столбце действий таблицы.

Блок «Выданные сертификаты»

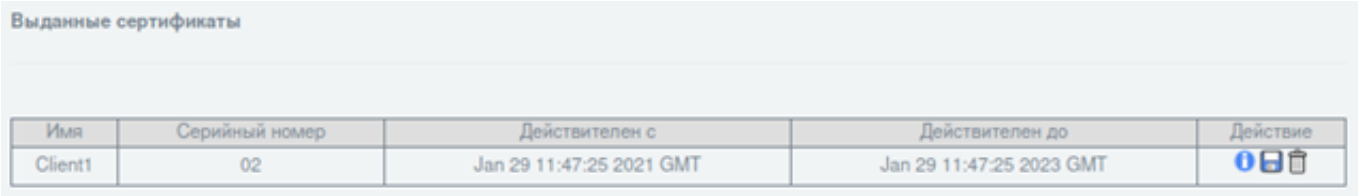

Рис. 206

В таблице 99 приведено описание элементов блока «Выданные сертификаты».

Таблица 99 – Описание элементов блока «Выданные сертификаты»

Элемент	Описание
Кнопка « »	Кнопка «Информация». Предназначена для отображения полной информации о выданном сертификате
Кнопка « »	Кнопка «Скачать». Предназначена для сохранения сертификата на ЭВМ администратора
Кнопка « »	Кнопка «Удалить». Предназначена для удаления выданного сертификата

4.9. Раздел «Журналы»

Раздел «Журналы» содержит следующие подразделы:

1) «Настройки журналирования»;

2) «Журнал межсетевого экрана»;

3) «Журнал обнаружения атак»;

4) «Системный протокол».

4.9.1. Подраздел «Настройки журналирования»

Подраздел «Настройки журналирования» (см. рис. 207) предназначен для установки параметров отображения и ведения журналов.

Подраздел «Настройки журналирования»

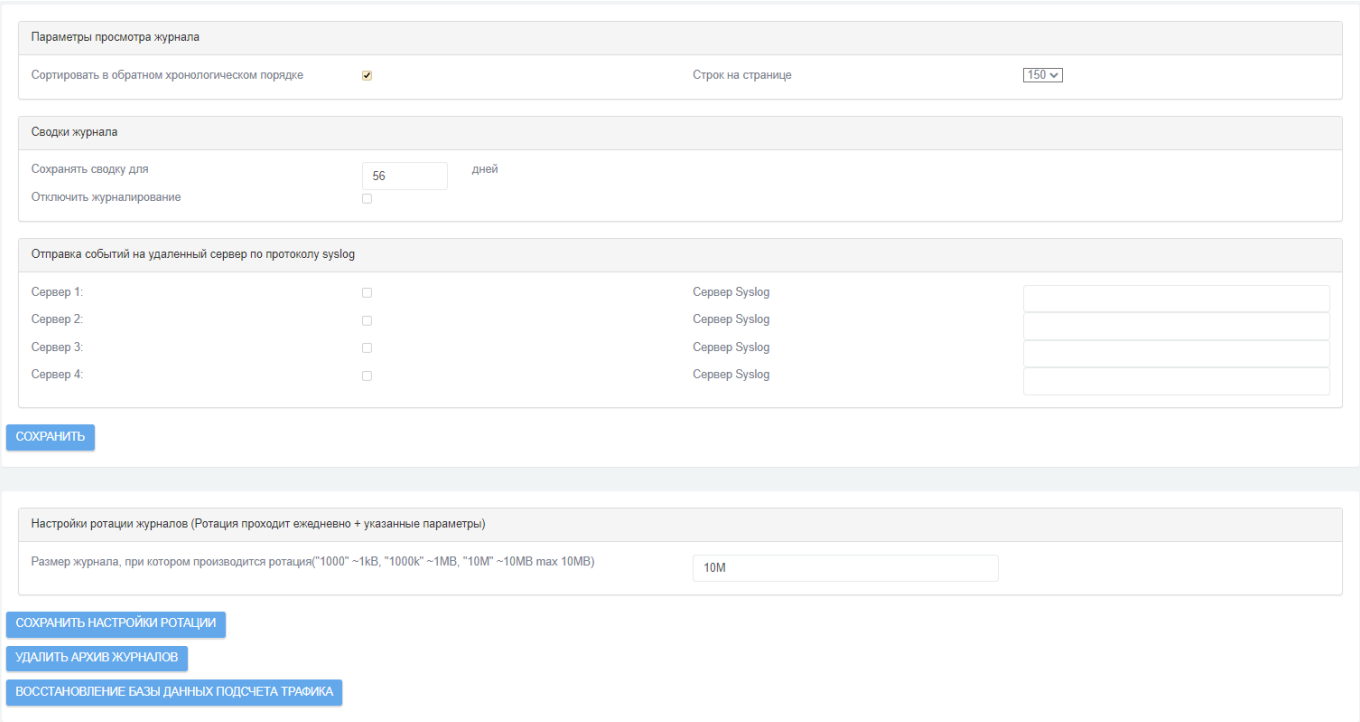

Рис. 207

В таблице 100 приведено описание элементов подраздела «Настройки журналирования».

Таблица 100 – Описание элементов подраздела «Настройки журналирования»

Элемент	Описание
Чекбокс «Сортировать в обратном хронологическом порядке»	Предназначен для выбора включения/отключения сортировки записей в обратном хронологическом порядке
Выпадающий список «Строк на странице»	Предназначен для выбора количества строк записей на странице. Доступны для выбора следующие параметры: – «15»; – «50»; – «100»; – «150»; – «250»; – «500»
Поле «Сохранять сводку для»	Предназначено для ввода количества дней, за которые сохраняется сводка
Чекбокс «Отключить журналирование»	Предназначен для выбора включения/отключения функции журналирования

Элемент	Описание
Чекбоксы «Сервер **порядковый номер**»	Предназначены для выбора включения/отключения, соответствующего указанному порядковому номеру, сервера
Поля «Сервер Syslog»	Предназначены для ввода адреса и порта сервера «Syslog» (в формате: <IP-адрес>:<порт>) для соответствующего сервера (в выбранной строке слева)
Кнопка «Сохранить»	Предназначена для сохранения введенных ранее пользователем настроек секции
Поле «Размер журнала, при котором производится ротация ("1000" ~1kB, "1000k" ~1MB, "10M" ~10MB max 10MB)»	Предназначено для ввода максимального размера журнала, при котором происходит его перезапись
Кнопка «Сохранить настройки ротации»	Предназначена для сохранения введенных ранее пользователем настроек перезаписи журнала
Кнопка «Удалить архив журналов»	Предназначена для удаления архива журналов пользователем
Кнопка «Восстановление базы данных подсчета трафика»	Предназначена для восстановления базы данных трафика в изделии при изменении системного времени пользователем вручную. Примечания: 1. Включение функции подсчета трафика находится на странице «Состояние» → «Подсчет трафика» → «Конфигурация подсчета трафика». 2. После восстановления базы данных подсчета трафика произойдет удаление подсчитанного трафика за все время использования изделия. База данных подсчета трафика очистится и придет к состоянию по умолчанию

4.9.2. Подраздел «Журнал межсетевого экрана»

Подраздел «Журнал межсетевого экрана» (см. рис. 208) предназначен для вывода общего отчета о системе за определенный период.

Подраздел «Журнал межсетевого экрана»

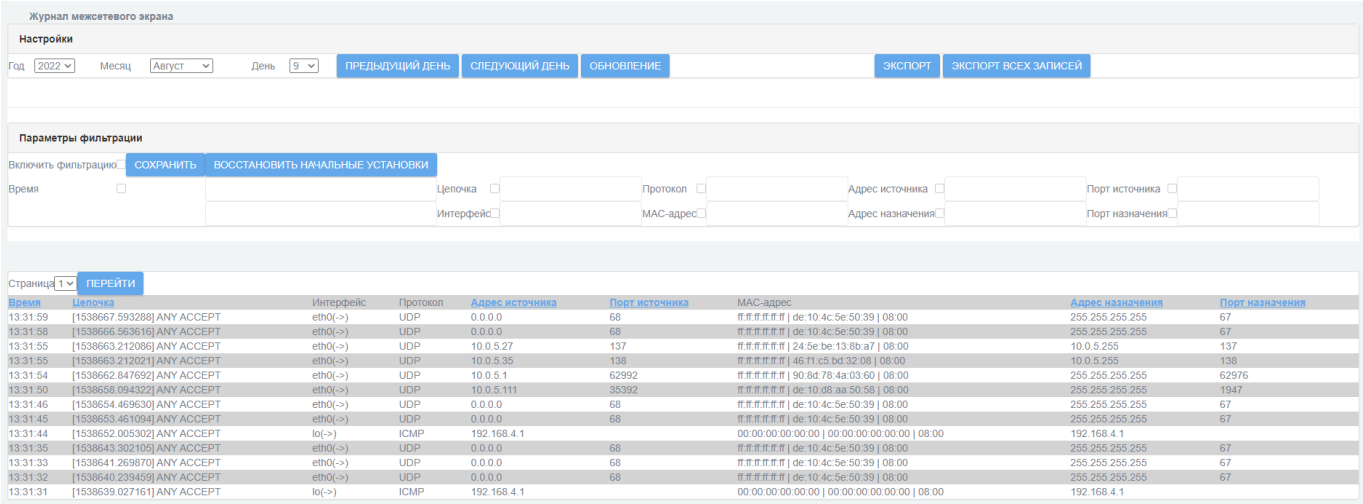

Рис. 208

В таблице 101 приведено описание элементов подраздела «Журнал межсетевого экрана».

Таблица 101 – Описание элементов подраздела «Журнал межсетевого экрана»

Элемент	Описание
Выпадающий список «Год»	Предназначен для выбора отображения информации за указанный год
Выпадающий список «Месяц»	Предназначен для выбора отображения информации за указанный месяц
Выпадающий список «День»	Предназначен для выбора отображения информации за указанный день
Кнопка «Предыдущий день»	Предназначена для выбора отображения информации на один день раньше от просматриваемого
Кнопка «Следующий день»	Предназначена для выбора отображения информации на один день позже от просматриваемого
Кнопка «Обновление»	Предназначена для обновления отображенной информации для выбранного периода времени
Кнопка «Экспорт»	Предназначена для экспорта на ЭВМ администратора отсортированных (отображенных в данный момент на странице) данных в текстовом виде в формате «.dat»
Кнопка «Экспорт всех записей»	Предназначена для экспорта всех данных с момента первого запуска изделия в виде архива «.zip». Записи будут представлены в текстовом виде и/или в формате «.gz» для внутренних архивов с логами
Чекбокс «Включить фильтрацию»	Предназначен для выбора включения/отключения функции фильтрации по заданным пользователем категориям

Элемент	Описание
Кнопка «Сохранить»	Предназначена для сохранения выбранных пользователем настроек фильтрации
Кнопка «Восстановить начальные установки»	Предназначена для восстановления на изделии настроек фильтрации по умолчанию
Чекбокс «Время»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем времени
Поля «Время»	Предназначены для ввода периода времени, по которому будут выбраны и отображены результаты фильтрации журнала. Первое поле (верхнее) предназначено для ввода начального значения диапазона. Второе поле (нижнее) предназначено для ввода конечного значения диапазона. Примечание. В данные поля время необходимо записывать в следующем формате: часы/минуты/секунды, записанные через «:» (к примеру: «13:31:59»)
Чекбокс «Цепочка»	Предназначен для выбора включения/отключения фильтрации по указанной пользователем цепочке
Поле «Цепочка»	Предназначено для ввода цепочки, по которой будут выбраны и отображены результаты фильтрации журнала
Чекбокс «Интерфейс»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем интерфейсу
Поле «Интерфейс»	Предназначено для ввода интерфейса, по которому будут выбраны и отображены результаты фильтрации журнала
Чекбокс «Протокол»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем протоколу
Поле «Протокол»	Предназначено для ввода протокола, по которому будут выбраны и отображены результаты фильтрации журнала
Чекбокс «MAC-адрес»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем MAC-адресу
Поле «MAC-адрес»	Предназначено для ввода MAC-адреса, по которому будут выбраны и отображены результаты фильтрации журнала
Чекбокс «Адрес источника»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем адресу источника
Поле «Адрес источника»	Предназначено для ввода адреса источника, по которому будут выбраны и отображены результаты фильтрации журнала
Чекбокс «Адрес назначения»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем адресу назначения
Поле «Адрес назначения»	Предназначено для ввода адреса назначения, по которому будут выбраны и отображены результаты фильтрации журнала
Чекбокс «Порт источника»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем порту источника
Поле «Порт источника»	Предназначено для ввода порта источника, по которому будут выбраны и отображены результаты фильтрации журнала
Чекбокс «Порт назначения»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем порту назначения
Поле «Порт назначения»	Предназначено для ввода порта назначения, по которому будут выбраны и отображены результаты фильтрации журнала
Выпадающий список «Страница»	Предназначен для выбора просматриваемой страницы в информационной таблице «Журнал межсетевого экрана»

Элемент	Описание
Кнопка «Перейти»	Предназначена для перехода на выбранную ранее пользователем (Выпадающий список «Страница») страницу в информационной таблице «Журнал межсетевого экрана»
Информационная таблица «Журнал межсетевого экрана»	Предназначена для отображения пользователю отчета о системе. Информация в таблице будет отсортирована согласно настройкам фильтрации пользователя

4.9.3. Подраздел «Журнал обнаружения атак»

Подраздел «Журнал обнаружения атак» (см. рис. 209) предназначен для отображения журнала СОВ.

Подраздел «Журнал обнаружения атак»

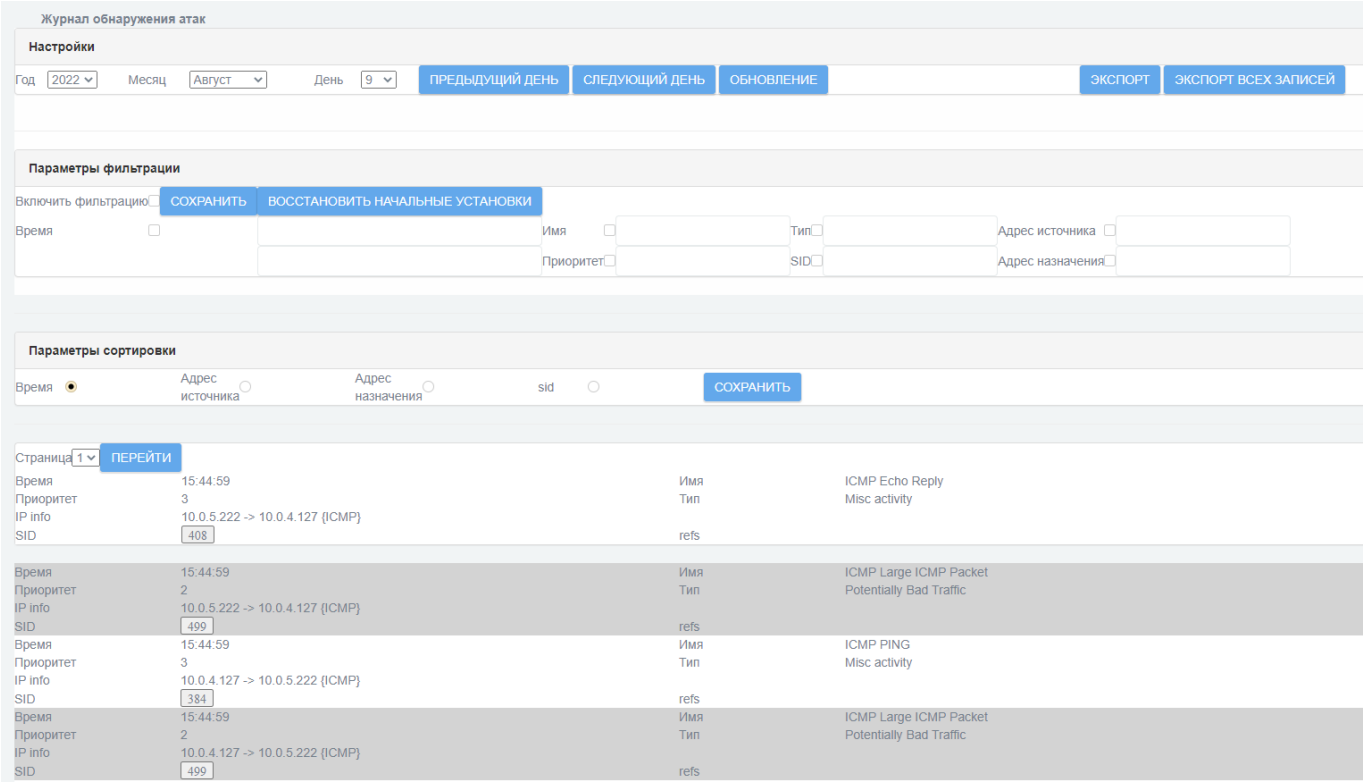

Рис. 209

В таблице 102 приведено описание элементов подраздела «Журнал обнаружения атак».

Таблица 102 – Описание элементов подраздела «Журнал обнаружения атак»

Элемент	Описание
Выпадающий список «Год»	Предназначен для выбора отображения информации за указанный год
Выпадающий список «Месяц»	Предназначен для выбора отображения информации за указанный месяц
Выпадающий список «День»	Предназначен для выбора отображения информации за указанный день
Кнопка «Предыдущий день»	Предназначена для выбора отображения информации на один день раньше от просматриваемого
Кнопка «Следующий день»	Предназначена для выбора отображения информации на один день позже от просматриваемого
Кнопка «Обновление»	Предназначена для обновления отображенной информации для выбранного периода времени
Кнопка «Экспорт»	Предназначена для экспорта на ЭВМ администратора отсортированных (отображенных в данный момент на странице) данных в текстовом виде в формате «.dat»
Кнопка «Экспорт всех записей»	Предназначена для экспорта всех данных с момента первого запуска изделия в виде архива «.zip». Записи будут представлены в текстовом виде и/или в формате «.gz» для внутренних архивов с логами
Чекбокс «Включить фильтрацию»	Предназначен для выбора включения/отключения функции фильтрации по заданным пользователем категориям
Кнопка «Сохранить»	Предназначена для сохранения выбранных пользователем настроек фильтрации
Кнопка «Восстановить начальные установки»	Предназначена для восстановления на изделии настроек фильтрации по умолчанию
Чекбокс «Время»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем времени
Поля «Время»	Предназначены для ввода периода времени, по которому будут выбраны и отображены результаты фильтрации журнала. Первое поле (верхнее) предназначено для ввода начального значения диапазона. Второе поле (нижнее) предназначено для ввода конечного значения диапазона. Примечание. В данные поля время необходимо записывать в следующем формате: часы/минуты/секунды, записанные через «:» (к примеру: «13:31:59»)
Чекбокс «Имя»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем имени правила
Поле «Имя»	Предназначено для ввода имени правила, по которому будут выбраны и отображены результаты фильтрации журнала
Чекбокс «Приоритет»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем приоритету
Поле «Приоритет»	Предназначено для ввода приоритету, по которому будут выбраны и отображены результаты фильтрации журнала
Чекбокс «Тип»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем типу, к которому относится правило

Элемент	Описание
Поле «Тип»	Предназначено для ввода типа, к которому относится правило, по которому будут выбраны и отображены результаты фильтрации журнала
Чекбокс «SID»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем SID
Поле «SID»	Предназначено для ввода SID по которому будут выбраны и отображены результаты фильтрации журнала
Чекбокс «Адрес источника»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем адресу источника
Поле «Адрес источника»	Предназначено для ввода адреса источника, по которому будут выбраны и отображены результаты фильтрации журнала
Чекбокс «Адрес назначения»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем адресу назначения
Поле «Адрес назначения»	Предназначено для ввода адреса назначения, по которому будут выбраны и отображены результаты фильтрации журнала
Чекбоксы «Параметры сортировки»	Предназначены для выбора включения/отключения одного из представленных видов сортировки. Для выбора доступны следующие чекбоксы: – «Время»; – «Адрес источника»; – «Адрес назначения»; – «sid». Для сохранения выбора пользователя необходимо после нажать справа от чекбоксов кнопку «Сохранить»
Выпадающий список «Страница»	Предназначен для выбора просматриваемой страницы в информационной таблице «Журнал обнаружения атак»
Кнопка «Перейти»	Предназначена для перехода на выбранную ранее пользователем (Выпадающий список «Страница») страницу в информационной таблице «Журнал обнаружения атак»
Информационная таблица «Журнал обнаружения атак»	Предназначена для отображения пользователю отчета о зафиксированных системой событий. Информация в таблице будет отсортирована согласно настройкам фильтрации пользователя

4.9.4. Подраздел «Системный протокол»

Подраздел «Системный протокол» (см. рис. 210) предназначен для отображения сообщений об ошибках изделия, а также отображения всех событий функционирования изделия.

Подраздел «Системный протокол»

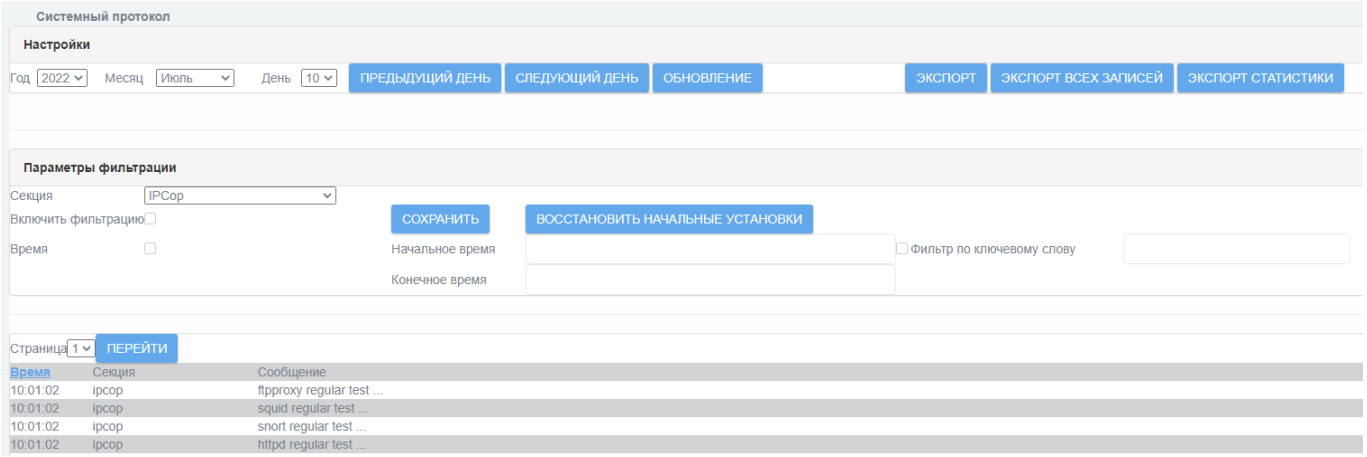

Рис. 210

В таблице 103 приведено описание элементов подраздела «Системный протокол».

Таблица 103 – Описание элементов подраздела «Системный протокол»

Элемент	Описание
Выпадающий список «Год»	Предназначен для выбора отображения информации за указанный год
Выпадающий список «Месяц»	Предназначен для выбора отображения информации за указанный месяц
Выпадающий список «День»	Предназначен для выбора отображения информации за указанный день
Кнопка «Предыдущий день»	Предназначена для выбора отображения информации на один день раньше от просматриваемого
Кнопка «Следующий день»	Предназначена для выбора отображения информации на один день позже от просматриваемого
Кнопка «Обновление»	Предназначена для обновления отображенной информации для выбранного периода времени
Кнопка «Экспорт»	Предназначена для экспорта на ЭВМ администратора отсортированных (отображенных в данный момент на странице) данных в текстовом виде в формате «.dat»
Кнопка «Экспорт всех записей»	Предназначена для экспорта всех данных с момента первого запуска изделия в виде архива «.zip». Записи будут представлены в текстовом виде и/или в формате «.gz» для внутренних архивов с логами

Элемент	Описание
Кнопка «Экспорт статистики»	Предназначена для экспорта статистики с данными на текущий момент времени в виде архива «.zip». В архиве, в формате «.log», будут находиться следующие файлы: – «chksum» (контрольные суммы); – «netstatus» (информация о сети); – «nftables» (информация о правилах МЭ); – «status» (информация о состоянии системы); – «sysinfo» (информация о системе)
Выпадающий список «Секция»	Предназначен для выбора одного из параметров фильтрации
Чекбокс «Включить фильтрацию»	Предназначен для выбора включения/выключения фильтрации по заданным категориям
Кнопка «Сохранить»	Предназначена для сохранения внесенных изменений в настройки фильтрации пользователем
Кнопка «Восстановить начальные установки»	Предназначена для восстановления в изделии настроек по умолчанию
Чекбокс «Время»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем времени
Поле «Начальное время»	Предназначено для ввода начального значения диапазона времени, по которому будут выбраны и отображены результаты фильтрации журнала. Примечание. В данное поле время необходимо записывать в следующем формате: часы/минуты/секунды, записанные через «:» (к примеру: «13:31:59»)
Поле «Конечное время»	Предназначено для ввода конечного значения диапазона времени, по которому будут выбраны и отображены результаты фильтрации журнала. Примечание. В данное поле время необходимо записывать в следующем формате: часы/минуты/секунды, записанные через «:» (к примеру: «13:31:59»)
Чекбокс «Фильтр по ключевому слову»	Предназначен для выбора включения/отключения фильтрации по указанному пользователем ключевому слову
Поле «Фильтр по ключевому слову»	Предназначено для ввода ключевого слова
Выпадающий список «Страница»	Предназначен для выбора просматриваемой страницы в информационной таблице «Системный протокол»
Кнопка «Перейти»	Предназначена для перехода на выбранную ранее пользователем (Выпадающий список «Страница») страницу в информационной таблице «Системный протокол»
Информационная таблица «Системный протокол»	Предназначена для отображения пользователю отчета о сообщениях об ошибках в изделии, а также отображения всех событий его функционирования. Информация в таблице будет отсортирована согласно настройкам фильтрации пользователя

5. ДЕЙСТВИЯ ПОСЛЕ СБОЕВ И ОШИБОК ЭКСПЛУАТАЦИИ

В ходе эксплуатации изделия могут возникнуть сбои и допускаться ошибки эксплуатации.

Сбои в работе изделия могут возникнуть вследствие:

1) отказа оборудования;

2) сбоев в работе программного обеспечения;

3) внесения некорректных изменений в настройки конфигурации устройства и реализуемых устройством функций безопасности;

4) нарушений порядка работы с устройством и режима эксплуатации, определенных Политикой безопасности и эксплуатационной документацией на изделие.

Наличие сбоев и неполадок в работе изделия может быть идентифицировано по следующим признакам:

1) сообщения об ошибках (текстовые сообщения), отображаемые в веб-интерфейсе ЭВМ администратора (пользователя);

2) отсутствие отклика устройства через веб-интерфейс ЭВМ администратора (пользователя), сообщения браузера об отсутствии связи с устройством;

3) сообщения средств мониторинга защищаемой сети об отсутствии отклика от устройства;

4) сообщения об отказе программного ядра ПО изделия, отображаемые в консоли восстановления.

Примечание. Доступные для изделия типовые сообщения при возникновении аварийных ситуаций, а также перечень сообщений об ошибках и предупреждений представлены подробно в разделе «Текстовые сообщения» руководства администратора НПЕШ.465614.005РА.

При появлении признаков сбоя или неполадок рекомендуется следующее:

1) восстановить программные настройки изделия, используя функцию резервного копирования (см. п. 4.2.5 настоящего документа);

2) переустановить ПО изделия согласно подразделу «Процедура переустановки ПО» руководства администратора НПЕШ.465614.005РА.

Возможны перезагрузки оборудования с установленным ПО изделия, вызванные сбоями в питании. При кратковременном сбое изделие может перезагрузиться самостоятельно, но чаще всего требуется включение вручную.

При выключении изделия сохраняются настройки и состояние сервисов, которые автоматически восстанавливаются после запуска. Однако для контроля ошибок рекомендуется не ранее чем через 30 секунд после запуска вручную проверять состояние запущенных сервисов.

В случае продолжения проблем с работой устройства его следует направить для диагностики и устранения неисправностей в авторизованный сервисный центр предприятия-изготовителя (АО «НПО «Эшелон»).

ПРИЛОЖЕНИЕ 1.

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

C – *(англ. Country)* – название страны

CARP – *(англ. Common Address Redundancy Protocol)* – протокол резервирования общего адреса

CISSP – *(англ. Certified Information Security Systems Professional)* – сертифицированный специалист по информационной безопасности

CN – *(англ. Common name)* – стандартное имя

CRE – *(англ. Classroom Extension)* – расширение групп классов по управлению

DN – *(англ. Distinguished name)* – уникальное имя

DPD – *(англ. Dead Peer Detection)* – метод обнаружения неработающих одноранговых интернет-ключей

ESP – *(анг. Encapsulating Security Payload)* – протокол обеспечивает конфиденциальность (шифрование) передаваемой информации и ограничение потока конфиденциального трафика

GRE – *(англ. Generic Routing Encapsulation)* – протокол туннелирования сетевых пакетов, который инкапсулирует пакеты некоторых протоколов сетевого уровня в пакеты других протоколов

IKE – *(англ. Internet Key Exchange)* – управляющий протокол набора протоколов IPsec, используется для обеспечения защищенного взаимодействия в виртуальных частных сетях

L – *(англ. Locality)* – Местонахождение

LZO – *(англ. Lempel-Ziv-Oberhumer)* – алгоритм сжатия данных без потерь

MTU – *(англ. Maximum transmission unit)* – максимальный размер пакета

O – *(англ. Organization)* – организация

OU – *(англ. Organization unit)* – подразделение организации

PFS *(англ. Perfect Forward Secrecy)* – совершенная опережающая секретность. Свойство некоторых протоколов согласования ключа, которое гарантирует, что сессионные ключи, полученные при помощи набора ключей долговременного пользования, не будут скомпрометированы при компрометации одного из долговременных ключей

S – *(англ. StateOrProvinceName)* – название области или района

SID – *(англ. Security Identifier)* – идентификатор безопасности

VRRP – *(англ. Virtual Router Redundancy Protocol)* – протокол резервирования виртуального маршрутизатора

БРП – база решающих правил

ДМЗ – *(англ. Demilitarized Zone (DMZ))* – демилитаризованная зона

ИС – информационная система

МЭ – межсетевой экран

ОС – операционная система

ПО – программное обеспечение

СОВ – система обнаружения вторжений

УЦ – удостоверяющий центр

ЭВМ – электронно-вычислительная машина

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
Изм.	измененных	замененных	новых	аннулированных					