УТВЕРЖДЕН

НПЕШ.465614.003 РА-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «КОМПЛЕКС ПРОТИВОДЕЙСТВИЯ ПРОГРАММНО-АППАРАТНЫМ ВОЗДЕЙСТВИЯМ (КП ПАВ) «РУБИКОН» С ФУНКЦИЕЙ ОДНОНАПРАВЛЕННОГО ШЛЮЗА»

НПЕШ.465614.003

Руководство администратора

НПЕШ.465614.003 РА

Листов 343

2021

АННОТАЦИЯ

В документе содержатся сведения о функциях, структуре, системных настройках и особенностях администрирования изделия «Комплекс противодействия программно-аппаратным воздействиям (КП ПАВ) «Рубикон» с функцией однонаправленного шлюза» НПЕШ.465614.003 (далее – «Рубикон», изделие).

В документе представлены инструкции по безопасным подготовке, первому запуску, настройке и установке изделия, его администрированию в ходе эксплуатации, даны необходимые описания интерфейса и инструкции по реализации основных функций администрирования.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение и область применения

Программно-аппаратный комплекс «Комплекс противодействия программно-аппаратным воздействиям (КП ПАВ) «Рубикон» с функцией однонаправленного шлюза» (далее ОО, ПАК «Рубикон», «Рубикон») НПЕШ.465614.003 объединяет функции межсетевого экрана и системы обнаружения вторжений. 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, для обнаружения и блокирования атак на ресурсы защищаемой сети, а также для однонаправленной передачи данных в автоматизированных системах между сегментами сети.

Изделие «Рубикон» представляет собой программно-техническое средство, реализующее функции контроля и фильтрации в соответствии с заданными правилами транзитных информационных потоков, используемое в целях обеспечения защиты (некриптографическими методами) информации ограниченного доступа и обеспечивающее 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, с реализацией следующих функций безопасности:

- контроль и фильтрация сетевого трафика;
- идентификация и аутентификация;
- регистрация событий безопасности;
- обеспечение бесперебойного функционирования и восстановления;
- тестирование и контроль целостности;
- преобразование сетевых адресов;
- маскирование;
- приоритизация информационных потоков;
- управление;
- взаимодействие с другими средствами защиты информации;
- обнаружение вторжений;
- реализация однонаправленной передачи файлов.

1.2 Функциональные возможности изделия

«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 ИС и нарушениях безопасности с помощью отображения соответствующего сообщения на консоли управления, отсылки сообщений электронной почты;

69) возможность автоматизированного обновления базы решающих правил;

70) возможность верификации целостности БРП СОВ;

71) возможность маскирования наличия датчика «Рубикон» в составе контролируемой ИС, противодействие выявлению его на сетевом уровне стандартными средствами 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;

82) реализация однонаправленной передачи файлов.

1.3 Состав изделия

В состав изделия входят следующие основные компоненты:

1) аппаратная платформа (состоит из двух частей: приемник и передатчик);

2) предустановленное ПО «Рубикон», обеспечивающее реализацию функциональных возможностей изделия.

1.3.1 Комплектность поставки

Состав комплекта поставки «Рубикон» представлен в таблице 1.

Таблица 1 – Состав комплекта поставки «Рубикон»

Наименование	Обозначение	Кол., шт.	Заводской номер	Примечание
Программно-аппаратный комплекс «Комплекс противодействия программно-аппаратным воздействиям (КП ПАВ) «Рубикон» с функцией однонаправленного шлюза» в составе:	НПЕШ.465614.003	–		ПО «Рубикон» предустановлено на аппаратную часть комплекса
Составные части изделия				
– Аппаратная платформа ПРМ (приемник)	НПЕШ.465614.003.01	1		С установленным гигабитным сетевым интерфейсным адаптером «ДИОД-GR» из комплекта DIOD 1000-SX (DIOD-G) КБДЖ.467113.043
– Аппаратная платформа ПРД (передатчик)	НПЕШ.465614.003.02	1		С установленным гигабитным сетевым интерфейсным адаптером «ДИОД-GT» из комплекта DIOD 1000-SX (DIOD-G) КБДЖ.467113.043
– Программное изделие «Рубикон»	НПЕШ.00502-01	1		Поставляется на оптическом носителе НПЕШ.00502-01 ЛКД

Наименование	Обозначение	Кол., шт.	Заводской номер	Примечание
– Программное изделие «Рубикон»	НПЕШ.00502-01	1		Поставляется на флеш-носителе НПЕШ.00502-01 ФНИ
– Винт м5х12 с потайной головкой	б/о	8		
– Шайба коническая м5	б/о	8		
– Одноволоконный оптический кабель SC-SC, ММ	б/о	1		
– Кабель сетевой 220 V	б/о	2		
Документация				
Ведомость эксплуатационных документов	НПЕШ.465614.003 ВЭ	1		Папка №1
Краткое руководство пользователя	б/о	1		Поставляется на бумажном носителе
Гарантийный талон	б/о	1		Поставляется на бумажном носителе
Сертификат на техническую поддержку	б/о	1		Поставляется на бумажном носителе
Упаковка				
Упаковка	б/о	2		
* б/о – без обозначения				

1.3.2 Требования к АРМ администратора

Для управления интерфейсом администрирования «Рубикон» используется графический веб-интерфейс, доступ к которому осуществляется с использованием веб-браузера. Требования к АРМ администратора указаны в таблице 2.

Таблица 2 – Требования к АРМ администратора «Рубикон»

Элемент среды функционирования	**Параметры**
Вычислительная платформа АРМ администратора ПО «Рубикон»	Процессор с частотой не менее 1,2 ГГц Оперативная память: от 4 Гб Жесткий диск: от 120 ГБ Сетевая карта: 100 Мбит/с; Сетевая карта однонаправленного приема/передачи сетевого потока
ОС АРМ администратора	ОС семейства Linux/Unix 64 bit: – Astra Linux Common Edition (Орел) не ниже 1.11; – Astra Linux Special Edition (Смоленск) не ниже 1.5; ОС семейства Microsoft Windows 64 bit: – Windows Server 2019; – Windows 10
Веб-браузер	Windows 10/Windows Server 2019: – IE (не ниже 11.1.17134.0); – Microsoft Edge (не ниже 42.17134.1.0); – Firefox не ниже 76.0.1 (64-битный); – Chrome (не ниже 83.0.4103.61); Astra Linux 1.6: – Firefox не ниже 60.0.2 (64-битный)

1.3.3 Функциональная структура ПО

Функциональная структура ПО «Рубикон» представлена следующими подсистемами:

1) подсистема обеспечения сетевого взаимодействия;
2) подсистема идентификации / аутентификации;
3) подсистема бесперебойного функционирования и восстановления;
4) подсистема регистрации событий;
5) подсистема взаимодействия с внешними системами;
6) подсистема управления;
7) подсистема обнаружения вторжений;
8) веб-интерфейс;
9) операционная система;
10) подсистема BIOS.

1.3.3.1 Подсистема обеспечения сетевого взаимодействия

Подсистема обеспечения сетевого взаимодействия представлена следующими модулями:

1) модуль фильтрации;
2) модуль маршрутизации;
3) модуль преобразования адресов;
4) модуль приоритизации;
5) модуль управления состояниями;
6) модуль сетевого посредника;
7) модуль настройки сетевых интерфейсов;
8) модуль однонаправленной передачи данных.

1.3.3.1.1 Модуль фильтрации

Модуль фильтрации является ядром подсистемы обеспечения сетевого взаимодействия и используется для работы модуля управления состоянием, модуля тестирования и контроля целостности и модуля сетевого посредника. Модуль фильтрации осуществляет фильтрацию информационных потоков, основанную на следующих типах атрибутов безопасности:

1) сетевой адрес узла отправителя и получателя;
2) логический или физический сетевой интерфейс КП ПАВ «Рубикон», через который проходит пакет;
3) сетевой протокол, который используется для взаимодействия;
4) направление пакета (входящий/исходящий);
5) транспортный протокол, который используется для взаимодействия;

6) порты источника и получателя в рамках сеанса (сессии);

7) флаг фрагментации;

8) мандатная метка;

9) команды (разрешенные/запрещенные), параметры команд; последовательности используемых команд - для FTP протокола;

10) мобильный код (разрешенный/запрещенный) для языков программирования Java и JavaScript;

11) прикладное ПО (разрешенное/запрещенное) для веб-браузеров (Internet Explorer, Mozilla Firefox, Google Chrome и др).

1.3.3.1.2 Модуль маршрутизации

Программный модуль КП ПАВ «Рубикон», предназначенный для выполнения статической маршрутизации.

1.3.3.1.3 Модуль преобразования адресов

Программный модуль КП ПАВ «Рубикон», позволяющий проводить трансляцию сетевых адресов (NAT) при экспорте информации сетевого трафика за пределы КП ПАВ «Рубикон» и осуществлять замену сетевого адреса КП ПАВ «Рубикон» на маскирующий (подставной) адрес.

1.3.3.1.4 Модуль приоритизации

Программный модуль КП ПАВ «Рубикон», обеспечивающий приоритизацию информационных потоков на основе установленных приоритетов значений сетевого адреса и используемого порта.

1.3.3.1.5 Модуль управления состояниями

Программный модуль КП ПАВ «Рубикон», предназначенный для проверки каждого пакета по таблице состояний для определения того, не противоречит ли состояние пакета ожидаемому состоянию.

1.3.3.1.6 Модуль сетевого посредника

Программный модуль КП ПАВ «Рубикон», осуществляющий посредничество в передаче информации сетевого трафика, основанное на следующих типах атрибутов безопасности:

a) сетевой адрес и порт отправителя и получателя;

b) сетевой трафик (FTP, HTTP);

c) разрешенные/ запрещенные атрибуты информации в заголовках пакетов.

1.3.3.1.7 Модуль настройки сетевых интерфейсов

Программный модуль КП ПАВ «Рубикон», осуществляющий маскирование датчика СОВ на сетевом уровне и позволяющий настраивать сетевые интерфейсы.

1.3.3.1.8 Модуль однонаправленной передачи данных

Аппаратный модуль ОО, предназначен для осуществления однонаправленной передачи данных.

1.3.3.2 Подсистема идентификации / аутентификации

Подсистема идентификации / аутентификации представлена модулем аутентификации веб-сервера.

1.3.3.2.1 Модуль аутентификации веб-сервера

Модуль аутентификации веб-сервера обеспечивает идентификацию и аутентификацию администраторов КП ПАВ «Рубикон», а также идентификацию и аутентификацию субъектов межсетевого взаимодействия до передачи межсетевым экраном информационного потока получателю.

1.3.3.3 Подсистема бесперебойного функционирования и восстановления

Подсистема бесперебойного функционирования и восстановления представлена следующими модулями:

1) модуль тестирования и контроля целостности;
2) модуль восстановления;
3) модуль кластеризации.

1.3.3.3.1 Модуль тестирования и контроля целостности

Программный модуль КП ПАВ «Рубикон», обеспечивающий контроль целостности исполняемых файлов КП ПАВ «Рубикон» путем контрольного суммирования, а также проверку работоспособности служб КП ПАВ «Рубикон» и сетевого соединения.

1.3.3.3.2 Модуль восстановления

Программный модуль КП ПАВ «Рубикон», обеспечивающий автоматическое восстановление устойчивых и безопасных состояний HTTP сервера, прокси сервера, VPN сервера, сервиса аудита, службы времени, службы СОВ и DHCP.

1.3.3.3.3 Модуль кластеризации

Программный модуль КП ПАВ «Рубикон», обеспечивающий кластеризацию КП ПАВ «Рубикон» с помощью резервирования КП ПАВ «Рубикон».

1.3.3.4 Подсистема регистрации событий

Данная подсистема представлена модулем работы с журналом.

1.3.3.4.1 Модуль работы с журналом

Программный модуль КП ПАВ «Рубикон», предназначенный для создания, хранения и просмотра записей аудита. КП ПАВ «Рубикон» поддерживает уровни доступа (роли) пользователей. Все действия пользователей отслеживаются, и соответствующие записи помещаются в файлы регистрации событий безопасности. Модуль работы с журналом предоставляет уполномоченным пользователям (администратор КП ПАВ «Рубикон», аудитор КП ПАВ «Рубикон») возможность читать всю информацию из записей аудита, осуществлять поиск, сортировать записи аудита.

1.3.3.5 Подсистема взаимодействия с внешними системами

Данная подсистема состоит из следующих модулей:

1) модуль взаимодействия с внешними СЗИ;
2) модуль связи с сервером журналирования.

1.3.3.5.1 Модуль взаимодействия с внешними СЗИ

Программный модуль КП ПАВ «Рубикон», обеспечивающий взаимодействия КП ПАВ «Рубикон» с САВЗ по протоколу адаптации Интернет-контента (ICAP).

1.3.3.5.2 Модуль связи с сервером журналирования

Программный модуль КП ПАВ «Рубикон», обеспечивающий взаимодействие с сервером журналирования.

1.3.3.6 Подсистема управления

Данная подсистема представлена следующими модулями:

1) модуль веб-сервера;
2) модуль преобразования конфигурации браузера.

1.3.3.6.1 Модуль веб-сервера

Программный модуль КП ПАВ «Рубикон», обеспечивающий выполнение запросов пользователей.

1.3.3.6.2 Модуль преобразования конфигурации браузера

Программный модуль КП ПАВ «Рубикон», обеспечивающий представление информации для пользователей.

1.3.3.7 Подсистема обнаружения вторжений

Подсистема обнаружения вторжений представлена следующими модулями:

1) модуль «Агент обновления»;
2) модуль сигнатурного анализа сетевого трафика;
3) модуль эвристического анализа сетевого трафика;
4) модуль реагирования.

1.3.3.7.1 Модуль «Агент обновления»

Программный модуль КП ПАВ «Рубикон», предназначенный для получения актуальной базы решающих правил СОВ с сервера обновлений.

1.3.3.7.2 Модуль сигнатурного анализа сетевого трафика

Программный модуль КП ПАВ «Рубикон», предназначенный для поиска определенных в базе решающих правил СОВ сигнатур атак в сетевых пакетах.

1.3.3.7.3 Модуль эвристического анализа сетевого трафика

Программный модуль КП ПАВ «Рубикон», предназначенный для обнаружения вторжений с помощью эвристического анализа.

1.3.3.7.4 Модуль реагирования

Программный модуль КП ПАВ «Рубикон», позволяет уведомлять администратора об обнаруженных вторжениях и выдачу управляющих сигналов межсетевому экрану.

1.3.3.8 Веб-интерфейс

Веб-интерфейс реализует интерфейс модуля «Программа управления», позволяет решать задачи по администрированию СОВ.

1.3.3.9 Операционная система

Операционная система, помимо реализации профильных функций по умолчанию, дополнительно представлена следующими модулями:

1) модуль выдачи меток времени;
2) модуль захвата и разбора трафика.

1.3.3.9.1 Модуль выдачи меток времени

Программный модуль КП ПАВ «Рубикон», предоставляющий надежные метки времени для собственного использования (при генерации записей в журнале аудита).

1.3.3.9.2 Модуль захвата и разбора трафика

Программный модуль КП ПАВ «Рубикон», предназначенный для захвата, буферизации и управления последовательностью обработки сетевых пакетов.

1.3.3.10 Подсистема BIOS

Подсистема BIOS представлена модулем BIOS.

1.3.3.10.1 Модуль BIOS

Программный модуль, обеспечивающий инициализацию работы аппаратной платформы и передачу управления загрузчику ПО «Рубикон».

1.4 Подготовка к работе

1.4.1 Действия по приемке изделия

Приемка изделия осуществляется в следующем порядке:

1) проверка комплектности;
2) проверка маркировки и пломбирования;
3) проверка контрольных сумм компонентов установочного дистрибутива ПО «Рубикон».

1.4.1.1 Проверка комплектности

Проверка комплектности при приемке изделия производится в соответствии и таблицей 1, если в Договоре поставки не указано иное.

1.4.1.2 Проверка маркировки и пломбирования

Проверка маркировки и пломбирования производится в следующей последовательности:

1) проверка маркировки упаковочной тары;
2) проверка маркировки носителей установочного дистрибутива ПО «Рубикон» (флеш-накопителя и CD диска);
3) проверка маркировки оптического носителя с эксплуатационной документацией;
4) проверка маркировки и пломбирования изделия.

1.4.1.2.1 Проверка маркировки упаковочной тары

Проверка маркировки упаковочной тары производится посредством визуального осмотра внешней поверхности упаковочной тары. Упаковочная тара должна маркироваться наклейками, содержащими следующую информацию:

1) наименование компании-производителя,
2) контактная информация компании-производителя,
3) наименование и обозначение изделия, серийный номер изделия.

1.4.1.2.2 Проверка маркировки носителя установочного дистрибутива ПО «Рубикон»

Проверка маркировки флеш-накопителя и установочного CD диска производится путем визуального контроля надписей, нанесенных на шильдик, расположенный на внешней поверхности. Маркировка (шильдик) должна содержать следующую информацию:

1) наименование программного продукта;
2) серийный номер изделия;
3) логотип компании-изготовителя.

1.4.1.2.3 Проверка маркировки оптического носителя с документацией

Проверка маркировки оптического носителя с эксплуатационной документацией производится путем визуального контроля надписей, нанесенных на внешнюю поверхность накопителя. Маркировка должна содержать следующую информацию:

1) наименование, адрес, контактная информация компании-изготовителя;
2) наименование продукта;
3) наименование оптического носителя: «Диск с эксплуатационной документацией».

1.4.1.2.4 Проверка маркировки и пломбирования изделия

Проверка маркировки изделия производится посредством визуального контроля шильдиков, размещенных на фронтальных панелях передатчика и приемника из состава аппаратной платформы и размещенных на нижней части корпуса наклеек. Шильдик должен содержать:

1) наименование и обозначение изделия;
2) наименование компании-производителя.

Наклейка должна содержать:

1) наименование и обозначение изделия;
2) серийный номер изделия.

Проверка пломбирования изделия производится посредством визуального контроля наличия и состояния гарантийной пломбы, наклеиваемой при производстве изделия на его корпус и препятствующей вскрытию корпуса. На гарантийной пломбе должна отображаться следующая информация:

1) логотип компании-производителя;
2) надпись: «Гарантийная пломба. Повреждение лишает гарантии».

1.4.1.3 Проверка установочного дистрибутива ПО «Рубикон»

Подсчет контрольных сумм файлов дистрибутива Программного изделия «Рубикон» производится с помощью программного изделия «Программное обеспечение «Программа инспекционного контроля «ПИК Эшелон» (сертификат № 3752 выдан Министерством обороны Российской Федерации, по алгоритму «ГОСТ 34.11-2012 (256 бит)»). Перечень компонентов, составляющих установочный дистрибутив «Рубикон», и их контрольные суммы должны соответствовать таблице 2 документа Программно-аппаратный комплекс «Комплекс

противодействия программно-аппаратным воздействиям (КП ПАВ) «РУБИКОН» с функцией однонаправленного шлюза Технические Условия часть 1 НПЕШ.465614.003 ТУ.

1.4.2 Требования по безопасной установке и настройке

1.4.2.1 Требования к квалификации администратора

Администратор должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию «Рубикон», а также должен иметь профессиональные знания и практический опыт в области системного администрирования. Обязательны знакомство и практический опыт установки и администрирования серверных операционных систем семейства MS Windows и Linux, знание эксплуатационной документации «Рубикон».

1.4.2.2 Организационные меры по обеспечению безопасной настройки и установки

При эксплуатации «Рубикон» на объектах информатизации, на которых производится обработка информации ограниченного доступа, должно быть обеспечено выполнение следующих организационных мер:

1) наличие администратора безопасности, отвечающего за корректную эксплуатацию «Рубикон»;

2) сохранение в защищенной форме идентификаторов (имен) и паролей (кодов) администратора «Рубикон»;

3) обеспечение физической сохранности технических средств (устройства «Рубикон», терминала или ПЭВМ, использующейся в качестве терминала) и исключение возможности доступа к ним посторонних лиц;

4) обеспечение защиты АРМ администратора «Рубикон», в том числе, от деструктивного воздействия вредоносного ПО;

5) регламентацию использования дополнительного ПО, установленного на АРМ администратора «Рубикон»;

6) обеспечение сохранности оборудования и физической целостности системных блоков компьютеров;

7) ведение журнала учета работы компьютеров, проведения регламентных мероприятий и внесения изменений в конфигурацию технических и программных средств;

8) реализация мероприятий по антивирусной защите и обеспечение свободной от вирусов программной среды компьютеров.

К информационной среде, в которой функционирует «Рубикон», предъявляются следующие требования безопасности:

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

2) обеспечение 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) обеспечение установки, конфигурирования и управления «Рубикон» в соответствии с эксплуатационной документацией.

1.4.2.3 Подготовка к эксплуатации

1.4.2.3.1 Перечень используемой эксплуатационной документации

Перечень эксплуатационных документов, с которым необходимо ознакомиться перед началом работы с устройством «Рубикон»:

1) настоящее «Руководство администратора»;

2) формуляр устройства «Рубикон».

1.4.2.3.2 Первый запуск «Рубикон»

Первый запуск устройства «Рубикон» производится в следующем порядке:

1) устройство подключается к изолированной безопасной локальной сети, содержащей АРМ администратора, или подключается к нему посредством прямого подключения.

2) на устройство подается штатное питание и производится его включение;

3) с АРМ администратора производится подключение через веб-интерфейс к модулю управления «Рубикон».

Проверка наличия и функционирования «Рубикон» в подконтрольной сети выполняется посредством команды «ping 192.168.1.1» на любом из компьютеров, подключенных к защищаемой сети. Для прохождения процедур первичной идентификации и аутентификации необходимо выполнить следующие действия:

1) установить соединение с графическим интерфейсом «Рубикон», подключившись по защищенному https-соединению «https:// 192.168.1.1:8443»;

2) ввести идентификатор (логин) пользователя с ролью администратора в текстовое поле «Имя пользователя» формы авторизации. По умолчанию «admin»;

3) ввести пароль пользователя с ролью администратора в текстовое поле «Пароль» формы авторизации (по умолчанию: «radmin»), далее нажать кнопку «Вход».

При превышении трех неуспешных попыток ввода логина и пароля, доступ к «Рубикон» будет заблокирован. Спустя некоторое время есть возможность повторить попытку входа.

При первом подключении к административному интерфейсу необходимо изменить пароль на вкладке «Пользователи» раздела «Система» на пароль администратора безопасности.

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

1.4.2.3.3 Настройка функций безопасности

Настройка функций безопасности устройства «Рубикон» осуществляется администратором безопасности охраняемого IT-сегмента в соответствии с Политикой информационной безопасности.

1.4.2.3.4 Установка устройства «Рубикон»

По окончании настройки функций безопасности устройство «Рубикон» должно быть установлено и подключено согласно монтажным схемам и схемам подключения защищаемой информационной системы.

1.4.2.3.5 Проверка целостности установленного ПО

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

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 проверяется с периодичностью 1 час и по запросу администратора.

1.4.2.3.6 Проверка работоспособности

Проверка работоспособности считается выполненной при успешном выполнении процедур первого запуска и корректных результатах проверки контрольных сумм ПО «Рубикон», установленном на аппаратной платформе «Рубикон».

2 ОПИСАНИЕ ИНТЕРФЕЙСА

2.1 Описание главной страницы

2.1.1 Навигационное меню

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

Навигационное меню содержит элементы, представленные в таблице 3

Таблица 3 – Описание элементов навигационного меню

Элемент	Описание
	Кнопка открывает развернутое меню разделов
	Кнопка закрывает развернутое меню разделов
	Кнопка открывает всплывающее окно уведомлений
	Кнопка перехода в полноэкранный режим

2.1.2 Сокращенное меню

Сокращенное меню (рисунок 1) отображается при наведении курсора на кнопку «  » и представляет из себя колонку символов разделов основного меню.

Рисунок 1 – Сокращенное меню

При нажатии на сокращенное меню откроется развернутое меню.

Сокращенное меню содержит элементы, указанные в таблице 4.

Таблица 4 – Описание элементов сокращенного меню

Элемент	Описание
	Иконка раздела «Система»
	Иконка раздела «Состояние»
	Иконка раздела «Сеть»
	Иконка раздела «Службы»
	Иконка раздела «Система обнаружения вторжений»
	Иконка раздела Межсетевой экран»
	Иконка раздела «VPN»
	Иконка раздела «Журналы»
	Кнопка возврата к подразделу «Начало» раздела «Система» (стартовая страница)

2.1.3 Развернутое меню

Развернутое меню (рисунок 2) содержит символы отображения и названия разделов. Также развернутое меню содержит названия подразделов.

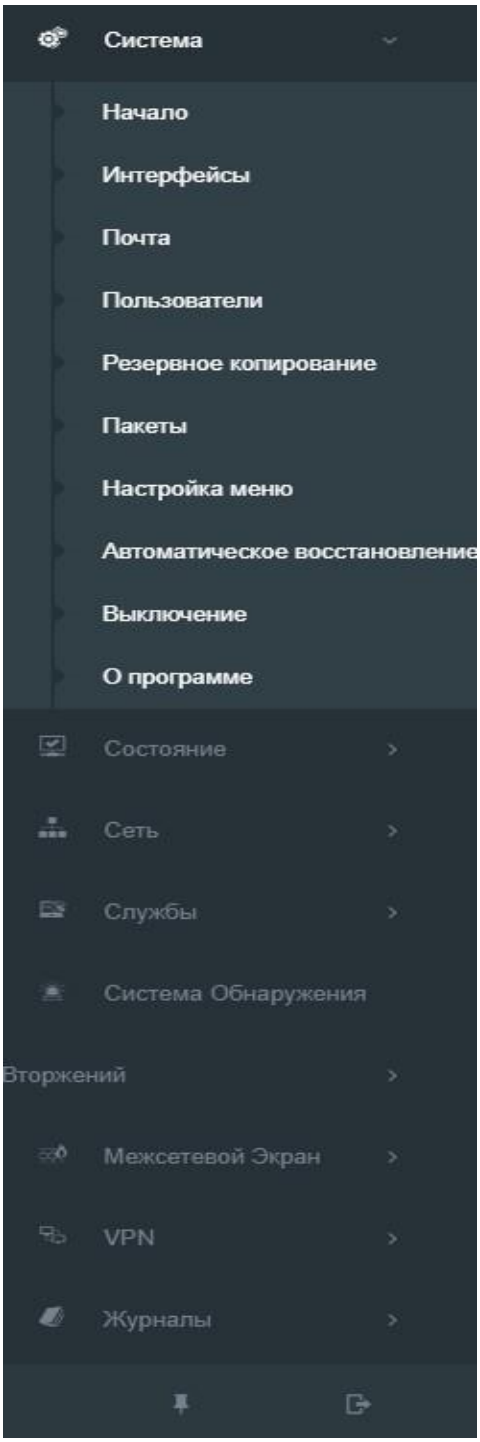


Рисунок 2 – Развернутое меню

Настройка отображения пунктов навигационного меню производится посредством подпункта «Настройка меню» (см. ниже).

Развернутое меню, в дополнение к элементам сокращенного меню, содержит элементы, указанные в таблице 5.

Таблица 5 – Описание элементов развернутого меню

Элемент	Описание
	Значок раскрывает всплывающий список подразделов
	Значок закрывает всплывающий список подразделов
	Кнопка закрепляет развернутое меню на экране
	Кнопка открепляет развернутое меню на экране
	Кнопка возврата к подразделу «Начало» раздела «Система» (стартовая страница)

2.1.4 Всплывающее окно «Уведомления»

Всплывающее окно «Уведомления» (рисунок 3) отображает перечень полученных уведомлений.

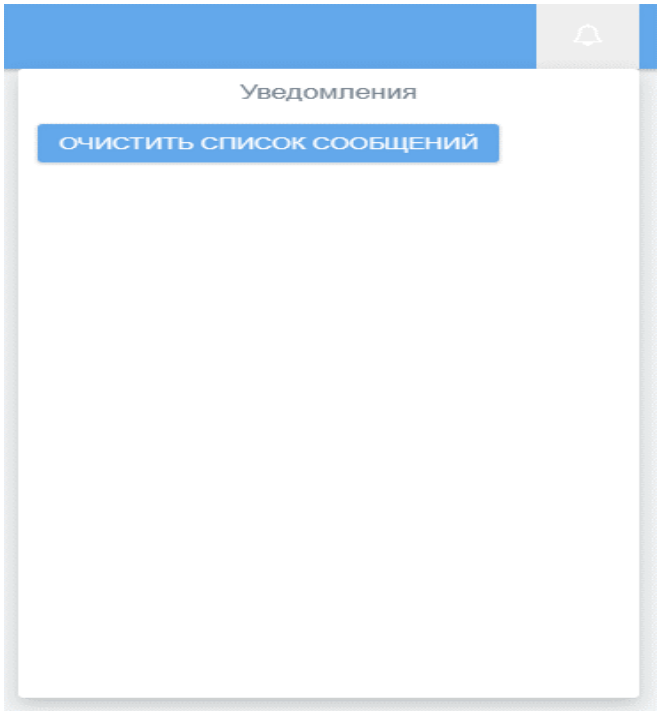


Рисунок 3 – Всплывающее окно «Уведомления»

Для очистки перечня уведомлений необходимо нажать кнопку « ОЧИСТИТЬ СПИСОК СООБЩЕНИЙ ».

2.2 Раздел «Система»

Раздел «Система» содержит следующие подразделы:

– «Начало» (стартовая страница);

– «Интерфейсы»;

– «Почта»;

– «Пользователи»;

– «Резервное копирование»;

– «Настройка меню»;

– «Автоматическое восстановление»;

– «Выключение»;

– «О программе».

2.2.1 Подраздел «Начало» (стартовая страница)

Подраздел «Начало» представлен в виде информационного окна (рисунок 4). Подраздел «Начало» (стартовая страница) отображает следующую информацию:

– текущее календарное время;

– длительность непрерывной работы сервера;

– количество пользователей на сервере;

– load average – средняя нагрузка;

– объем трафика на красных интерфейсах;

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

В случае изменений контрольных сумм выдается сообщение об ошибке (рисунок 5).

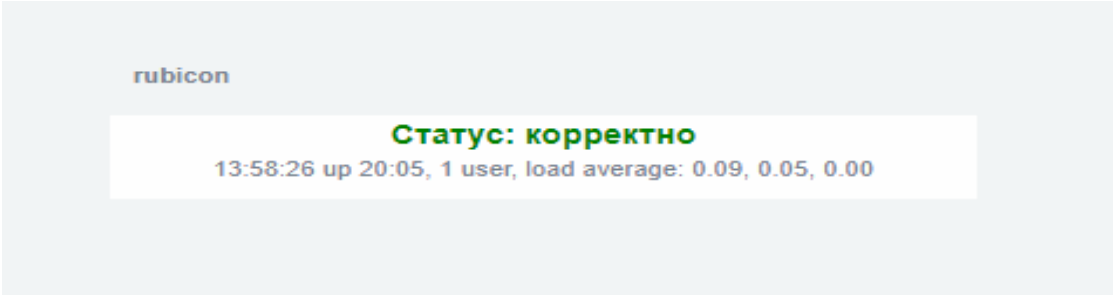


Рисунок 4 – Подраздел «Начало» (стартовая страница)

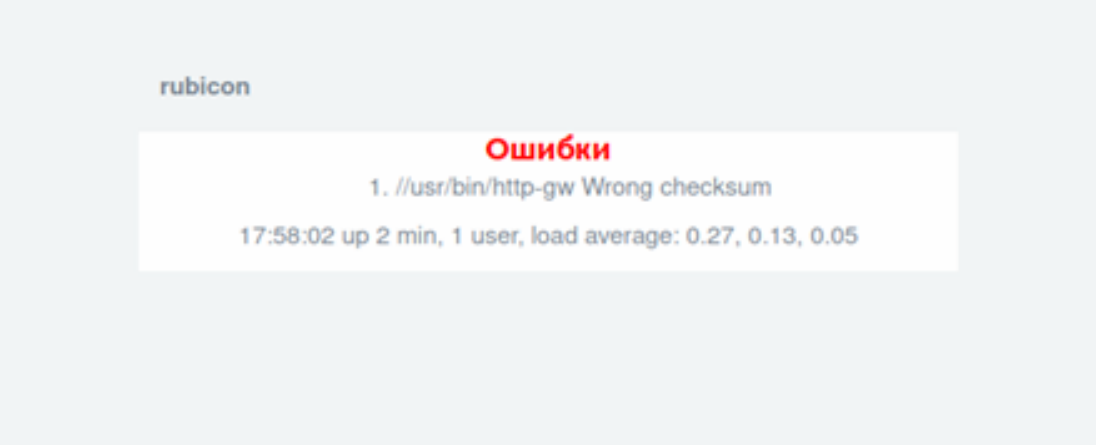


Рисунок 5 – Раздел «Система», подраздел «Начало» (стартовая страница). Сообщение об ошибке

При наличии одного и более красных интерфейсов в подразделе «Начало» отображаются функциональные кнопки (рисунок 6).

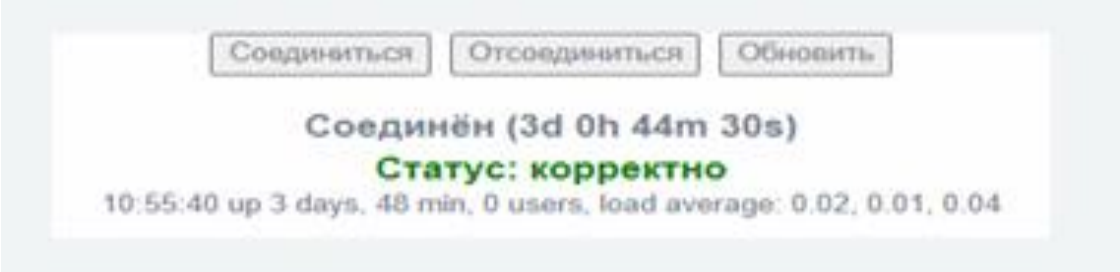


Рисунок 6 – Подраздел «Начало». Отображение функциональных кнопок

Подраздел «Начало» может отображать следующие кнопки, имеющие отношение к «красным» интерфейсам:

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

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

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

2.2.2 Подраздел «Интерфейсы»

Подраздел «Интерфейсы» (рисунок 7) предназначен для настройки сетевых интерфейсов.

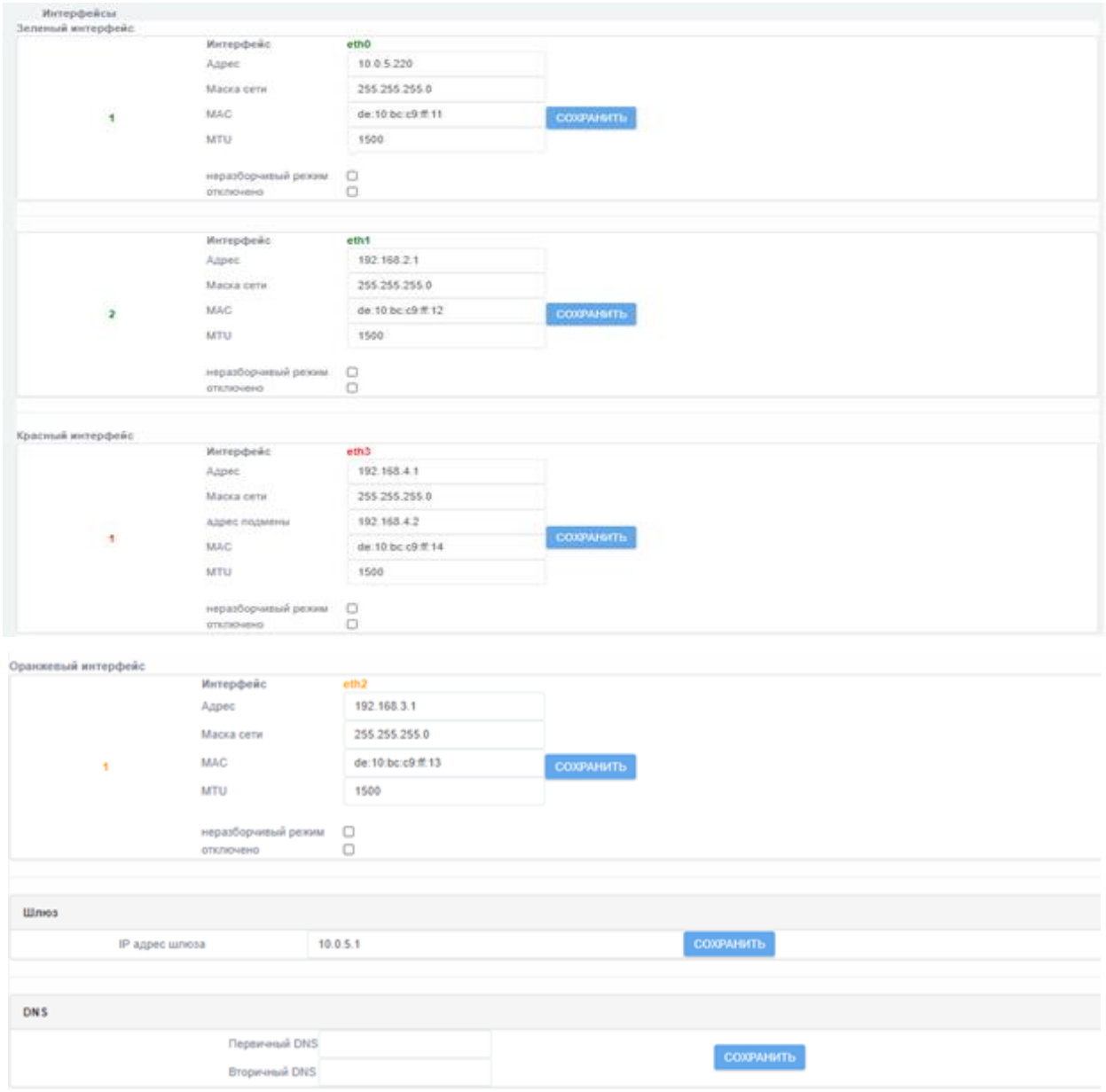


Рисунок 7 – Подраздел «Интерфейсы» раздела «Система»

В таблице 6 приведено описание полей подраздела «Интерфейсы».

Таблица 6 – Описание полей подраздела «Интерфейсы»

Название поля	**Краткое описание**
Интерфейсы	
Интерфейс	Название и тип интерфейса
Адрес	IP адрес интерфейса
Маска сети	Маска сети интерфейса
MAC	MAC адрес оборудования интерфейса
MTU	Максимальный размер пакета, передаваемого по сетям
Неразборчивый режим	Предназначен для включения режима приема всех сетевых пакетов, появляющихся на сетевом адаптере независимо от назначения
Отключено	Отключение интерфейса
Шлюз	
IP адрес шлюза	IP адрес шлюза
DNS	
Первичный DNS	IP адрес первичного DNS-сервера
Вторичный DNS	IP адрес вторичного DNS-сервера

Подраздел «Интерфейсы» содержит элементы, указанные в таблице 7.

Таблица 7 – Описание элементов подраздела «Интерфейсы»

Элемент	Описание
	Поле для ввода необходимой информации
	Пустое поле для проставления флажка
	Поле с проставленным флажком
	Кнопка «Сохранить» сохраняет введенную информацию

2.2.3 Подраздел «Почта»

Подраздел «Почта» (рисунок 8) предназначен для настройки процедур отправки уведомлений на заданные адреса электронной почты.

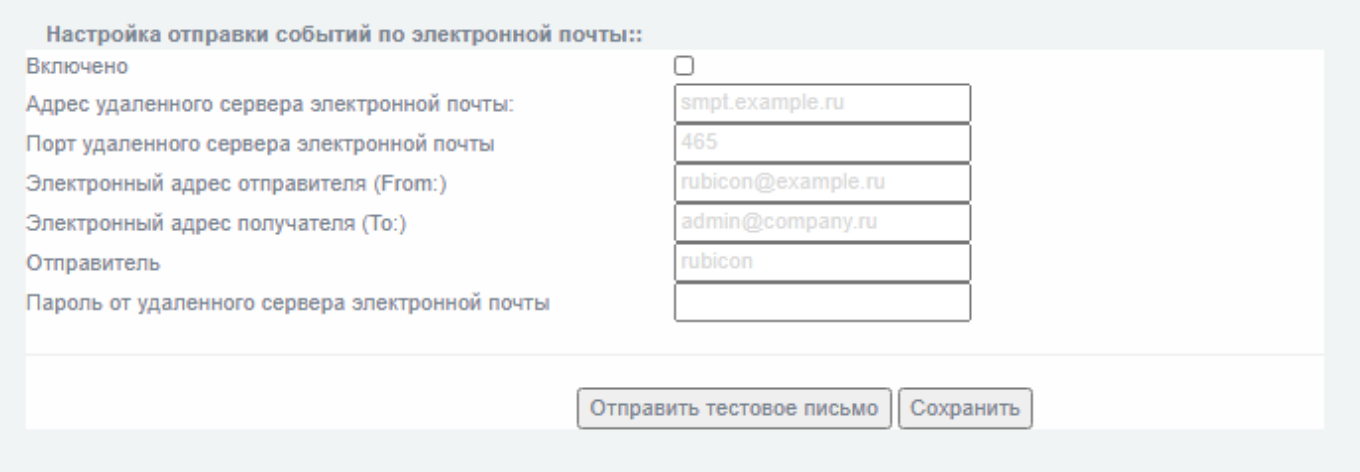


Рисунок 8 – Подраздел «Почта» раздела «Система»

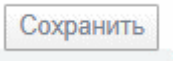
В таблице 8 представлено описание полей подраздела «Почта».

Таблица 8 – Описание полей подраздела «Почта»

Название поля	Краткое описание
Включено	Флажок включения / отключения отправки уведомлений на заданный почтовый адрес
Сервер электронной почты отправителя	Адрес сервера электронной почты отправителя
Порт удаленного сервера электронной почты	Порт сервера электронной почты отправителя
Электронный адрес отправителя (From:)	Адрес электронной почты отправителя
Электронный адрес получателя (To:)	Адрес электронной почты адресата
Отправитель	Имя отправителя
Пароль от удаленного сервера электронной почты	Пароль отправителя

Подраздел «Почта» содержит элементы, указанные в таблице 9.

Таблица 9 – Описание элементов подраздела «Почта»

Элемент	Описание
	Поле для ввода необходимой информации
	Пустое поле для проставления флажка
	Поле с проставленным флажком
	Кнопка, позволяющая отправить тестовое письмо
	Кнопка «Сохранить» сохраняет введенную информацию

2.2.4 Подраздел «Пользователи»

Подраздел «Пользователи» (рисунок 9) предназначен для управления учетными записями пользователей:

– создание нового пользователя;

– редактирование учетной записи пользователя;

– удаление учетной записи пользователя.

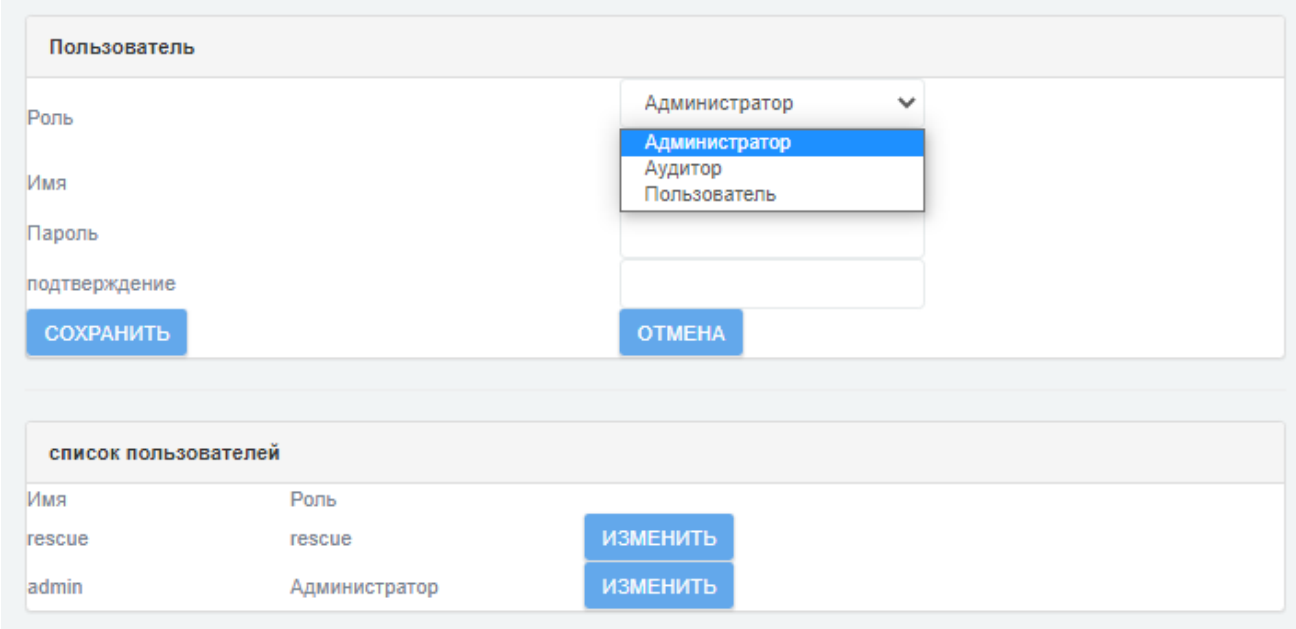


Рисунок 9 – Подраздел «Пользователи»

Для учетных записей пользователей предусмотрены следующие роли:

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

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

– «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 «Рубикону».

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

В таблице 10 приведено описание полей подраздела «Пользователи».

Таблица 10 – Описание полей подраздела «Пользователи»

Название поля	**Краткое описание**
Пользователь	
Роль	Поле выбора роли (администратор, аудитор или пользователь) для новой учетной записи или при редактировании существующей учетной записи
Имя	Имя для учетной записи
Пароль	Пароль для учетной записи
Подтверждение	Подтверждение пароля для учетной записи
Список пользователей	
Имя	Имя учетной записи
Роль	Роль учетной записи пользователя

Подраздел «Пользователи» содержит функциональные элементы, указанные в таблице 11.

Таблица 11 – Описание элементов подраздела «Пользователи»

Элемент	Описание
	Поле для ввода необходимой информации
СОХРАНИТЬ	Кнопка сохранения введенной информации
ОТМЕНА	Кнопка отмены изменений
ИЗМЕНИТЬ	Кнопка редактирования учетной записи
УДАЛИТЬ	Кнопка удаления учетной записи

2.2.5 Подраздел «Резервное копирование»

Подраздел «Резервное копирование» (рисунок 10) предназначен для управления резервными копиями. Функционально состоит из двух блоков: создания новой резервной копии и имеющихся резервных копий. Кнопки действий с резервными копиями появятся на экране **только после создания** хотя бы одной резервной копии.

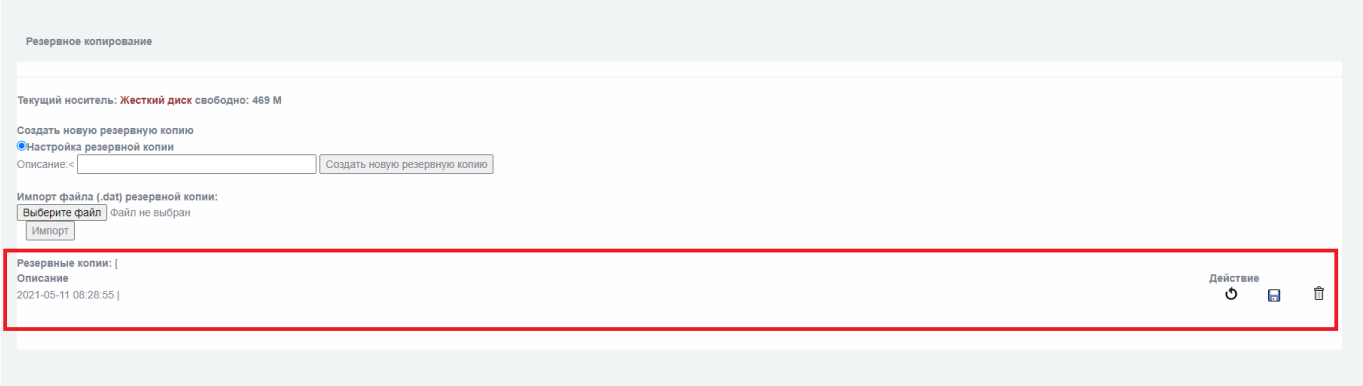


Рисунок 10 – Подраздел «Резервное копирование»

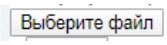
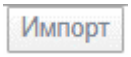
В таблице 12 приведено описание полей подраздела «Резервное копирование».

Таблица 12 – Описание полей подраздела «Резервное копирование»

Название поля	**Краткое описание**
Резервное копирование	
Текущий носитель	Описание текущего носителя для хранения резервной копии
Создать новую резервную копию	
Описание	Поле для ввода названия резервной копии
Резервные копии	
Описание	Краткое описание резервной копии (Дата создания, время, название)
Действие	Возможные действия для управления резервной копии

Подраздел «Резервное копирование» содержит элементы, указанные в таблице 13.

Таблица 13 – Описание элементов подраздела «Резервное копирование»

Элемент	**Описание**
	Поле для ввода необходимой информации
	Кнопка создания резервной копии
	Кнопка открытия формы выбора файла для загрузки
	Кнопка импорта выбранного файла
	Кнопка загрузки выбранной резервной копии
	Кнопка загрузки выбранной резервной копии на локальный жесткий диск
	Кнопка удаления резервной копии

2.2.6 Подраздел «Пакеты»

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

Пользователь должен 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» (рисунок 11).

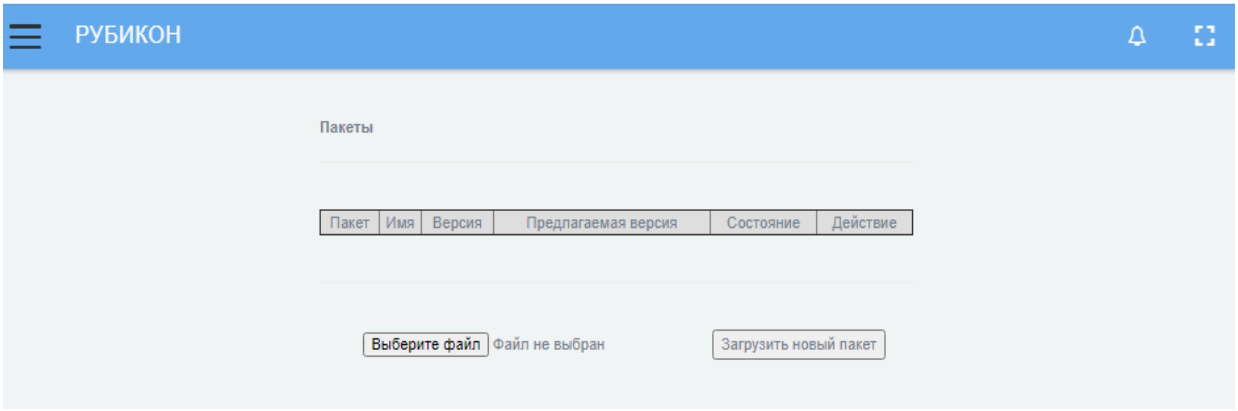


Рисунок 11 – Подраздел «Пакеты»

После загрузки пакета в файловую структуру изделия информация о пакете отобразится в отображаемой для пользователя таблице «Пакеты». В таблице указаны: имя файла пакета, название пакета, установленная в системе версия пакета для этого названия, предлагаемая пакетом версия, состояние (установлен или не установлен) и действие ( ), означающее возможность установки загруженного пакета. Для включения пакета в системе необходимо выбрать действие ( ). Описание активных элементов подраздела «Пакеты» представлено в таблице 14.

Таблица 14 – Описание активных элементов подраздела «Пакеты»

Элемент	Описание
Выберите файл	Кнопка выбора пакета из локального каталога пользователя
Загрузить новый пакет	Кнопка загрузки выбранного пакета

2.2.7 Подраздел «Настройка меню»

Подраздел «Настройка меню» раздела «Система» (рисунки 12 – 13) предназначен для включения и отключения отображения разделов и подразделов в навигационном меню.

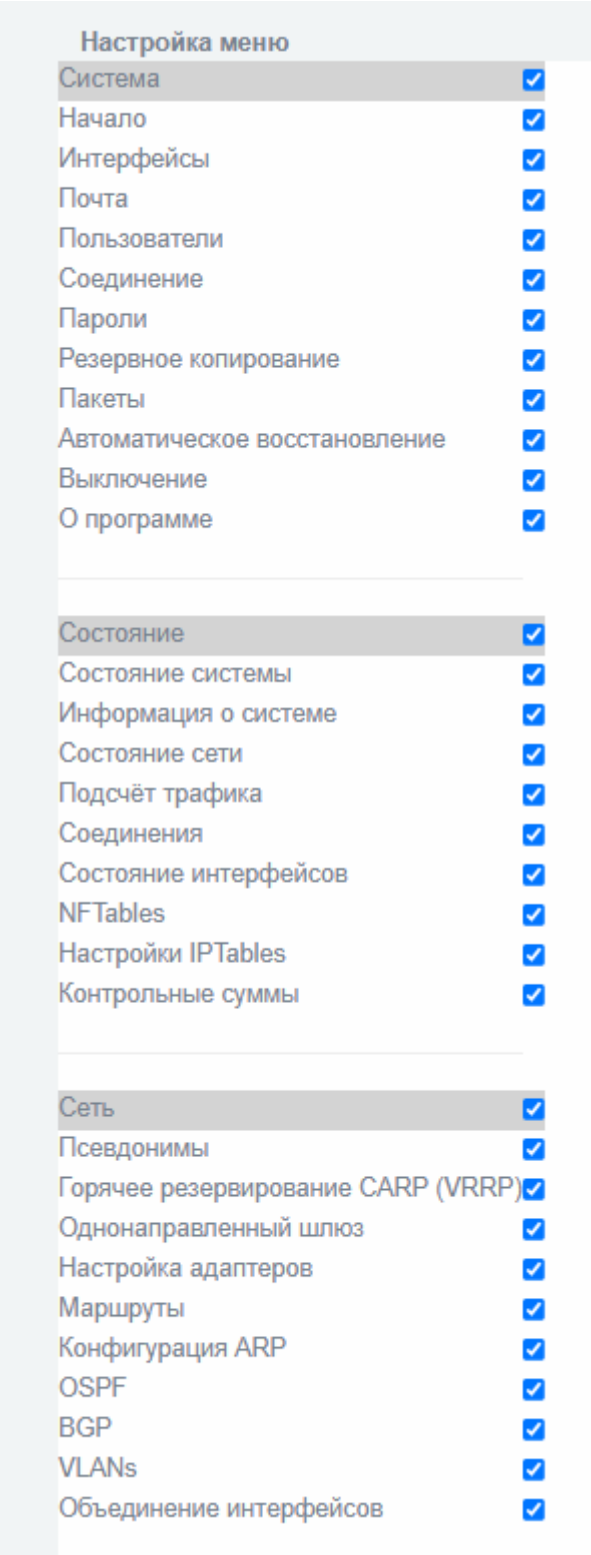


Рисунок 12 – Подраздел «Настройка меню». Часть 1

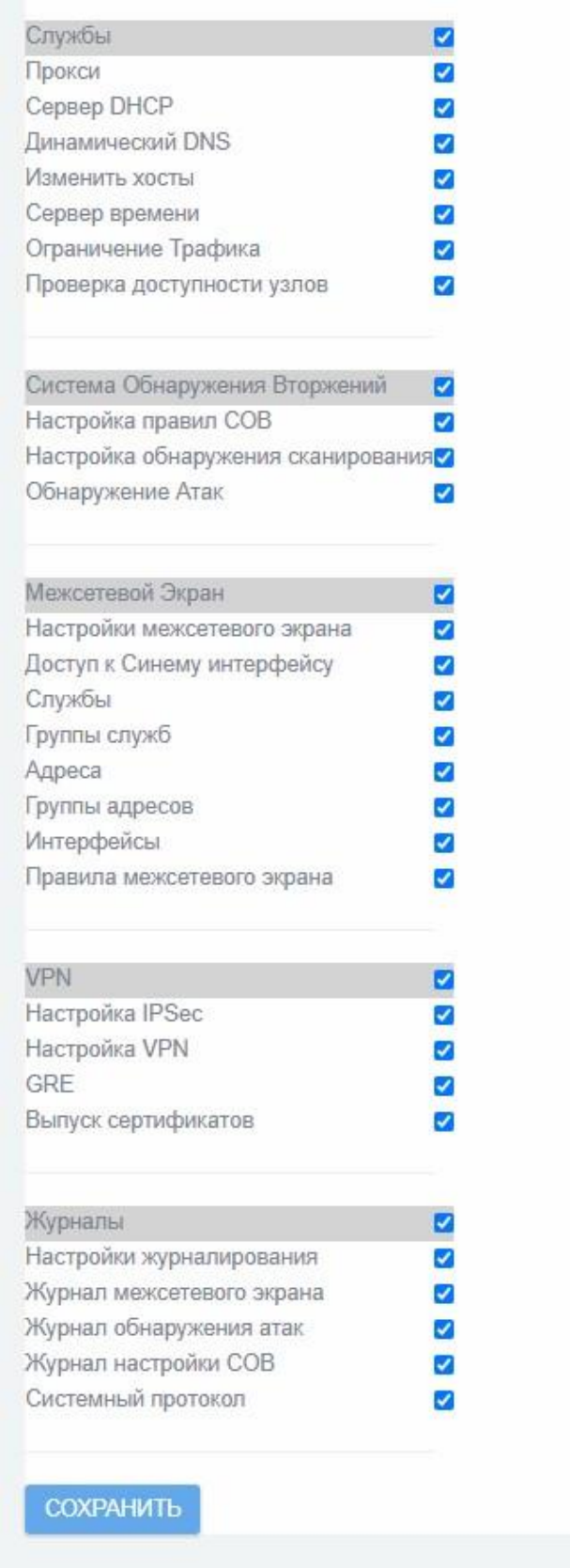
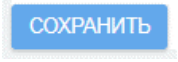


Рисунок 13 – Подраздел «Настройка меню». Часть 2

Подраздел «Настройка меню» содержит элементы, указанные в таблице 15.

Таблица 15 – Описание элементов подраздела «Настройка меню»

Элемент	Описание
	Пустое поле для проставления флажка
	Поле с проставленным флажком
	Кнопка «Сохранить» сохраняет введенную информацию

Примечание – Дополнительное расширение меню также предусмотрено в разделе «Межсетевой экран», посредством выбора опции (чекбокса) «Расширенный режим» в поле «Настройки» подраздела «Настройки межсетевого экрана».

2.2.8 Подраздел «Автоматическое восстановление»

Подраздел «Автоматическое восстановление» (рисунок 14) предназначен для настройки автоматических действий при возникновении указанных в подразделе неисправностях.

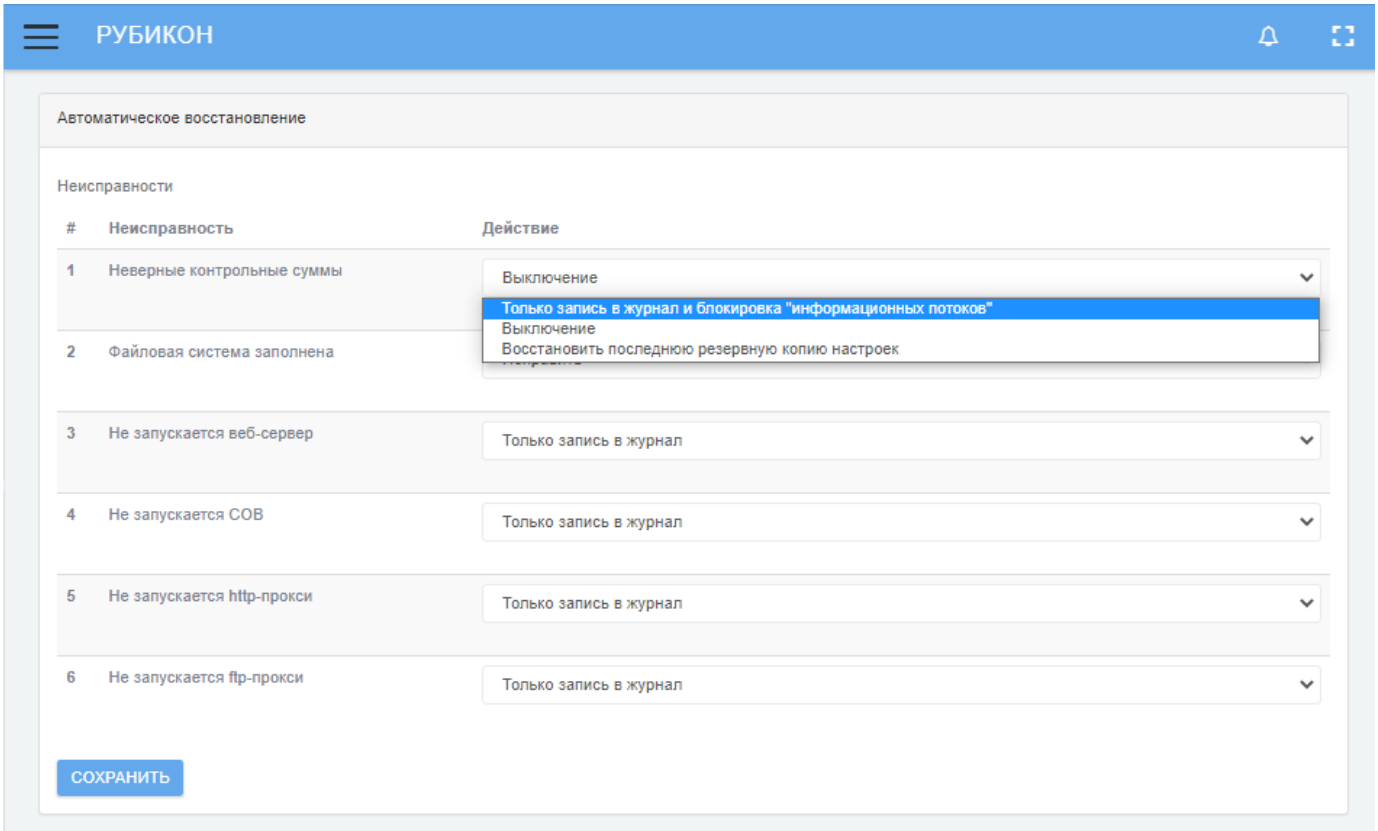


Рисунок 14 – Подраздел «Автоматическое восстановление»

В подразделе выделены следующие типы неисправностей:

– неверные контрольные суммы;

– файловая система заполнена;

– не запускается веб-сервер;

– не запускается СОВ;

– не запускается http-прокси;

– не запускается ftp-прокси.

Существуют следующие решения для автоматизации действий при возникновении указанной неисправности:

– только запись в журнал;

– только запись в журнал и блокировка информационных потоков;

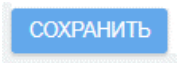
– исправить;

– выключение;

– восстановить последнюю резервную копию настроек.

Подраздел «Настройка меню» содержит элементы, указанные в таблице 16.

Таблица 16 – Описание элементов подраздела «Автоматическое восстановление»

Элемент	Описание
	Значок открытия ниспадающего списка
	Кнопка «Сохранить» сохраняет введенную информацию

2.2.9 Подраздел «Выключение»

Подраздел «Выключение» (рисунок 15) предназначен для программного выключения или перезагрузки аппаратной части изделия.

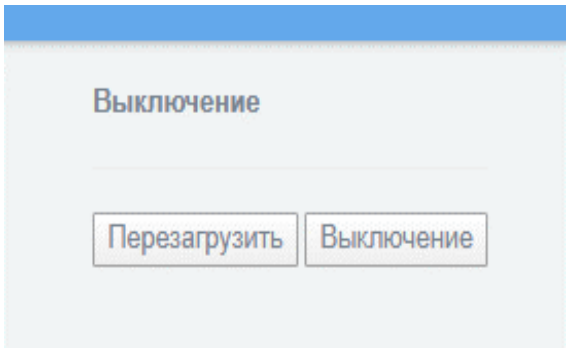


Рисунок 15 – Подраздел «Выключение»

Для перезагрузки «Рубикон» необходимо нажать кнопку «Перезагрузить».

Для выключения «Рубикон» необходимо нажать кнопку «Выключение».

2.2.10 Подраздел «О программе»

Подраздел «О программе» (рисунок 16) предназначен для отображения основной информации о ПО.

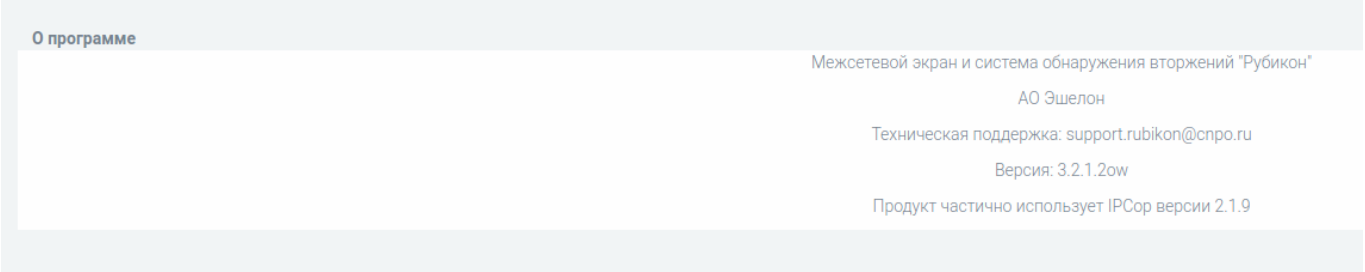


Рисунок 16 – Подраздел «О программе»

В подразделе отображается следующая информация:

– полное название программы;

– версия программы;

– электронная почта технической поддержки;

– версия используемых плагинов.

2.3 Раздел «Состояние»

Раздел «Состояние» содержит следующие подразделы:

– подраздел «Состояние системы»;

– подраздел «Информация о системе»;

– подраздел «Состояние сети»;

– подраздел «Подсчет трафика»;

– подраздел «Соединения»;

– подраздел «Состояние интерфейсов»;

– подраздел «IPTables»;

– подраздел «Контрольные суммы».

2.3.1 Подраздел «Состояние системы»

Подраздел «Состояние системы» (рисунок 17) предназначен для отображения полной информации о состоянии изделия, где установлен «Рубикон».

Рисунок 17 – Подраздел «Состояние системы»

Для удобства навигации по подразделу предусмотрены следующие вкладки:

– вкладка «Службы»;

– вкладка «Память»;

– вкладка «Использование диска»;

– вкладка «Использование структур inode»;

– вкладка «Время работы и пользователи»;

– вкладка «Версия ядра»;

– вкладка «Статистика журналов».

2.3.1.1 Вкладка «Службы»

Во вкладке «Службы» (рисунок 18) отображается перечень служб, объем используемой ими оперативной памяти, их статус (остановлен / запущен).

Рисунок 18 – Вкладка «Службы»

2.3.1.2 Вкладка «Память»

Во вкладке «Память» (рисунок 19) отображается информация о всех видах памяти в «Рубикон».

Память:

	Размер	Используется	свободно	Проценты	Общий	5.15 MB
RAM	996.34 MB	381.75 MB	138.98 MB	38%	буферы	475.61 MB
Подкачка	659.00 MB	44.13 MB	614.87 MB	6%	кэширован	447.69 MB

Рисунок 19 – Вкладка «Память»

Информация о памяти распределяется по следующим параметрам:

– «-» – наименование типа памяти;

– «Размер» – объем памяти;

– «Используется» – количество задействованной памяти;

– «Свободно» – количество свободной памяти;

– «Проценты» – процент используемой памяти на устройстве;

– «Общий» – объем общей памяти;

– «Буферы» – объем буферной памяти;

– «Кэширован» – объем кэш-памяти.

2.3.1.3 Вкладка «Использование диска»

Во вкладке «Использование диска» (рисунок 20) отображается информация о всех физических и виртуальных дисках.

Использование диска:

Устройство	Смонтирован на	Размер	Используется	свободно	Проценты
tmpfs	/run	99.64 MB	11.21 MB	88.43 MB	12%
/dev/sda1	/	1.34 GB	791.84 MB	512.16 MB	61%
tmpfs	/dev/shm	498.17 MB	0.00 KB	498.17 MB	0%
tmpfs	/run/lock	5.00 MB	0.00 KB	5.00 MB	0%
tmpfs	/sys/fs/cgroup	498.17 MB	0.00 KB	498.17 MB	0%
/dev/sda7	/store	14.68 GB	37.51 MB	13.89 GB	1%
/dev/sda6	/var	14.68 GB	87.55 MB	13.85 GB	1%

Рисунок 20 – Вкладка «Использование диска»

Информация о дисках распределяется по следующим параметрам:

– «Устройство» – название устройства;

– «Смонтирован на» – адрес устройства;

– «Размер» – размер диска;

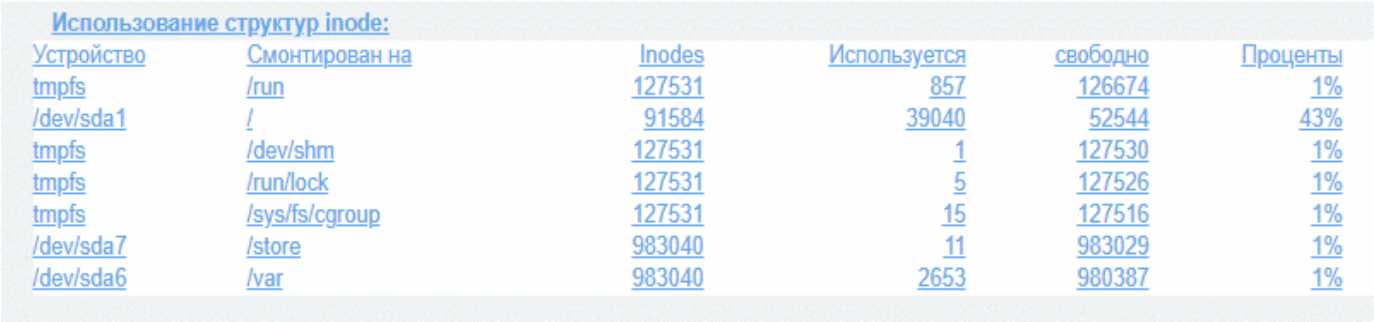
– «Используется» – используемое место на диске;

– «Свободно» – свободное место на диске;

– «Проценты» – процентное заполнение диска.

2.3.1.4 Вкладка «Использование структур inode»

Во вкладке «Использование структур inode» (рисунок 21) отображается информация об использовании структур с индексными дескрипторами.



Использование структур inode:

Устройство	Смонтирован на	Inodes	Используется	свободно	Проценты
tmpfs	/run	127531	857	126674	1%
/dev/sda1	/	91584	39040	52544	43%
tmpfs	/dev/shm	127531	1	127530	1%
tmpfs	/run/lock	127531	5	127526	1%
tmpfs	/sys/fs/cgroup	127531	15	127516	1%
/dev/sda7	/store	983040	11	983029	1%
/dev/sda6	/var	983040	2653	980387	1%

Рисунок 21 – Вкладка «Использование структур inode»

Информация об использовании структур с индексными дескрипторами распределяется по следующим параметрам:

– «Устройство» – название устройства;

– «Смонтирован на» – адрес устройства;

– «inodes» – количество индексных дескрипторов;

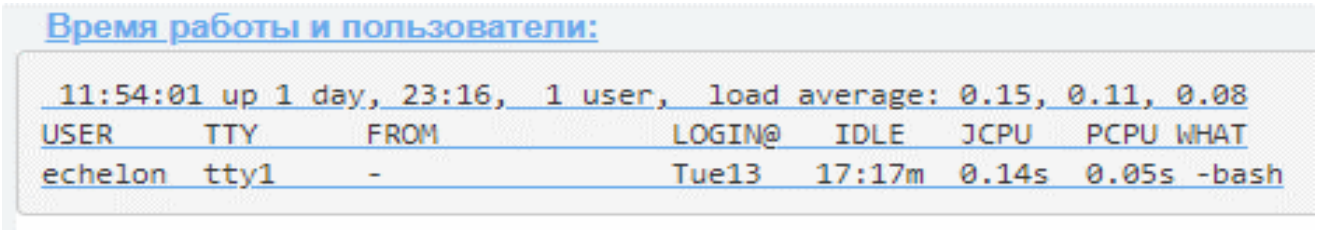
– «Используется» – используется дескрипторов;

– «Свободно» – свободно дескрипторов;

– «Проценты» – процентное соотношение используемых дескрипторов.

2.3.1.5 Вкладка «Время работы и пользователи»

Во вкладке «Время работы и пользователи» (рисунок 22) отображается информация о времени беспрерывной работы «Рубикон» и количестве пользователей в сети.



Время работы и пользователи:

```
 11:54:01 up 1 day, 23:16,  1 user,  load average: 0.15, 0.11, 0.08
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
echelon  tty1     -                Tue13   17:17m  0.14s  0.05s -bash
```

Рисунок 22 – Вкладка «Время работы и пользователи»

2.3.1.6 Вкладка «Версия ядра»

Во вкладке «Версия ядра» (рисунок 23) отображается информация о версии ядра.

Рисунок 23 – Вкладка «Версия ядра»

2.3.1.7 Вкладка «Статистика журналов»

Во вкладке «Статистика журналов» (рисунок 24) отображается информация о журналах.

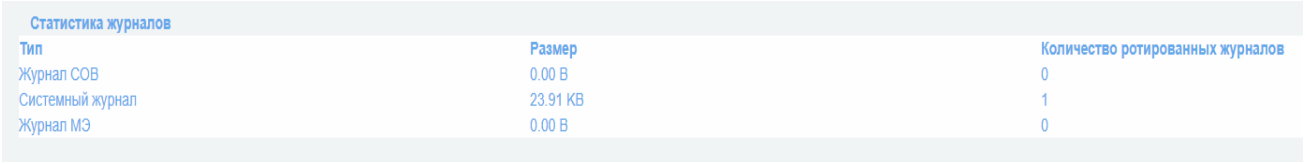


Рисунок 24 – Поле «Статистика журналов»

Информация о журналах распределяется по следующим параметрам:

– «Тип» – тип журнала;

– «Размер» – размер журнала;

– «Количество ротированных журналов» – количество ротаций журнала.

2.3.2 Подраздел «Информация о системе»

Подраздел «Информация о системе» (рисунок 25) предназначен для отображения подробной информации о физических компонентах.

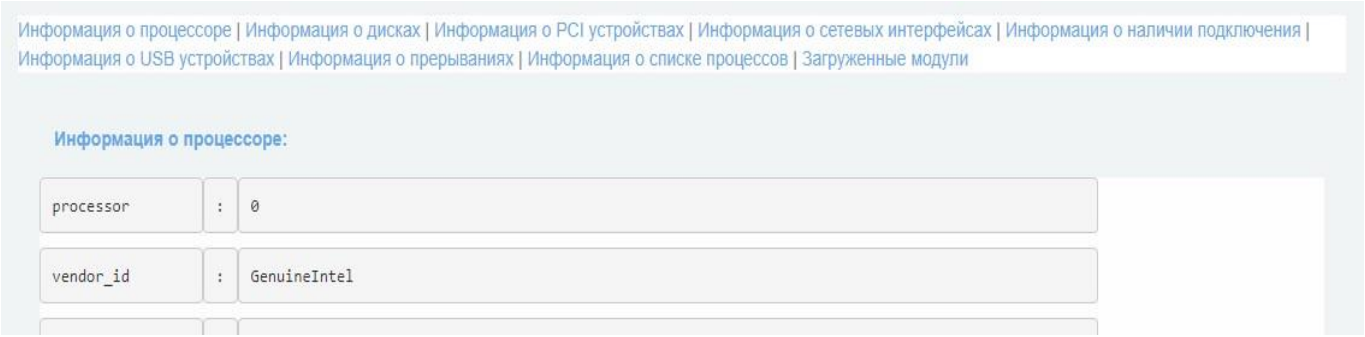


Рисунок 25 – Подраздел «Информация о системе»

Для удобства навигации по подразделу предусмотрены следующие вкладки, расположенные в верхней части интерфейсного окна:

– вкладка «Информация о процессоре»;

– вкладка «Информация о жестких дисках»;

– вкладка «Информация о PCI устройствах»;

– вкладка «Информация о сетевых интерфейсах»;

– вкладка «Информация о наличии подключения»;

– вкладка «Информация о USB устройствах»;

– вкладка «Информация о прерываниях»;

– вкладка «Информация о списке процессов»;

– вкладка «Загруженные модули»;

– вкладка «Системные переменные».

При нажатии на вкладку, экран переносится на соответствующее поле с информацией.

2.3.2.1 Вкладка «Информация о процессоре»

Во вкладке «Информация о процессоре» (рисунок 26) отображается полная техническая информация о процессоре.

Рисунок 26 – Вкладка «Информация о процессоре»

2.3.2.2 Вкладка «Информация о жестких дисках»

Во вкладке «Информация о жестких дисках» (рисунок 27) отображается техническая информация о подключенных физических жестких дисках.

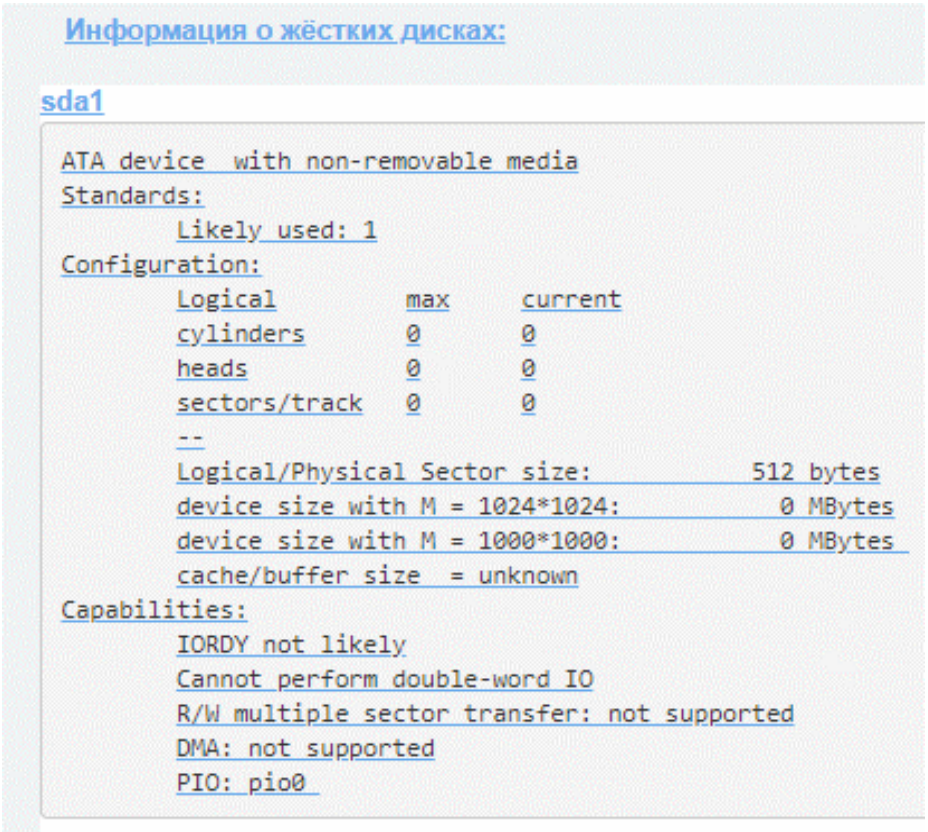


Рисунок 27 – Вкладка «Информация о дисках»

Информация по каждому жесткому диску отображается отдельным полем.

2.3.2.3 Вкладка «Информация о PCI устройствах»

Во вкладке «Информация о PCI устройствах» (рисунок 28) отображается информация о подключенных устройствах к шине PCI.

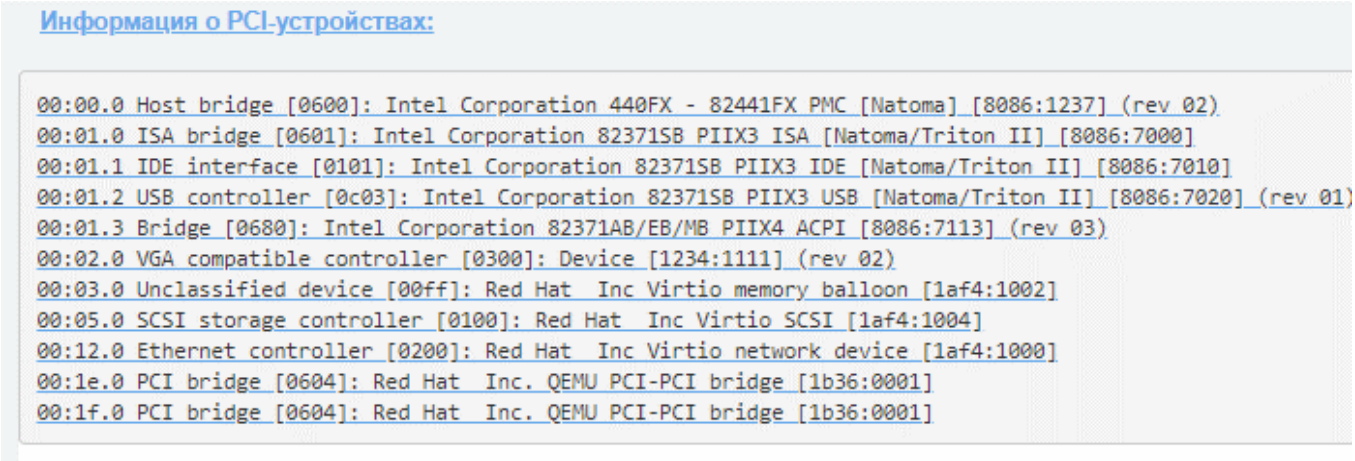


Рисунок 28 – Вкладка «Информация о PCI устройствах»

2.3.2.4 Вкладка «Информация о сетевых интерфейсах»

Во вкладке «Информация о сетевых интерфейсах» (рисунок 29) отображается информация о сетевых контроллерах.

Рисунок 29 – Вкладка «Информация о сетевых интерфейсах»

2.3.2.5 Вкладка «Информация о наличии подключения»

Во вкладке «Информация о наличии подключения» (рисунок 30) приведена информация о подключении по сетевым интерфейсам.

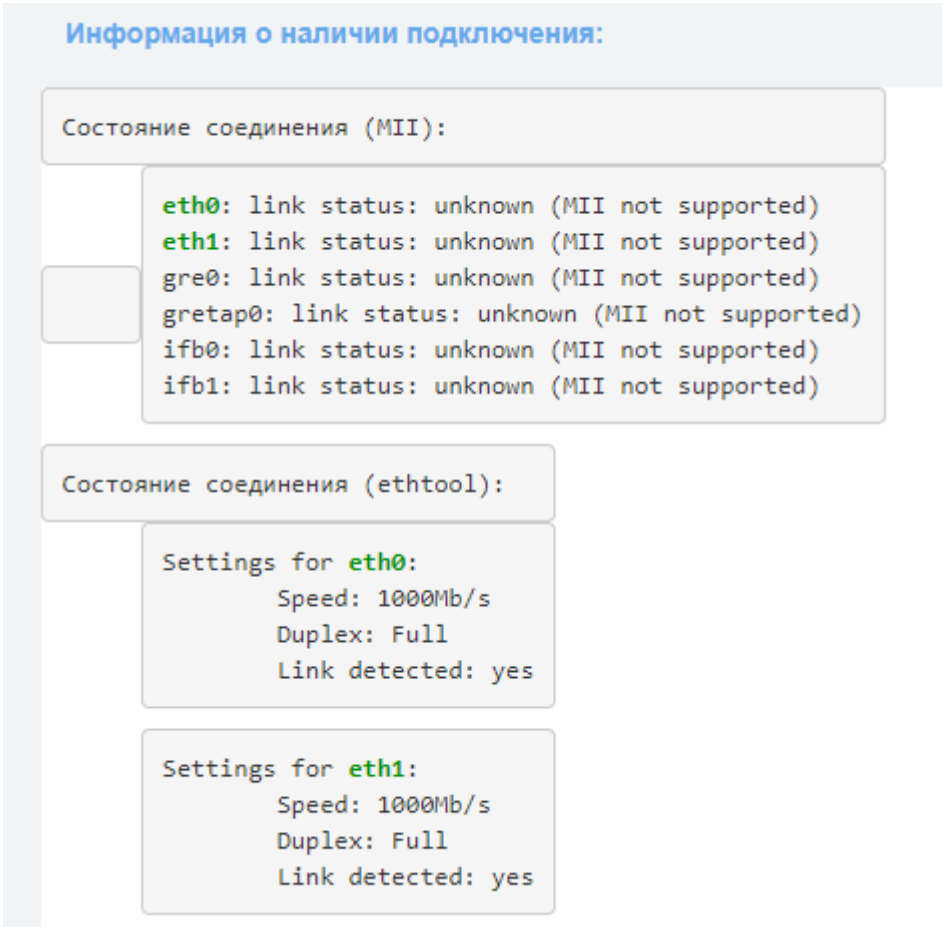


Рисунок 30 – Вкладка «Информация о наличии подключения»

2.3.2.6 Вкладка «Информация о USB устройствах»

Во вкладке «Информация о USB устройствах» (рисунок 31) приведена информация о подключениях по портам USB.

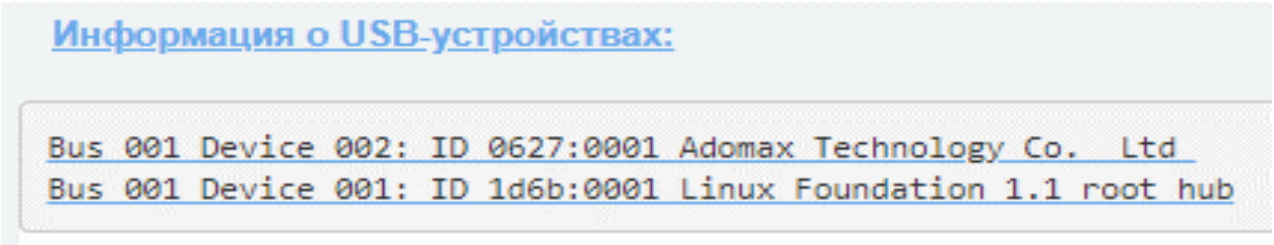


Рисунок 31 – Вкладка «Информация о USB устройствах»

2.3.2.7 Вкладка «Информация о прерываниях»

Во вкладке «Информация о прерываниях» (рисунок 32) приведена информация о прерываниях.

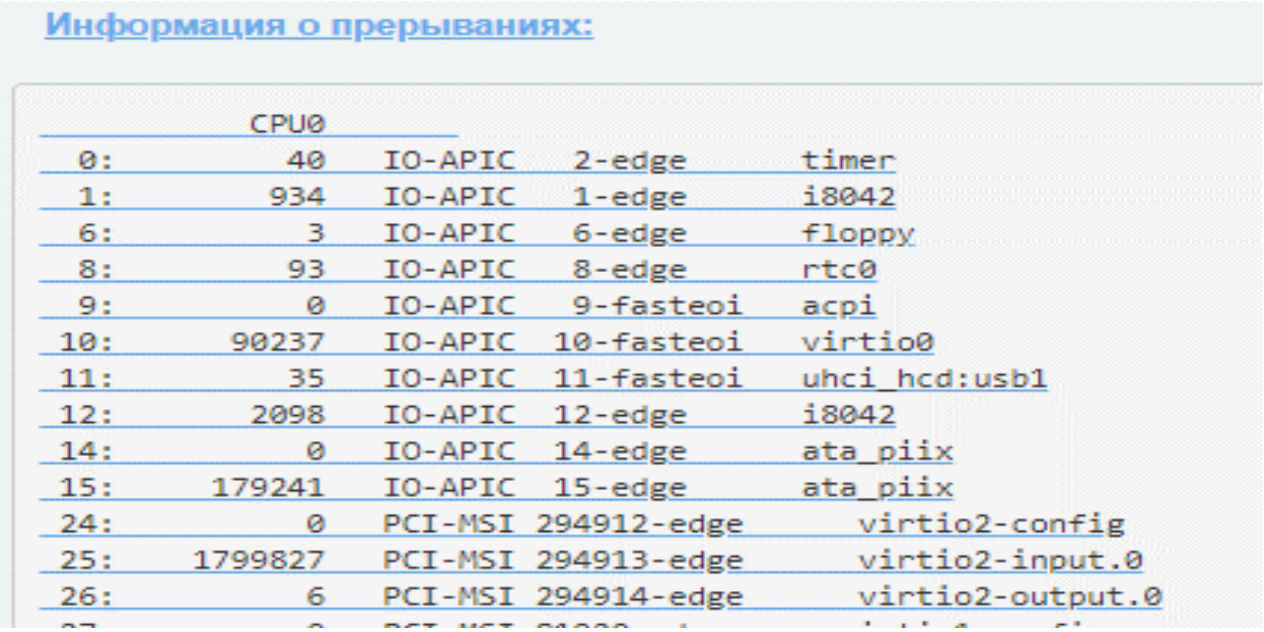


Рисунок 32 – Вкладка «Информация о прерываниях»

2.3.2.8 Вкладка «Информация о списке процессов»

Во вкладке «Информация о списке процессов» (рисунок 33) приводится информация о всех программных процессах, запущенных в изделии.

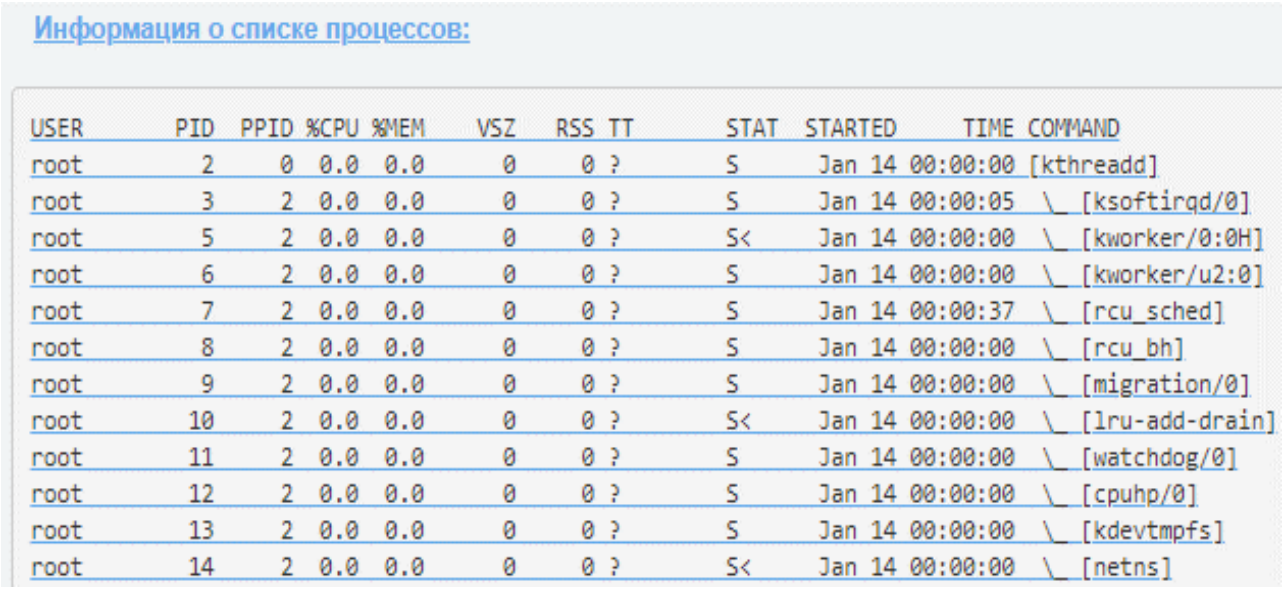


Рисунок 33 – Вкладка «Информация о списке процессов»

Информация о списке программных процессов распределяется по следующим параметрам:

– «USER» – имя пользователя, запустившего процесс;

– «PID» – идентификатор процесса;

– «PPID» – идентификатор родительского процесса;

– «%CPU» – процент использования процессорной мощности;

– «%MEM» – процент использования памяти;

– «VSZ» – размер виртуальной памяти;

– «RSS» – размер задействованной оперативной памяти;

– «TT» – терминал TTY;

– «STAT» – текущее стояние процесса;

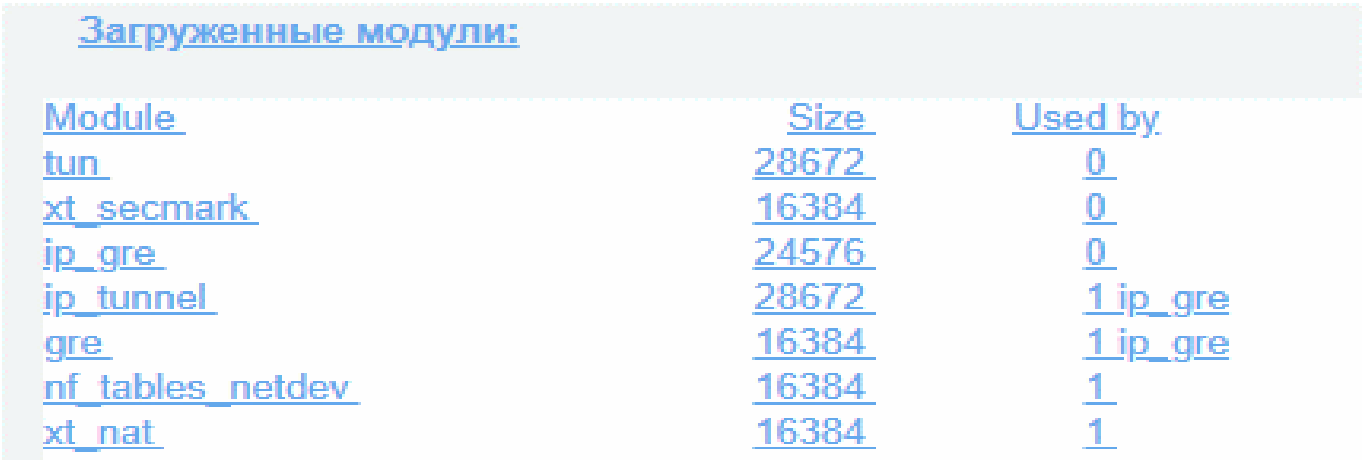
– «STARTED» – время начала процесса;

– «TIME» – время работы процесса;

– «COMMAND» – префикс процесса.

2.3.2.9 Вкладка «Загруженные модули»

Во вкладке «Загруженные модули» (рисунок 34) приводится информация о всех загруженных модулях.


Загруженные модули:

Module	Size	Used by
tun	28672	0
xt_secmark	16384	0
ip_gre	24576	0
ip_tunnel	28672	1 ip_gre
gre	16384	1 ip_gre
nf_tables_netdev	16384	1
xt_nat	16384	1

Рисунок 34 – Вкладка «Загруженные модули»

Информация о загруженных модулях распределяется по следующим параметрам:

– «Module» – название модуля;

– «Size» – размер модуля;

– «Used by» – используется сетевым интерфейсом.

2.3.2.10 Вкладка «Системные переменные»

Во вкладке «Системные переменные» (рисунок 35) приводится информация о системных переменных.

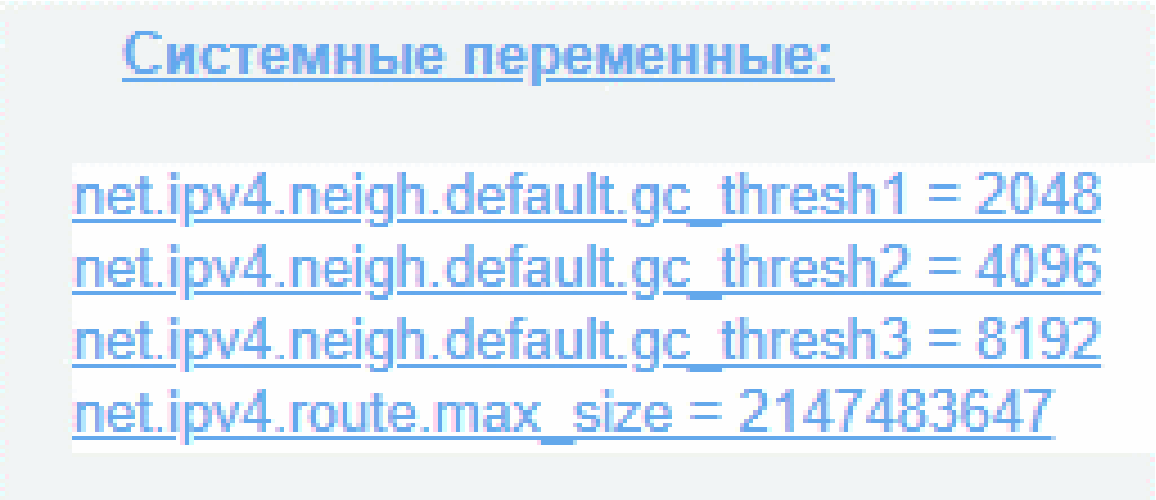


Рисунок 35 – Вкладка «Системные переменные»

2.3.3 Подраздел «Состояние сети»

Подраздел «Состояние сети» (рисунок 36) предназначен для отображения информации по всем сетевым интерфейсам.

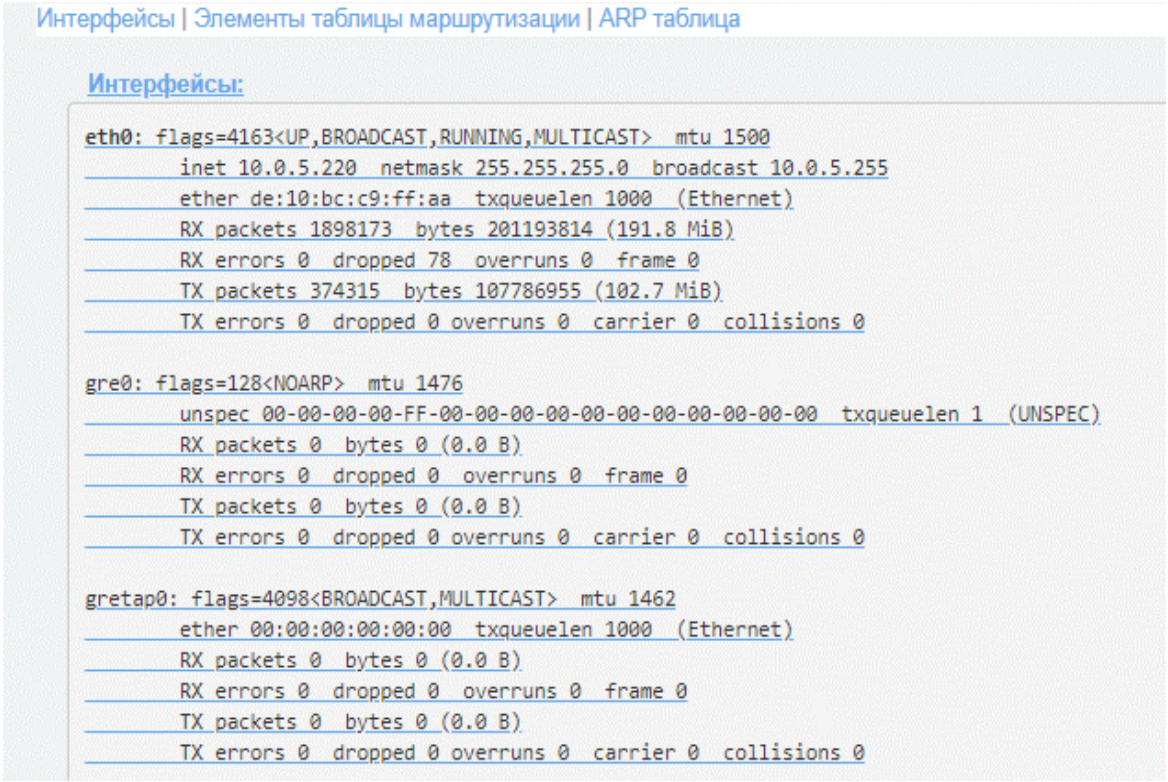


Рисунок 36 – Подраздел «Состояние сети»

Для удобства навигации по подразделу предусмотрены следующие вкладки:

– вкладка «Интерфейсы»;

– вкладка «Элементы таблицы маршрутизации»;

– вкладка «ARP таблица».

При нажатии на вкладку, экран переносится на соответствующее поле с информацией.

2.3.3.1 Вкладка «Интерфейсы»

Во вкладке «Интерфейсы» (рисунок 37) представлена информация по всем сетевым интерфейсам.

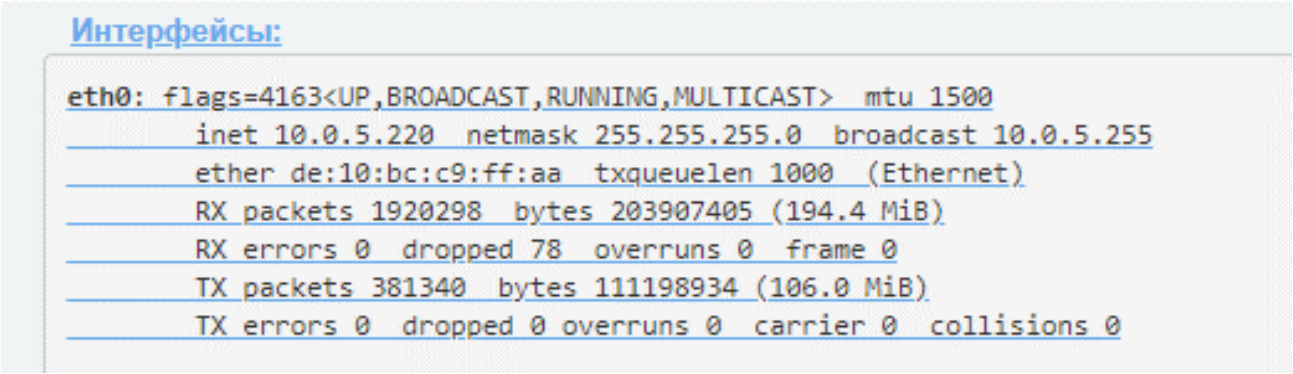


Рисунок 37 – Вкладка «Интерфейсы»

Информация приводится по каждому сетевому интерфейсу.

2.3.3.2 Вкладка «Элементы таблицы маршрутизации»

Во вкладке «Элементы таблицы маршрутизации» (рисунок 38) приведена информация по всем таблицам маршрутизации.

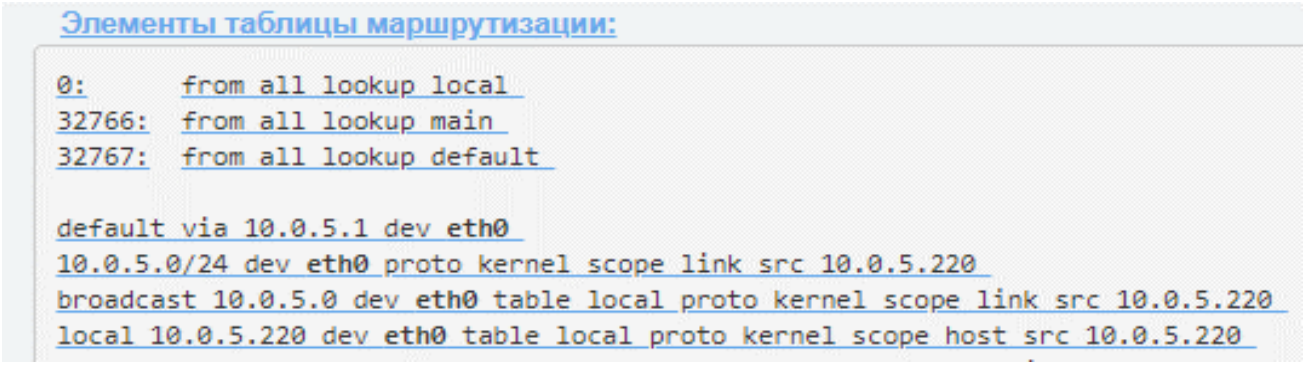


Рисунок 38 – Вкладка «Элементы таблицы маршрутизации»

2.3.3.3 Вкладка «ARP таблица»

Во вкладке «ARP таблица» (рисунок 39) приведена информация по всем MAC-адресам, привязанным к IP-адресам.

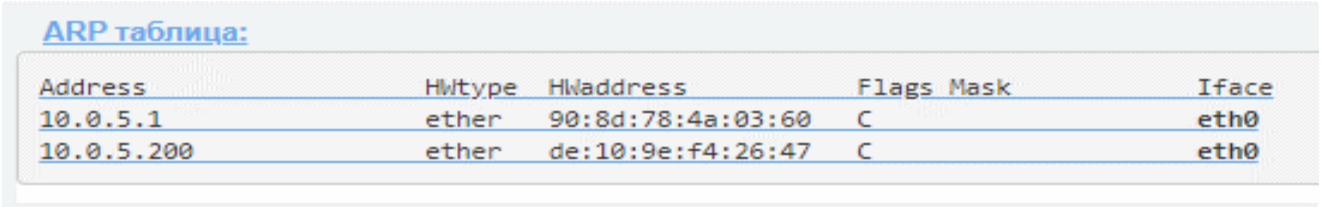


Рисунок 39 – Поле «ARP таблица»

Информация о ARP-таблицах распределяется по следующим параметрам:

– «Address» – IP-адрес устройства;

– «HWtype» – тип устройства;

– «HWaddress» – MAC-адрес устройства;

– «Flags Mask» – тип записи;

– «Iface» – название интерфейса.

2.3.4 Подраздел «Подсчет трафика»

Подраздел «Подсчет трафика» (рисунок 40) предназначен для отображения количества трафика в детализации по аппаратным сетевым интерфейсам за определенный период времени.

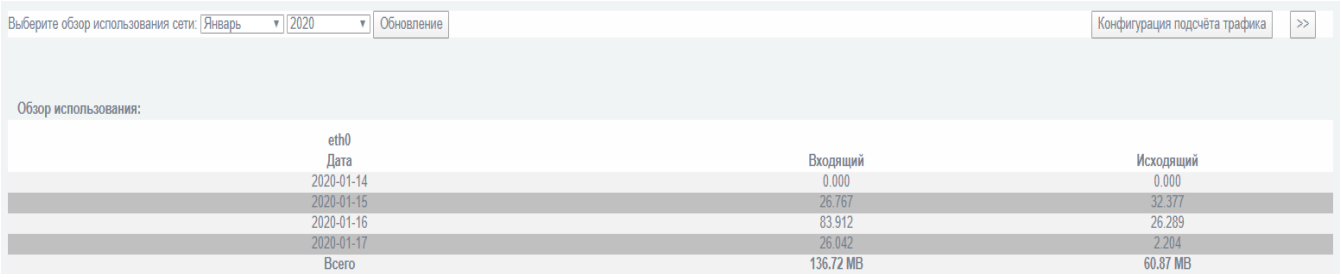


Рисунок 40 – Подраздел «Подсчет трафика»

Информация по подсчету трафика распределяется по следующим параметрам:

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

– «Входящий» – количество входящего трафика;

– «Исходящий» – количество исходящего трафика.

Для удобства просмотра предусмотрена возможность деления таблицы подсчета трафика на главной странице подраздела в период 1 месяц (рисунок 41).

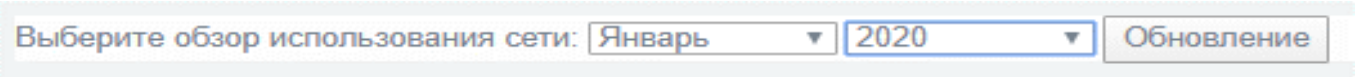
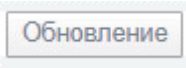


Рисунок 41 – Строка настройки деления таблицы подсчета трафика

Для этого необходимо выбрать интересующий период и нажать кнопку «Обновление».

Подраздел «Подсчет трафика» содержит элементы, указанные в таблице 17.

Таблица 17 – Описание элементов подраздела «Подсчет трафика»

Элемент	Описание
	Значок раскрытия ниспадающего списка
	Кнопка обновления таблицы подсчета трафика
	Кнопка открытия меню «Конфигурации подсчета трафика»
	Кнопка перехода к подробному подсчету трафика

2.3.4.1 Меню «Конфигурация подсчета трафика»

Меню «Конфигурация подсчета трафика» (рисунок 42) предназначено для настройки функции подсчета трафика и отображения результатов подсчета.

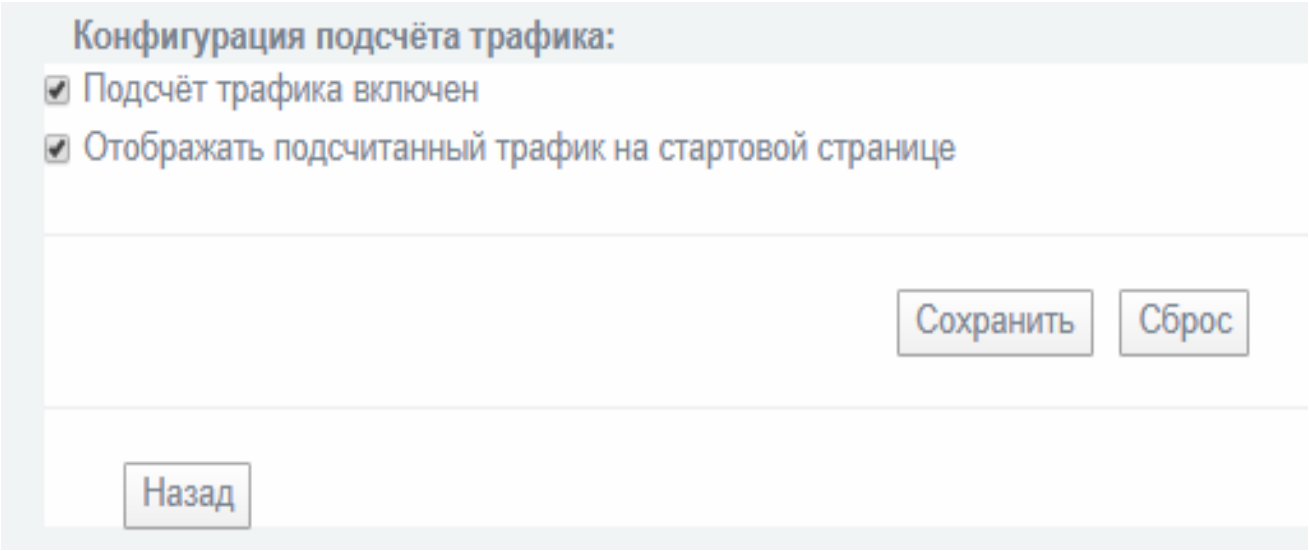


Рисунок 42 – Меню «Конфигурация подсчета трафика»

Меню «Конфигурация подсчета трафика» содержит элементы, указанные в таблице 18.

Таблица 18 – Описание элементов меню «Конфигурация подсчета трафика»

Элемент	Описание
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Кнопка сохранения измененных параметров меню
	Кнопка сброса настроек меню до заводских параметров
	Кнопка возвращение в подраздел «Подсчет трафика»

Меню «Конфигурация подсчета трафика» имеет следующие варианты настройки:

– «Подсчет трафика включен» – включение функции подсчета трафика;

– «Отображать подсчитанный трафик на стартовой странице» – Включение отображения результатов подсчета трафика в подразделе «Начало» (стартовая страница) (рисунок 43).

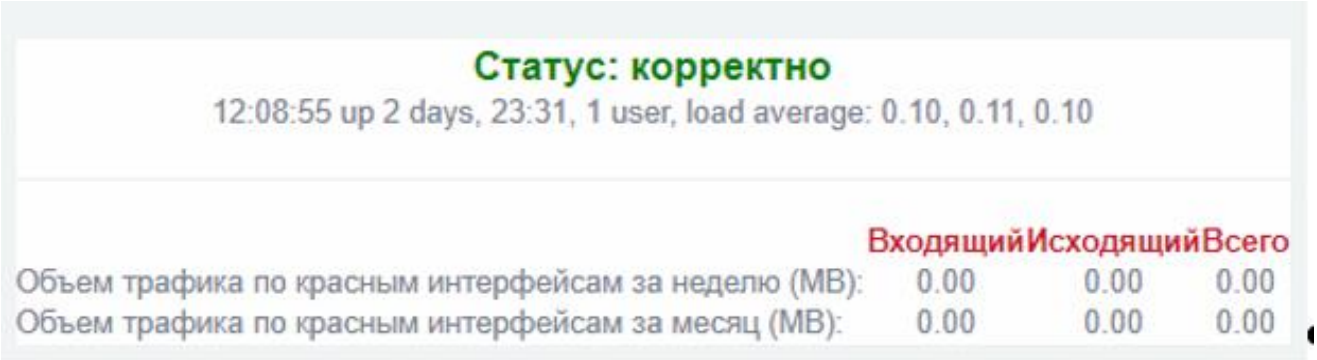


Рисунок 43 – Отображение результатов подсчета трафика в подразделе «Начало» (стартовая страница)

2.3.4.2 Подробный подсчет трафика

Подробный подсчет трафика предполагает подсчет входящего и исходящего трафика за период от одного календарного дня. Для просмотра подробного подсчета трафика необходимо нажать кнопку [>>] в подразделе «Подсчет трафика» (рисунок 44).

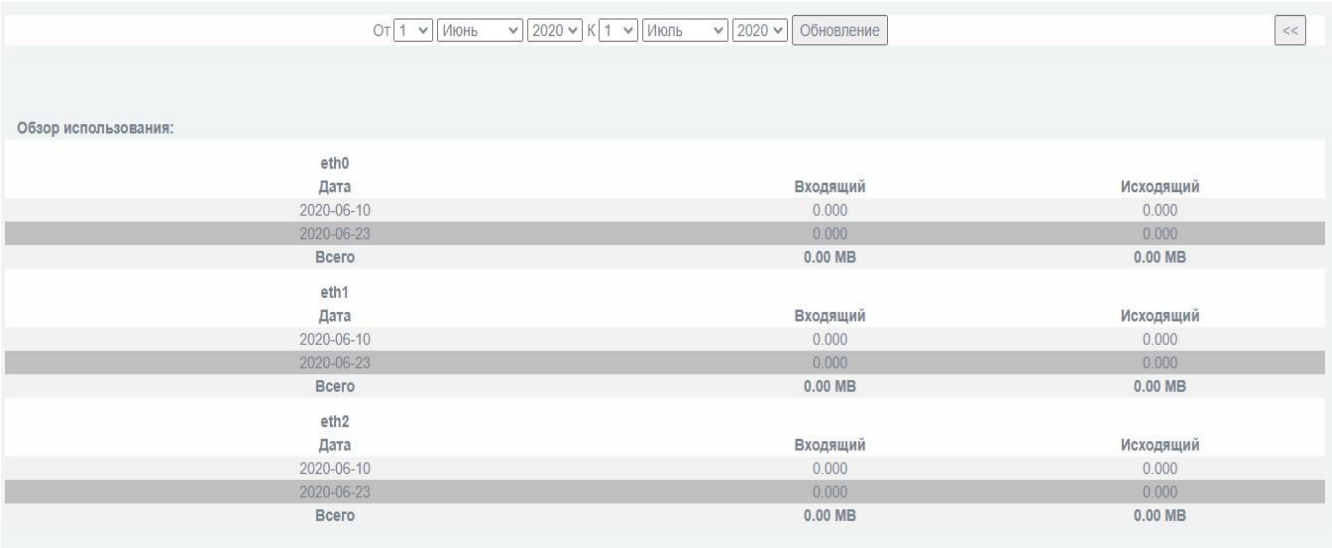


Рисунок 44 – Подробный подсчет трафика

Информация по подробному подсчету трафика распределяется по следующим параметрам:

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

– «Входящий» – количество входящего трафика;

– «Исходящий» – количество исходящего трафика.

Для подсчета входящего и исходящего трафика необходимо выбрать интересующий период и нажать кнопку «Обновление».

Кнопка «<<» осуществляет переход к подразделу «Подсчет трафика».

2.3.5 Подраздел «Соединения»

Подраздел «Соединения» (рисунки 46 – 47) предназначен для отображения информации об активных соединениях.

Информационная таблица подраздела отображается по следующим типам:

– «Состояние»;

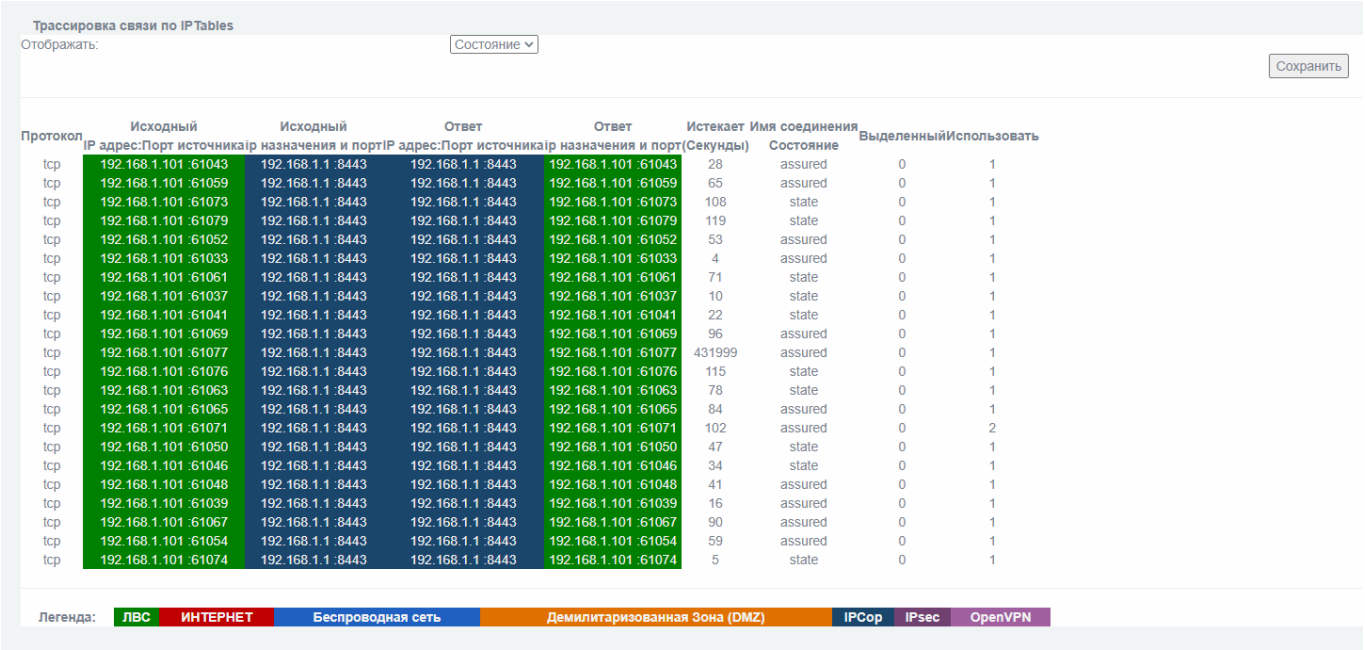
– «Трафик».

Для переключения между типами таблиц необходимо выбрать соответствующий тип в поле (рисунок 45) и нажать кнопку «Сохранить».

Рисунок 45 – Поле типа таблицы

2.3.5.1 Таблица «Состояние»

Таблица «Состояние» (рисунок 46) отображает актуальное состояние действующих соединений.



Протокол	Исходный IP адрес:Порт источника	Исходный IP назначения и порт	Ответ IP адрес:Порт источника	Ответ IP назначения и порт	Истекает (Секунды)	Имя соединения Состояние	Выделенный	Использовать
tcp	192.168.1.101 :61043	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61043	28	assured	0	1
tcp	192.168.1.101 :61059	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61059	65	assured	0	1
tcp	192.168.1.101 :61073	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61073	108	state	0	1
tcp	192.168.1.101 :61079	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61079	119	state	0	1
tcp	192.168.1.101 :61052	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61052	53	assured	0	1
tcp	192.168.1.101 :61033	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61033	4	assured	0	1
tcp	192.168.1.101 :61061	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61061	71	state	0	1
tcp	192.168.1.101 :61037	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61037	10	state	0	1
tcp	192.168.1.101 :61041	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61041	22	state	0	1
tcp	192.168.1.101 :61069	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61069	96	assured	0	1
tcp	192.168.1.101 :61077	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61077	431999	assured	0	1
tcp	192.168.1.101 :61076	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61076	115	state	0	1
tcp	192.168.1.101 :61063	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61063	78	state	0	1
tcp	192.168.1.101 :61065	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61065	84	assured	0	1
tcp	192.168.1.101 :61071	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61071	102	assured	0	2
tcp	192.168.1.101 :61050	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61050	47	state	0	1
tcp	192.168.1.101 :61046	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61046	34	state	0	1
tcp	192.168.1.101 :61048	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61048	41	assured	0	1
tcp	192.168.1.101 :61039	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61039	16	assured	0	1
tcp	192.168.1.101 :61067	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61067	90	assured	0	1
tcp	192.168.1.101 :61054	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61054	59	assured	0	1
tcp	192.168.1.101 :61074	192.168.1.1 :8443	192.168.1.1 :8443	192.168.1.101 :61074	5	state	0	1

Рисунок 46 – Подраздел «Соединения». Таблица «Состояние»

Информация по соединениям распределяется по следующим параметрам:

– «Протокол» – название протокола соединения;

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

– «Исходный IP назначения и порт» – ответ от адреса и порта назначения;

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

– «Ответ IP назначения и порт» – ответ с адреса и порта назначения;

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

– «Имя соединения Состояние» – состояние соединения;

– «Выделенный» – принадлежность к выделенным каналам;

– «Использовать» – использовано ли на данный момент.

2.3.5.2 Таблица «Трафик»

Таблица «Трафик» (рисунок 47) подсчитывает количество переданных пакетов в действующих соединениях.

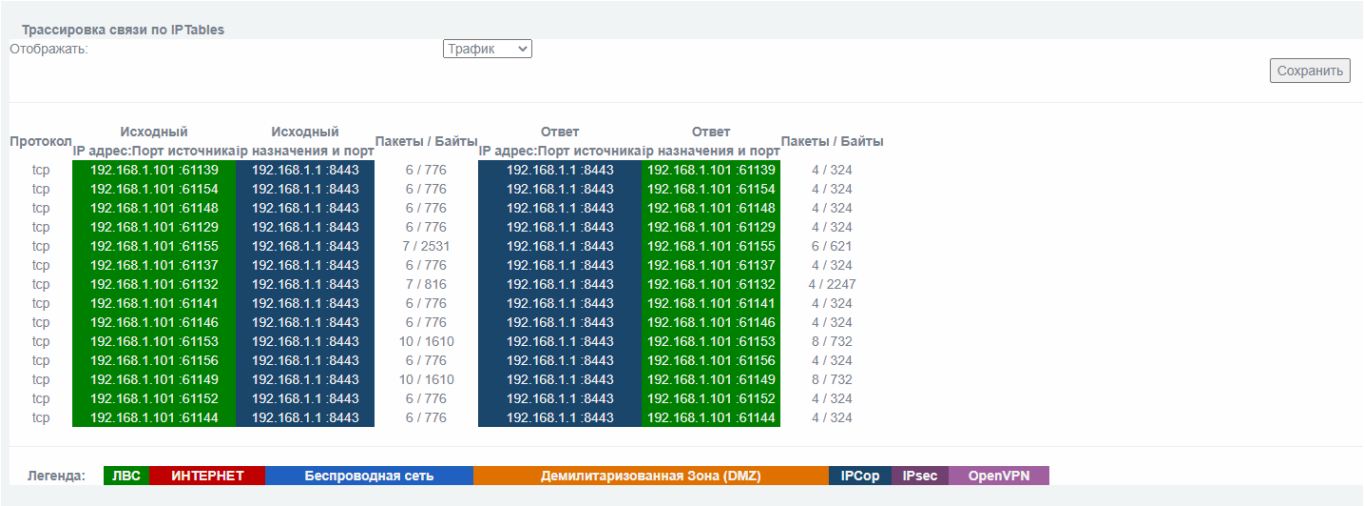


Рисунок 47 – Подраздел «Соединения». Таблица «Трафик»

Информация по соединениям распределяется по следующим параметрам:

– «Протокол» – название протокола соединения;

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

– «Исходный IP назначения и порт» – ответ от адреса и порта назначения;

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

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

– «Ответ IP назначения и порт» – ответ с адреса и порта назначения;

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

Внизу интерфейсного окна представлена легенда цветовой политики настройки сетевых интерфейсов.

2.3.6 Подраздел «Состояние интерфейсов»

Подраздел «Состояние интерфейсов» (рисунок 48) предназначен для отображения текущего состояния сетевых интерфейсов.

Рисунок 48 – Подраздел «Состояние интерфейсов»

Каждый сетевой интерфейс отображается в собственном поле. Для каждого сетевого интерфейса отображается скорость приема (Mbit/s) и скорость передачи (Mbit/s).

2.3.7 Подраздел «IPTables»

Подраздел «IPTables» (рисунок 49) предназначен для отображения информации по IPTables.

Таблица может быть следующих типов:

a) «filter» – таблица предназначена для отображения правил фильтрации по различным полям сетевого пакета;

b) «mangle» – таблица предназначена для отображения правил классификации и маркировки пакетов, а также модификации заголовков TTL и TOS;

c) «nat» – таблица предназначена для отображения правил изменения полей сетевого пакета при осуществлении трансляции NAT/PAT;

d) «raw» – таблица предназначена для отображения правил фильтрации сетевого пакета, выполняемых до процедуры отслеживания соединения.

Для изменения типа таблицы необходимо выбрать соответствующий тип в ниспадающем меню (см. рисунок

Рисунок 49) и нажать кнопку « Обновить ».

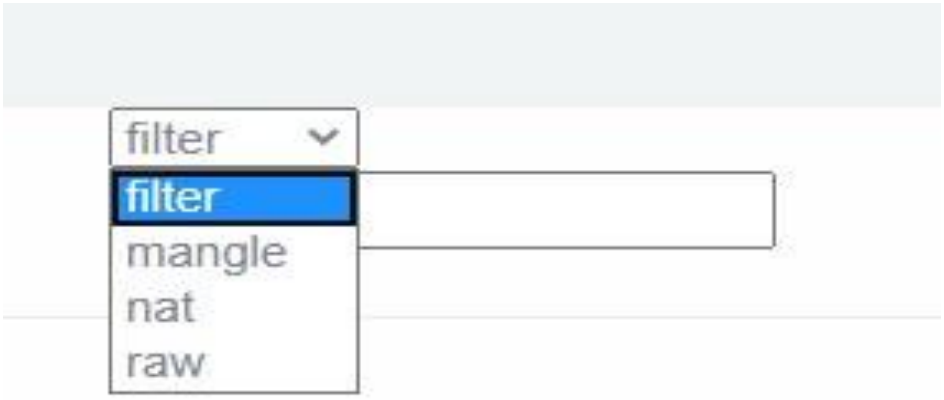


Рисунок 49 – Список типов таблиц

2.3.7.1 Таблица «filter»

Для фильтрации информации в подразделе «IPTables» необходимо выбрать «filter» и нажать кнопку « Обновить ».

Таблица «filter» предназначен для отображения правил фильтрации по различным полям сетевого пакета (рисунок 50).

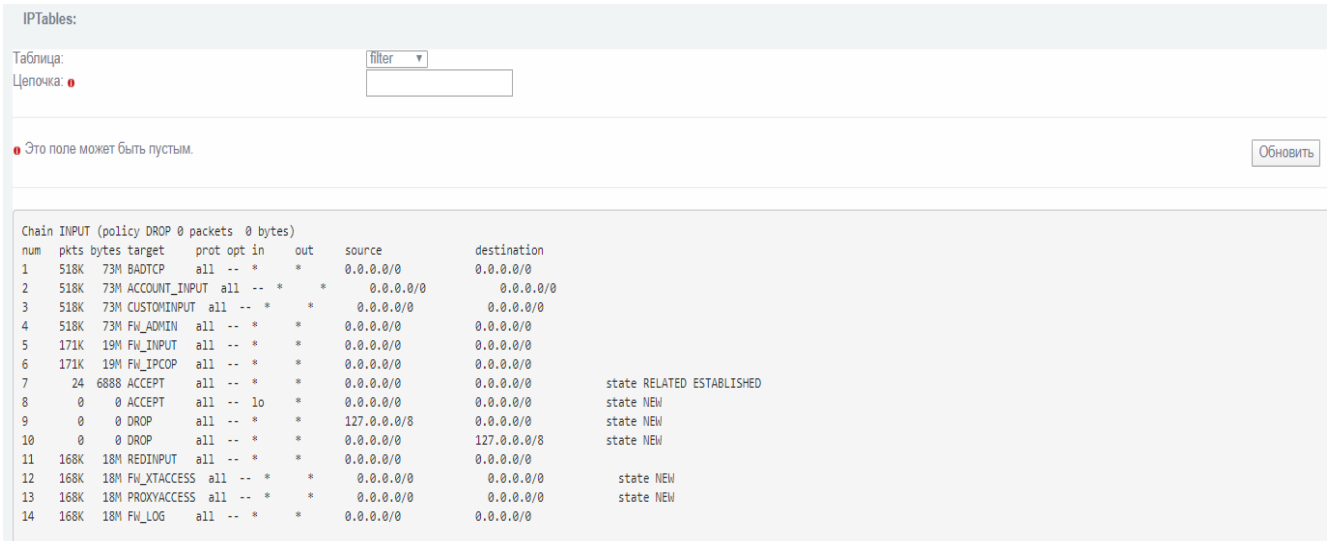


Рисунок 50 – Подраздел «Настройки IPTables». Таблица «filter»

2.3.7.2 Таблица «mangle»

Для фильтрации информации в подразделе «IPTables» необходимо выбрать «mangle» и нажать кнопку « Обновить ».

Таблица «mangle» (рисунок 51) предназначен для отображения правил классификации и маркировки пакетов, а также модификации заголовков TTL и TOS.

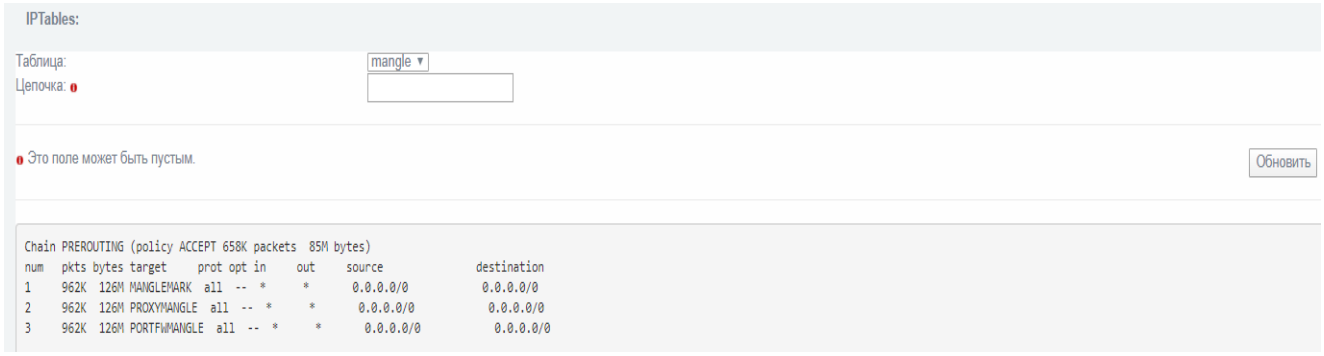


Рисунок 51 – Подраздел «IPTables». Таблица «mangle»

2.3.7.3 Таблица «nat»

Для фильтрации информации в подразделе «IPTables» необходимо выбрать «nat» и нажать кнопку « Обновить ».

Таблица «nat» (рисунок 52) предназначен для отображения правил изменения полей сетевого пакета при осуществлении трансляции NAT/PAT.

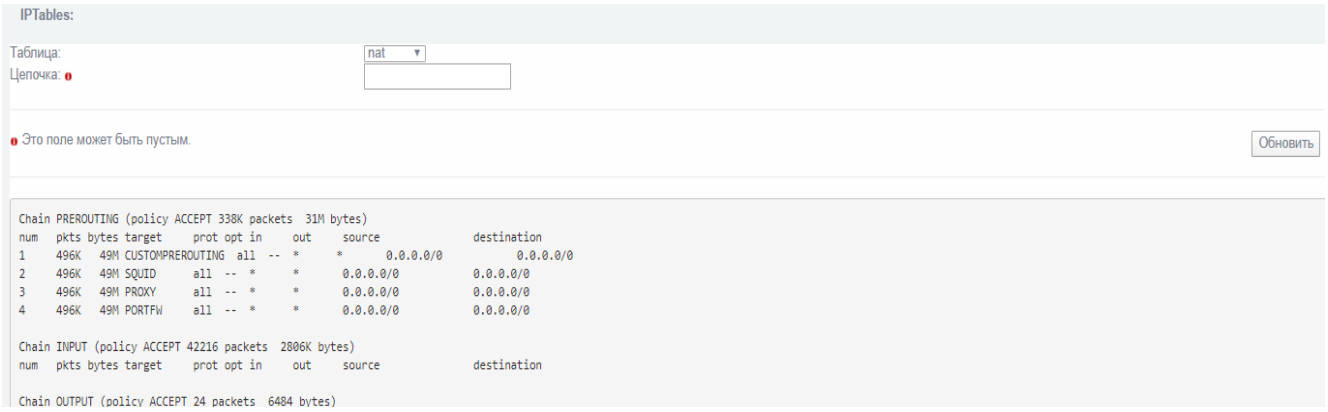


Рисунок 52 – Подраздел «IPTables». Таблица «nat»

2.3.7.4 Таблица «raw»

Для фильтрации информации в подразделе «IPTables» необходимо выбрать «raw» и нажать кнопку « Обновить ».

Таблица «raw» (рисунок 52-b) предназначена для отображения информации о правилах высокоприоритетной фильтрации сетевого пакета. В текущей версии «Рубикон» настройка данных правил не предусмотрена.

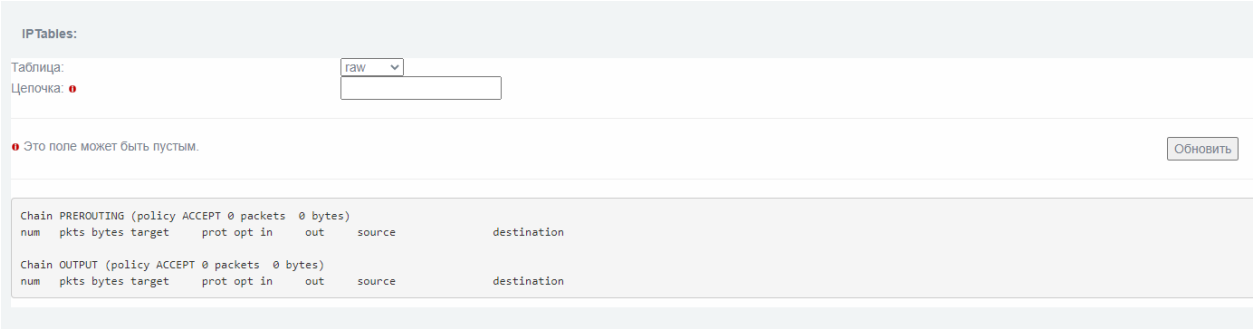


Рисунок 52-b – Подраздел «IPTables». Таблица «raw»

2.3.8 Подраздел «NFTables»

Подраздел «NFTables» (рисунок 49-b) предназначен для отображения информации по NFTables.

Таблица может быть следующих типов:

a) «filter» – таблица предназначена для отображения правил фильтрации по различным полям сетевого пакета;

b) «mangle» – таблица предназначена для отображения правил классификации и маркировки пакетов, а также модификации заголовков TTL и TOS;

c) «nat» – таблица предназначена для отображения правил изменения полей сетевого пакета при осуществлении трансляции NAT/PAT;

d) «bridge filter» – таблица предназначена для отображения правил фильтрации сетевого пакета.

Для изменения типа таблицы необходимо выбрать соответствующий тип в ниспадающем меню (см. рисунок

Рисунок 49-b) и нажать кнопку « Обновить ».

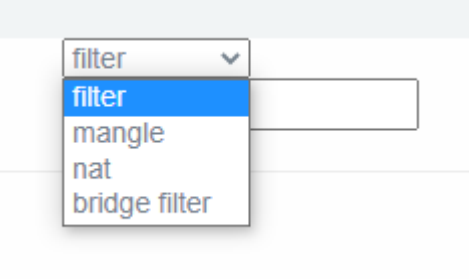


Рисунок 49-b – Список типов таблиц

2.3.8.1 Таблица «filter»

Для фильтрации информации в подразделе «NFTables» необходимо выбрать «filter» и нажать кнопку « Обновить ».

Таблица «filter» предназначена для отображения правил фильтрации по различным полям сетевого пакета (рисунок 50-b).

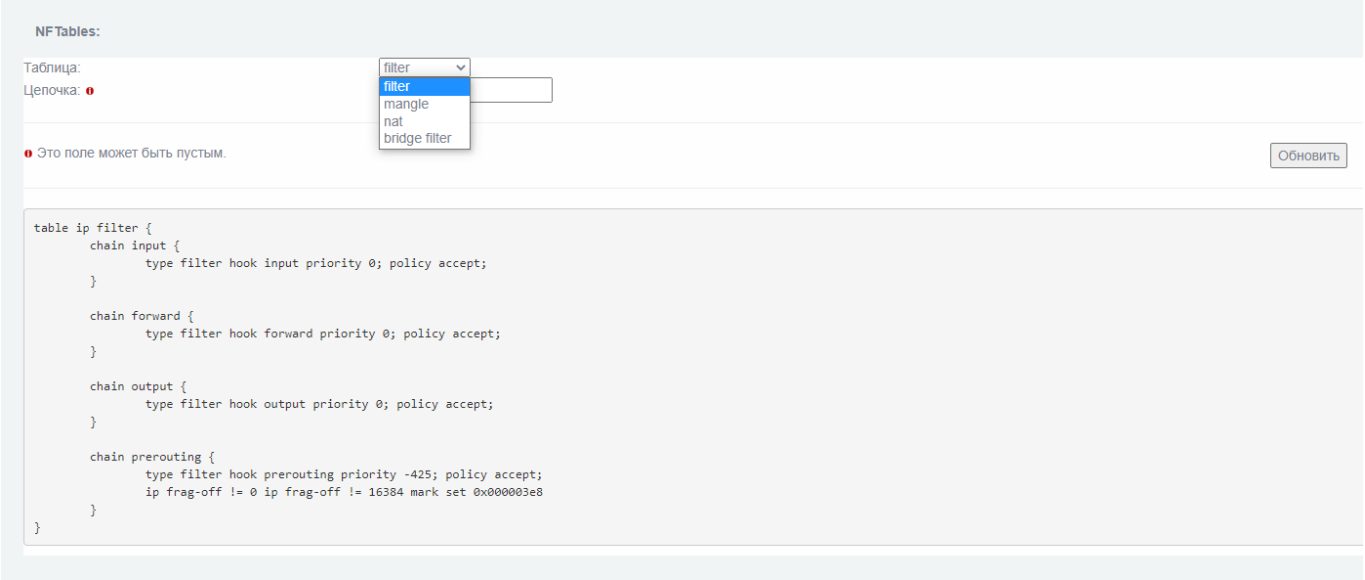


Рисунок 50-b – Подраздел «Настройки NFTables». Таблица «filter»

2.3.8.2 Таблица «mangle»

Для фильтрации информации в подразделе «NFTables» необходимо выбрать «mangle» и нажать кнопку « Обновить ».

Таблица «mangle» (рисунок 51-b) предназначена для отображения правил классификации и маркировки пакетов, а также модификации заголовков TTL и TOS. В настоящей версии «Рубикон» настройка данных правил не предусмотрена. При обращении к таблице предоставляется сообщение о ее отсутствии.

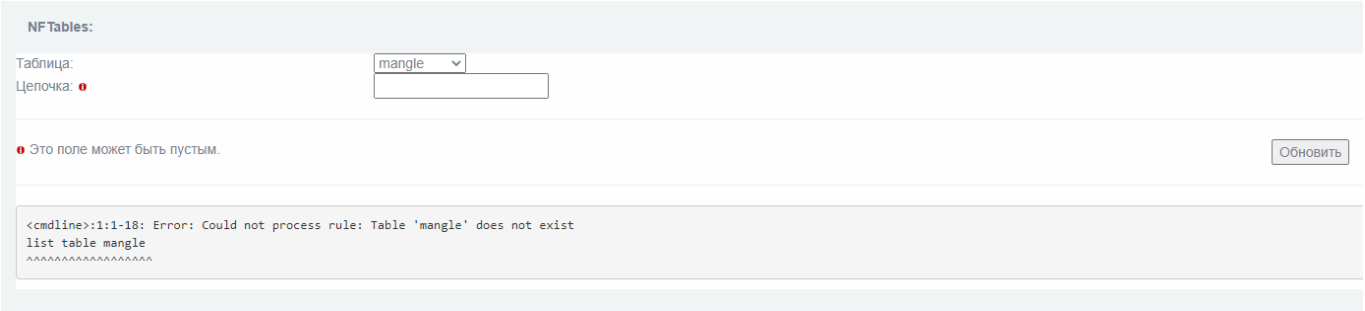


Рисунок 51-b – Подраздел «NFTables». Таблица «mangle»

2.3.8.3 Таблица «nat»

Для фильтрации информации в подразделе «NFTables» необходимо выбрать «nat» и нажать кнопку « Обновить ».

Таблица «nat» (рисунок 52-b) предназначена для отображения правил изменения полей сетевого пакета при осуществлении трансляции NAT/PAT. В настоящей версии «Рубикон» настройка данных правил не предусмотрена. При обращении к таблице предоставляется сообщение о ее отсутствии.

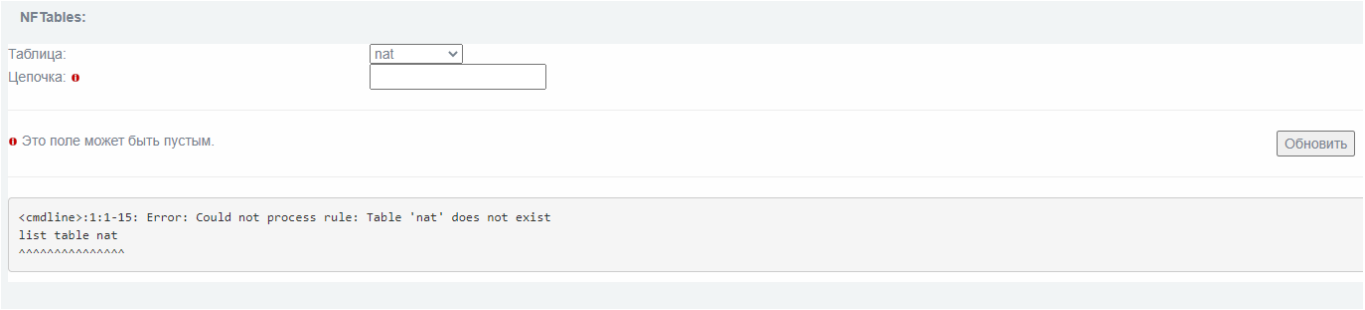


Рисунок 52-b – Подраздел «NFTables». Таблица «nat»

2.3.8.4 Таблица «bridge filter»

Для фильтрации информации в подразделе «NFTables» необходимо выбрать «bridge filter» и нажать кнопку « Обновить ».

Таблица «bridge filter» (рисунок 53) предназначена для отображения информации о правилах фильтрации сетевого пакета.

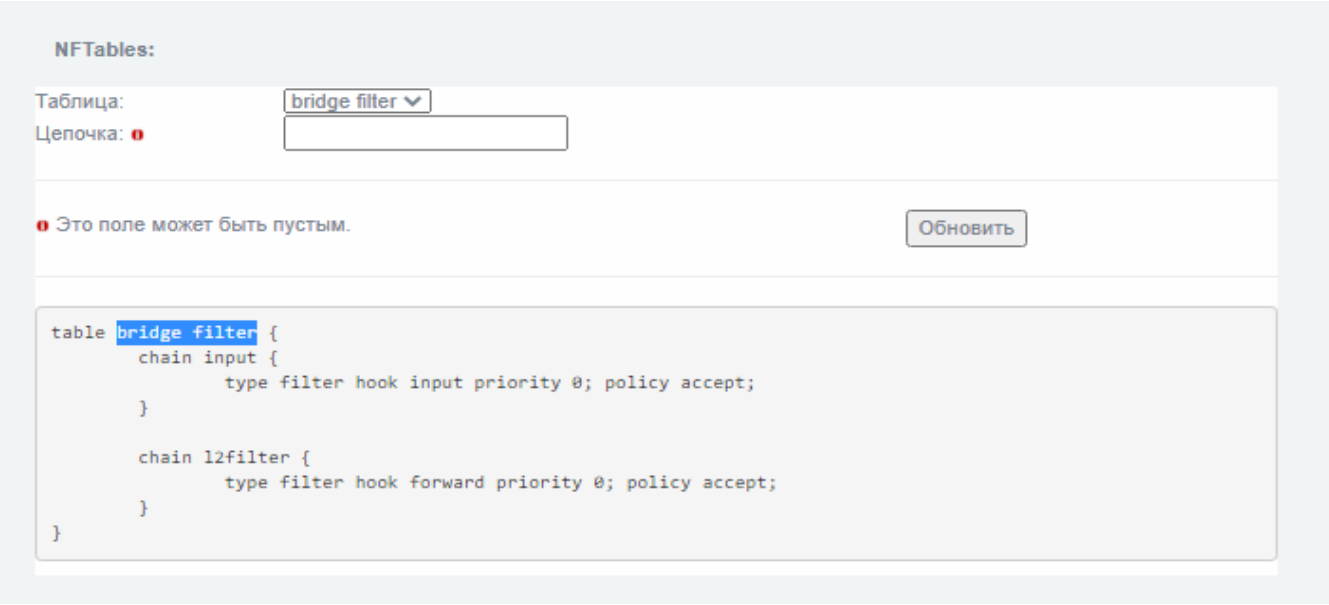


Рисунок 53 – Подраздел «NFTables». Таблица «bridge filter»

2.3.9 Подраздел «Контрольные суммы»

Подраздел «Контрольные суммы» (рисунок 54) предназначен для проверки контрольных сумм изделия и сопоставления этих сумм с эталонными суммами.

Рисунок 54 – Подраздел «Контрольные суммы»

Проверка контрольных сумм происходит по следующим категориям:

– контрольная сумма решающих правил СОВ;

– контрольная сумма файла конфигурации межсетевого экрана;

– 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 «Рубикон» выдаст сообщение – «Контрольные суммы ОК» (см. рисунок 54).

В случае возникновения неисправностей или разночтений появятся сообщения в полях «Ошибки» или «Предупреждения» (рисунок 55).

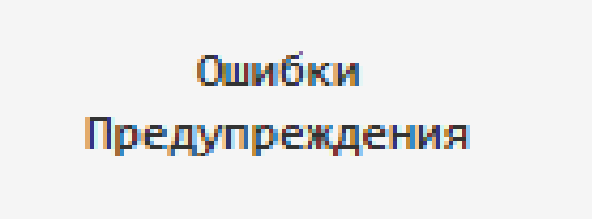


Рисунок 55 – Поля «Ошибки» или «Предупреждения»

2.4 Раздел «Сеть»

Раздел «Сеть» содержит следующие подразделы:

– подраздел «Псевдонимы»;

– подраздел «Горячее резервирование CARP»;

– подраздел «Настройка адаптеров»;

– подраздел «Маршруты»;

– подраздел «Конфигурация ARP»;

– подраздел «OSPF»;

– подраздел «BGP»;

– подраздел «VLANs»;

– подраздел «Мосты»

– подраздел «Объединение интерфейсов».

2.4.1 Подраздел «Псевдонимы»

Подраздел «Псевдонимы» (рисунок 56) предназначен для задания псевдонимов сетевых адресов. Данная возможность применяется для назначения нескольких сетевых псевдонимов для разделения внутренних ресурсов по сетевому адресу.

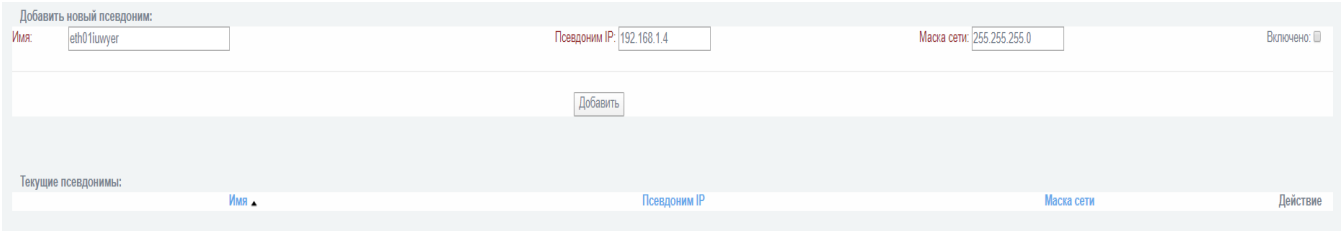


Рисунок 56 – Подраздел «Псевдонимы»

Подраздел «Псевдонимы» содержит элементы, указанные в таблице 19.

Таблица 19 – Описание элементов подраздела «Конфигурация подсчета трафика»

Элемент	Описание
	Поле для ввода необходимой информации
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
Кнопка «  »	Предназначена для сохранения настроек псевдонима сетевого адреса

Элемент	Описание
Параметр «Включено»	Предназначен для включения или выключения данного псевдонима
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок включения сортировки в перечне псевдонимов

Перечень псевдонимов распределяется по следующим параметрам:

– «Имя»;

– «Псевдоним IP»;

– «Маска сети».

Псевдоним в перечне можно редактировать или удалить. Все возможные действия с псевдонимом изображены в столбце «Действие» (рисунок 57).

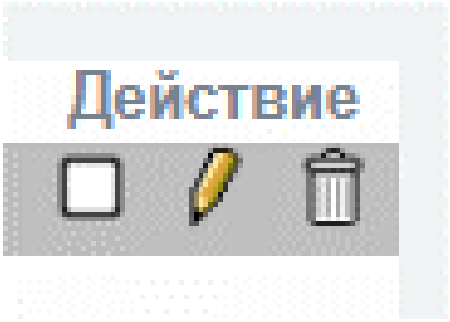


Рисунок 57 – Столбец «Действие»

Столбец «Действие» содержит элементы, указанные в таблице 20.

Таблица 20 – Описание элементов столбца «Действие»

Элемент	Описание
	Активировано (нажмите для деактивации псевдонима)
	Деактивировано (нажмите для активации псевдонима)
	Изменить псевдоним
	Удалить псевдоним

2.4.2 Подраздел «Горячее резервирование CARP (VRRP)»

Подраздел «Горячее резервирование CARP (VRRP)» (рисунок 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.

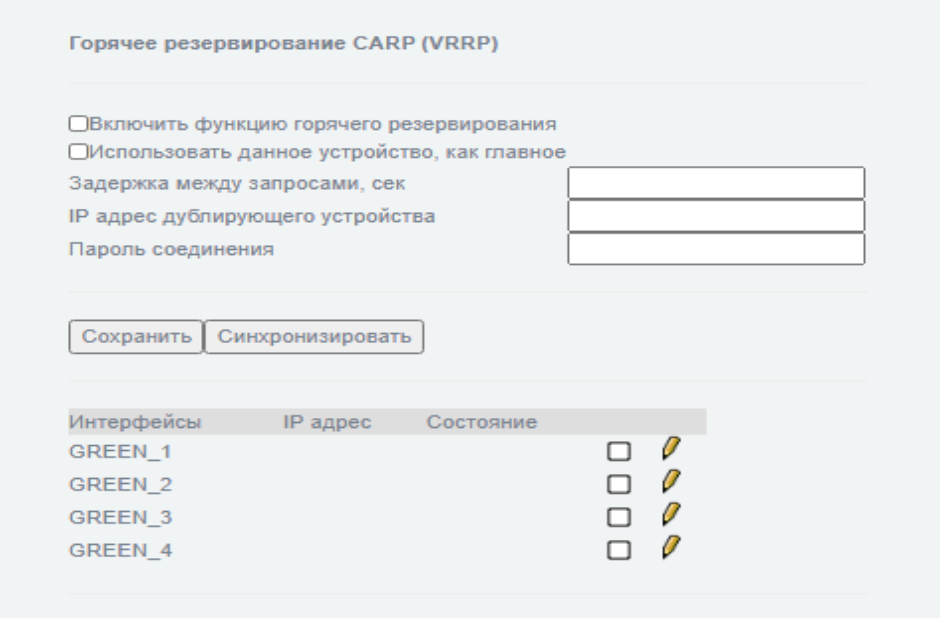


Рисунок 58 – Подраздел «Горячее резервирование CARP (VRRP)»

Подраздел «Горячее резервирование CARP (VRRP)» содержит элементы, указанные в таблице 21.

Таблица 21 – Описание элементов подраздела «Горячее резервирование CARP (VRRP)»

Элемент	Описание
☑	Поле с проставленным флажком (параметр включен)
☐	Пустое поле для проставления флажка (параметр выключен)

Элемент	Описание
Параметр «Включить функцию горячего резервирования»	Параметр предназначен для включения функции горячего резервирования
Параметр «Использовать данное устройство, как главное»	Параметр предназначен для указания включения в качестве главного устройства
	Поле для ввода необходимой информации
Поле «IP адрес дублирующего устройства»	Предназначено для указания IP адреса устройства, которое находится в резерве. По указанному адресу будет осуществляться синхронизация устройств
Поле «Пароль соединения»	Предназначено для ввода пароля соединения
Кнопка «Сохранить»	Предназначена для сохранения параметров функции горячего резервирования
Кнопка «Синхронизировать»	Кнопка обновления данных

Перечень интерфейсов приведен на рисунке 59.

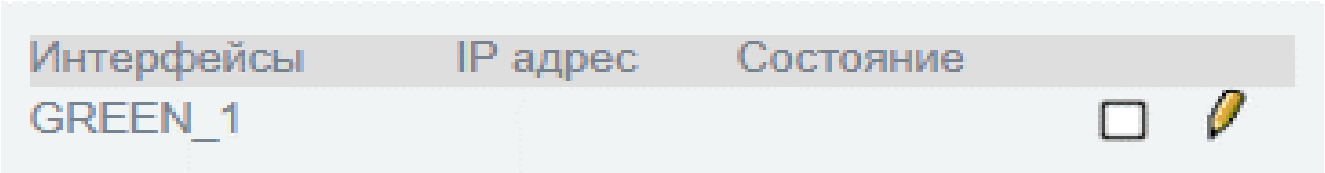


Рисунок 59 – Перечень интерфейсов

Перечень интерфейсов распределяется по следующим параметрам:

– «Интерфейсы»;

– «IP адрес»;

– «Состояние».

Перечень интерфейсов подраздела «Горячее резервирование CARP (VRRP)» содержит элементы, указанные в таблице 22.

Таблица 22 – Описание элементов подраздела «Горячее резервирование CARP (VRRP)»

Элемент	Описание
Значок « »	Переход па страницу редактирования параметров резервирования интерфейса
Значок « »	Предназначен для индикации состояния (ВКЛ/ВЫКЛ) сервиса резервирования указанного интерфейса. Если стоит галочка, указанный интерфейс будет резервироваться в случае отказа устройства

После нажатия на значок « » откроется меню редактирования интерфейса (рисунок 60).

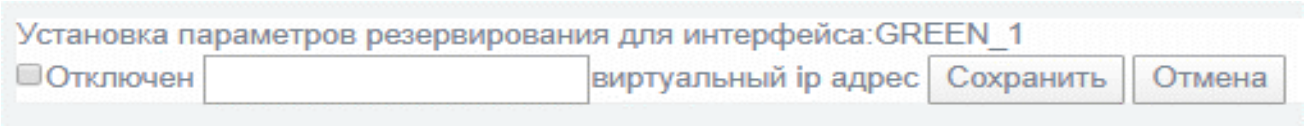


Рисунок 60 – Меню редактирования интерфейса

Меню редактирования интерфейса подраздела «Горячее резервирование CARP (VRRP)» содержит элементы, указанные в таблице 23.

Таблица 23 – Описание элементов меню редактирования интерфейса подраздела «Горячее резервирование CARP (VRRP)»

Элемент	Описание
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле для ввода необходимой информации. В данном случае – виртуальный IP адрес
Кнопка « Сохранить »	Предназначена для сохранения введенной информации
Кнопка « Отмена »	Кнопка предназначена для удаления введенной информации и возврату в подраздел «Горячее резервирование CARP (VRRP)»
Кнопка « Синхронизировать »	Кнопка обновления данных

2.4.3 Подраздел «Настройка адаптеров»

Подраздел «Настройка адаптеров» (рисунок 61) предназначен для присвоения цветов существующим аппаратно-реализованным сетевым интерфейсам (адаптерам).

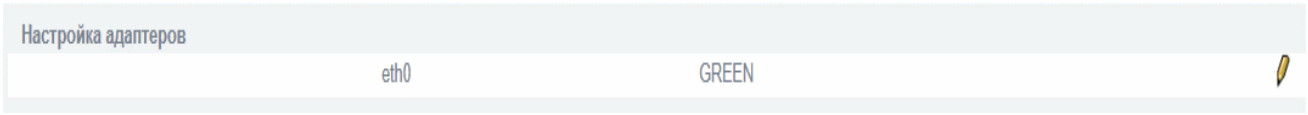


Рисунок 61 – Подраздел «Настройка адаптеров»

Значок « » открывает меню редактирования выбранного адаптера (рисунок 62).

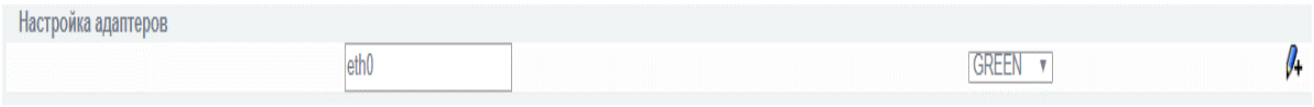


Рисунок 62 – Меню редактирования адаптера

Меню редактирования адаптера содержит элементы, указанные в таблице 24.

Таблица 24 – Описание элементов меню редактирования адаптера

Элемент	Описание
	Поле для ввода необходимой информации. В данном случае – название интерфейса
GREEN	Ниспадающий список для назначения цвета адаптера
	Значок сохранения введенной информации и возвращения в подраздел «Настройка адаптеров»

Интерфейсы подразделяются на следующие цвета:

– красный (RED). Сетевой интерфейс, подключаемый к внешней сети. По умолчанию все пакеты, маршрутизируемые с красного интерфейса на зеленый (кроме пакетов, принадлежащих открытым TCP-сессиям), блокируются межсетевым экраном;

– зеленый (GREEN). Сетевой интерфейс, подключаемый к внутренней сети. По умолчанию все пакеты, маршрутизируемые между различными зелеными интерфейсами, не блокируются;

– синий (BLUE). Сетевой интерфейс, подключаемый к беспроводной сети. Для этого интерфейса включен режим «белого списка», то есть запрещены как входящие, так и перенаправляемые пакеты от всех адресов, кроме специально разрешенных в разделе «Межсетевой экран»;

– оранжевый (ORANGE). Демилитаризованная зона. По умолчанию все пакеты, маршрутизируемые с оранжевого интерфейса на зеленый (кроме пакетов, принадлежащих открытым TCP- сессиям), блокируются. При этом возможна настройка проброса портов с красного интерфейса на оранжевый для обеспечения работоспособности внешних сервисов.

2.4.4 Подраздел «Маршруты»

Подраздел «Маршруты» (рисунок 63) предназначен для создания маршрутов.

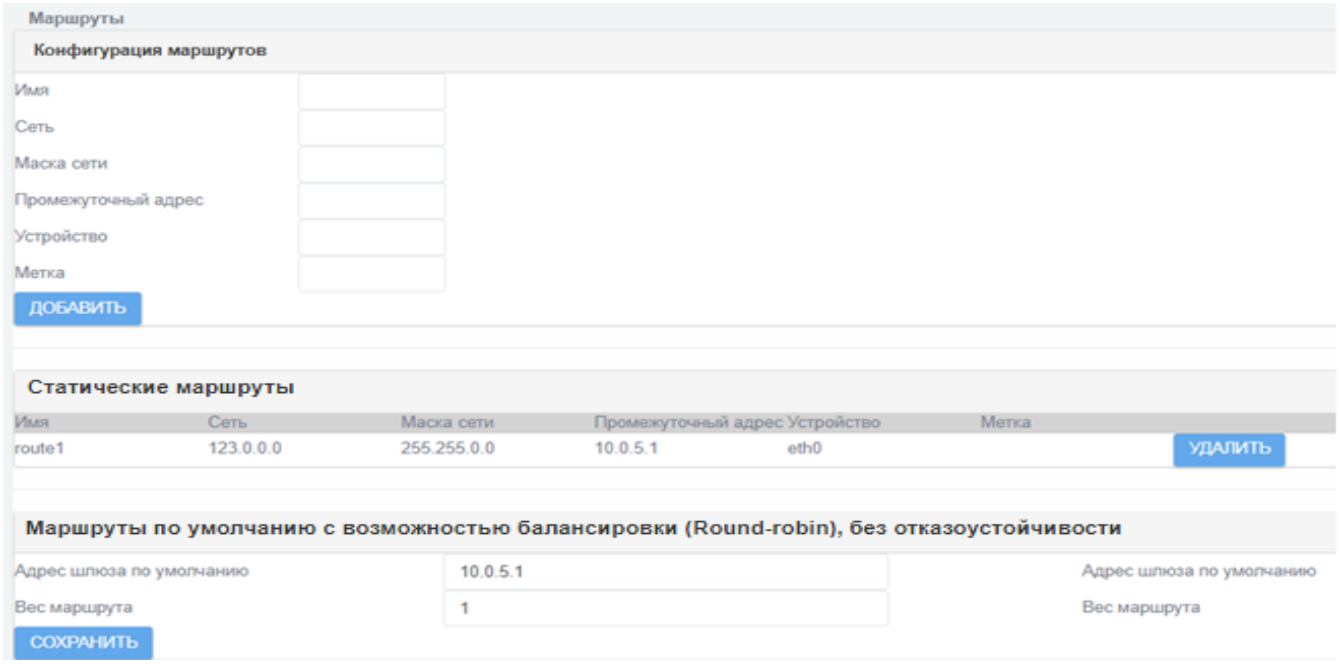


Рисунок 63 – Подраздел «Маршруты»

Подраздел «Маршруты» содержит элементы, указанные в таблице 25.

Таблица 25 – Описание элементов подраздела «Маршруты»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «Имя»	Предназначено для указания имени сетевого маршрута. Имя должно состоять из латинских букв и цифр. Оно

Элемент	Описание
	предназначено для удобства администратора и не влияет на работу межсетевого экрана
Поле «Сеть»	Предназначено для указания маршрутизируемой сети
Поле «Маска сети»	Предназначено для указания маски маршрутизируемой сети. Маска задается в полном десятичном виде
Поле «Промежуточный адрес»	Сетевой адрес шлюза, через который будет проложен маршрут. Указанный шлюз должен находиться в прямой видимости «Рубикон»
Поле «Устройство»	Предназначено для указания имени сетевого устройства, через которое будет проложен маршрут
Поле «Метка»	Предназначено для указания метки, присваиваемой пакету межсетевым экраном для маршрутизации, управляемой межсетевым экраном
Кнопка «ДОБАВИТЬ»	Сохранение введенных данных

Все сохраненные маршруты отображаются в перечне сохраненных маршрутов (рисунок 64).

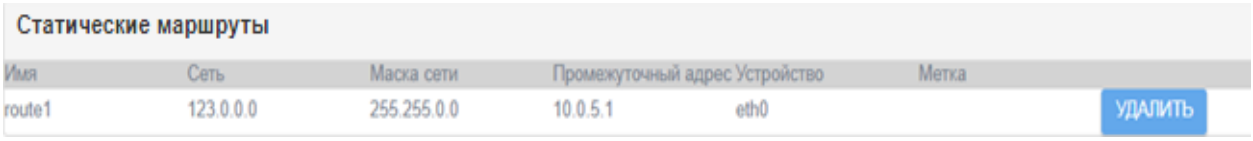


Рисунок 64 – Перечень сохраненных маршрутов

Перечень сохраненных маршрутов распределяется по следующим параметрам:

– «Имя»;

– «Сеть»;

– «Маска сети»;

– «Промежуточный адрес»;

– «Устройство»;

– «Метка».

Для удаления маршрута из перечня сохраненных маршрутов необходимо нажать кнопку «УДАЛИТЬ».

Подраздел «Маршруты» содержит описание маршрута, установленного по умолчанию (рисунок 65).

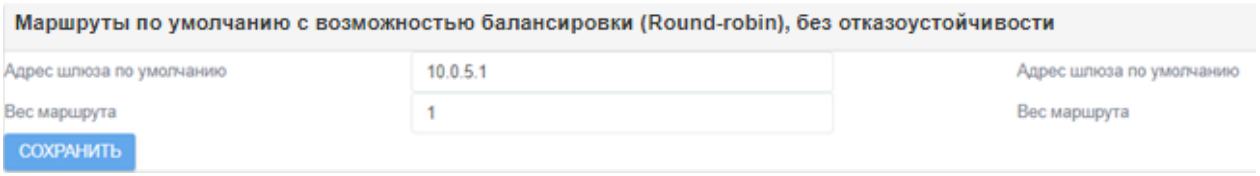


Рисунок 65 – Маршрут, установленный по умолчанию

Описание маршрута по умолчанию содержит элементы, указанные в таблице 26.

Таблица 26 – Описание элементов маршрутов по умолчанию

Элемент	Описание
	Поле для ввода необходимой информации
Адрес шлюза по умолчанию	Поле ввода IP-адреса шлюза, используемого по умолчанию
Вес маршрута	Указание приоритета маршрута
Кнопка «СОХРАНИТЬ»	Кнопка сохранения введенных данных

2.4.5 Подраздел «Конфигурация ARP»

Подраздел «Конфигурация ARP» предназначен для конфигурации протокола ARP для определения MAC-адреса по известному IP-адресу (рисунок 66).

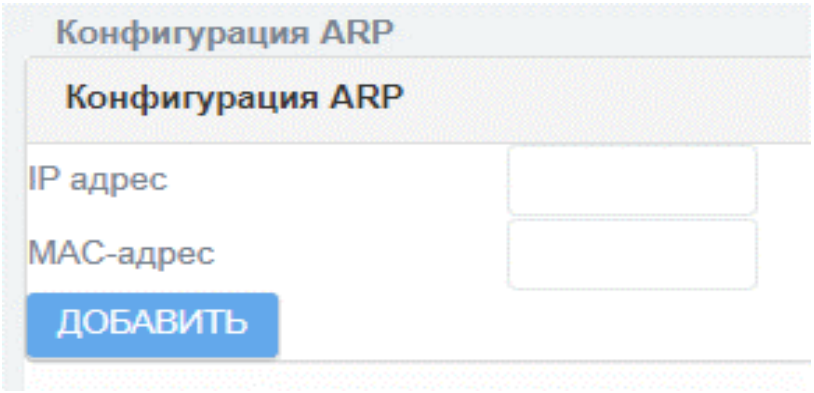


Рисунок 66 – Подраздел «Конфигурация ARP»

Подраздел «Конфигурация ARP» содержит элементы, указанные в таблице 27.

Таблица 27 – Описание элементов подраздела «Конфигурация ARP»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «IP Адрес»	Предназначено для указания IP-адреса
Поле «MAC-адрес»	Предназначено для указания соответствующего MAC-адреса
Кнопка «ДОБАВИТЬ»	Предназначена для внесения записи о соответствии MAC-адреса и IP-адреса в таблицу ARP

После нажатия кнопки «ДОБАВИТЬ», конфигурация ARP отображается в виде списка в нижней части окна (рисунок 67).

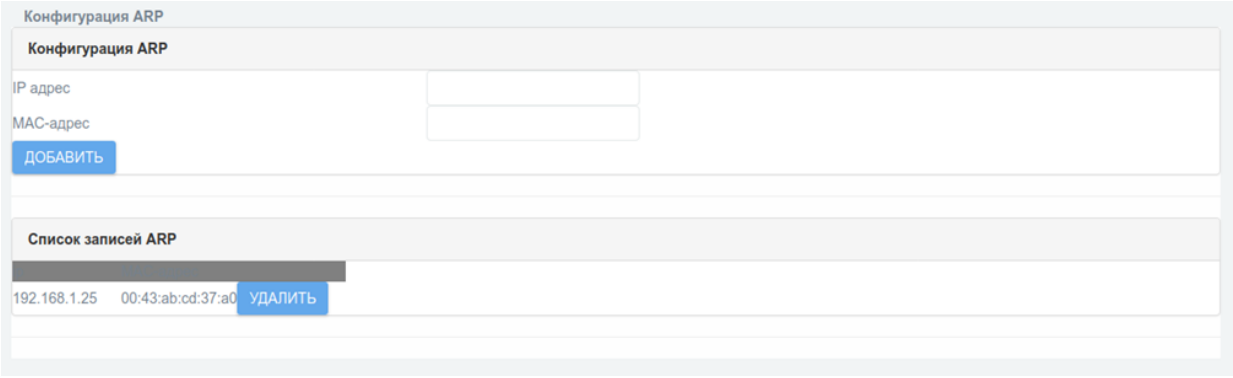


Рисунок 67 – Список записей ARP

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» → «Таблица ARP» запись элемента таблицы

маркируется дополнительно флагом «M». Это показывает, что запись добавлена на постоянной основе (рисунок 68).

Рисунок 68 – Таблица ARP

В случае ошибочного ввода параметров будет выдано сообщение о невозможности создания требуемой ARP-записи в таблице (рисунок 69).

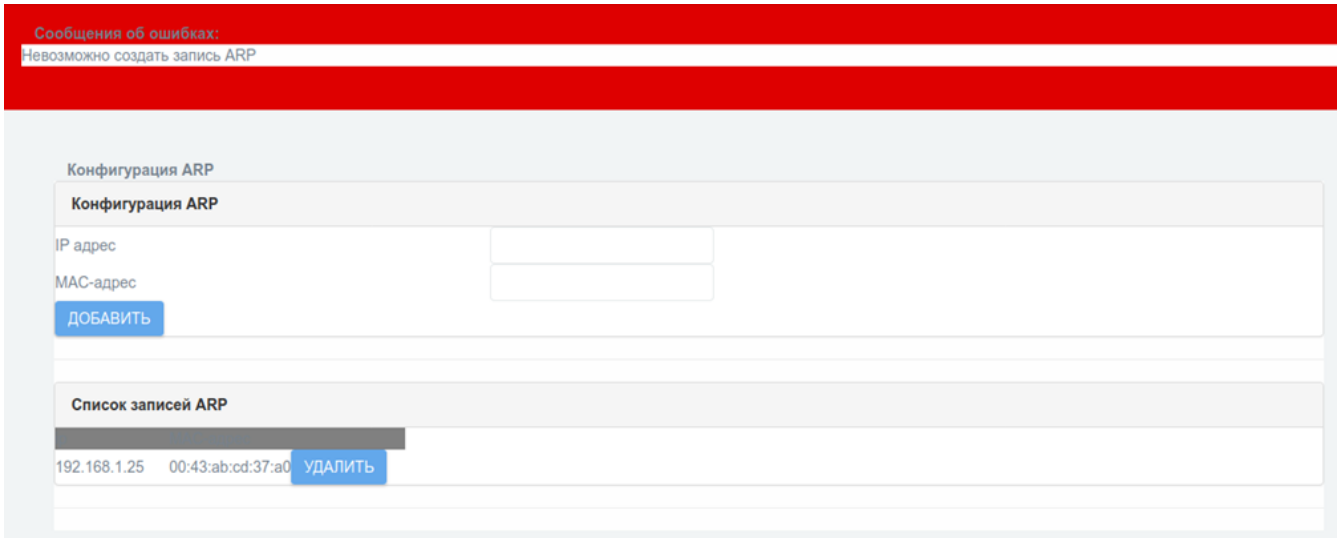


Рисунок 69 – Сообщение о невозможности создания требуемой ARP-записи в таблице

2.4.6 Подраздел «OSPF»

Подраздел «OSPF» (рисунок 70) предназначен для управления службой динамической маршрутизации по протоколу OSPF.

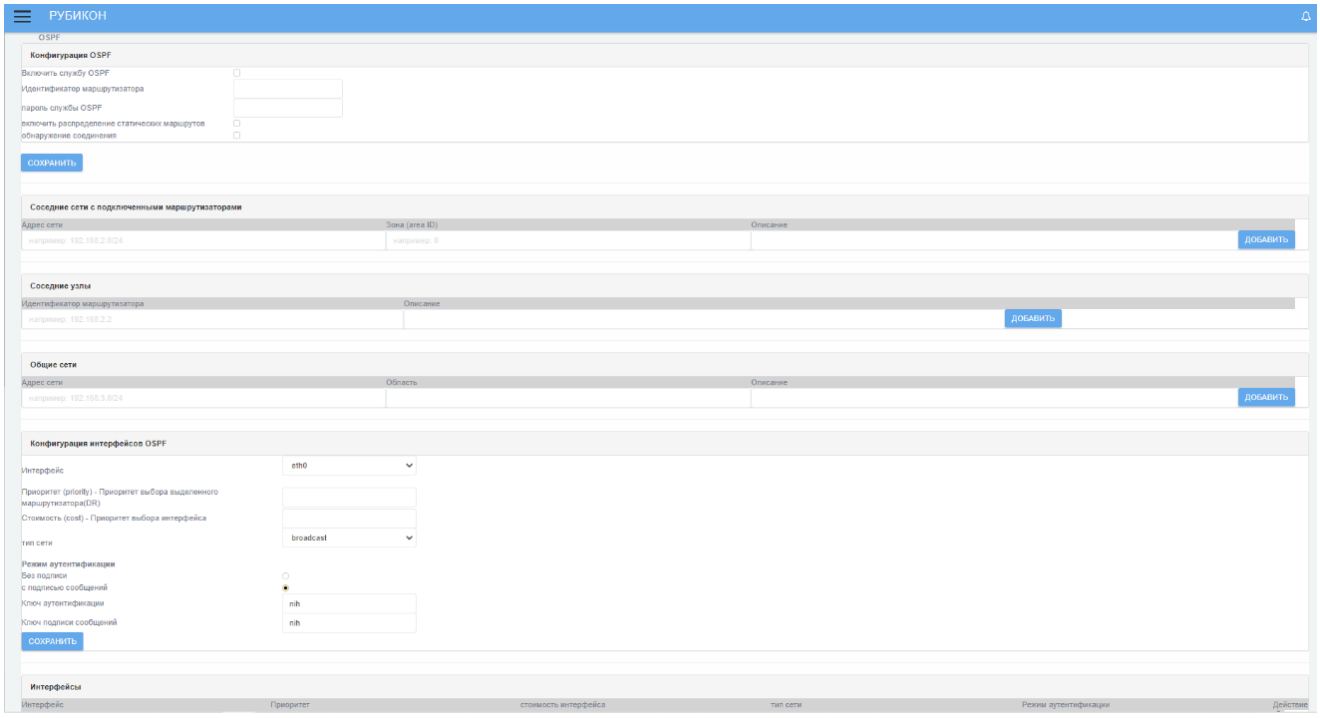


Рисунок 70 – Подраздел «OSPF»

Подраздел «OSPF» состоит из следующих полей:

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

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

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

– «Общие сети» — сети, информация о которых анонсируется по протоколу OSPF.

– «Конфигурация интерфейсов OSPF» – настройка сетевых интерфейсов устройства, используемых для взаимодействия по протоколу OSPF.

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

2.4.6.1 Поле «Конфигурация OSPF»

Поле «Конфигурация OSPF» содержит элементы, указанные в таблице 28.

Таблица 28 – Описание элементов поля «Конфигурация OSPF»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Чекбокс «Включить службу OSPF»	Чекбокс предназначен для включения/выключения службы OSPF
Поле «Идентификатор маршрутизатора»	Поле 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»	Поле предназначено для указания пароля службы OSPF
Чекбокс «включить распределение статических маршрутов»	Чекбокс предназначен для включения распределения статических маршрутов
Чекбокс «обнаружение соединения»	Чекбокс предназначен для использования режима отслеживания связи при работе службы OSPF

Подраздел «OSPF» включает в себя следующие поля:

– «Сети»;
– «Соседние узлы»;
– «Общие сети»;
– «Config interface»;

– «Интерфейсы».

2.4.6.2 Поле «Соседние сети с подключенными маршрутизаторами»

Поле «Соседние сети с подключенными маршрутизаторами» (рисунок 71) содержит список всех доступных сетей и состоит из следующих параметров:

– «Адрес сети»;

– «Зона (area ID)»;

– «Описание».

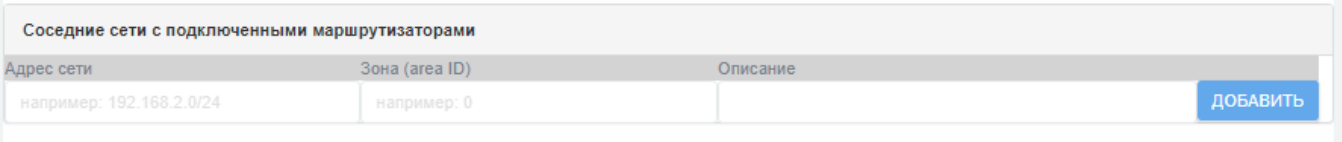


Рисунок 71 – Поле «Соседние сети с подключенными маршрутизаторами»

Перечень «Соседние сети с подключенными маршрутизаторами» содержит элементы, указанные в таблице 29.

Таблица 29 – Описание элементов перечня «Соседние сети с подключенными маршрутизаторами»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «Адрес сети»	IP-адрес сети
Поле «Зона (area ID)»	Поле для ввода идентификатора зоны. Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса
Поле «Описание»	Краткое описание сети
ДОБАВИТЬ	Кнопка добавления новой сети в перечень «Сети»

2.4.6.3 Поле «Соседние узлы»

Поле «Соседние узлы» (рисунок 72) содержит список всех доступных узлов и состоит из следующих параметров:

– «Идентификатор маршрутизатора»;

– «Описание».

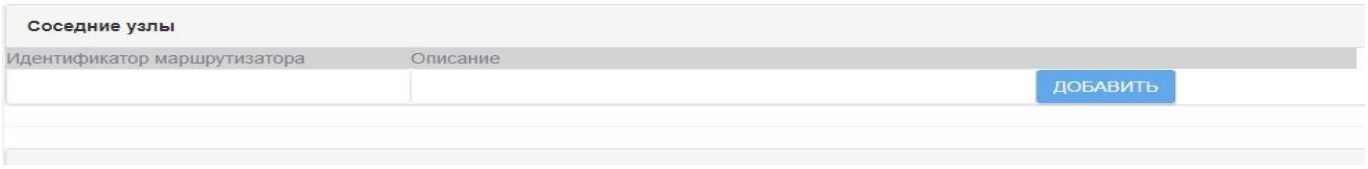


Рисунок 72 – Поле «Соседние узлы»

Перечень «Соседние узлы» содержит элементы, указанные в таблице 30.

Таблица 30 – Описание элементов перечня «Соседние узлы»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «Идентификатор маршрутизатора»	IP-адрес маршрутизатора
Поле «Описание»	Краткое описание узла сети
ДОБАВИТЬ	Кнопка добавления нового узла сети в перечень «Соседние узлы»

2.4.6.4 Поле «Общие сети»

Поле «Общие сети» (рисунок 73) содержит список всех общих сетей и состоит из следующих параметров:

– «Адрес»;

– «Область»;

– «Описание».

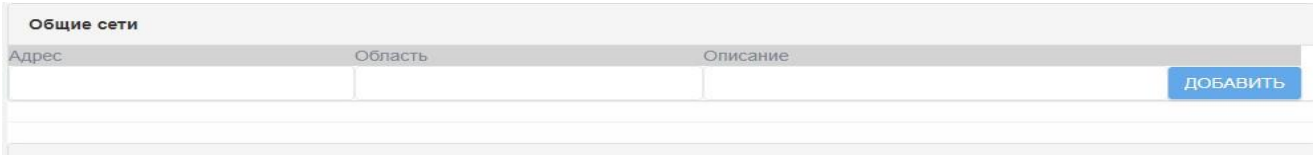
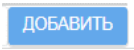


Рисунок 73 – Поле «Общие сети»

Поле «Общие сети» содержит элементы, указанные в таблице 31.

Таблица 31 – Описание элементов перечня «Общие сети»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «Адрес»	IP-адрес сети
Поле «Область»	Поле для ввода идентификатора зоны. Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса
Поле «Описание»	Краткое описание сети
	Значок удаления сети
	Кнопка добавления новой сети в перечень «Общие сети»

2.4.6.5 Поле «Конфигурация интерфейсов OSPF»

Поле «Конфигурация интерфейсов OSPF» (рисунок 74) содержит список всех интерфейсов.

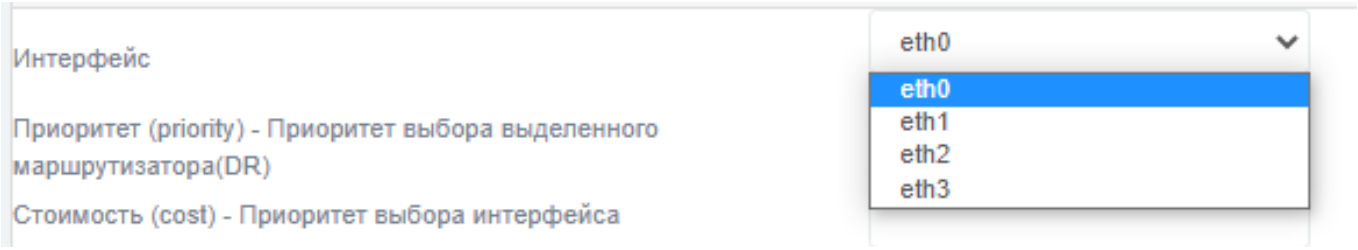


Рисунок 74 – Перечень «Интерфейсы»

Для изменения настроек интерфейса и перехода в меню редактирования OSPF интерфейсов (рисунок 75) необходимо нажать кнопку «Сохранить».

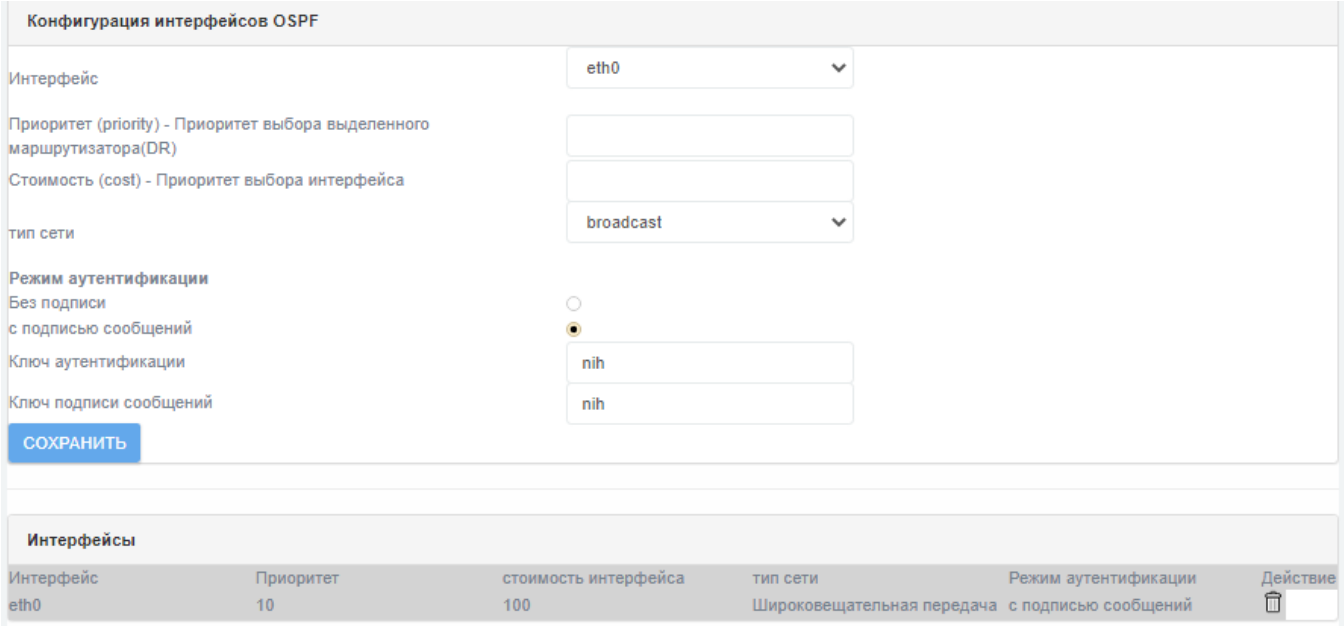


Рисунок 75 – Меню редактирования «Конфигурация интерфейсов OSPF»

Меню редактирования «Конфигурация интерфейсов OSPF» содержит элементы, указанные в таблице 32.

Таблица 32 – Описание элементов меню редактирования «Конфигурация интерфейсов OSPF»

Элемент	Описание
	Поле для ввода необходимой информации
	Активация ниспадающего списка
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Поле «Интерфейс»	Из ниспадающего списка выполняется выбор интерфейса для использования по протоколу OSPF
Поле «Приоритет (priority) - Приоритет выбора выделенного маршрутизатора (DR)»	Вводится номер приоритета выбора выделенного маршрутизатора. Диапазон значений: от 1 до 254

Элемент	Описание
Поле «Стоимость (cost) - приоритет по пропускной способности»	Параметр определяет предпочтения по прохождению трафика. В алгоритме OSPF 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
Ниспадающий список «тип сети»	Позволяет выбрать один из следующих параметров: – broadcast; – non-broadcast; – point-to-multipoint; – point-to-point
Поле «Режим аутентификации»	Выбор метода аутентификации. Может иметь либо значение «Без подписи» в случае отсутствия аутентификации, либо «с подписью сообщений» в случае аутентификации на основе MD5 HMAC. В случае режима аутентификации «с подписью сообщений» необходимо задавать также параметр «ключ подписи сообщений»
Чекбокс «Без подписи»	Режим аутентификации без подписи
Чекбокс «с подписью сообщений»	Режим аутентификации с подписью
Поле «Ключ аутентификации»	Поле для ввода ключа, используемого для осуществления парольной аутентификации. «Допустимые значения» — строки алфавитно-цифровых символов (латинский алфавит и цифры 0-9) длиной до 8 символов
Поле «Ключ подписи сообщений»	Поле для ввода ключа, используемого для защиты сообщений с помощью алгоритма MD5 HMAC. Допустимые

Элемент	Описание
	значения — строки алфавитно-цифровых символов (латинский алфавит и цифры 0-9) длиной не более 16 символов
СОХРАНИТЬ	Кнопка сохранения введенной информации

2.4.6.6 Поле «Интерфейсы»

Поле «Интерфейсы» (рисунок 76) содержит перечень всех интерфейсов и отображает следующие параметры:

– «Интерфейс»;

– «Приоритет»;

– «Стоимость интерфейса»;

– «Тип сети»;

– «Режим аутентификации»;

– «Действие».

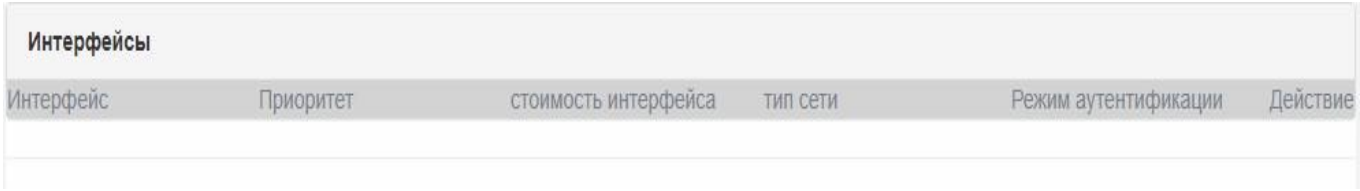


Рисунок 76 – Поле «Интерфейсы»

2.4.7 Подраздел «BGP»

Подраздел «BGP» (рисунок 77) предназначен для управления службой динамической маршрутизации по протоколу BGP.

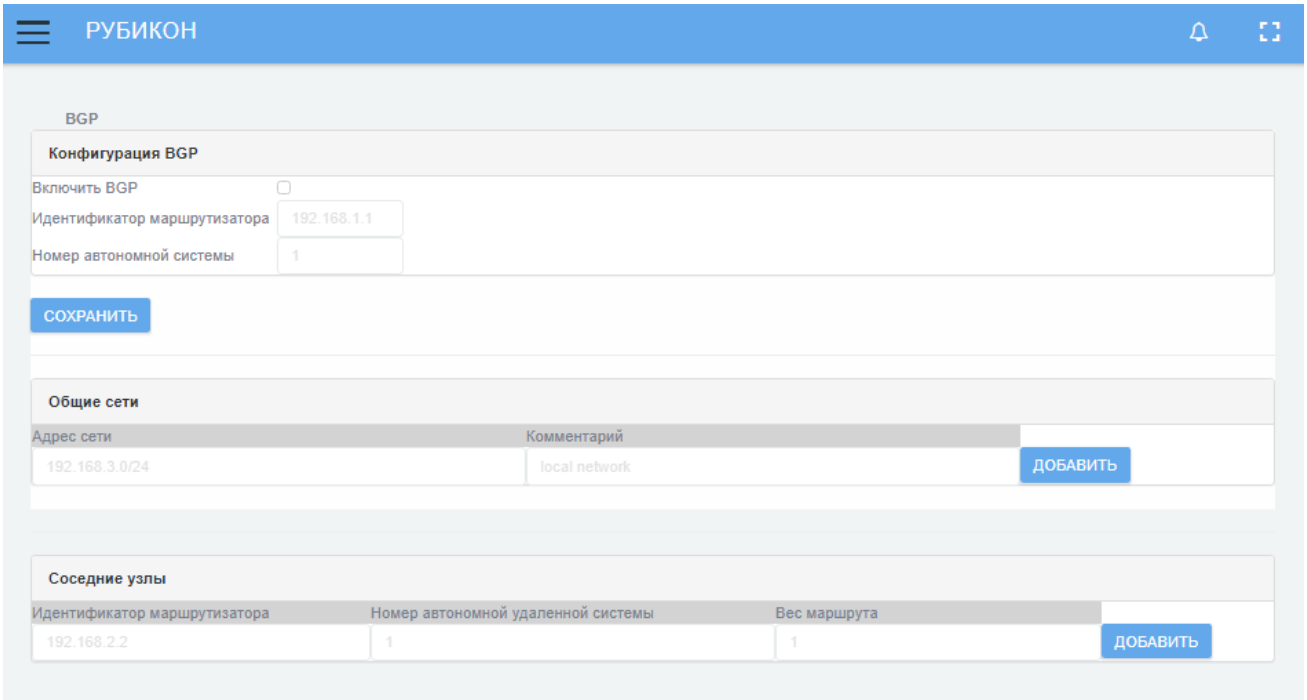


Рисунок 77 – Подраздел «BGP»

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

1) «Конфигурация BGP» — задание параметров самого 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» содержит элементы, указанные в таблице 33.

Таблица 33 – Описание элементов подраздела «BGP»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)

Элемент	Описание
Параметр «Включить BGP»	Параметр предназначен для указания необходимости включения/выключения службы BGP
Поле «Идентификатор маршрутизатора»	Поле предназначено для указания идентификатора маршрутизатора BGP. Идентификатор маршрутизатора — идентификатор в сети, однозначно определяющих маршрутизатор 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»	Поле предназначено для указания номера автономной системы, которой принадлежит маршрутизатор (диапазон возможных значений равен 1 – 65535: для публичных номеров используется диапазон 1 – 64495, для приватных 64512 – 65535)

Применение параметров настройки узла BGP в секции «Конфигурация BGP» осуществляется с помощью кнопки «Сохранить».

2.4.7.1 Поле «Общие сети»

Поле «Общие сети» (рисунок 78) содержит список всех доступных сетей и состоит из следующих параметров:

– «Адрес сети»;

– «Комментарий».

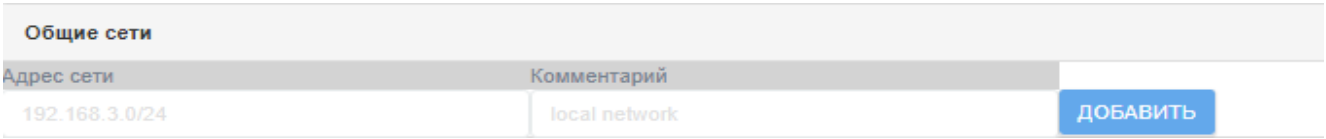
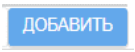


Рисунок 78 – Поле «Общие сети»

Поле «Общие сети» содержит элементы, указанные в таблице 34.

Таблица 34 – Описание элементов перечня «Сети»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «Адрес сети»	Предназначено для указания IP-адреса сети, маршрутная информация о которой будет распространяться
Поле «Комментарий»	Предназначено для описания сети
	Кнопка добавления новой сети в перечень «Сети»

При корректном заполнении параметров информация об анонсируемой сети добавляется в список. Удаление сети может быть выполнено нажатием кнопки « » .

2.4.7.2 Поле «Соседние узлы»

Поле «Соседние узлы» содержит список всех доступных узлов (рисунок 79).

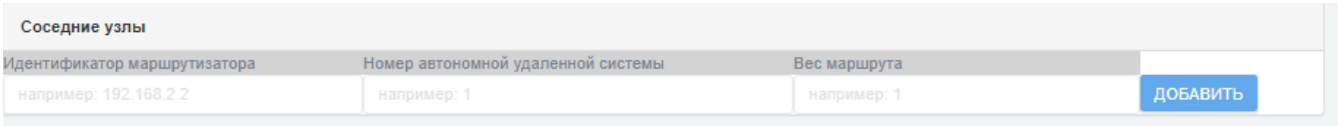


Рисунок 79 – Поле «Соседние узлы»

Перечень «Соседние узлы» распределяется по следующим параметрам:

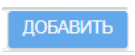
– «Идентификатор маршрутизатора»;

– «Номер автономной удаленной системы»;

– «Вес маршрута».

Перечень «Соседние узлы» содержит элементы, указанные в таблице 35.

Таблица 35 – Описание элементов перечня «Соседние узлы»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «Идентификатор маршрутизатора»	Предназначено для указания 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
Поле «Номер автономной удаленной системы»	Предназначено для указания 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
Поле «Вес маршрута»	Поле 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
	Кнопка добавления нового узла сети в перечень «Соседние узлы». В случае ввода и применения некорректных параметров, выводится сообщение об ошибке: 

2.4.8 Подраздел «VLANs»

Подраздел «VLANs» (рисунок 80) предназначен для создания виртуальных сетей.

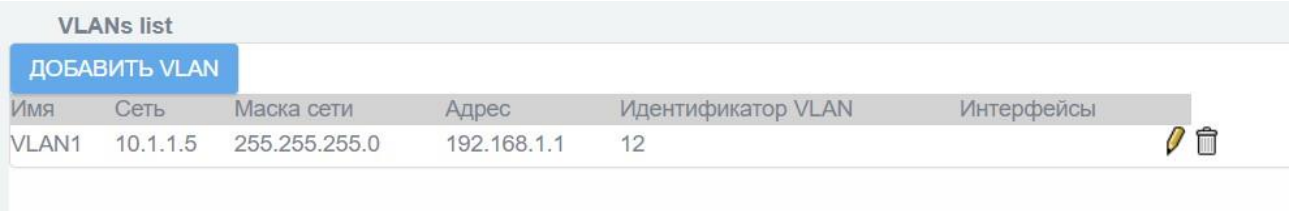


Рисунок 80 – Подраздел «VLANs»

Подраздел «VLANs» содержит перечень виртуальных сетей, распределенных по следующим параметрам:

– «Имя»;

– «Сеть»;

– «Маска сети»;

– «Адрес»;

– «Идентификатор VLAN»;

– «Интерфейсы».

Значок « » открывает меню редактирования VLAN.

Значок « » удаляет выбранную виртуальную сеть.

Кнопка « ДОБАВИТЬ VLAN » открывает меню создания виртуальной сети.

Пункт меню настройки МЭ «VLANs» предназначен для настройки виртуальных локальных сетей на канальном уровне модели OSI при создании логической топологии сети (рисунок 81).

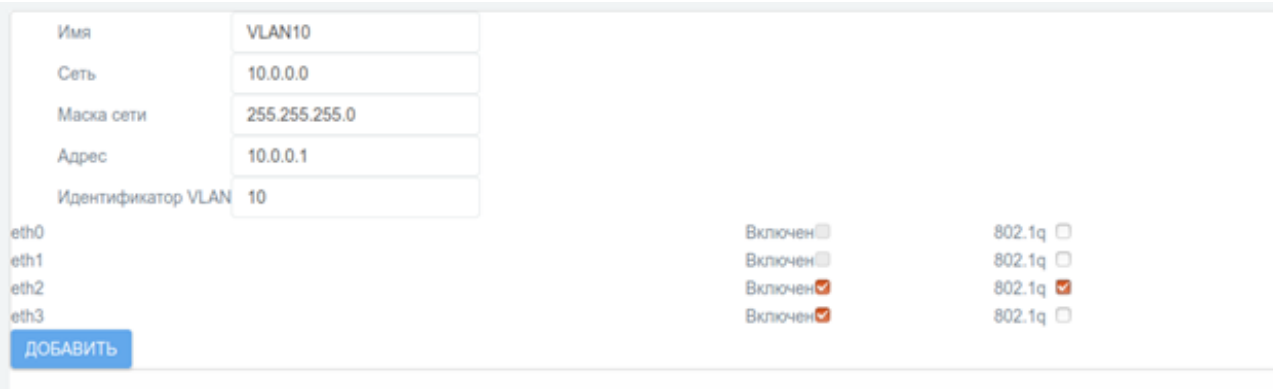


Рисунок 81 – Пример ввода параметров сети

На странице «Сеть → VLANs» отображается список существующих виртуальных сетей VLAN, взаимодействие которых обеспечивает комплекс «Рубикон» (рисунок 82).

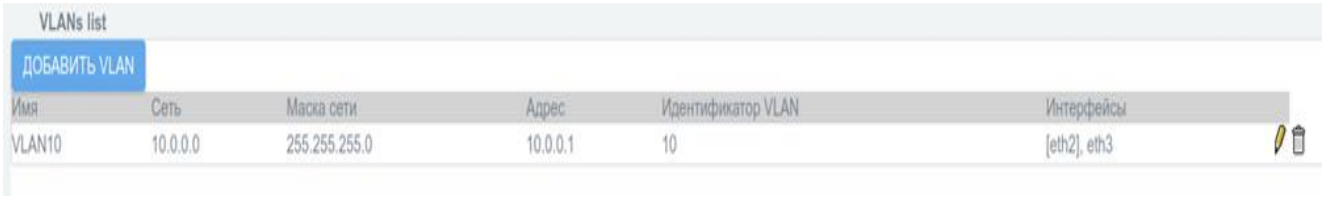


Рисунок 82 – Подраздел «VLANs». Список существующих виртуальных сетей VLAN

Для добавления новой виртуальной сети используется кнопка «Добавить VLAN».

При нажатии на кнопку «Добавить VLAN» пользователю предоставляется страница настройки параметров виртуальной сети VLAN. Необходимо задать следующие параметры:

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

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

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

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

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

Также необходимо выбрать сетевые интерфейсы, которые будут использоваться при создании виртуальной сети VLAN. При выборе сетевых интерфейсов необходимо учитывать, что:

a) 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;

b) в том случае, если настраиваемый сетевой интерфейс используется при создании нескольких виртуальных сетей VLAN, то для этого сетевого интерфейса необходимо установить флаг применения протокола 802.1q.

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 (рисунок 83).

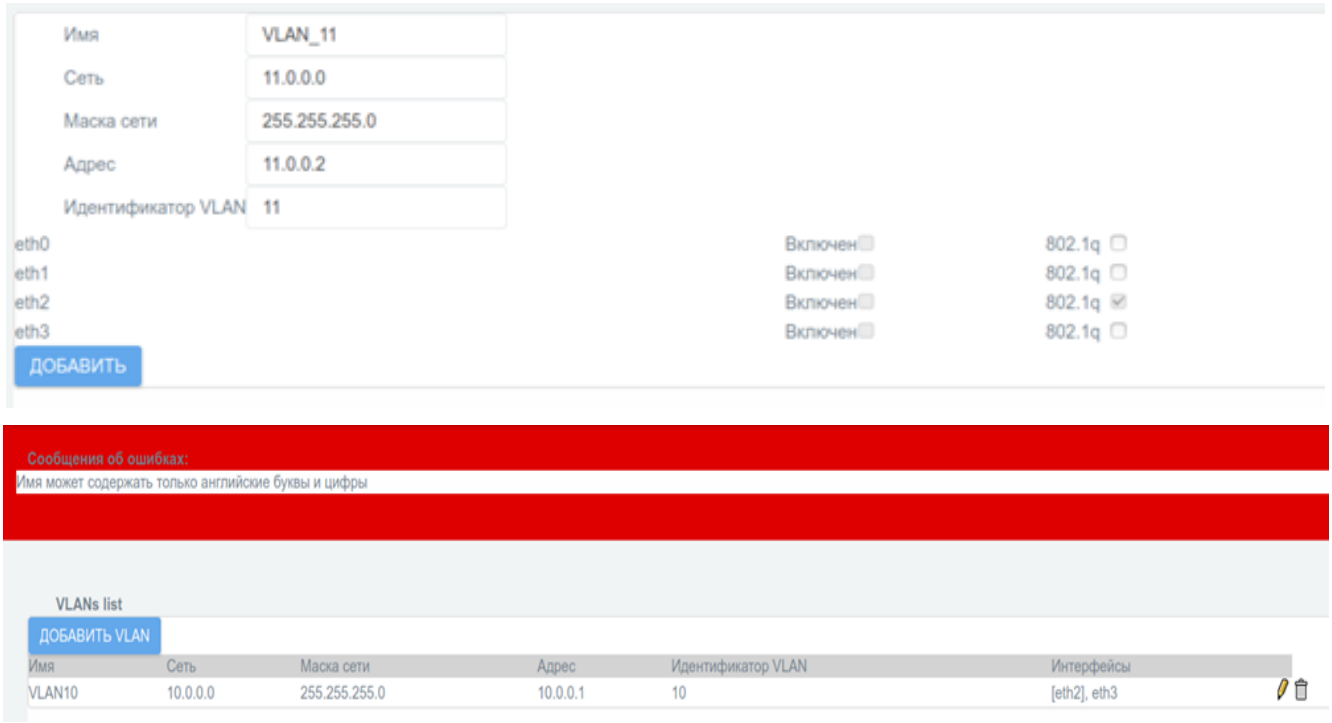


Рисунок 83 – Сообщение об ошибке при некорректном заполнении поля «Имя»

2.4.8.1 Меню создания виртуальной сети

Меню создания виртуальной сети (рисунок 84) предназначено для создания новой виртуальной сети. Меню создания новой виртуальной сети отрывается кнопкой «Добавить WLAN».

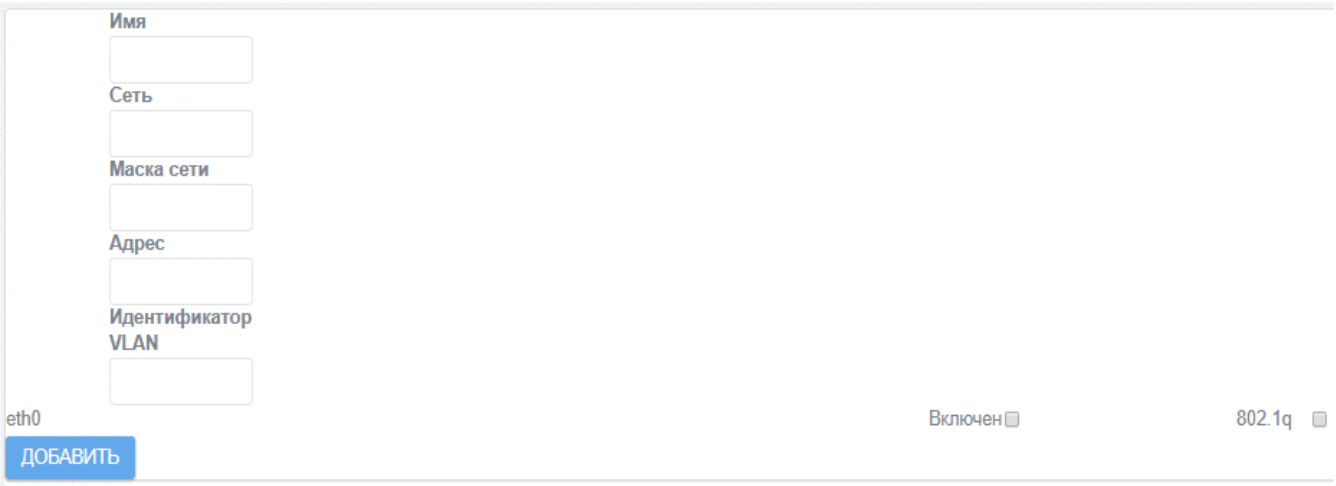


Рисунок 84 – Меню создания виртуальной сети

Меню создания виртуальной сети содержит элементы, указанные в таблице 36.

Таблица 36 – Описание элементов меню создания виртуальной сети

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Поле «Имя»	Поле ввода названия виртуальной сети
Поле «Сеть»	Предназначено для указания IP-сети VLAN
Поле «Маска сети»	Поле ввода маски виртуальной сети
Поле «Адрес»	Поле ввода IP-адреса виртуальной сети
Поле «Идентификатор VLAN»	Поле ввода идентификатора виртуальной сети
Параметр «Включен»	Включение виртуальной сети
Параметр «802.1q»	Включение процедуры тегирования трафика для передачи информации о принадлежности к VLAN по сетям стандарта IEEE 802.3ab Ethernet
	Кнопка добавления новой виртуальной сети

2.4.8.2 Меню редактирования виртуальной сети

Меню редактирования виртуальной сети (рисунок 85) предназначено для внесения изменений в существующую виртуальную сеть.

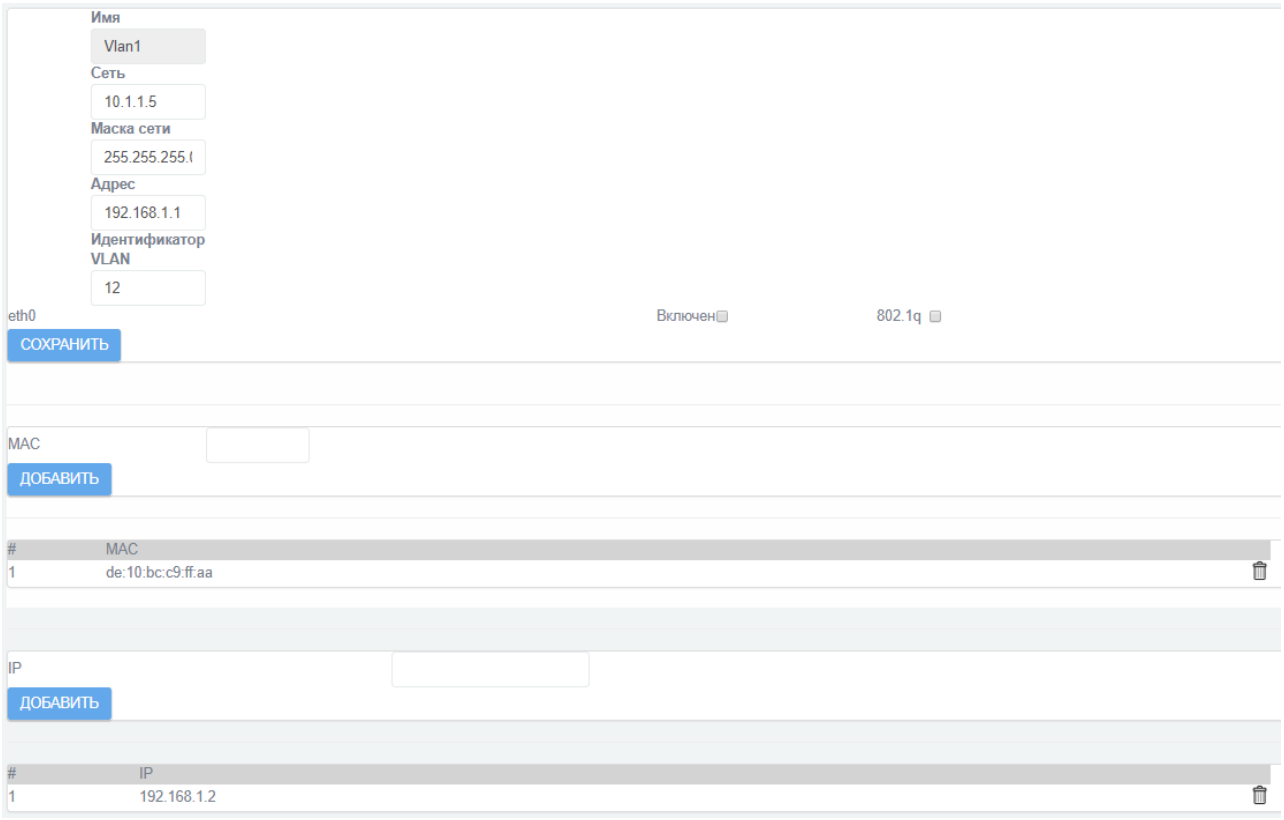


Рисунок 85 – Меню редактирования виртуальной сети

Меню редактирования виртуальной сети содержит элементы, указанные в таблице 37.

Таблица 37 – Описание элементов меню редактирования виртуальной сети

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Поле «Сеть»	Предназначено для указания IP-сети VLAN
Поле «Маска сети»	Поле ввода маски виртуальной сети
Поле «Адрес»	Поле ввода IP-адреса виртуальной сети

Элемент	Описание
Поле «Идентификатор VLAN»	Поле ввода идентификатора виртуальной сети
Параметр «Включен»	Включение виртуальной сети в МЭ
Параметр «802.1q»	Включение процедуры тегирования трафика для передачи информации о принадлежности к VLAN по сетям стандарта IEEE 802.3ab Ethernet
СОХРАНИТЬ	Кнопка сохранения измененных данных виртуальной сети

Меню редактирования виртуальной сети содержит следующие перечни:

– «MAC»;

– «IP».

2.4.8.3 Перечень «MAC»

Перечень «MAC» (рисунок 86) – перечень MAC-адресов устройств, находящихся в виртуальной сети.

Рисунок 86 – Перечень «MAC»

Перечень «MAC» содержит элементы, указанные в таблице 38.

Таблица 38 – Описание элементов перечня «MAC»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «MAC»	Поле ввода нового MAC-адреса
	Значок удаления MAC-адреса

Элемент	Описание
ДОБАВИТЬ	Кнопка добавления нового MAC-адреса

2.4.8.4 Перечень «IP»

Перечень «IP» (рисунок 87) – перечень IP-адресов, находящихся в виртуальной сети.

Рисунок 87 – Перечень «IP»

Перечень «IP» содержит элементы, указанные в таблице 39.

Таблица 39 – Описание элементов перечня «IP»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «IP»	Поле ввода нового IP-адреса
	Значок удаления IP-адреса
ДОБАВИТЬ	Кнопка добавления нового IP-адреса

Элемент	Описание

2.4.9 Подраздел «Мосты»

Подраздел «Мосты» (рисунок 88) позволяет объединить два или более ethernet сегментов в одну L2 сеть.

Рисунок 88 – Подраздел «Мосты»

2.4.9.1 Меню создания моста

Меню создания моста (рисунок 89, таблица 40).

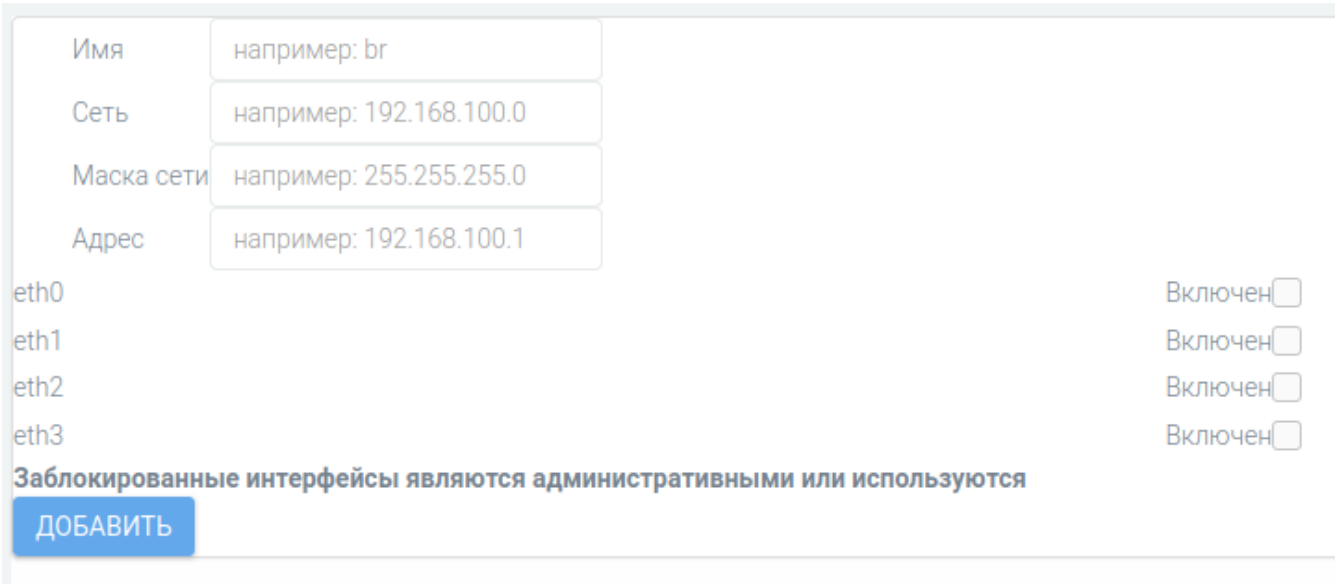


Рисунок 89 – Меню создания моста

Таблица 40 – Меню создания моста

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)

Элемент	Описание
Поле «Имя»	Предназначено для ввода названия моста
Поле «Сеть»	Предназначено для указания сети
Поле «Маска сети»	Предназначено для указания маски сети
Поле «Адрес»	Предназначено для ввода адреса сети
«eth0», «eth2», «eth1», «tun0», «tun2», «tun4»	Сетевые интерфейсы, которые активируются проставлением флажка
ДОБАВИТЬ	Кнопка добавления нового IP-адреса

2.4.10 Подраздел «Объединение интерфейсов»

Подраздел «Объединение интерфейсов» (рисунок 90) предназначен для задания конфигурации объединения интерфейсов.

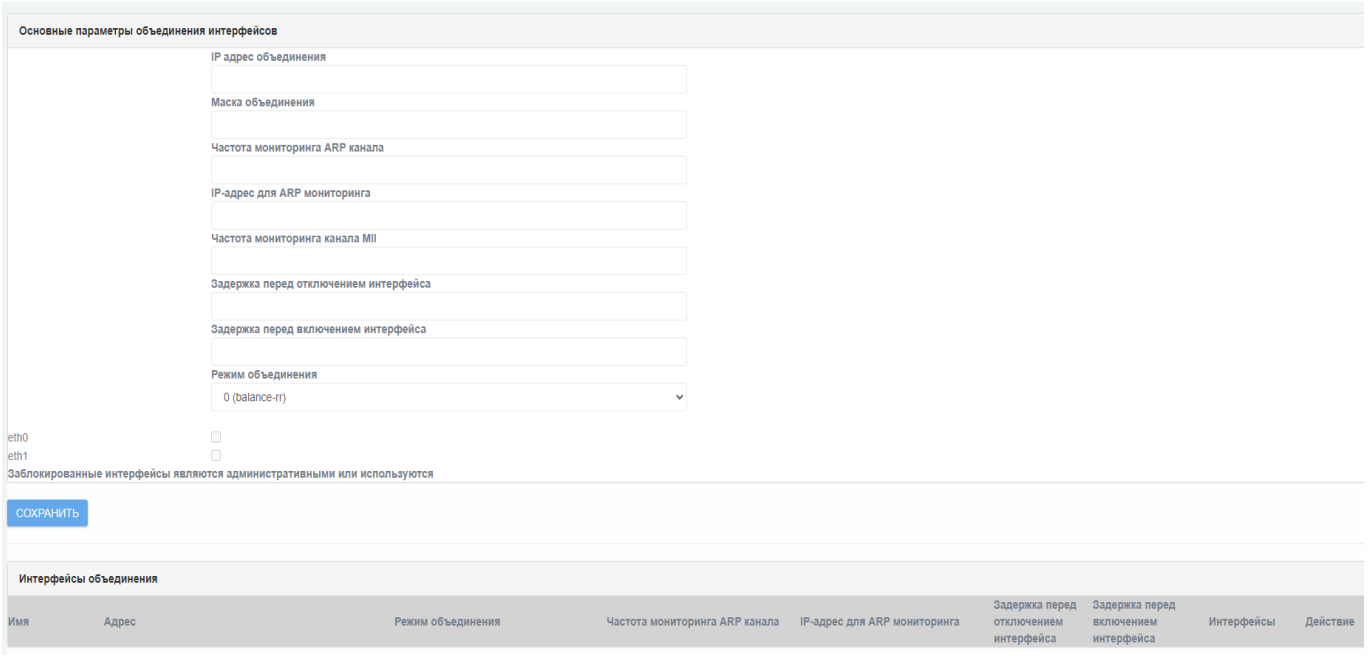
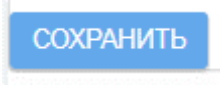


Рисунок 90 – Подраздел «Объединение интерфейсов»

Подраздел «Объединение интерфейсов» содержит элементы, указанные в таблице 41.

Таблица 41 – Описание элементов подраздела «Объединение интерфейсов»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок активации ниспадающего списка
Поле «IP адрес объединения»	Предназначено для указания общего IP-адреса для объединяемых интерфейсов
Поле «Маска объединения»	Предназначено для указания общей IP-маски для объединяемых интерфейсов
Частота мониторинга ARP канала	Определяет ARP мониторинг канала (в миллисекундах). Значение по умолчанию «0» (выключен). ARP мониторинг периодически проверяет на сетевых картах возможность приема и передачи трафика. Для проверки генерируются ARP запросы, отправляемые на адрес, указанный в поле «arp_ip_target»
IP-адрес для ARP мониторинга	Предназначено для указания IP-адреса для ARP мониторинга (используется если arp_ip_target>0). Например, IP-адрес указывается не как число, а как строка в формате xxx.xxx.xxx.xxx (для ipvIPV4). На эти адреса будут отправляться ARP запросы, для определения возможности приема-передачи через интерфейсы. Значение по умолчанию: без IP-адреса
Частота мониторинга канала MII	Устанавливает периодичность MII мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию «0» – отключает MII мониторинг

Элемент	Описание
Задержка перед отключением интерфейса	Предназначено для определения времени задержки (в миллисекундах) перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для MII мониторинга и значение параметра должно быть кратным значениям miimon. Значение по умолчанию «0»
Задержка перед включением интерфейса	Предназначено для задания времени задержки в миллисекундах, перед тем как поднять линк при обнаружении восстановления канала. Этот параметр возможен только при MII мониторинге, значение параметра должно быть кратным значениям miimon
Ниспадающий список «Режим объединения»	Предназначен для указания режима объединения, в котором будут работать выбранные интерфейсы. Ниспадающий список имеет следующие опции: – «0» (balance-rr); – «1» (active-backup); – «2» (balance-xor); – «3» (broadcast); – «4» (802.3ad); – «5» (balance-tlb); – «6» (balance-alb)
«eth0», «eth2», «eth1», «tun0», «tun2», «tun4»	Сетевые интерфейсы, которые активируются проставлением флажка
	Кнопка сохранения введенных данных

Основные параметры объединения интерфейсов требуют ввод следующих полей:

1) «Включение объединения» — переключатель для включения или выключения функции объединения сетевых интерфейсов;

2) «IP адрес объединения» — 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;

3) «Маска объединения» — маска, определяющая диапазон адресов в подсети агрегированных интерфейсов в формате четырех десятичных чисел, разделенных точками;

4) «Режим объединения» — режим, в котором согласованно работают включенные в объединение сетевые интерфейсы. Существует 7 режимов:

– «0» (balance-rr) — режим балансировки (совместного использования интерфейсов с уравниванием пропускной способности), в котором сетевые пакеты поочередно отправляются через участвующие в объединении интерфейсы;

– «1» (active-backup) — режим, при котором используется только один сетевой интерфейс (активный), а второй, резервный, подключается только при отсутствии передачи через первый. В текущей версии не используется;

– «2» (balance-xor) — режим балансировки (совместного использования интерфейсов с уравниванием пропускной способности), в котором решение о направлении сетевых пакетов через участвующие в объединении интерфейсы принимается на основании вычисления функции взятия остатка от деления на количество резервируемых интерфейсов от двоичной операции XOR адреса источника и адреса;

– «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;

– «5» (balance-tlb) — режим балансировки (совместного использования интерфейсов с уравниванием пропускной способности), в котором решение о направлении сетевых пакетов через участвующие в объединении интерфейсы принимается на основании текущей загрузки канала;

– «6» (balance-alb) — режим балансировки (совместного использования интерфейсов с уравниванием пропускной способности), в котором решение о направлении сетевых пакетов через участвующие в объединении интерфейсы принимается на основании текущей загрузки канала и

ARP-ответов принимающего узла.

2.5 Раздел «Службы»

Раздел «Службы» содержит следующие подразделы:

– подраздел «Прокси»;

– подраздел «FTP посредник»;

– подраздел «Сервер DHCP»;

– подраздел «Динамический DNS»;

– подраздел «Задать имена хостов»;

– подраздел «Сервер времени»;

– подраздел «Ограничение Трафика»;

– подраздел «Проверка доступности узлов».

2.5.1 Подраздел «Прокси»

Подраздел «Прокси» (рисунок 91) предназначен для настройки прокси-сервера.

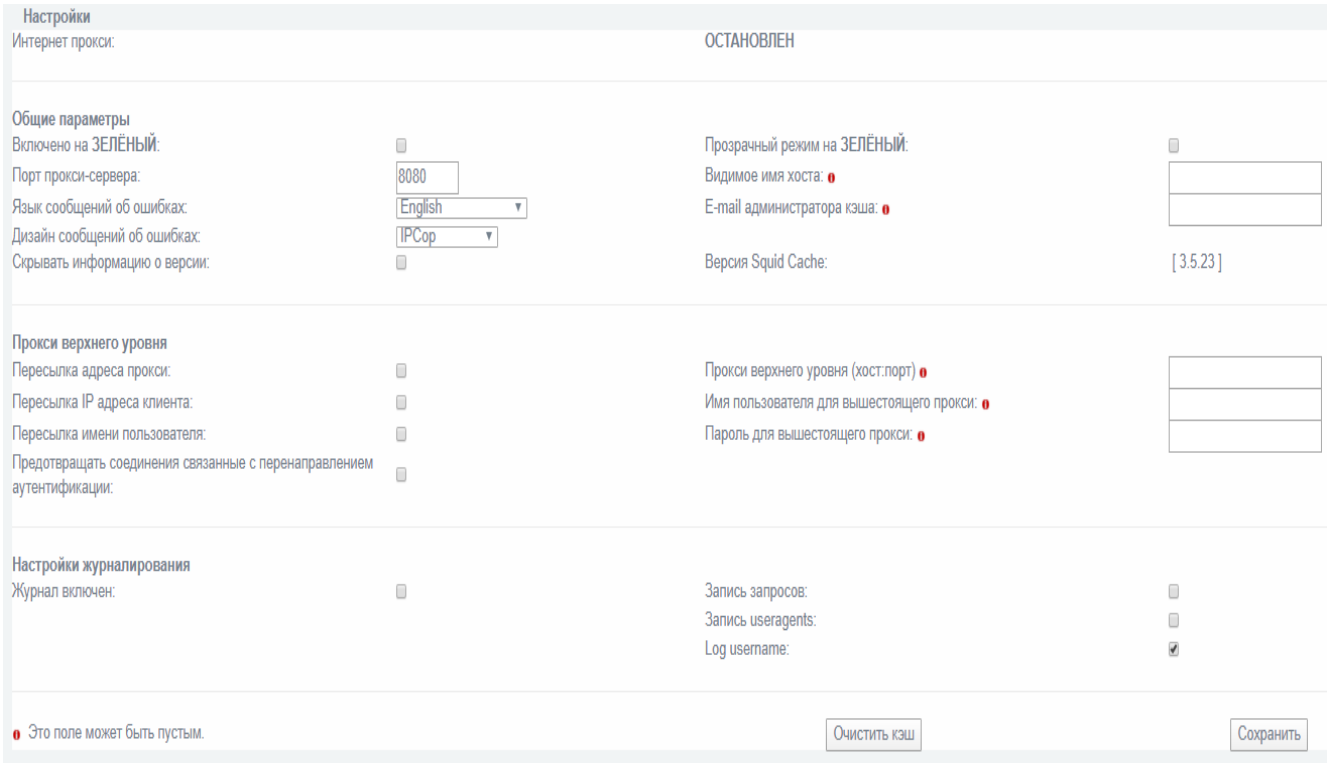


Рисунок 91 – Подраздел «Прокси»

Подраздел «Прокси» состоит из следующих блоков:

а) «Настройки»:

– «Общие параметры»;

– «Прокси верхнего уровня»;

– «Настройки журналирования»;

b) «Расширенные настройки:

– «Управление кэшем»;

– «Порты назначения»;

– «Контроль доступа по адресу»;

– «Классные расширения»;

– «Список URL фильтрации»;

– «Ограничение по времени»;

– «Лимиты передачи»;

– «Регулирование закачки»;

– «Фильтр MIME типов»;

– «Веб-браузер»;

– «Конфиденциальность;

– «Redirectors»;

– «Метод аутентификации»;

– «Взаимодействие с сервером ICAP»;

– «Фильтрация скриптов».

2.5.1.1 Общие параметры настроек

Настройки состоят из следующих блоков:

– «Общие параметры»;

– «Прокси верхнего уровня»;

– «Настройки журналирования».

В таблице 42 указаны общие элементы для блоков «Настройки».

Таблица 42 – Общие элементы блоков «Настройки»

Элемент	Описание
Интернет прокси	Статус прокси
	Поле для ввода необходимой информации

Элемент	Описание
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок активации ниспадающего списка
	Значок необязательности заполнения поля
	Кнопка предназначена для очистки информации из хранилища кэш
	Кнопка сохранения введенных данных

2.5.1.2 Блок «Общие параметры»

Блок «Общие параметры» (рисунок 92) предназначен для ввода общих настроек прокси сервера.

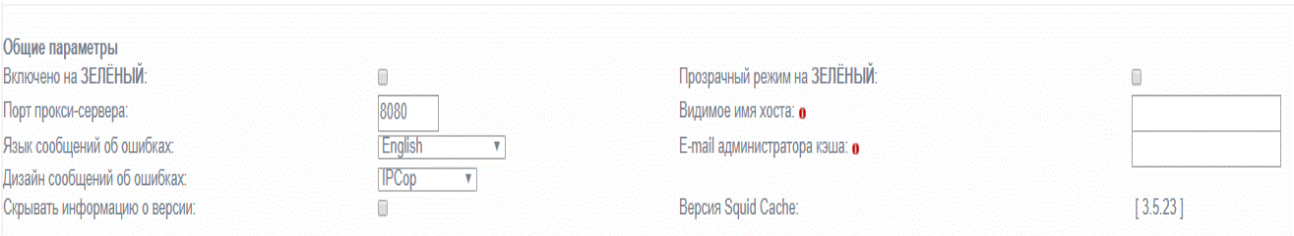


Рисунок 92 – Блок «Общие параметры»

Блок «Общие параметры» состоит из следующих вариантов настроек (таблица 43).

Таблица 43 – Параметры настроек блока «Общие параметры»

Настройка	Описание
Параметр «Включено на ЗЕЛЁНЫЙ»	Параметр предназначен для указания необходимости включения/отключения службы прокси-сервера на зеленом интерфейсе
Поле «Порт прокси-сервера»	Поле предназначено для указания номера сетевого порта, на котором работает служба прокси-сервера

Настройка	Описание
Ниспадающий список «Язык сообщений об ошибках»	Ниспадающий список предназначен для указания языка сообщений об ошибках
Ниспадающий список «Дизайн сообщений об ошибках»	Предназначен для указания варианта дизайна сообщения об ошибках: – IPCop; – Стандартный
Параметр «Скрывать информацию о версии»	Предназначен для указания необходимости скрытия/отображения пользователю информации о версии прокси-сервера
Параметр «Прозрачный режим на ЗЕЛЁНЫЙ»	Предназначен для указания необходимости включения/отключения службы прокси-сервера в прозрачном режиме. То есть без необходимости пользователю настройки параметров прокси-сервера на стороне клиента
Поле «Видимое имя хоста»	Предназначено для указания имени узла прокси-сервера, которое будет передано клиенту при подключении
Поле «E-mail администратора кэша»	Предназначено для указания адреса электронной почты администратора механизма кэширования прокси-сервера
Текст «Версия Squid Cache»	Информация о версии прокси-сервера

2.5.1.3 Блок «Прокси верхнего уровня»

Блок «Прокси верхнего уровня» (рисунок 93) предназначен для настройки параметров верхнеуровневого прокси сервера.

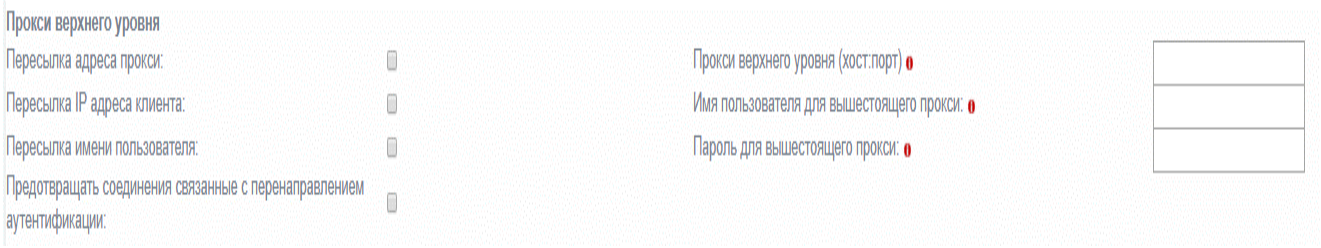


Рисунок 93 – Блок «Прокси верхнего уровня»

Блок «Прокси верхнего уровня» состоит из следующих вариантов настроек (таблица 44).

Таблица 44 – Параметры настроек блока «Прокси верхнего уровня»

Настройка	Описание
Параметр «Пересылка адреса прокси»	Предназначен для указания необходимости пересылки адреса прокси-серверу верхнего уровня
Параметр «Пересылка IP адреса клиента»	Предназначен для указания необходимости пересылки IP-адреса клиента прокси-серверу верхнего уровня
Параметр «Пересылка имени пользователя»	Предназначен для указания необходимости пересылки имени пользователя прокси-серверу верхнего уровня
Параметр «Предотвращать соединения связанные с перенаправлением аутентификации»	Предназначен для указания необходимости предотвращения соединений, связанных с перенаправлением аутентификации
Поле «Прокси верхнего уровня (хост: порт)»	Предназначено для указания адреса и порта для прокси-сервера верхнего уровня
Поле «Имя пользователя для вышестоящего прокси»	Предназначено для указания имени пользователя для прокси-сервера верхнего уровня
Поле «Пароль для вышестоящего прокси»	Предназначено для указания пароля прокси-сервера верхнего уровня

2.5.1.4 Блок «Настройки журналирования»

Блок «Настройки журналирования» (рисунок 94) предназначен для настройки параметров журналирования.

Рисунок 94 – Блок «Настройки журналирования»

Блок «Настройки журналирования» состоит из следующих вариантов настроек (таблица 45).

Таблица 45 – Параметры настроек блока «Настройки журналирования»

Настройка	Описание
Параметр «Журнал включен»	Предназначен для указания необходимости журналирования
Параметр «Запись запросов»	Предназначен для указания необходимости записи запросов HTTP в журнал
Параметр «Запись useragents»	Предназначен для указания необходимости записи параметра useragent в журнал
Параметр «Log username»	Предназначен для указания необходимости записи имени пользователя в журнал

2.5.1.5 Общие параметры расширенных настроек

Расширенные настройки состоят из следующих блоков:

– «Управление кэшем»;

– «Порты назначения»;

– «Контроль доступа по адресу»;

– «Классные расширения»;

– «Список URL фильтрации;

– «Ограничение по времени»;

– «Лимиты передачи»;

– «Регулирование закачки;

– «Фильтр MIME типов»;

– «Веб-браузер»;

– «Конфиденциальность»;

– «Redirectors»;

– «Метод аутентификации»;

– «Взаимодействие с сервером ICAP»;

– «Фильтрация скриптов».

В таблице 46 указаны общие элементы для блоков «Расширенные настройки».

Таблица 46 – Общие элементы блоков «Расширенные настройки»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок активации ниспадающего списка
	Значок изменения размера поля ввода данных
test eicar	Загрузка стандартного файла, применяемого для проверки работоспособности антивируса
	Значок необязательности заполнения поля
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)

Элемент	Описание
Очистить кэш	Кнопка предназначена для очистки информации из хранилища кэш
Сохранить	Кнопка сохранения введенных данных

2.5.1.6 Блок «Управление кэшем»

Блок «Управление кэшем» (рисунок 95) предназначен для настройки параметров кэширования.

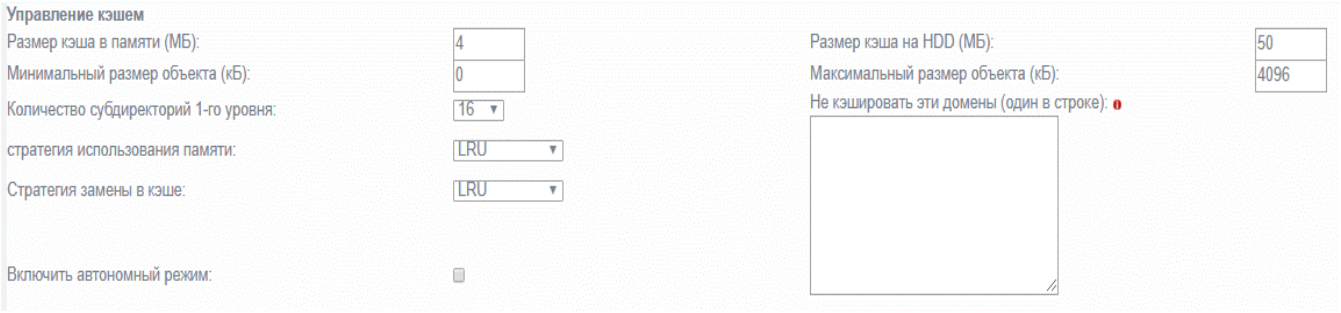


Рисунок 95 – Блок «Управление кэшем»

Блок «Управление кэшем» состоит из следующих вариантов настроек (таблица 47).

Таблица 47 – Параметры настроек блока «Управление кэшем»

Настройка	Описание
Поле «Размер кэша в памяти (МБ)»	Предназначено для указания размера кэша в памяти
Поле «Минимальный размер объекта (кБ)»	Предназначено для указания минимального размера объекта
Ниспадающий список «Количество субдиректорий 1-го уровня»	Ниспадающий список состоит из следующих параметров: – 16; – 32; – 64; – 128; – 256

Настройка	Описание
Ниспадающий список «стратегия использования памяти»	Ниспадающий список состоит из следующих параметров: – LRU; – heap LFUDA; – heap GDSF; – heap LRU
Ниспадающий список «Стратегия замены в кэше»	Ниспадающий список состоит из следующих параметров: – LRU; – heap LFUDA; – heap GDSF; – heap LRU
Параметр «Включить автономный режим»	Включение автономного режима
Поле «Размер кэша на HDD (МБ)»	Размер кэша на жестком диске
Поле «Максимальный размер объекта (кБ)»	Предназначено для указания максимального размера объекта
«Не кэшировать эти домены (один в строке)»	Предназначено для внесения перечня доменов вручную

2.5.1.7 Блок «Порты назначения»

Блок «Порты назначения» (рисунок 96) предназначен для настройки параметров портов.

Рисунок 96 – Блок «Порты назначения»

Блок «Порты назначения» состоит из следующих вариантов настроек (таблица 48).

Таблица 48 – Параметры настроек блока «Порты назначения»

Настройка	Описание
Поле «Разрешенные стандартные порты (один в строке)»	Предназначено для внесения разрешенных стандартных портов
Поле «Разрешенные SSL порты (один в строке)»	Предназначено для внесения разрешенных SSL портов

2.5.1.8 Блок «Контроль доступа по адресу»

Блок «Контроль доступа по адресу» (рисунок 97) предназначен для настройки параметров доступа по заранее заданным адресам. Параметры настроек блока представлены ниже (таблица 49).

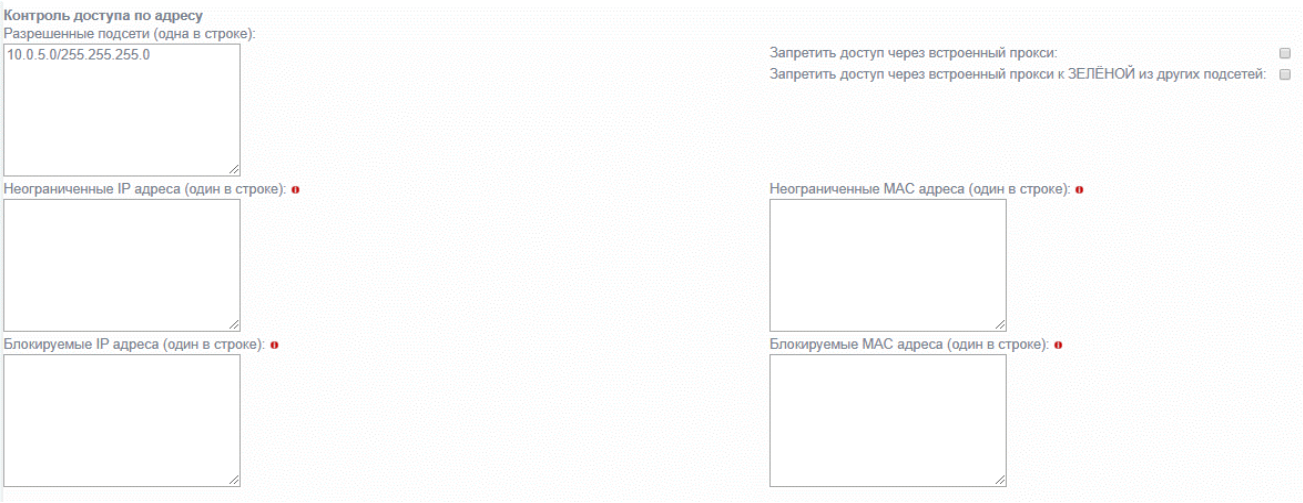


Рисунок 97 – Блок «Контроль доступа по адресу»

Таблица 49 – Параметры настроек блока «Контроль доступа по адресу»

Настройка	**Описание**
Поле «Разрешенные подсети (одна в строке)»	Предназначено для внесения разрешенных подсетей. Для всех перечисленных подсетей разрешен доступ к прокси-серверу
Поле «Неограниченные IP адреса (один в строке)»	Предназначено для внесения 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 ЭВМ (доступно, если включена проверка подлинности)
Поле «Блокируемые IP адреса (один в строке)»	Предназначено для внесения IP-адресов, все запросы от которых будут заблокированы

Настройка	Описание
Поле «Неограниченные MAC адреса (один в строке)»	Предназначено для внесения 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 внесения MAC-адресов, все запросы от которых будут заблокированы
	Значок необязательности заполнения поля

2.5.1.9 Блок «Классные расширения»

Блок «Классные расширения» (рисунок 98) предназначен для настройки параметров расширений. Параметры настроек блока представлены ниже (таблица 50).

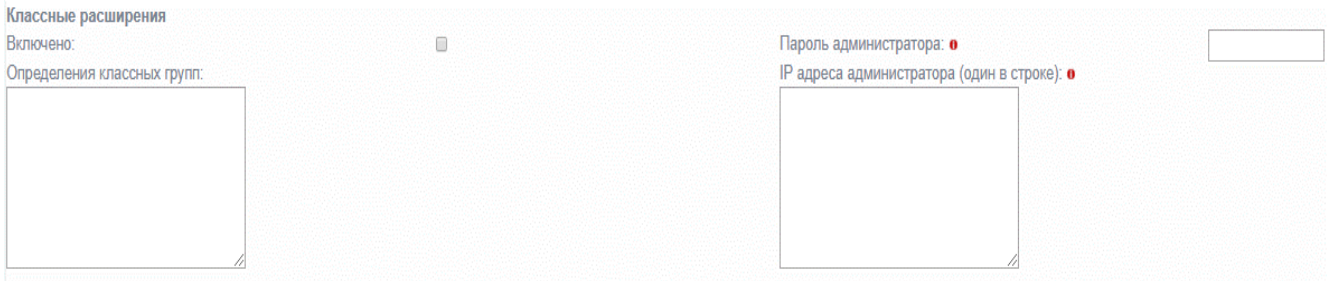


Рисунок 98 – Блок «Классные расширения»

Таблица 50 – Параметры настроек блока «Классные расширения»

Настройка	Описание
	Поле для ввода необходимой информации

Настройка	Описание
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
«Включено»	Установите флажок, чтобы включить административный интерфейс управления веб-доступом
«Пароль администратора»	Если пароль установлен, введите пароль для управления веб-доступом
Поле «Определение классных групп»	Предназначено для внесения классных групп. Формат групп: – [Example group 1]; – 192.168.1.11; – 192.168.1.12; – 192.168.1.13; – [Example group 2]; – 192.168.1.21-192.168.1.25
Поле «IP-адреса администратора»	Предназначено для внесения IP-адресов. Это поле позволяет определить IP-адреса, которые смогут управлять веб-доступом
	Значок необязательности заполнения поля

2.5.1.10 Блок «Список URL фильтрации»

Блок «Список URL фильтрации» (рисунок 99) дает возможность блокирования web-запросов по ключевому слову в адресе с помощью задания «черных» и «белых» списков. Параметры настроек блока представлены ниже (таблица 51).

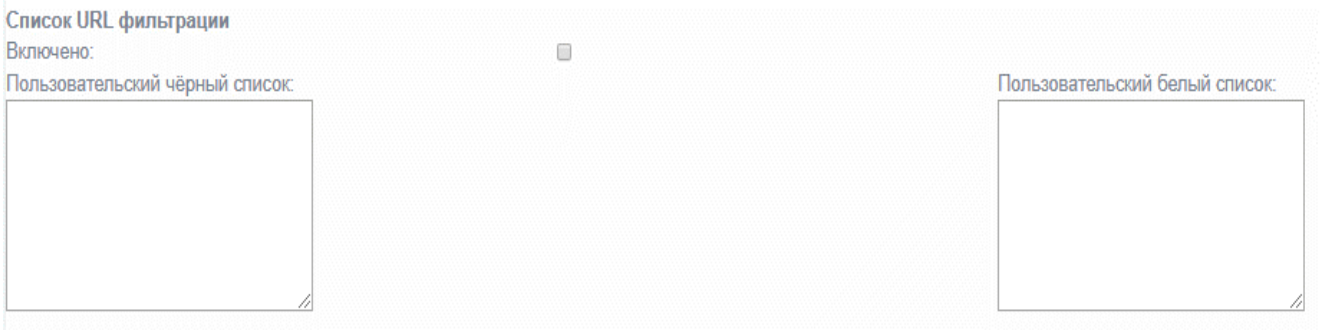


Рисунок 99 – Блок «Список URL фильтрации»

Таблица 51 – Параметры настроек блока «Список URL фильтрации»

Настройка	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
«Включено»	Установите флажок, чтобы включить URL фильтрацию
Поле «Пользовательский черный список»	Предназначено для создания «черного» списка
Поле «Пользовательский белый список»	Предназначено для создания «белого» списка

2.5.1.11 Блок «Ограничение по времени»

Блок «Ограничение по времени» (рисунок 100) предназначен для настройки параметров ограничения времени.

Рисунок 100 – Блок «Ограничение по времени»

Блок «Ограничение по времени» состоит из следующих вариантов настроек (таблица 52).

Таблица 52 – Параметры настроек блока «Ограничение по времени»

Настройка	Описание
Ниспадающий список «доступ»	Определение возможности доступа для указанного времени: – разрешить; – запретить
Параметр «Пн – Вс»	Указание дня недели, для которого будет действовать правило ограничения по времени
Ниспадающий список «с – по»	Указание времени для ограничения по времени

2.5.1.12 Блок «Лимиты передачи»

Блок «Лимиты передачи» (рисунок 101) предназначен для настройки параметров лимитов передачи.

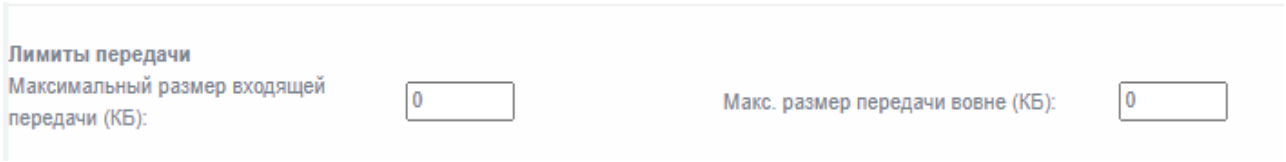


Рисунок 101 – Блок «Лимиты передачи»

Блок «Лимиты передачи» состоит из следующих вариантов настроек (таблица 53).

Таблица 53 – Параметры настроек блока «Лимиты передачи»

Настройка	Описание
Поле «Лимиты передач»	Контроль и уменьшение объема трафика
Поле «Макс. размер передачи вовне (КБ)»	Максимально разрешенный размер передачи вовне

2.5.1.13 Блок «Регулирование закачки»

Блок «Регулирование закачки» (рисунок 102) предназначен для регулирования параметров скорости и контента закачки.

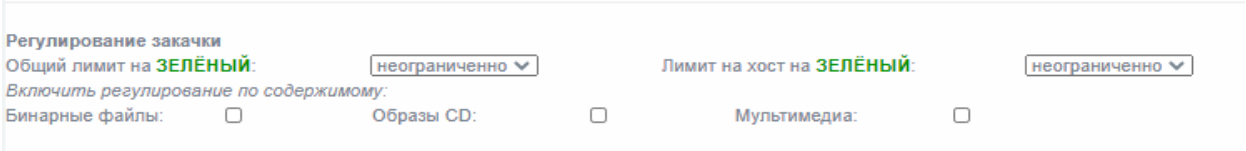


Рисунок 102 – Блок «Регулирование закачки»

Блок «Регулирование закачки» состоит из следующих настроек (таблица 54).

Таблица 54 – Параметры настроек блока «Лимиты передачи»

Настройка	Описание
☑	Поле с проставленным флажком (параметр включен)
☐	Пустое поле для проставления флажка (параметр выключен)
Ниспадающий список «Общий лимит на ЗЕЛЕНЫЙ»	Ниспадающий список: – 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
Ниспадающий список «Лимит на хост на ЗЕЛЕНЫЙ»	
Поле «Бинарные файлы»	Регулирование контента применяется к бинарным файлам: bz2, r, dmg, exe, sea, tar, tgz, zip

Настройка	Описание
☑	Поле с проставленным флажком (параметр включен)
☐	Пустое поле для проставления флажка (параметр выключен)
Поле «Образы CD»	Регулирование контента применяется к образам CD: ccd, cdi, img, iso, raw, tib
Поле «Мультимедиа»	Регулирование контента применяется к мультимедийным файлам: aiff, avi, divx, mov, mp3, mp4, mpeg, qt

2.5.1.14 Блок «Фильтр MIME типов»

Блок «Фильтр MIME типов» (рисунок 103) предназначен для настройки параметров фильтра MIME типов. Фильтр MIME включает фильтрацию по MIME типов может быть настроен на блокирование содержимого в зависимости от его типа.

Рисунок 103 – Блок «Фильтр MIME типов»

Блок «Фильтр MIME типов» состоит из следующих вариантов настроек (таблица 55).

Таблица 55 – Параметры настроек блока «Фильтр MIME типов»

Настройка	Описание
Параметр «Включено»	Параметр включения фильтра MIME типов. Если фильтр включен, проверяются все входящие заголовки MIME типов

Настройка	Описание
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Поле «Блокировать эти MIME типы»	Предназначено для добавления MIME типов (каждый тип добавляют на отдельной строке). Например: video/mpeg video/quicktime
Поле «Не фильтровать следующие направления»	Предназначено для добавления доменов, субдоменов, имен хостов, IP-адресов, URL (каждый на отдельной строке)
	Значок необязательности заполнения поля

2.5.1.15 Блок «Веб-браузер»

Блок «Веб-браузер» (рисунок 104) предназначен для настройки параметров проверки и разрешения использования веб-браузера.

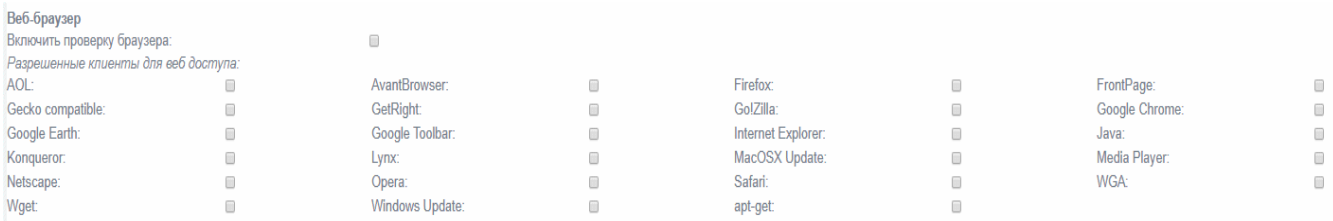


Рисунок 104 – Блок «Веб-браузер»

Блок «Веб-браузер» состоит из следующих вариантов настроек (таблица 56).

Таблица 56 – Параметры настроек блока «Веб-браузер»

Настройка	Описание
Параметр «Включить проверку браузера»	Параметр включения проверки веб-браузера на соответствие разрешенному типу
Параметр «Разрешенные клиенты для веб доступа»	Указание типа веб-браузера, разрешенного к использованию

2.5.1.16 Блок «Конфиденциальность»

Блок «Конфиденциальность» (рисунок 105) предназначен для настройки параметров конфиденциальности.

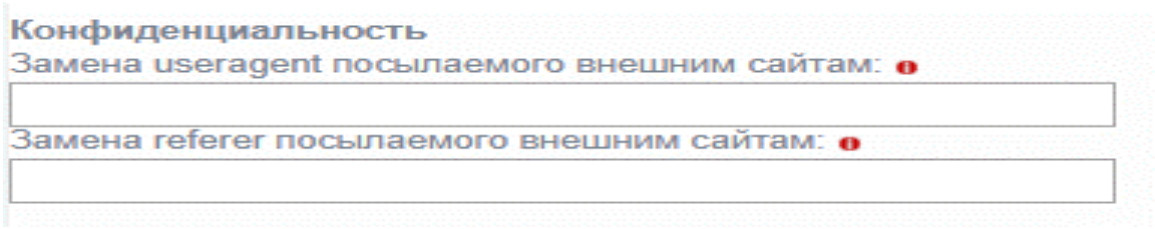


Рисунок 105 – Блок «Конфиденциальность»

Блок «Конфиденциальность» состоит из следующих вариантов настроек (таблица 57).

Таблица 57 – Параметры настроек блока «Конфиденциальность»

Настройка	Описание
Поле «Замена useragent посылаемого внешним сайтам»	По умолчанию параметр useragent в данный момент, используемый веб-браузером будет предоставлен на внешние веб-сервера. Некоторые динамические веб-сайты генерируют контент в зависимости от представленной строки useragent. Эта строка также записывается в лог-файлы веб-сервера
Поле «Замена referer посылаемого внешним сайтам»	При нажатии на гиперссылку, URL-адрес источника будет представлен сайту назначения. Эта опция может быть отключена путем введения пользователем определенной строки. Эта строка будет представлена вместо реального

Настройка	Описание
	адреса. Опция может быть полезна для защиты конфиденциальности
	Значок необязательности заполнения поля

2.5.1.17 Блок «Redirectors»

Блок «Redirectors» (рисунок 106) предназначен 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.

Рисунок 106 – Блок «Redirectors»

Блок «Redirectors» состоит из следующих вариантов настроек (таблица 58).

Таблица 58 – Параметры настроек блока «Redirectors»

Настройка	Описание
Параметр «Включено»	Установите флажок, чтобы включить перенаправление
Поле «Number of redirector processes»	Предназначено для увеличения или уменьшения количества активных процессов фильтрации. Количество процессов зависит от пропускной способности и числа одновременных пользователей. Значение по умолчанию «5»
Поле «Available redirectors»	Предназначено для отображения установленных redirectors
Параметр «URL filter»	Установите флажок, чтобы включить URL filter. Включенный URL-filter дает возможность блокировать веб-запросы по ключевому слову

2.5.1.18 Блок «Метод аутентификации»

Блок «Метод аутентификации» (рисунок 107) предназначен для настройки параметров метода аутентификации.

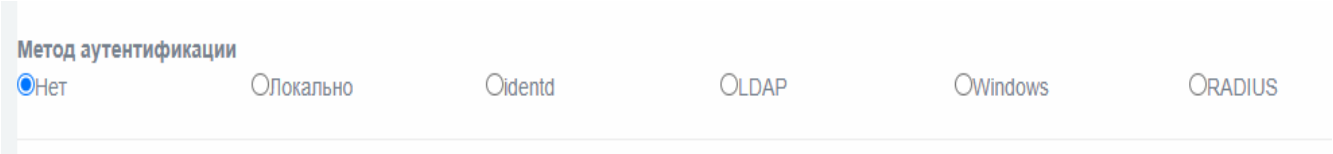


Рисунок 107 – Блок «Метод аутентификации»

Блок «Метод аутентификации» состоит из следующих вариантов настроек (таблица 59).

Таблица 59 – Параметры настроек блока «Метод аутентификации»

Настройка	Описание
Параметр «Метод аутентификации»	Параметр для выбора одного из нескольких методов аутентификации, указанных в списке: – Нет; – Локально; – Identd; – LDAP; – Windows; – RADIUS

2.5.1.19 Блок «Взаимодействие с сервером ICAP»

Блок «Взаимодействие с сервером ICAP» (рисунок 108) предназначен для настройки параметров взаимодействия с сервером ICAP.

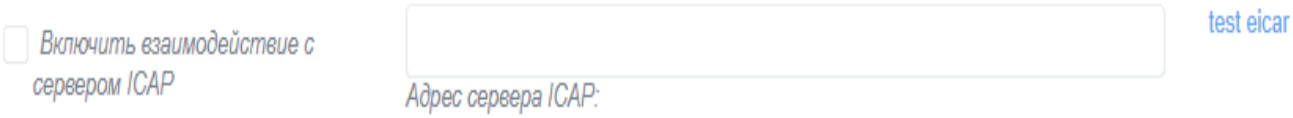


Рисунок 108 – Блок «Взаимодействие с сервером ICAP»

Блок «Взаимодействие с сервером ICAP» состоит из следующих вариантов настроек (таблица 60).

Таблица 60 – Параметры настроек блока «Взаимодействие с сервером ICAP»

Настройка	Описание
Параметр «Включить взаимодействие с сервером ICAP»	Параметр включения взаимодействия с сервером ICAP
Поле «Адрес сервера ICAP»	Адрес сервера ICAP
Ссылка «test eicar»	Загрузка стандартного файла, применяемого для проверки работоспособности антивируса

2.5.1.20 Блок «Фильтрация скриптов»

Блок «Фильтрация скриптов» (рисунок 109) предназначен для настройки параметров фильтрации скриптов.

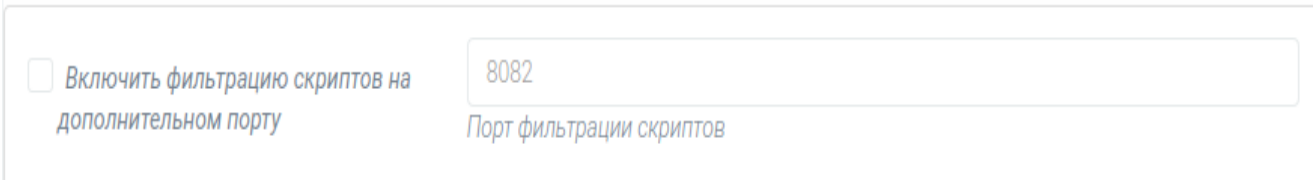


Рисунок 109 – Блок «Фильтрация скриптов»

Блок «Фильтрация скриптов» предназначен для разрешения или блокирования скриптов в ответах HTTP сервера. Блок состоит из следующих вариантов настроек (таблица 61).

Таблица 61 – Параметры настроек блока «Фильтрация скриптов»

Настройка	Описание
Параметр «Включить фильтрацию скриптов на дополнительном порту»	Параметр включения фильтрации скриптов
Параметр «Разрешить скрипты»	Параметр включения скриптов

Настройка	Описание
Поле «Порт HTTP фильтра»	Поле указания порта HTTP фильтра

2.5.2 Подраздел «FTP посредник»

Подраздел «FTP посредник» (рисунок 110) предназначен для настройки FTP прокси.

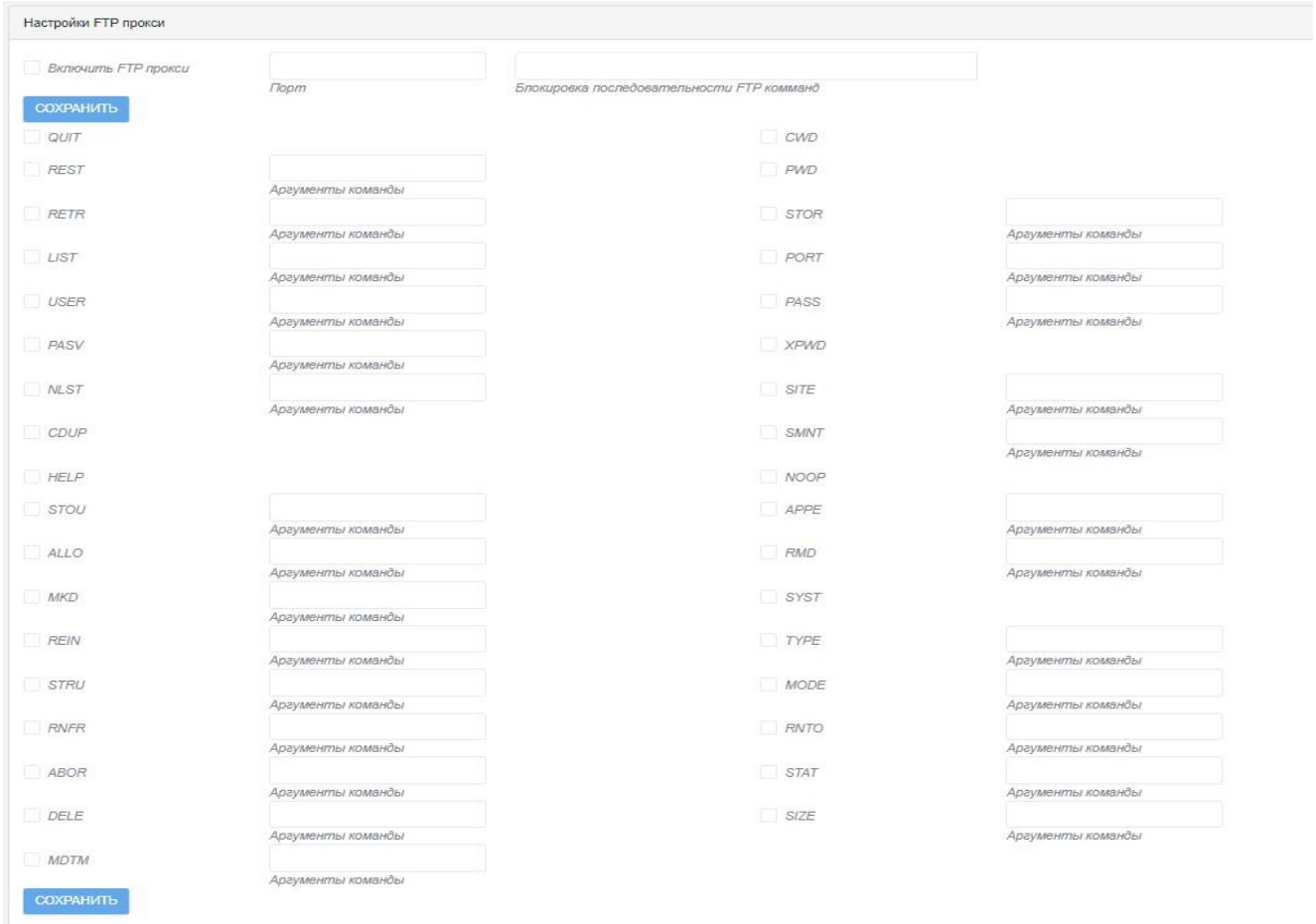


Рисунок 110 – Подраздел «Настройки FTP прокси»

Подраздел «FTP посредник» содержит элементы, указанные в таблице 62.

Таблица 62 – Описание элементов подраздела «FTP посредник»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Параметр «Включить FTP прокси»	Предназначен для указания необходимости включения/выключения FTP-прокси
Поле «Порт»	Предназначено для ввода порта, на котором работает служба FTP-прокси
Поле «Блокировка последовательности FTP команд»	Предназначено для ввода последовательности FTP-команд, блокируемой службой FTP-прокси
Перечень команд	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);

Элемент	Описание
	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; HELP– выдает список поддерживаемых команд; 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. MODE – активировать пассивный режим; RNFR – выбрать файл для переименования (аргумент – имя файла);

Элемент	Описание
	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)
Поле «Аргументы команды»	Предназначено для ввода аргументов команды
Кнопка «СОХРАНИТЬ»	Сохранение введенных данных

2.5.3 Подраздел «Сервер DHCP»

Подраздел «Сервер DHCP» (рисунок 111) предназначен для настройки DHCP.

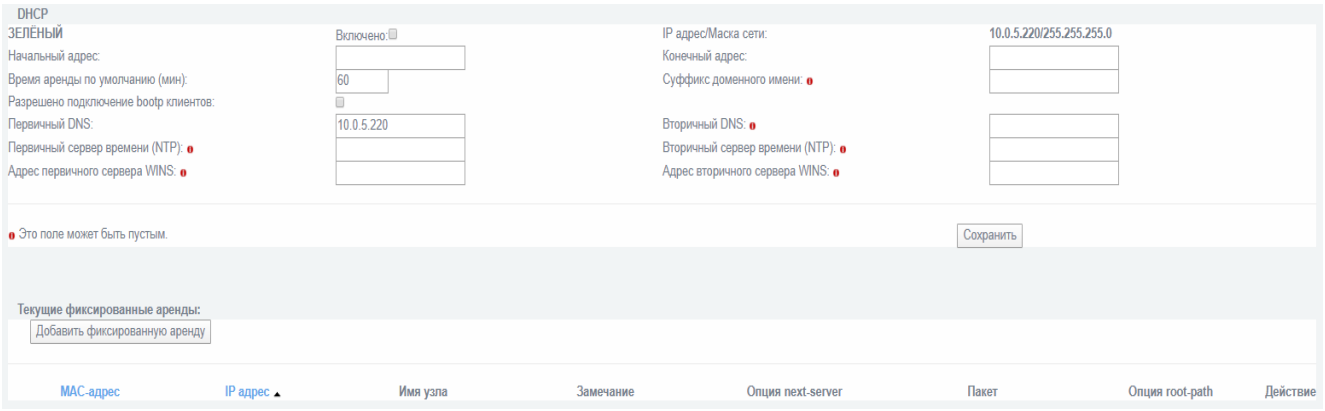


Рисунок 111 – Подраздел «Сервер DHCP»

Подраздел «Сервер DHCP» содержит элементы, указанные в таблице 63.

Таблица 63 – Описание элементов подраздела «Сервер DHCP»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок необязательности заполнения поля
Параметр «ЗЕЛЕНЫЙ Включено»	Параметр включения сервера DHCP
Поле «Начальный адрес»	Предназначено для задания начального адреса из диапазона адресов, выдаваемых DHCP-сервером
Поле «Время аренды по умолчанию (мин)»	Предназначено для задания времени аренды IP адреса. По истечении этого срока IP адрес освобождается, если DHCP-клиент не прислал запроса на продление аренды
Параметр «Разрешено подключение bootp клиентов»	Предназначен для включения возможности подключения клиентов по протоколу bootp
Поле «Первичный DNS»	Предназначено для задания IP адреса первичного DNS-сервера
Поле «Первичный сервер времени (NTP)»	Предназначено для задания IP адреса первичного сервера времени
Поле «Адрес первичного сервера WINS»	Предназначено для задания IP адреса первичного сервера WINS
Поле «IP адрес/Маска сети»	В поле уже прописаны IP-адрес и маска сети текущего интерфейса
Поле «Конечный адрес»	Предназначено для задания конечного адреса из диапазона адресов, выдаваемых DHCP-сервером

Элемент	Описание
Поле «Суффикс доменного имени»	Предназначено для задания суффикса доменного имени
Поле «Вторичный DNS»	Предназначено для задания IP адреса вторичного (резервного) DNS-сервера
Поле «Вторичный сервер времени (NTP)»	Предназначено для задания IP адреса вторичного (резервного) сервера времени
Поле «Адрес вторичного сервера WINS»	Предназначено для задания IP адреса вторичного (резервного) сервера WINS
Кнопка «Сохранить»	Сохранение введенных данных

2.5.3.1 Перечень «Текущие фиксированные аренды»

Текущие фиксированные аренды представлены в перечне «Текущие фиксированные аренды» (рисунок 112).

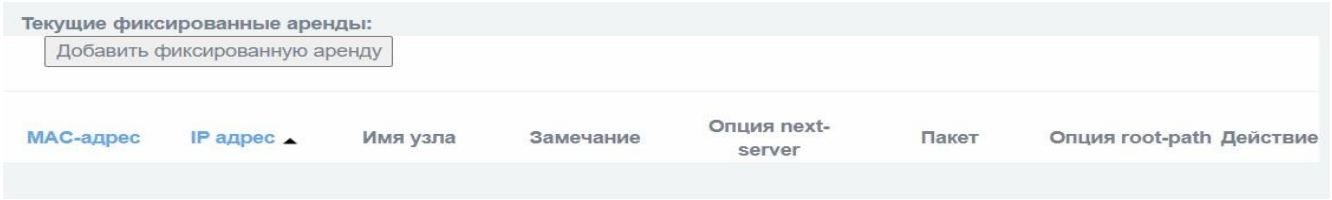


Рисунок 112 – Перечень «Текущие фиксированные аренды»

Перечень «Текущие фиксированные аренды» содержит перечень текущих фиксированных аренд, распределенных по следующим параметрам:

– «MAC-адрес»;

– «IP адрес»;

– «Имя узла»;

– «Замечание»;

– «Опция next-server»;

– «Пакет»;

– «Опция root-path»;

– «Действие».

2.5.3.2 Меню добавления фиксированной аренды

Меню добавления фиксированной аренды (рисунок 113) предназначено для добавления фиксированной аренды DHCP.

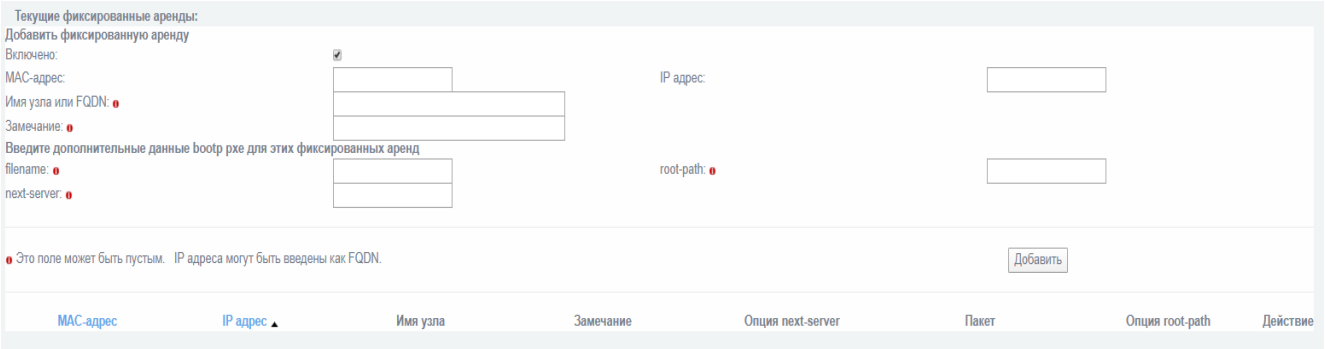


Рисунок 113 – Меню добавления фиксированной аренды

Меню добавления фиксированной аренды содержит элементы, указанные в таблице 64.

Таблица 64 – Описание элементов меню добавления фиксированной аренды

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок необязательности заполнения поля
Параметр «Включено»	Предназначен для включения или выключения фиксированной аренды IP адреса
Поле «MAC адрес»	Предназначено для указания MAC адреса компьютера, которому назначается IP адрес
Поле «Имя узла или FQDN»	Предназначено для указания имени узла или FQDN

Элемент	Описание
Поле «Замечание»	Предназначено для указания замечаний (необязательное поле). Не влияет на работу DHCP-сервера
Поле «filename»	Предназначено для указания имени файла- образа для загрузки по протоколу bootp
Поле «next-server»	Предназначено для указания адреса сервера, содержащего файл-образ для загрузки
Поле «IP адрес»	Предназначено для указания назначаемого IP адреса
Поле «root-path»	Предназначено для указания пути загрузки для файла-образа.
Кнопка «Добавить»	Кнопка предназначена для добавления новой фиксированной аренды

2.5.4 Подраздел «Динамический DNS»

Подраздел «Динамический DNS» (рисунок 114) предназначен для создания службы DNS.

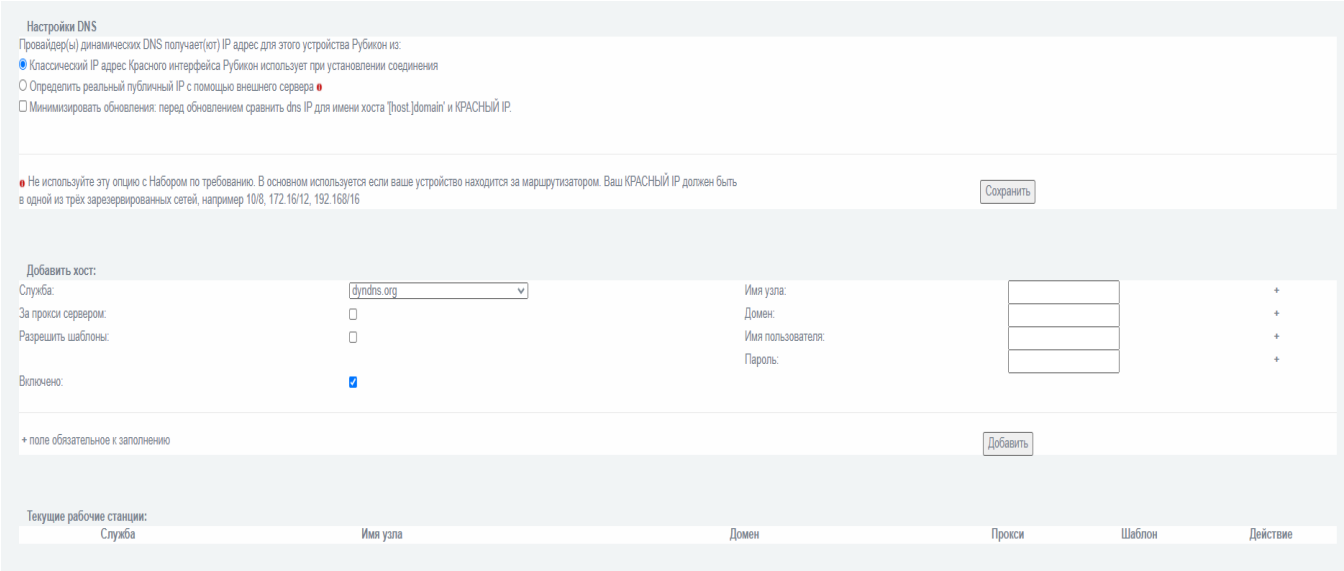


Рисунок 114 – Подраздел «Динамический DNS»

Подраздел «Динамический DNS» состоит из следующих блоков:

– «Настройки DNS»;

– «Добавление хоста»;

– «Перечень текущих рабочих станций».

2.5.4.1 Блок «Настройки DNS»

Блок «Настройки DNS» (рисунок 115) предназначен для ввода основных настроек DNS.

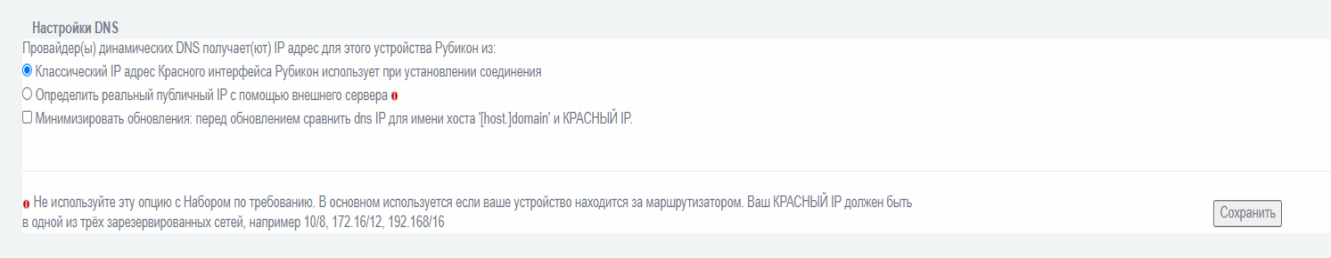


Рисунок 115 – Блок «Настройки DNS»

Блок «Настройки DNS» содержит элементы, указанные в таблице 65.

Таблица 65 – Описание элементов блока «Настройки DNS»

Элемент	Описание
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок необязательности заполнения поля
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Классический IP адрес Красного интерфейса Рубикон использует при установлении соединения»	Данные параметры предназначены для выбора механизма взаимодействия с внешним DNS-сервером
Параметр «Определить реальный публичный IP с помощью внешнего сервера»	
Параметр «Минимизировать обновления: перед обновлением сравнить dns IP для имени хоста '[host.] domain' и КРАСНЫЙ IP»	

Элемент	Описание
Кнопка « Сохранить »	Кнопка сохраняет введенные данные

2.5.4.2 Блок «Добавление хоста»

Блок «Добавление хоста» (рисунок 116) предназначен для ввода настроек нового хоста и добавления его в перечень текущих рабочих станций.

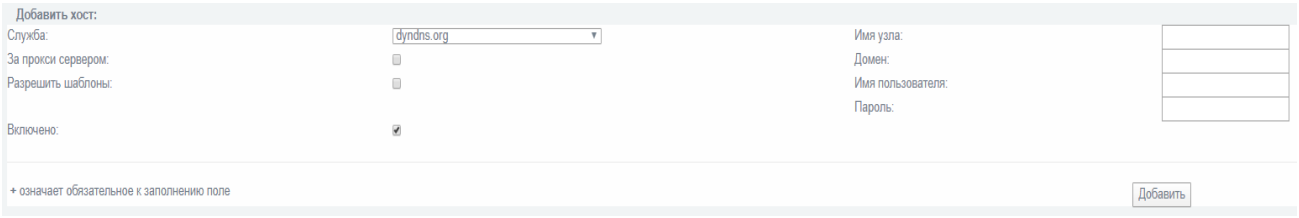


Рисунок 116 – Блок «Добавление хоста»

Блок «Добавление хоста» содержит элементы, указанные в таблице 66.

Таблица 66 – Описание элементов блока «Добавление хоста»

Элемент	Описание
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле для ввода необходимой информации
	Значок активации ниспадающего списка
	Значок обязательного заполнения поля
Ниспадающий список «Служба»	Ниспадающий список служб DNS
Параметр «За прокси сервером»	Располагает сервер DNS за прокси-сервером
Параметр «Разрешить шаблоны»	Включает шаблоны
Параметр «Включено»	Автоматически включает DNS после его добавления к общему списку

Элемент	Описание
Поле «Имя узла»	Ввод имени узла. Обязательное поле для заполнения. Допустимы символы латинского алфавита, цифры 0-9
Поле «Домен»	Ввод имени домена. Обязательное поле для заполнения. Строка, содержащая домен, которому принадлежит узел. Допустимо имя в формате FQDN
Поле «Имя пользователя»	Ввод имени пользователя. Обязательное поле для заполнения. Строка, содержащая имя пользователя выбранной службы динамического DNS. Допустимы символы латинского алфавита и цифры 0-9
Поле «Пароль»	Ввод пароля. Обязательное поле для заполнения. Строка, содержащая пароль пользователя выбранной службы динамического DNS. Допустимы символы латинского алфавита, цифры 0-9, служебные символы
Кнопка «Добавить»	Кнопка добавления нового хоста в перечень текущих рабочих станций

2.5.4.3 Блок «Текущие рабочие станции»

Блок «Текущие рабочие станции» (рисунок 117) предназначен для отображения перечня всех рабочих станций и управления ими.

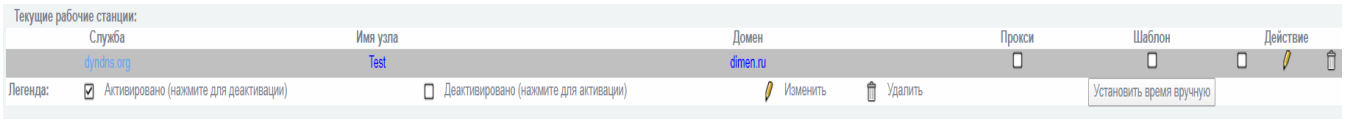


Рисунок 117 – Блок «Текущие рабочие станции»

Перечень текущих рабочих станций распределяет станции по следующим параметрам:

– «Служба»;

– «Имя узла»;

– «Домен»;

– «Прокси»;

– «Шаблон»;

– «Действие».

Блок «Текущие рабочие станции» содержит элементы, указанные в таблице 67.

Таблица 67 – Описание элементов блока «Перечень текущих рабочих станций»

Элемент	Описание
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок редактирования рабочей станции
	Значок удаления рабочей станции
	Ссылка на службу DNS
Кнопка «  »	Кнопка установки времени

2.5.5 Подраздел «Настройка правил СОВ»

Подраздел «Настройка правил СОВ» (рисунок 128) предназначен для включения (отключения) срабатывания конкретного решающего правила.

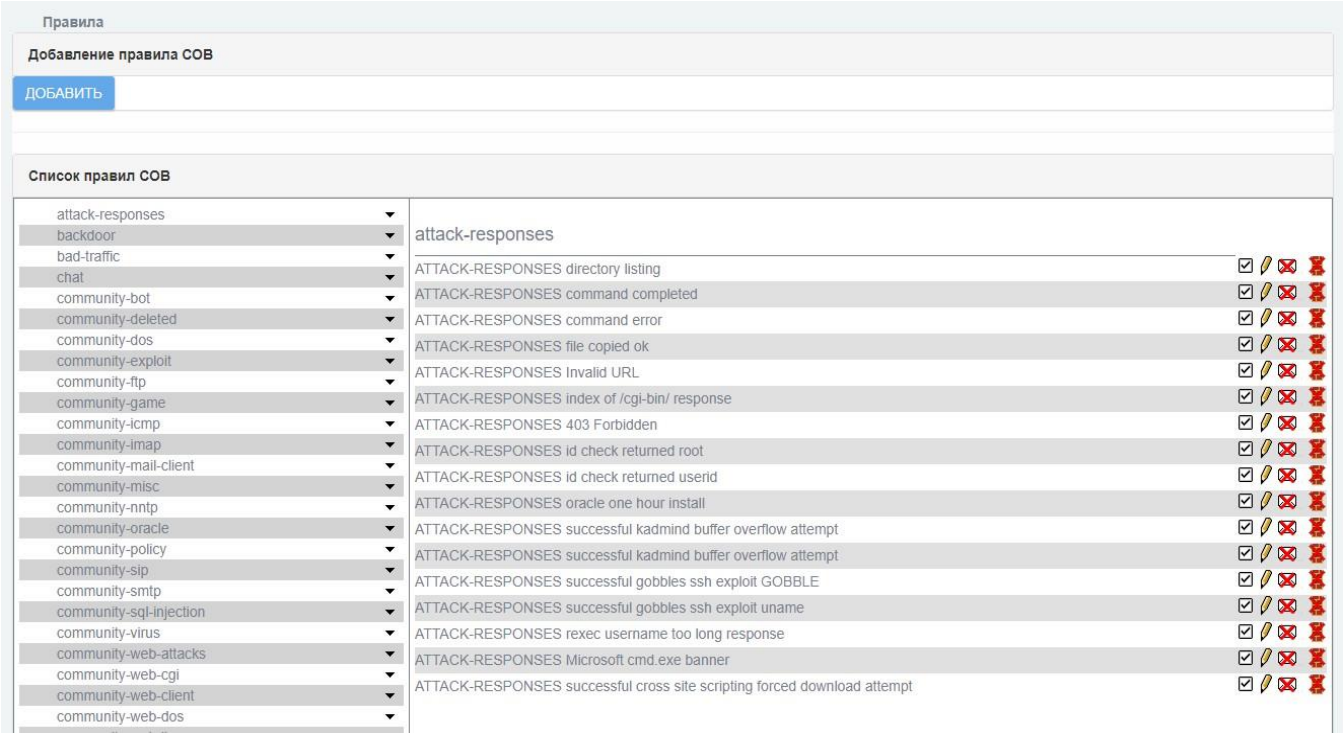


Рисунок 128 – Подраздел «Настройка правил СОВ»

Подраздел «Настройка правил СОВ» разделен на следующие блоки:

– «Добавление правил СОВ»;

– «Список правил СОВ».

2.5.5.1 Блок «Добавление правил СОВ»

Блок «Добавление правил СОВ» (рисунок 129) предназначен для настройки правил СОВ и добавления их в список правил СОВ.

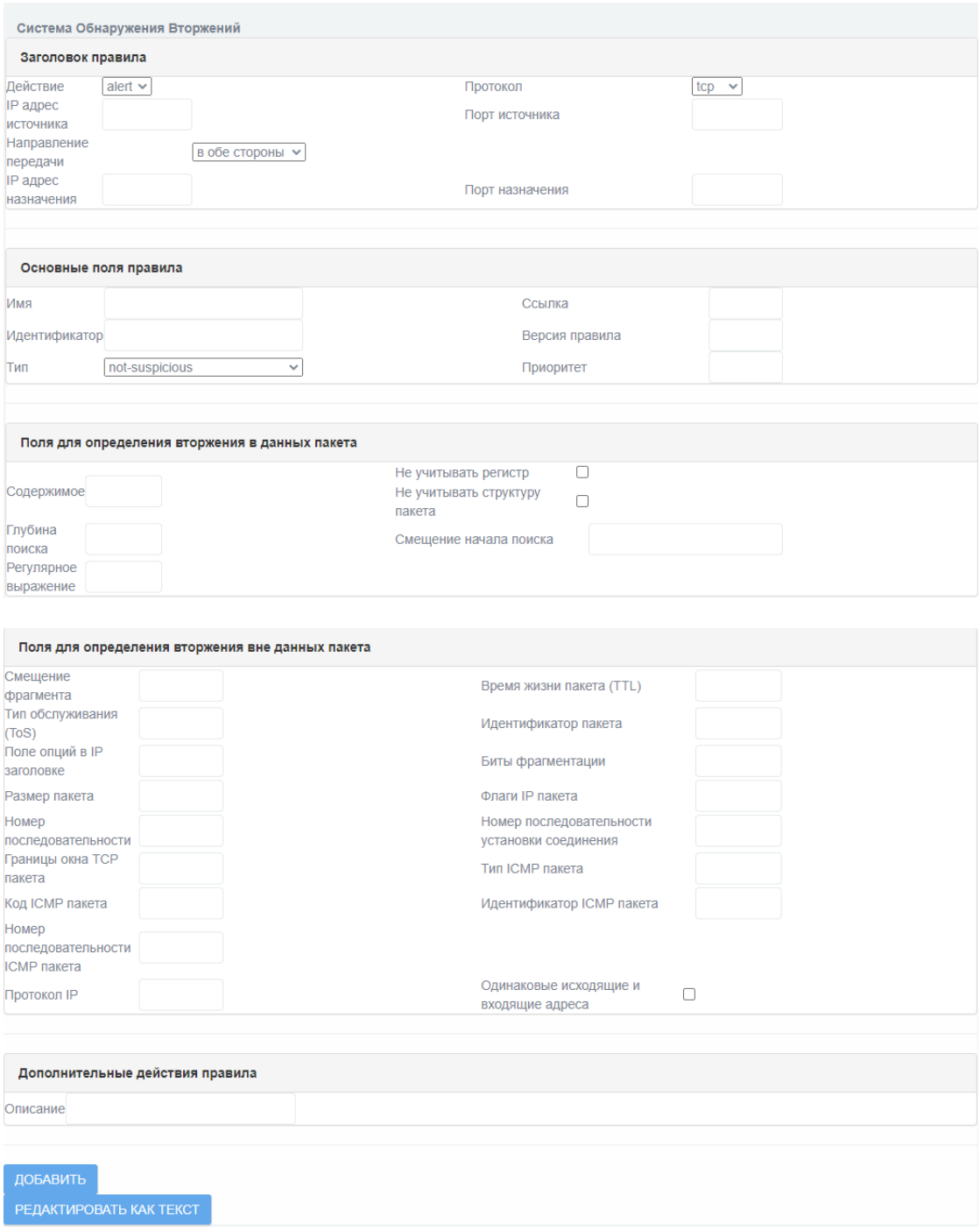


Рисунок 129 – Блок «Добавление правил СОВ»

Блок «Добавление правил СОВ» состоит из следующих блоков:

– «Заголовок правила»;

– «Основные поля правила»;

– «Поля для определения вторжения в данных пакета»;

– «Поля для определения вторжения вне данных пакета»;

– «Дополнительные действия правила».

2.5.5.1.1 Блок «Заголовок правила»

Блок «Заголовок правила» (рисунок 130) предназначен для создания заголовка правила.

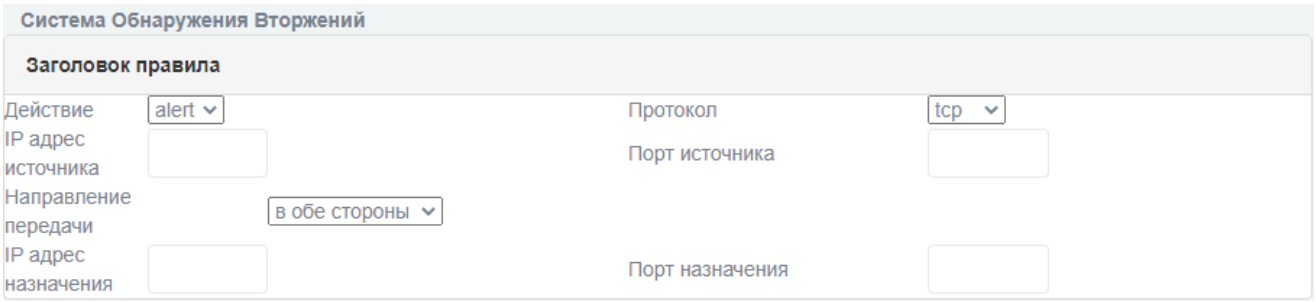


Рисунок 130 – Блок «Заголовок правила»

Блок «Заголовок правила» содержит элементы, указанные в таблице 74.

Таблица 74 – Описание элементов блока «Заголовок правила»

Элемент	Описание
	Поле для ввода необходимой информации
	Ниспадающий список
Ниспадающий список «Действие»	Ниспадающий список регламентирует действия «Рубикон» при срабатывании правила. Ниспадающий список состоит из следующих параметров: – drop; – alert
Поле «IP адрес источника»	Предназначено для указания IP-адреса источника сетевого пакета

Элемент	Описание
Ниспадающий список «Направление передачи»	Ниспадающее меню регламентирует направление передачи: – в обе стороны; – в одну сторону
Поле «IP адрес назначения»	Предназначено для указания IP-адреса назначения сетевого пакета
Ниспадающий список «Протокол»	Ниспадающее меню регламентирует использование протокола для правила. Доступны следующие протоколы: – TCP; – UDP; – ICMP; – IP
Поле «Порт источника»	Предназначено для указания номера порта источника сетевого пакета
Поле «Порт назначения»	Предназначено для указания номера порта назначения сетевого пакета

2.5.5.1.2 Блок «Основные поля правила»

Блок «Основные поля правила» представлен на рисунке ниже (рисунок 131).

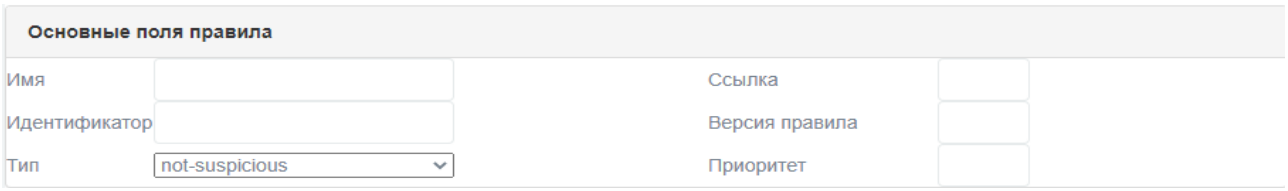


Рисунок 131 – Блок «Основные поля правила»

Блок «Основные поля правила» содержит элементы, указанные в таблице 75.

Таблица 75 – Описание элементов блока «Основные поля правила»

Элемент	Описание
	Поле для ввода необходимой информации
	Ниспадающий список
Поле «Имя»	Предназначено для указания имени правила
Поле «Идентификатор»	Предназначено для указания идентификатора правила
Ниспадающий список «Тип»	Доступные следующие типы правил: – not-suspicious; – НЕИЗВЕСТНЫЙ; – bad-unknown; – attempted-recon; – successful-recon-limited; – successful-recon-largescale; – attempted-dos; – successful-dos; – attempted-user; – unsuccessful-user; – successful-user; – attempted-admin; – rpc-portmap-decode; – shellcode-detect; – string-detect; – suspicious-filename-detect; – suspicious-login; – system-call-detect;

Элемент	Описание
	– tcp-connection; – trojan-activity; – unusual-client-port-connection; – network-scan; – denial-of-service; – non-standard-protocol; – protocol-command-decode; – web-application-activity; – web-application-attack; – misc-activity; – misc-attack; – icmp-event; – kickass-porn; – policy-violation; – default-login-attempt; – successful-admin
Поле «Ссылка»	Предназначено для указания ссылки на ресурсы, описывающие атаку, представленную данным правилом
Поле «Версия правила»	Предназначено для указания версии правила
Поле «Приоритет»	Предназначено для указания приоритета правила

2.5.5.1.3 Блок «Поля для определения вторжения в данных пакета»

Блок «Поля для определения вторжения в данных пакета» представлен на рисунке ниже (рисунок 132).

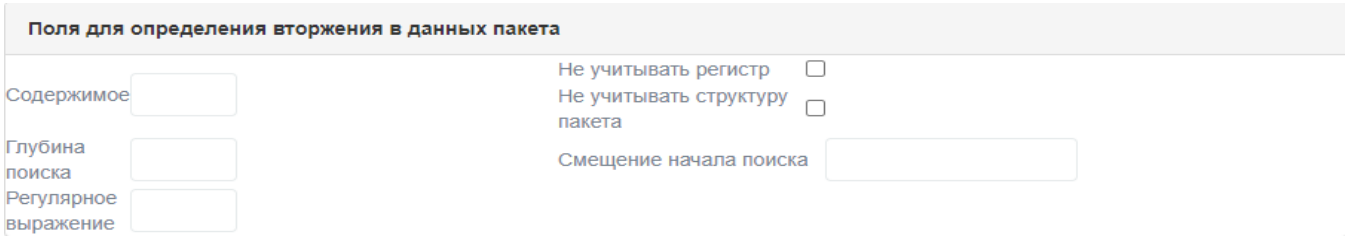


Рисунок 132 – Блок «Поля для определения вторжения в данных пакета»

Блок «Поля для определения вторжения в данных пакета» содержит элементы, указанные в таблице 76.

Таблица 76 – Описание элементов блока «Поля для определения вторжения в данных пакета»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Поле «Содержимое»	Предназначено для указания содержимого пакета, определяющего срабатывание правила
Поле «Глубина поиска»	Предназначено для указания длины последовательности относительно смещения, в которой осуществляется поиск требуемого содержимого
Поле «Регулярное выражение»	Предназначено для указания регулярного выражения для поиска последовательности, определяющей срабатывание правила
Параметр «Не учитывать регистр»	Предназначен для указания необходимости учета регистра в строке «Содержимое»
Параметр «Не учитывать структуру пакета»	Предназначен для указания необходимости учета структуры пакета

Элемент	Описание
Поле «Смещение начала поиска»	Предназначено для указания смещения относительно начала пакета, от которого начинается поиск требуемого содержимого

2.5.5.1.4 Блок «Поля для определения вторжения в заголовке пакета»

Блок «Поля для определения вторжения в заголовке пакета» представлен на рисунке ниже (рисунок 133).

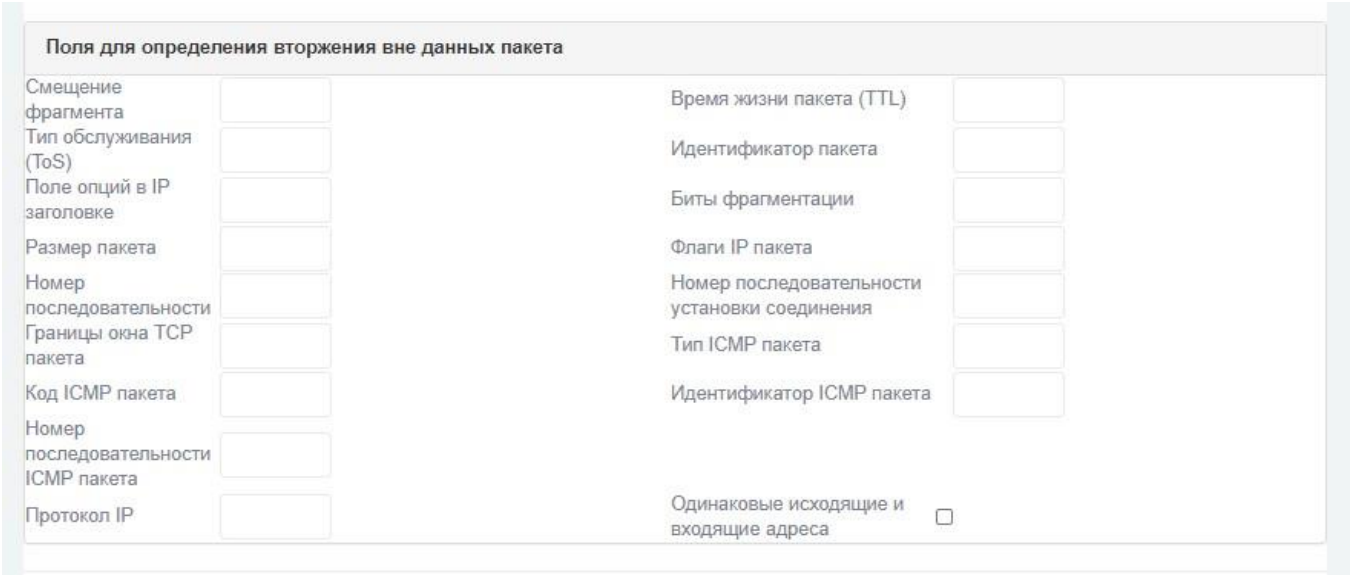


Рисунок 133 – Блок «Поля для определения вторжения в заголовке пакета»

Блок «Поля для определения вторжения в заголовке пакета» содержит элементы, указанные в таблице 77.

Таблица 77 – Описание элементов блока «Поля для определения вторжения в заголовке пакета»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Поле «Смещение фрагмента»	Предназначено для указания значения поля смещения фрагмента

Элемент	Описание
Поле «Тип обслуживания (ToS)»	Предназначено для указания значения поля ToS
Поле «Поле опций в IP заголовке»	Предназначено для указания значения поля опций в IP-заголовке пакета
Поле «Размер пакета»	Предназначено для указания значения размера пакета
Поле «Номер последовательности»	Предназначено для указания значения номера последовательности
Поле «Границы окна TCP пакета»	Предназначено для указания значения границы окна TCP-пакета
Поле «Код ICMP пакета»	Предназначено для указания кода ICMP-пакета
Поле «Номер последовательности ICMP пакета»	Предназначено для указания значения номера последовательности
Поле «Протокол IP»	Предназначено для указания протокола IP
Поле «Время жизни пакета (TTL)»	Предназначено для указания значения поля TTL
Поле «Идентификатор пакета»	Предназначено для указания значения поля идентификатора пакета
Поле «Биты фрагментации»	Предназначено для указания значения битов фрагментации
Поле «Флаги IP пакета»	Предназначено для указания значения флагов IP-пакета
Поле «Номер последовательности установки соединения»	Предназначено для указания значения номера последовательности при установке соединения
Поле «Тип ICMP пакета»	Предназначено для указания типа ICMP-пакета

Элемент	Описание
Поле «Идентификатор ICMP пакета»	Предназначено для указания идентификатора ICMP-пакета
Параметр «Одинаковые исходящие и входящие адреса»	Предназначен для указания необходимости отслеживания одинаковых исходящих и входящих адресов

2.5.5.1.5 Блок «Дополнительные действия правила»

Блок «Дополнительные действия правила» предназначен для введения дополнительных действий правила (рисунок 134).

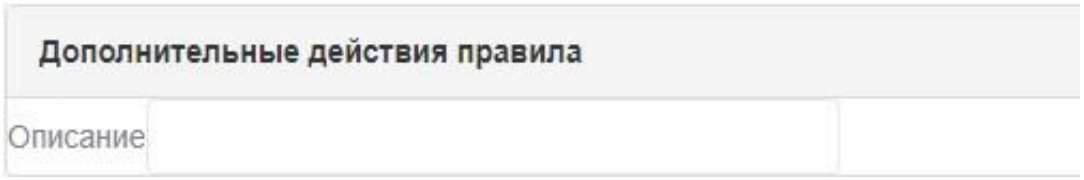


Рисунок 134 – Блок «Дополнительные действия правила»

Блок «Дополнительные действия правила» содержит элементы, указанные в таблице 78.

Таблица 78 – Описание элементов блока «Дополнительные действия правила»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «Описание»	Предназначено для указания текстового описания правила

2.5.5.2 Блок «Список правил СОВ»

Блок «Список правил СОВ» (рисунок 135) содержит перечень правил СОВ с возможностью их редактирования.

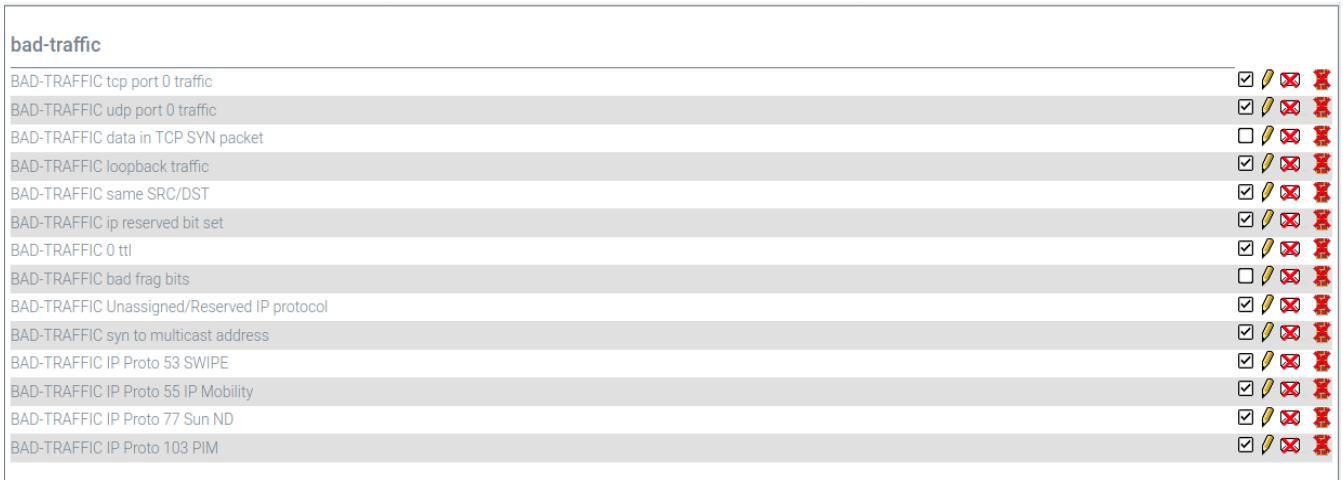


Рисунок 135 – Блок «Список правил СОВ»

Блок «Список правил СОВ» содержит элементы, указанные в таблице 79.

Таблица 79 – Описание элементов блока «Список правил СОВ»

Элемент	Описание
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Значок «  »	Значок, раскрывающий однотипную группу правил
Значок «  »	Включение / отключение правила позволяет пользователю включать или отключать выбранное правило, не удаляя его
Значок «  »	Редактирование правила, при нажатии значка открывается форму редактирования правил
Значок «  »	Уведомления на почту о срабатывании правила выключены

2.5.6 Подраздел «Задать имена хостов»

Подраздел «Задать имена хостов» (рисунок 118) предназначен для настройки параметров сетевых узлов.

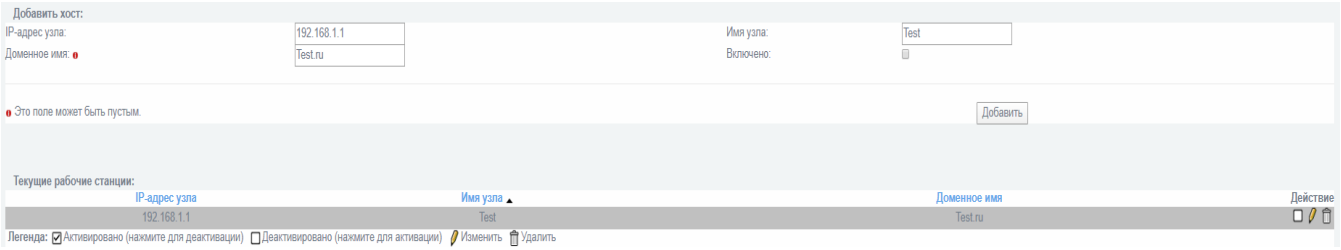


Рисунок 118 – Подраздел «Задать имена хостов»

Подраздел «Задать имена хостов» содержит элементы, указанные в таблице 68.

Таблица 68 – Описание элементов подраздела «Задать имена хостов»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок необязательности заполнения поля
	Значок редактирования рабочей станции
	Значок удаления рабочей станции
Поле «IP-адрес узла»	Предназначено для указания IP-адреса узла
Поле «Доменное имя»	Предназначено для указания доменного имени
Поле «Имя узла»	Предназначено для указания имени узла
Параметр «Включено»	Автоматически включает хост после добавления
Кнопка «  »	Сохранение введенной информации и добавление хоста

2.5.7 Подраздел «Сервер времени»

Подраздел «Сервер времени» (рисунок 119) предназначен для установки параметров времени.

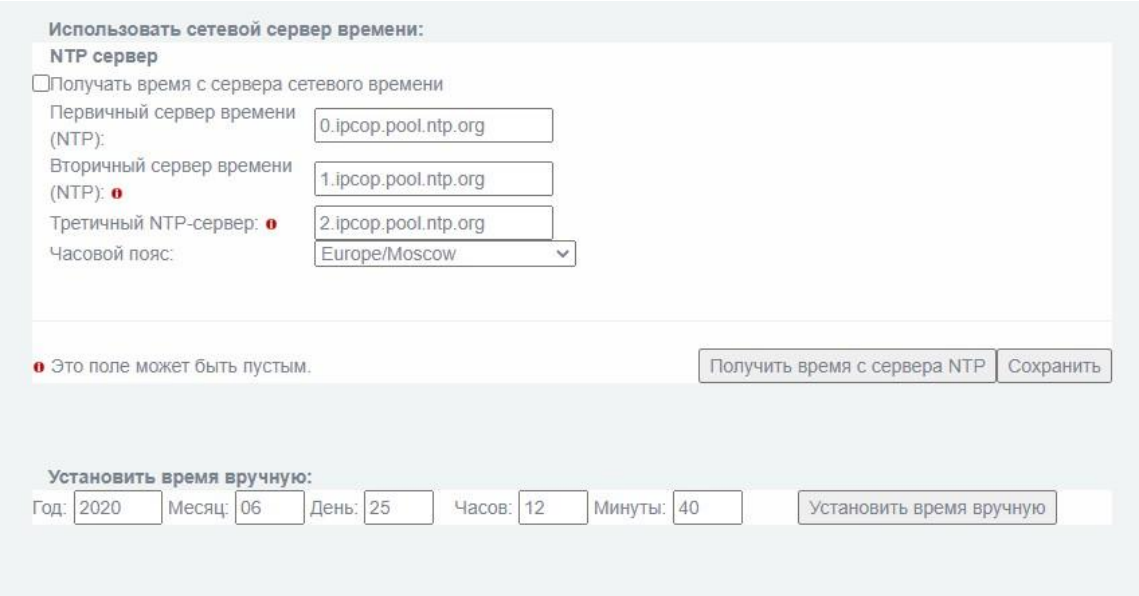


Рисунок 119 – Подраздел «Сервер времени»

Подраздел «Сервер времени» делится на следующие блоки:

– NTP сервер;

– Установить время вручную.

2.5.7.1 Блок «NTP сервер»

Блок «NTP сервер» (рисунок 120) предназначен для указания внешнего сервера времени.

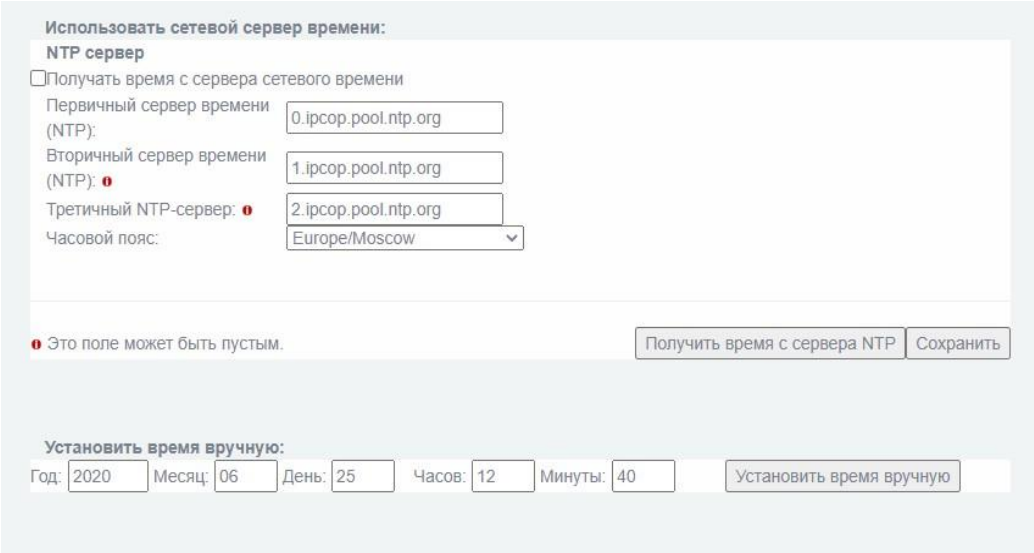
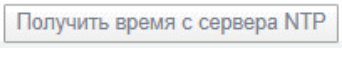


Рисунок 120 – Блок «NTP сервер»

Блок «NTP сервер» содержит элементы, указанные в таблице 69.

Таблица 69 – Описание элементов блока «NTP сервер»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок необязательности заполнения поля
	Значок активации ниспадающего списка
Параметр «Получать время с сервера сетевого времени»	Параметр для включения использования внешнего сервера времени
Поле «Первичный Сервер Времени (NTP)»	Предназначено для указания адреса первичного сервера времени
Поле «Вторичный Сервер Времени (NTP)»	Предназначено для указания адреса вторичного сервера времени
Поле «Третичный NTP-сервер»	Предназначено для указания адреса третичного сервера времени
Ниспадающее меню «Часовой пояс»	В ниспадающем меню можно выбрать город нахождения «Рубикон» или самый ближайший к нему город
Кнопка «  »	Позволяет обновить время, полученное с указанных выше серверов
Кнопка «  »	Кнопка сохранения введенных данных

2.5.7.2 Блок «Установка времени вручную»

Блок «Установить время вручную» (рисунок 121) предназначен для установки времени вручную.

Рисунок 121 – Блок «Установить время вручную»

Блок «Установить время вручную» содержит элементы, указанные в таблице 70.

Таблица 70 – Описание элементов блока «Установить время вручную»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «Год»	Предназначено для указания текущего года при ручном обновлении системного времени
Поле «Месяц»	Предназначено для указания текущего месяца при ручном обновлении системного времени
Поле «День»	Предназначено для указания текущего числа при ручном обновлении системного времени
Поле «Часов»	Предназначено для указания текущего часа при ручном обновлении системного времени
Поле «Минуты»	Предназначено для указания текущей минуты при ручном обновлении системного времени
Кнопка «  »	Если сервера недоступны, то можно задать время вручную при помощи данной кнопки

2.5.8 Подраздел «Ограничение Трафика»

Подраздел «Ограничение Трафика» (рисунок 122) предназначен для ограничения трафика по определенным интерфейсам и для выставления приоритета трафика для служб.

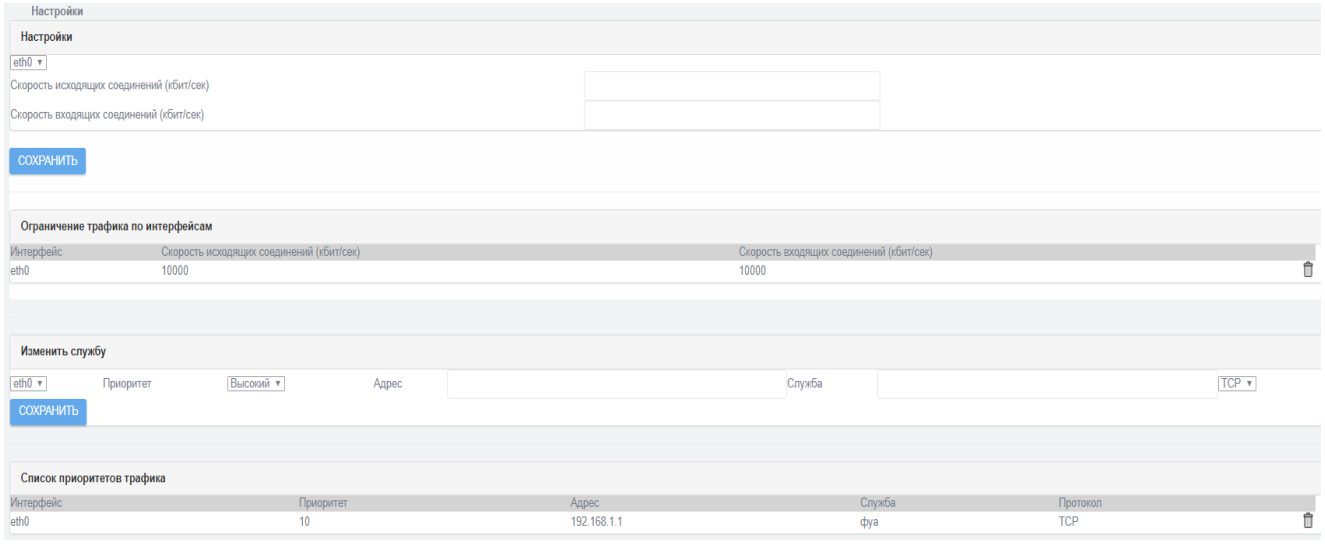


Рисунок 122 – Подраздел «Ограничение Трафика»

Подраздел «Ограничение Трафика» состоит из следующих блоков:

– «Настройка ограничения трафика»;

– «Ограничение трафика по интерфейсам»;

– «Настройка приоритизации трафика»;

– «Список приоритетов трафика».

2.5.8.1 Блок «Настройка ограничения трафика»

Блок «Настройка ограничения трафика» (рисунок 123) предназначен для настройки ограничения трафика по указанным интерфейсам.

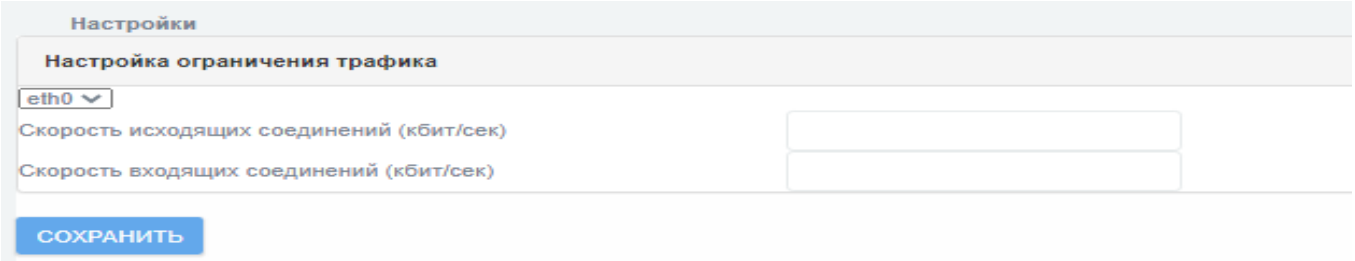


Рисунок 123 – Блок «Настройка ограничения трафика»

Блок «Настройки» содержит элементы, указанные в таблице 71.

Таблица 71 – Описание элементов блока «Настройки»

Элемент	Описание
	Поле для ввода необходимой информации
	Ниспадающий список для выбора интерфейса
Кнопка «  »	Сохраняет введенную информацию
Поле «Скорость исходящих соединений (кбит/сек)»	Параметр устанавливает скорость исходящих соединений
Поле «Скорость входящих соединений (кбит/сек)»	Параметр устанавливает скорость входящих соединений

2.5.8.2 Блок «Ограничение трафика по интерфейсам»

Блок «Ограничение трафика по интерфейсам» (рисунок 124) представляет собой перечень ограничений трафика.

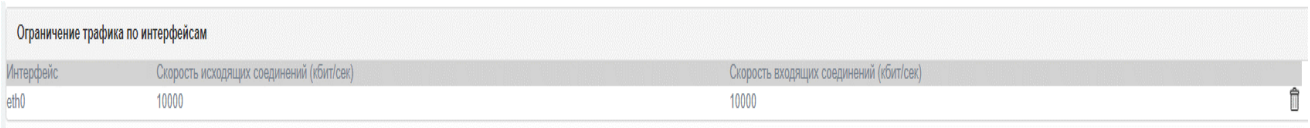


Рисунок 124 – Блок «Ограничение трафика по интерфейсам»

Перечень ограничения трафика распределяется по следующим параметрам:

– «Интерфейс»;

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

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

Для удаления ограничения трафика необходимо нажать на значок «  ».

2.5.8.3 Блок «Настройка приоритизации трафика»

Блок «Настройка приоритизации трафика» (рисунок 125) предназначен для добавления приоритетов ограничений трафика по интерфейсам и протоколам.

Рисунок 125 – Блок «Настройка приоритизации трафика»

Блок «Настройка приоритизации трафика» содержит элементы, указанные в таблице 72.

Таблица 72 – Описание элементов блока «Настройка приоритизации трафика»

Элемент	Описание
	Поле для ввода необходимой информации
	Ниспадающий список для выбора интерфейса
Кнопка «  »	Сохраняет введенную информацию
Ниспадающий список «Приоритет»	Выставление приоритета для службы: – Низкий; – Средний; – Высокий
Поле «Адрес»	В строке указывается адрес выбираемой службы
Поле «Служба»	В строке вписывается имя выбираемой службы
Ниспадающий список протоколов	Ниспадающий список для выбора сетевого протокола: – TCP; – UDP. TCP – транспортный протокол передачи данных в сетях TCP/IP, предварительно устанавливающий соединение с сетью. UDP – транспортный протокол, передающий сообщения-датаграммы без необходимости установки соединения в IP-сети

2.5.8.4 Блок «Список приоритетов трафика»

Блок «Список приоритетов трафика» (рисунок 126) представляет собой перечень ограничений трафика с приоритетами.

Рисунок 126 – Блок «Список приоритетов трафика»

Перечень ограничений трафика с приоритетами распределяется по следующим параметрам:

– «Интерфейс»;

– «Приоритет»;

– «Адрес»;

– «Служба»;

– «Протокол».

Для удаления ограничения трафика необходимо нажать на значок «  ».

2.5.9 Подраздел «Проверка доступности узлов»

Данный подраздел осуществляет проверку сетевого соединения с удаленным узлом (рисунок 127).

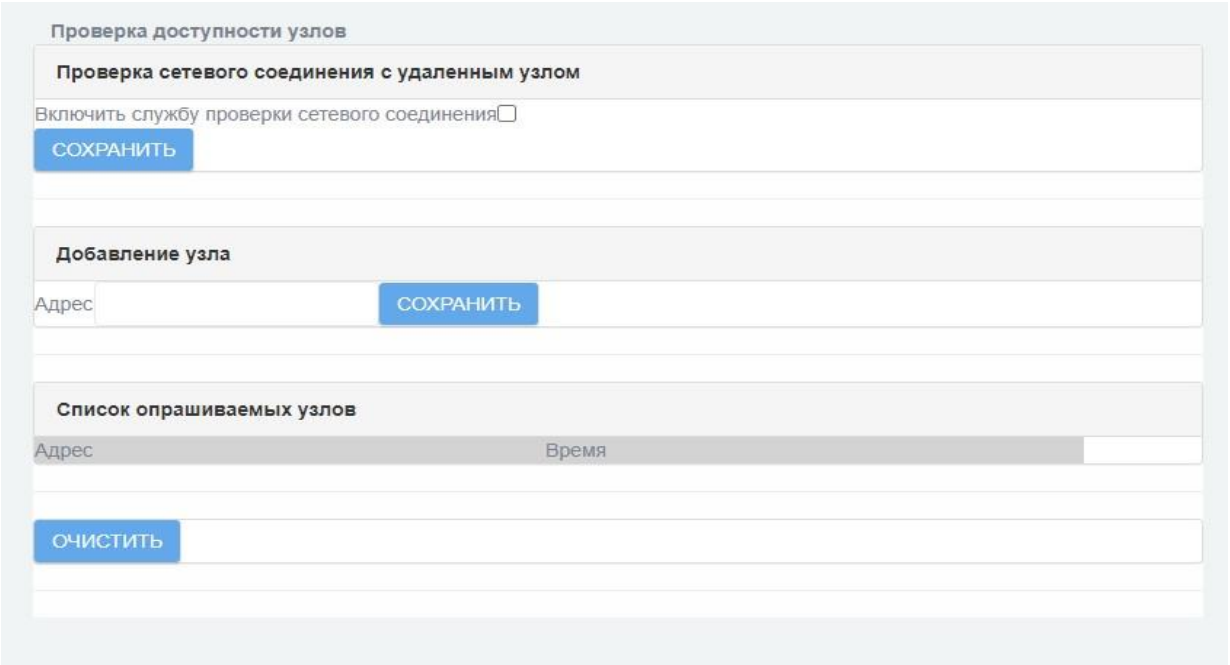
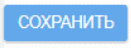


Рисунок 127 – Подраздел «Проверка доступности узлов»

Подраздел «Проверка доступности узлов» содержит элементы, указанные в таблице 73.

Таблица 73 – Элементы подраздела «Проверка доступности узлов»

Элемент	Описание
	Поле для включения/выключения службы проверки сетевого соединения
	Поле для добавления узла
Кнопка «  »	Сохраняет введенную информацию
Кнопка «  »	Удаляет введенные узлы

2.6 Раздел «Система обнаружения вторжений»

Раздел «Система обнаружения вторжений» содержит следующие подразделы:

– «Настройка правил СОВ»;

– «Настройка обнаружения»;

– «Обнаружение Атак»;

– «Переменные СОВ».

2.6.1 Подраздел «Настройка правил СОВ»

Подраздел «Настройка правил СОВ» (рисунок 128) предназначен для включения (отключения) срабатывания конкретного решающего правила.

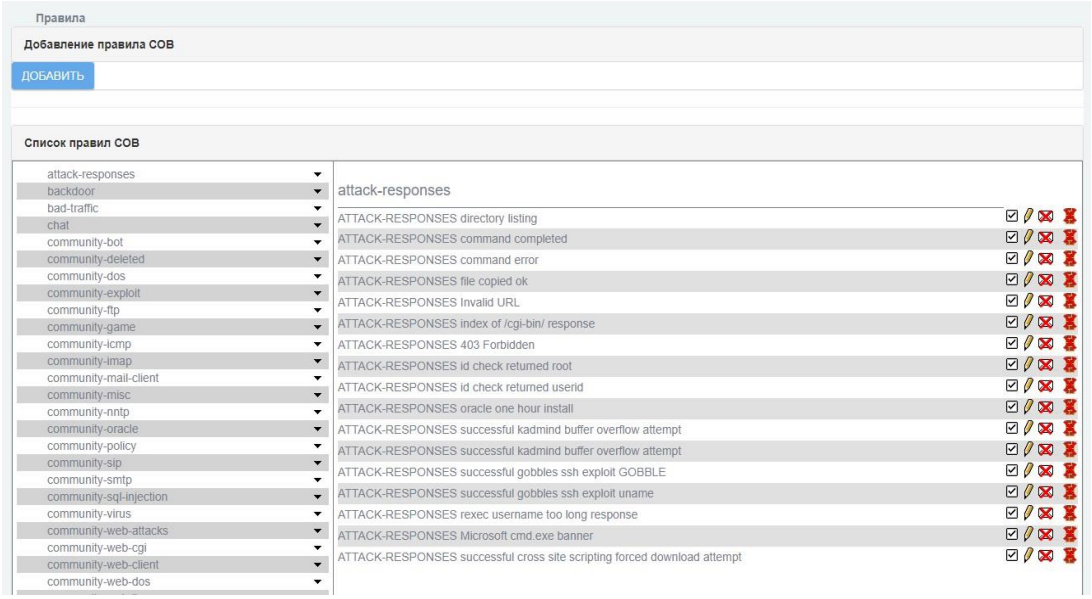


Рисунок 128 – Подраздел «Настройка правил СОВ»

2.6.2 Подраздел «Настройка обнаружения»

Подраздел «Настройка обнаружения» (рисунок 129) предназначен для настройки на предмет обнаружения сканирования.

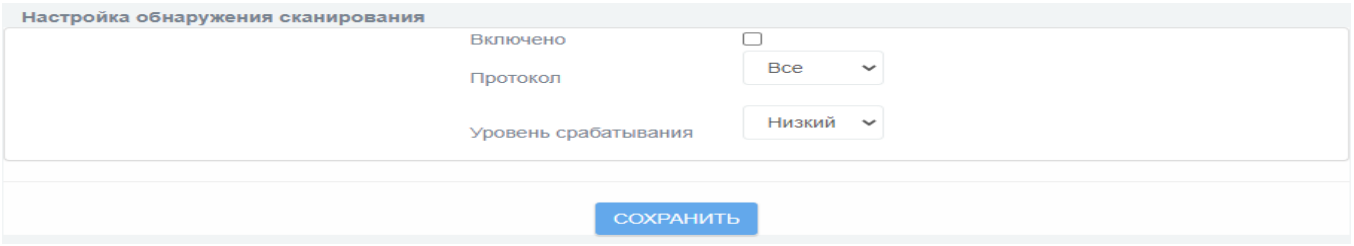
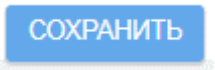


Рисунок 129 – Подраздел «Настройка обнаружения»

Подраздел «Настройка обнаружения сканирования» содержит элементы, указанные в таблице 80.

Таблица 80 – Описание элементов подраздела «Настройка обнаружения»

Элемент	Описание
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Ниспадающий список
Параметр «Включено»	Параметр «Включено» включает систему обнаружения сканирования
Ниспадающий список «Протокол»	Ниспадающий список «Протокол» содержит список основных протоколов: – Все; – TCP; – UDP; – ICMP; – Протокол IP
Ниспадающий список «Уровень срабатывания»	Ниспадающий список «Уровень срабатывания» содержит выбор из 3 уровней срабатывания: – Высокий;

Элемент	Описание
	– Средний; – Низкий
Кнопка «  »	Предназначена для сохранения внесенных изменений

2.6.3 Подраздел «Обнаружение Атак»

Подраздел «Обнаружение Атак» (рисунок 130) предназначен для установки параметров обнаружения атак и загрузки наборов правил.

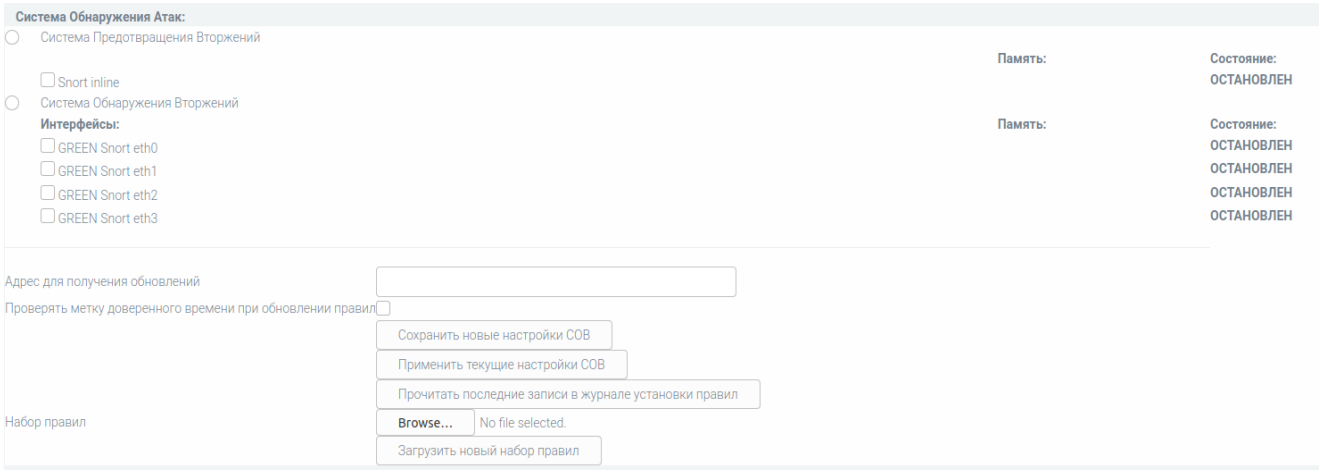


Рисунок 130 – Подраздел «Обнаружение Атак»

Подраздел «Обнаружение Атак» содержит элементы, указанные в таблице 81.

Таблица 81 – Описание элементов подраздела «Обнаружение Атак»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)

Элемент	Описание
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Система Предотвращения Вторжений»	Включение/выключение системы предотвращения вторжений
Параметр «Snort inline»	Предназначен для включения обнаружения атак на указанном физическом сетевом интерфейсе
Параметр «Система Обнаружения Вторжений»	Включение/выключение системы обнаружения вторжений
Параметр «GREEN Snort eth0»	Сетевой интерфейс, подключаемый к внутренней сети. По умолчанию все пакеты, маршрутизируемые между различными зелеными интерфейсами, не блокируются
Параметр «GREEN Snort eth1»	
Параметр «GREEN Snort eth2»	
Параметр «BRIDGE Snort idsbr»	При объединении интерфейсов в мост создается интерфейс моста
Поле «Адрес для получения обновлений»	Предназначено для введения адреса для получения обновлений
Параметр «Проверять метку доверенного времени при обновлении правил»	Включение/выключение проверки метки доверенного времени при обновлении правил
Кнопка «  »	Предназначена для сохранения настроек системы обнаружения вторжения. Внесенные изменения будут учтены при следующем запуске «Рубикон» или после нажатия кнопки «Применить»

Элемент	Описание
Кнопка «Применить»	Предназначена для немедленного применения установленных параметров обнаружения атак. Нажатие этой кнопки приводит к полному перезапуску системы обнаружения вторжений на указанных интерфейсах
Кнопка «Прочитать последние записи в журнале установки правил»	Предназначена для отображения последней записи в журнале установки правил
Кнопка «Выберите файл»	Кнопка входа в меню выбора файла с правилами
Кнопка «Загрузить новый набор правил»	Предназначена для загрузки нового набора базы решающих правил системы обнаружения вторжений из указанного файла

2.6.4 Подраздел «Переменные СОВ»

Подраздел «Переменные СОВ» (рисунок 131) предназначен для указания значений переменных в решающих правилах СОВ.

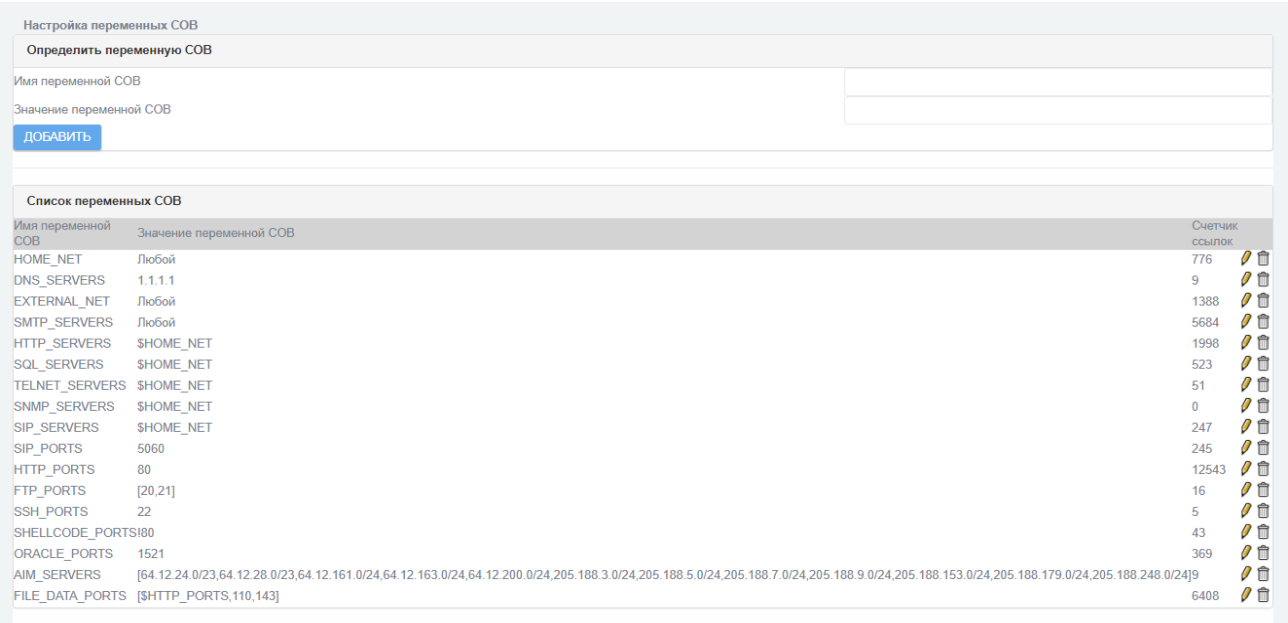


Рисунок 131 – Настройка переменных СОВ

Подраздел «Переменные СОВ» состоит из следующих блоков:

– «Определить переменную СОВ»;

– «Список переменных СОВ».

2.6.4.1 Блок «Определить переменную СОВ»

Блок «Определить переменную СОВ» предназначен для добавления переменной СОВ (рисунок 132).

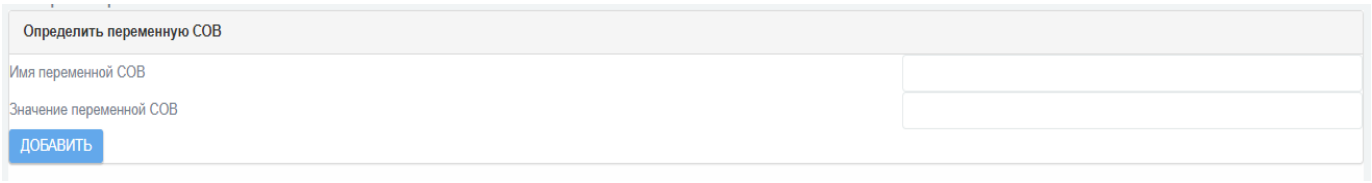
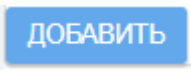


Рисунок 132 – Добавление переменной СОВ

Блок «Определить переменную СОВ» содержит элементы, указанные в таблице 82.

Таблица 82 – Описание элементов блока «Определить переменную СОВ»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «Имя переменной СОВ»	Предназначено для ввода имени переменной СОВ
Поле «Значение переменной СОВ»	Предназначено для указания сетевых объектов или сервисов. Допустимо пользоваться их перечислением через запятую (при этом содержание переменной нужно заключить в скобки), а также другими переменными (в формате $Имя_переменной)
Кнопка «  »	Кнопка добавления переменной СОВ в список переменных СОВ

2.6.4.2 Блок «Список переменных СОВ»

Блок «Список переменных СОВ» предназначен для отображения списка переменных СОВ и для редактирования переменных СОВ (рисунок 133).

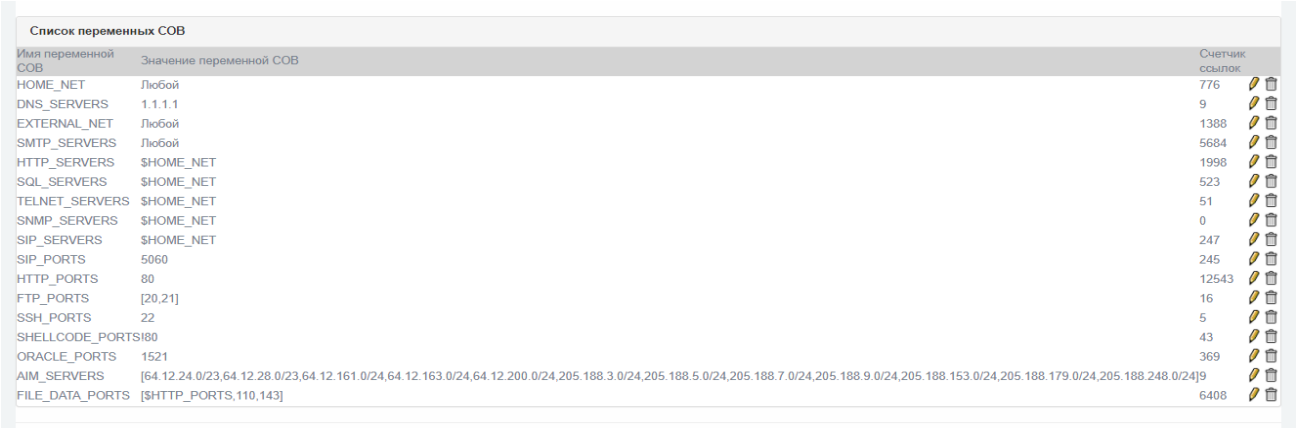


Рисунок 133 – Список переменных СОВ

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

Для редактирования значения переменной СОВ необходимо нажать кнопку «  », после чего данные в поле «Значение переменной СОВ» подлежат редактированию (рисунок 134). Для удаления переменной СОВ нажмите кнопку «  ».

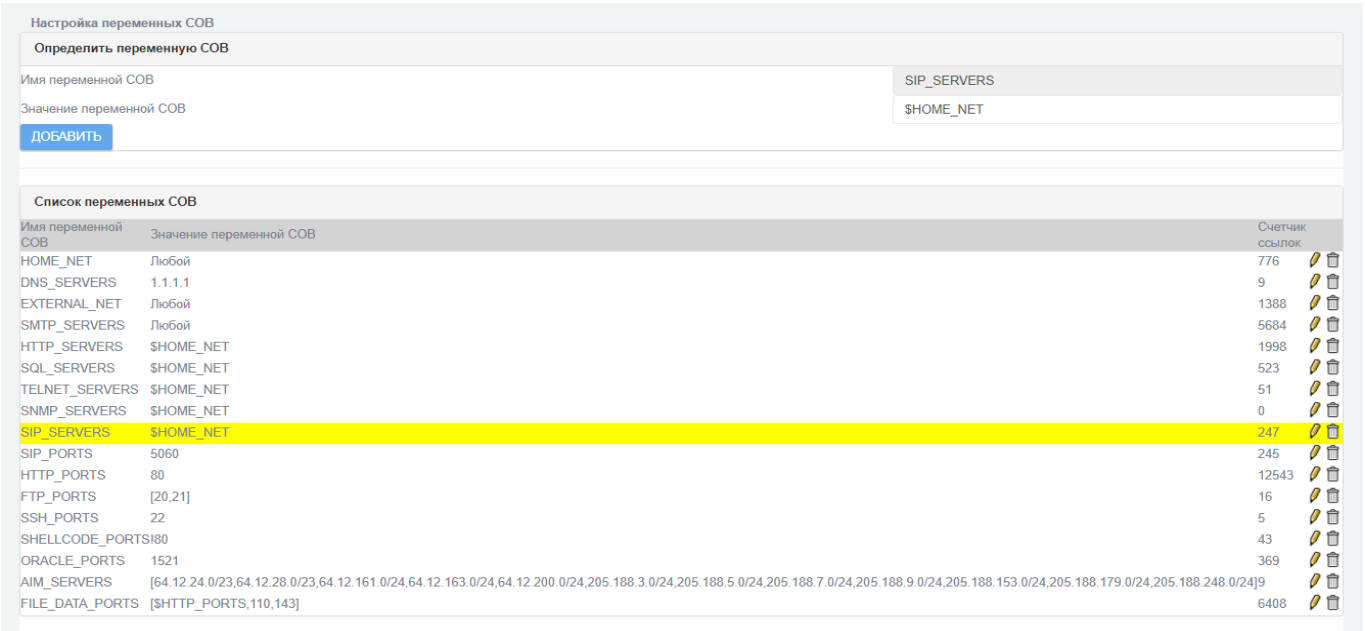


Рисунок 134 – Редактирование переменной СОВ

2.7 Раздел «Межсетевой экран»

При настройке межсетевого экрана возникает необходимость использовать заранее предопределенные мнемонические обозначения параметров, например, определенных портов или адресов, связанных с конкретной сетью, либо их групп. В комплексе «Рубикон» администратор межсетевого экрана может вносить дополнительные записи для следующих элементов:

a) адреса;

b) службы;

c) группы адресов;

d) группы служб;

e) сетевые интерфейсы;

f) группы состояний.

Раздел «Межсетевой экран» содержит следующие подразделы:

– «Настройки межсетевого экрана»;
– «Доступ к Синему интерфейсу»;
– «Службы»;
– «Группы служб»;
– «Адреса»;
– «Группы адресов»;
– «Интерфейсы»;
– «Группы состояний»;
– «Правила межсетевого экрана»;
– «Конфигурация DMZ».

2.7.1 Подраздел «Настройки межсетевого экрана»

Подраздел «Настройки межсетевого экрана» 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» состоит из следующих блоков:

– «Настройки»;

– «Политики сетевых интерфейсов».

2.7.1.1 Блок «Настройки»

Блок «Настройки» (рисунок 135) предназначен для ввода настроек межсетевого экрана.

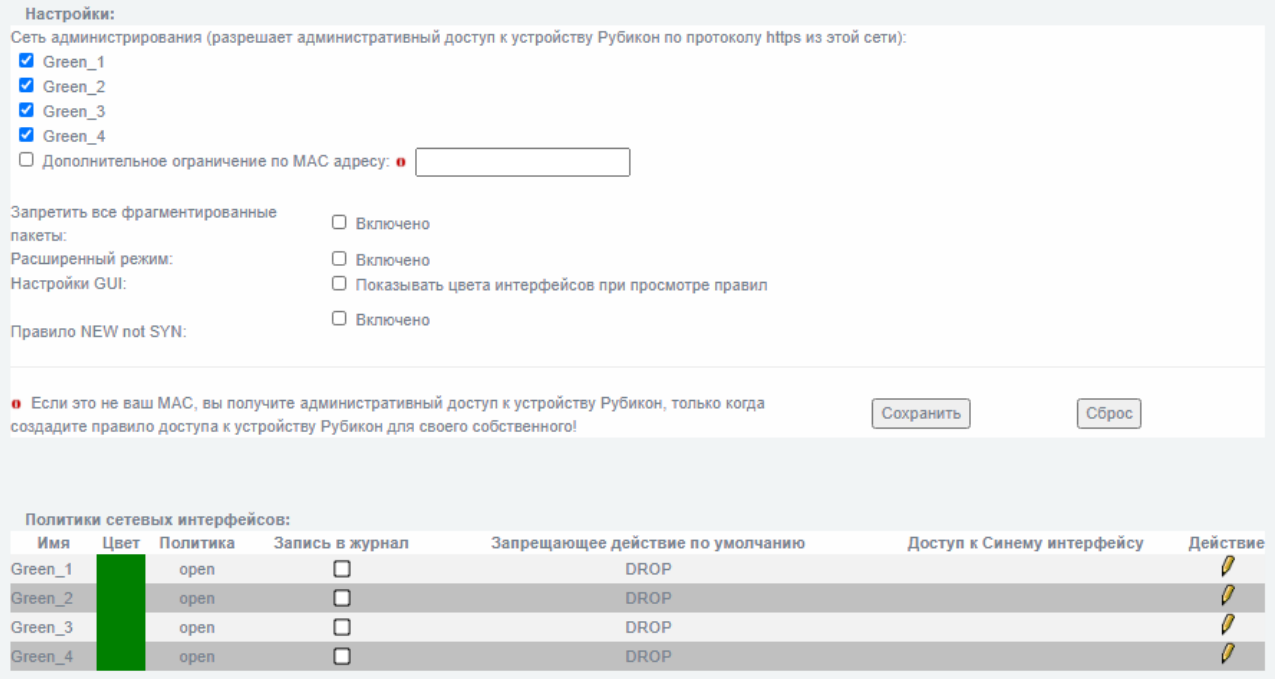


Рисунок 135 – Блок «Настройки»

Блок «Настройки» содержит элементы, указанные в таблице 83.

Таблица 83 – Описание элементов блока «Настройки»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Если это не ваш MAC, вы получите административный доступ к устройству «Рубикон», только когда создадите правило доступа к устройству «Рубикон» для своего собственного
Параметр «Green_1»	Сетевой интерфейс, подключаемый к внутренней сети. По умолчанию все пакеты, маршрутизируемые между различными зелеными интерфейсами, не блокируются
Параметр «Дополнительное	Включение MAC адреса компьютера, с которого возможно администрирование МЭ. После установки

Элемент	Описание
ограничение по MAC адресу»	данного параметра администрирование с других MAC адресов будет невозможно
Поле «Дополнительное ограничение по MAC адресу»	Предназначено для указания MAC адреса компьютера, с которого возможно администрирование МЭ. После установки данного параметра администрирование с других MAC адресов будет невозможно
Параметр «Запретить все фрагментированные пакеты»	При активации параметра сетевые пакеты с флагом фрагментации в IP-заголовке будут заблокированы
Параметр «Расширенный режим»	Предназначен для активации расширенного режим настроек МЭ
Параметр «Настройки GUI»	Предназначен для включения цветной индикации интерфейсов при просмотре правил МЭ
Параметр «Показывать цвета интерфейсов при просмотре правил»	
Параметр «Правило NEW not SYN»	Включение блокировки SYN-пакетов по протоколу TCP, для которых не было установлено соединение
Кнопка «Сохранить»	Кнопка сохранения введенных данных
Кнопка «Сброс»	Кнопка удаления введенных данных

2.7.1.2 Блок «Политики сетевых интерфейсов»

Блок «Политики сетевых интерфейсов» (рисунок 136) содержит перечень политик сетевых интерфейсов.

Рисунок 136 – Блок «Политики сетевых интерфейсов»

Блок «Политики сетевых интерфейсов» содержит элементы, указанные в таблице 84.

Блок «Политики сетевых интерфейсов» содержит перечень политик сетевых интерфейсов, распределенных по следующим параметрам:

– «Имя»;

– «Цвет»;

– «Политика;

– «Запись в журнал»;

– «Запрещающее действие по умолчанию»;

– «Доступ к Синему интерфейсу».

Таблица 84 – Описание элементов блока «Политики сетевых интерфейсов»

Элемент	Описание
Значок « ☑ »	Значок включения/отключения записи в журнал
Значок « ✎ »	Значок редактирования политики

2.7.2 Подраздел «Доступ к Синему интерфейсу»

В соответствии с цветовым профилем настроек межсетевого экрана узлы синего интерфейса могут иметь доступ в зеленый интерфейс только при наличии специальных разрешений. Такие разрешения устанавливаются в пункте меню «Межсетевой экран» → «Доступ к синему интерфейсу». Подраздел «Доступ к Синему интерфейсу» (рисунок 137) предназначен для настройки доступа узлов (источников) к синему интерфейсу.

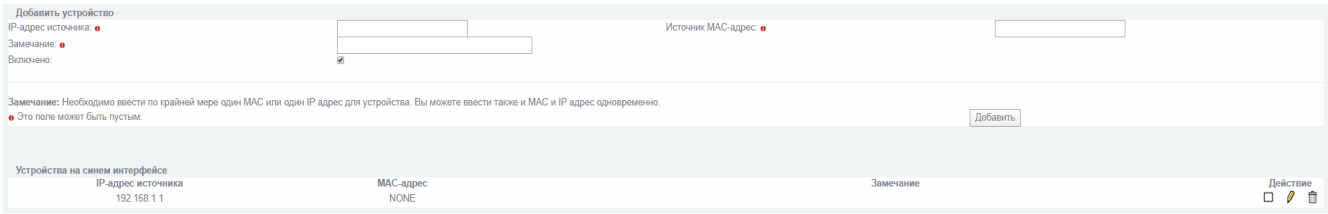
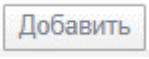


Рисунок 137 – Подраздел «Доступ к Синему интерфейсу»

Подраздел «Доступ к Синему интерфейсу» содержит элементы, указанные в таблице 85.

Таблица 85 – Описание элементов подраздела «Доступ к Синему интерфейсу»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле необязательно для заполнения
Поле «IP-адрес источника»	Добавление IP-адреса устройства
Поле «Замечание»	Добавление описания
Параметр «Включено»	Поставьте флажок, чтобы активировать параметр
Поле «Источник MAC-адрес»	Добавление MAC-адреса устройства
Кнопка «  »	Кнопка добавления устройства в перечень устройств на синем интерфейсе
Значок «  »	Значок показывает включено или выключено устройство
Значок «  »	Редактирование устройства
Значок «  »	Удаление устройства

2.7.3 Подраздел «Службы»

Подраздел «Службы» позволяет создавать новые сетевые службы для удобного задания правил МЭ, а также содержит список уже установленных служб. Межсетевой экран 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 межсетевым экраном «Рубикон» необходимо добавить ее в список служб в интерфейсе управления. Внесение дополнительной службы или определенного порта для взаимодействия на транспортном уровне осуществляется в подразделе «Службы» (рисунок 138).

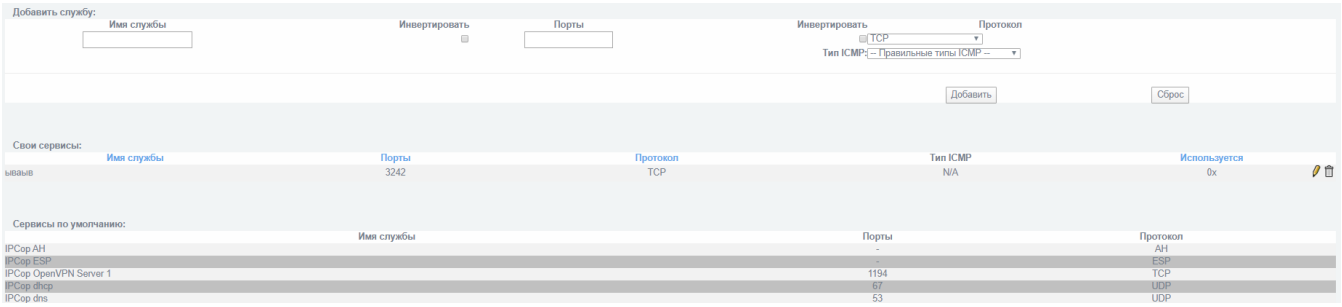


Рисунок 138 – Подраздел «Службы» раздела «Межсетевой экран»

Подраздел «Службы» содержит элементы, указанные в таблице 86.

Таблица 86 – Описание элементов подраздела «Службы»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок активации ниспадающего списка
Поле «Имя службы»	Строка, которая будет отображаться при добавлении службы. Допустимы символы латинского алфавита и цифры 0-9. В поле необходимо указать имя службы
Поле «Порты»	В поле необходимо указать порты для службы, ввести числовое значение в диапазоне от 1 до 65535, либо диапазон из начального и конечного порта, разделенных знаком «-», указывающее на транспортном уровне на порт, используемый при взаимодействии. Данное поле заполняется в том случае, если служба предполагает порты транспортного уровня. В случае, если нужно определить службу, которая не содержит указанных портов необходимо установить флаг «Инвертировать» перед полем «Порты». Служба OSPF не использует порты, поэтому заполнять это поле не требуется

Элемент	Описание
Параметр «Инвертировать»	Активация данного параметра позволяет инвертировать порт, то есть все порты кроме указанного
Ниспадающий список «Протокол»	Ниспадающий список позволяет выбрать протокол, который использует служба. В данном случае, это протокол TCP
Ниспадающий список «Тип ICMP»	Ниспадающий список позволяет выбрать тип ICMP
Значок « »	Предназначен для редактирования параметров указанной сетевой службы
Значок « »	Предназначен для удаления сетевой службы
Кнопка « Добавить »	Предназначена для добавления новой службы в список сетевых служб
Кнопка « Сброс »	Предназначена для отмены внесенных изменений в параметры редактируемой сетевой службы

В подразделе «Службы» присутствует перечень сервисов, установленных по умолчанию. Настроенная служба будет отображена в секции «Свои сервисы» (рисунок 139).

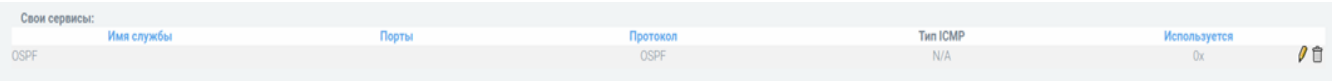


Рисунок 139 – Секция «Свои сервисы»

2.7.4 Подраздел «Группы служб»

Подраздел «Группы служб» (рисунок 140) позволяет группировать различные сетевые службы под одним обозначением для удобного задания правил МЭ.

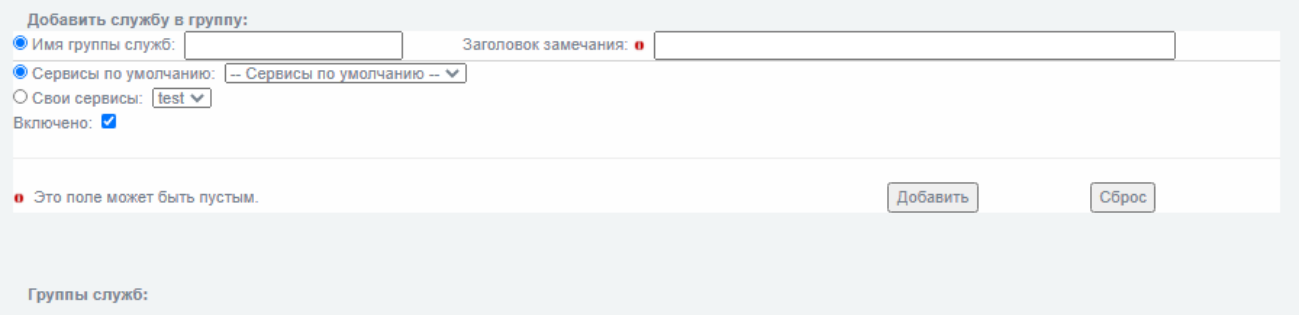


Рисунок 140 – Подраздел «Группы служб»

Подраздел «Группы служб» содержит элементы, указанные в таблице 87.

Таблица 87 – Описание элементов подраздела «Группы служб»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок активации ниспадающего списка
	Поле необязательно для заполнения
	Поле с проставленным флажком (параметр включен)
Параметр «Имя группы служб»	Предназначен для указания обозначения имени группируемых служб. Это имя может содержать латинские буквы и цифры и будет отображаться в правилах МЭ
Поле «Имя группы служб»	Предназначено для указания обозначения имени группируемых служб. Это имя может содержать латинские буквы и цифры и будет отображаться в правилах МЭ
Параметр «Сервисы по умолчанию»	Ниспадающий список предлагает выбрать уже имеющиеся службы

Элемент	Описание
Ниспадающий список «Сервисы по умолчанию»	
Параметр «Свои сервисы»	Ниспадающий список предлагает выбрать собственные службы, которые созданы в «Рубикон»
Ниспадающий список «Свои сервисы»	
Параметр «Включено»	Включает подключаемые сервисы
Поле «Заголовок замечания»	Поле для записи примечания к группе служб
Кнопка «Добавить»	Предназначена для добавления новой группы служб в список сетевых служб
Кнопка «Сброс»	Предназначена для отмены внесенных изменений в параметры редактируемой группы сетевых служб

2.7.5 Подраздел «Адреса»

Подраздел «Адреса» (рисунок 141) позволяет задавать предопределенные адреса для удобного задания правил межсетевого экрана.

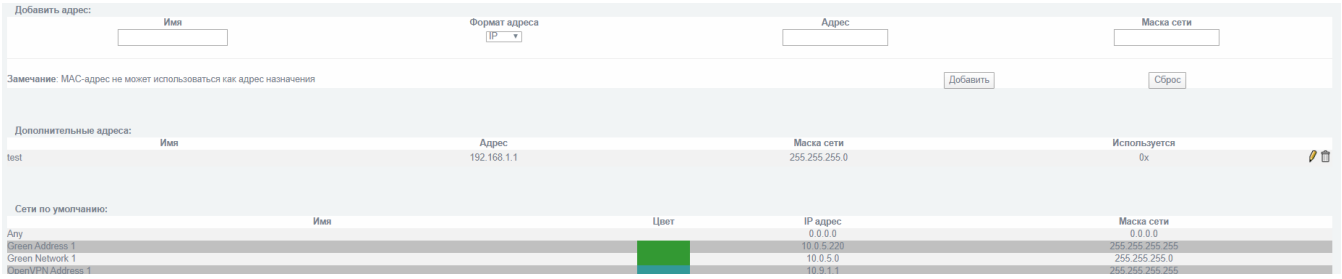


Рисунок 141 – Подраздел «Адреса»

Подраздел «Адреса» содержит элементы, указанные в таблице 88.

Таблица 88 – Описание элементов подраздела «Адреса»

Элемент	Описание
	Поле для ввода необходимой информации
	Значок активации ниспадающего списка
Поле «Имя»	Предназначено для указания обозначения имени предопределенного адреса. Это имя может содержать латинские буквы и цифры и будет отображаться в правилах МЭ
Ниспадающий список «Формат адреса»	Указывает формат адреса для строки ввода «Адрес» (MAC или IP, выбор MAC необходим для указания одиночного MAC-адреса сетевого устройства)
Поле «Адрес»	Предназначено для указания адреса
Поле «Маска сети»	Предназначено для указания маски сети в полном десятичном виде
Значок «  »	Значок позволяет редактировать адрес
Значок «  »	Значок позволяет удалять адрес
Кнопка «  »	Предназначена для добавления предопределенного адреса в список
Кнопка «  »	Предназначена для отмены внесенных изменений

Пример настройки дополнительного адреса сети 11.0.0.0/24:

1) в поле «Имя» ввести строку, которая будет представлять данный адрес в правилах межсетевого экрана;

2) выбрать формат адреса IP из ниспадающего списка (выбор MAC необходим для указания одиночного MAC-адреса сетевого устройства);

3) ввести требуемый адрес в поле «Адрес» (11.0.0.0);

4) ввести маску сети в поле «Маска сети» (255.255.255.0);

5) применить введенные параметры с помощью кнопки «Добавить» (рисунок 142).

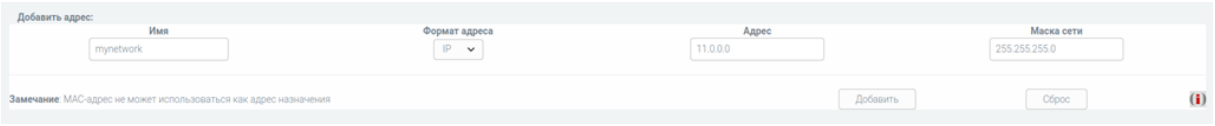


Рисунок 142 – Пример настройки дополнительного адреса сети 11.0.0.0/24

Введенная сеть будет отображена в поле «Дополнительные адреса» (рисунок 143).

Рисунок 143 – Поле «Дополнительные адреса»

2.7.6 Подраздел «Группы адресов»

Подраздел «Группы адресов» (рисунок 144) предназначен для группировки различных предопределенных адресов под одним наименованием для удобного задания правил МЭ.

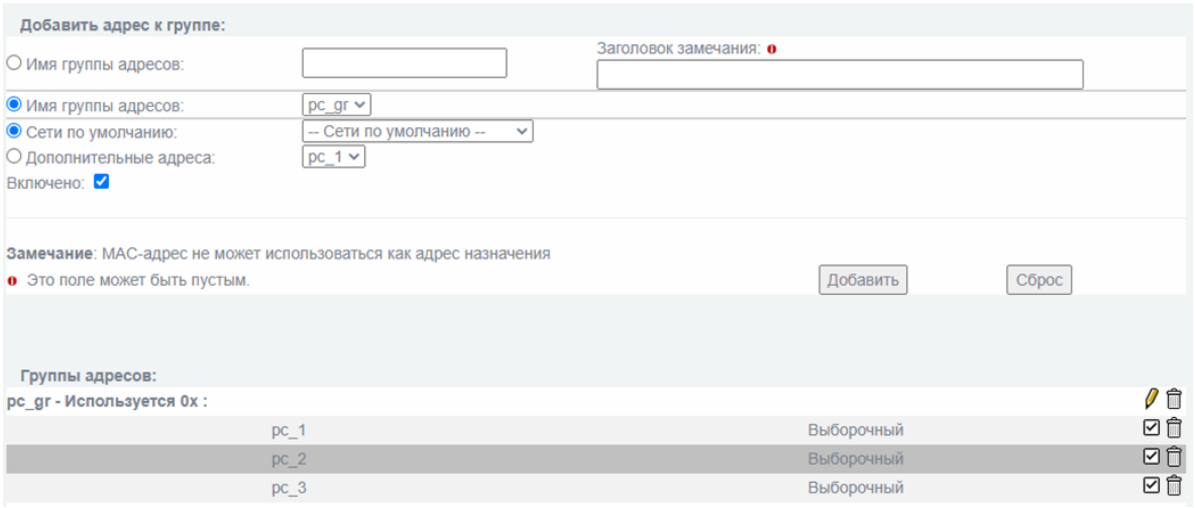
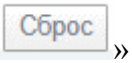


Рисунок 144 – Подраздел «Группы адресов»

Уменьшение количества одинаковых правил межсетевого экрана, описывающих одинаковую политику для разных сетевых узлов, может быть выполнено с помощью объединения необходимых адресов в группу. Внесение дополнительной группы адресов осуществляется в подразделе «Группы адресов». Подраздел «Группы адресов» содержит элементы, указанные в таблице 89.

Таблица 89 – Описание элементов подраздела «Группы адресов»

Элемент	Описание
	Поле для ввода необходимой информации
	Значок активации ниспадающего списка
	Неактивированный чекбокс (параметр выключен)
	Активированный чекбокс (параметр включен)
Чекбокс «Имя группы адресов»	Предназначен для указания использования адресной группы
Поле «Имя группы адресов»	Предназначено для указания названия адресной группы
Параметр «Сети по умолчанию»	Предназначен для указания одной из предопределенных сетей
Ниспадающий список «Сети по умолчанию»	Предназначен для указания одной из предопределенных сетей
Параметр «Дополнительные адреса»	Предназначен для указания дополнительных адресов, которые необходимо включить в группу адресов. Для отображения этого поля необходимо предварительно создать в системе дополнительные адреса, используя подраздел «Адреса»
Ниспадающий список «Дополнительные адреса»	Предназначен для указания дополнительных адресов, которые необходимо включить в группу адресов
Параметр «Включено»	Предназначен для активации указанного адреса в группе. Неактивные адреса не добавляются автоматически в правила межсетевого экрана
Поле «Заголовок замечания»	Предназначено для указания замечания (необязательное поле). Не влияет па работу межсетевого экрана
Значок «  »	Значок показывает включена или выключена группа адресов

Элемент	Описание
Значок «  »	Предназначен для редактирования параметров указанной группы адресов
Значок «  »	Предназначен для удаления указанного адреса из группы адресов
Кнопка «  »	Предназначена для добавления новой группы адресов в список адресов
Кнопка «  »	Предназначена для отмены внесенных изменений в параметры редактируемой группы адресов

Пример объединения в группу адреса третьего зеленого интерфейса и добавленной сети mynetwork:

1) задать поле «Имя группы адресов» - строку содержащее символьное обозначение группы, которое будет использоваться в правилах фильтрации;

2) в ниспадающем списке «Сети по умолчанию» выбрать сеть «Green address 3»;

3) применить настройки с помощью кнопки «Добавить»;

4) выбрать уже внесенное имя группы адресов из ниспадающего списка «Имя группы адресов»;

5) установить переключатель напротив поля «Дополнительные адреса»;

6) в ниспадающем списке «Дополнительные адреса» выбрать сеть «mynetwork»;

7) применить настройки с помощью кнопки «Добавить» (рисунок 145).

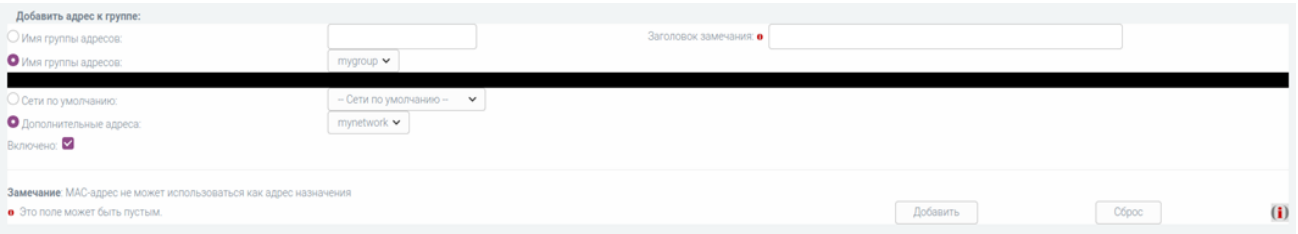


Рисунок 145 – Пример настройки объединения в группу адреса третьего зеленого интерфейса и добавленной сети «mynetwork»

Настроенная группа будет отображаться в поле «Группы адресов» (рисунок 146).

Рисунок 146 – Настроенная группа в поле «Группы адресов»

2.7.7 Подраздел «Интерфейсы по умолчанию»

В комплексе «Рубикон» существует два типа сетевых интерфейсов: интерфейсы непосредственно сетевых адаптеров и логические интерфейсы, которые могут быть добавлены для обеспечения сетевого взаимодействия. В качестве примера последних можно предложить 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 межсетевого экрана по именам соответствующим цветовым политикам (Green_1, Blue_3 и т. п.).

Внесение дополнительных логических интерфейсов осуществляется в пункте меню «Межсетевой экран» → «Интерфейсы по умолчанию» (рисунок 147). При этом межсетевой экран должен быть переведен в расширенный режим на странице «Межсетевой экран» → «Настройки межсетевого экрана».

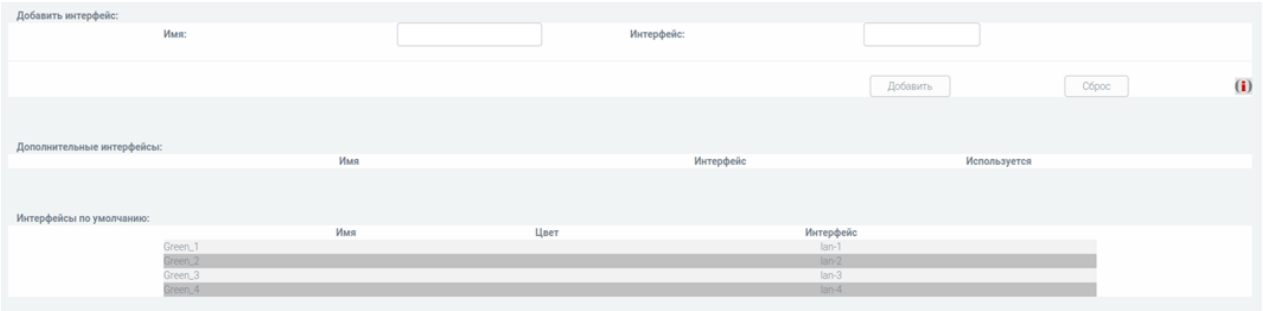


Рисунок 147 – Подраздел «Интерфейсы по умолчанию»

Задать дополнительные интерфейсы можно только в «Расширенном режиме». Чтобы включить данный режим, необходимо перейти в подраздел «Настройки межсетевого экрана» раздела «Межсетевой экран».

Группа настроек дополнительных интерфейсов содержит следующие поля:

a) «Добавить интерфейс» — для внесения данных о добавляемом интерфейсе;

b) «Дополнительные интерфейсы» — для отображения информации о добавленных интерфейсах;

c) «Интерфейсы по умолчанию» — для отображения списка интерфейсов установленных сетевых адаптеров.

2.7.8 Подраздел «Группы состояний»

Подраздел «Группы состояний» (рисунок 148) предназначен для создания и редактирования групп состояний.

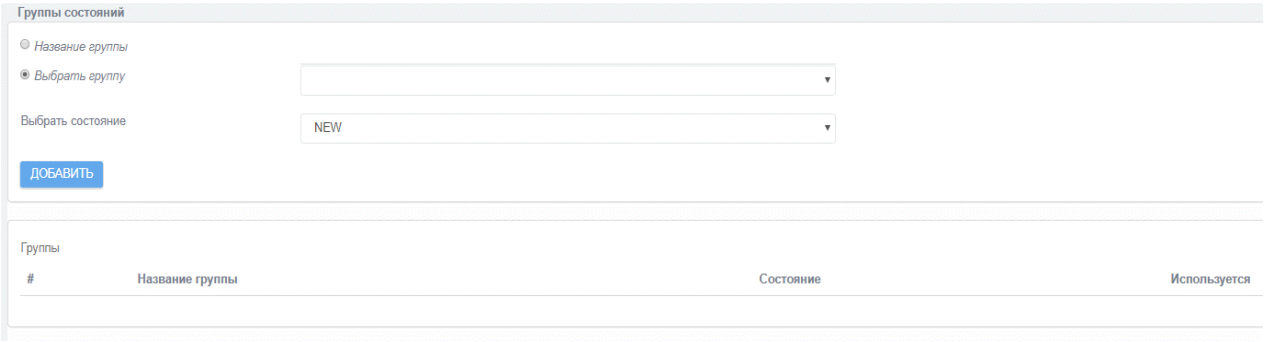


Рисунок 148 – Подраздел «Группы состояний»

Комплекс «Рубикон» является межсетевым экраном с контролем состояний соединений. Фильтрация может осуществляться на основе данных о том, в каком состоянии данное соединение находится в момент анализа сетевого пакета. Существует четыре возможных независимых состояний:

«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.

На основании одиночных состояний соединений есть возможность объединения их в группу. Внесение дополнительной группы состояний сетевого соединения осуществляется в пункте меню «Межсетевой экран → Группы состояний».

Подраздел «Группы адресов» содержит элементы, указанные в таблице 90.

Таблица 90 – Описание элементов подраздела «Группы адресов»

Элемент	Описание
	Значок активации ниспадающего списка
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Название группы»	Параметр выбора нового названия группы
Параметр «Выбрать группу»	Параметр предлагает выбрать из уже созданных групп
Ниспадающий список «Выбрать группу»	Ниспадающий список предлагает выбрать из уже созданных групп
Ниспадающий список «Выбрать состояние»	Ниспадающий список предлагает выбрать одно из уже имеющихся состояний
Кнопка «  »	Предназначена для добавления новой группы состояний

2.7.9 Подраздел «Правила межсетевого экрана»

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

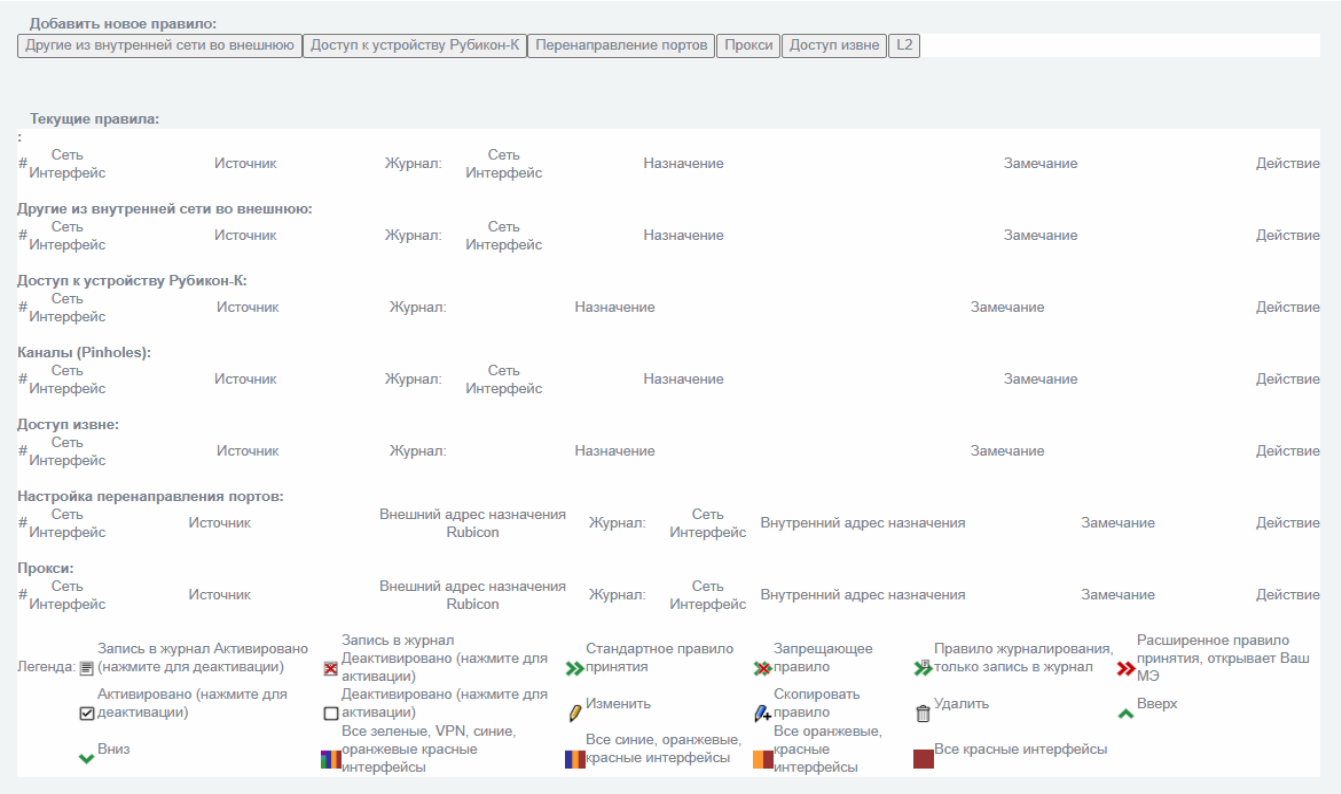


Рисунок 149 – Подраздел «Правила межсетевого экрана»

Подраздел «Правила межсетевого экрана» представляет собой информационное окно со следующим перечнем правил:

– «Другие из внутренней сети во внешнюю»;

– «Доступ к устройству Рубикон»;

– «Перенаправление портов»;

– «Прокси»;

– «Доступ извне»;

– «L2».

Перечни подраздела «Правила межсетевого экрана» содержит легенды, указанные в таблице 91.

Таблица 91 – Описание элементов подраздела «Правила межсетевого экрана»

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

2.7.9.1 Вкладка «Другие из внутренней сети во внешнюю»

Вкладка «Другие из внутренней сети во внешнюю» (рисунок 150) предназначена для добавления правил фильтрации сетевых пакетов, для которых адрес источника и адрес назначения

маршрутизируются из одного физического сетевого интерфейса в другой (например, при настройке взаимодействия зеленой-синей или зеленой-оранжевой подсетей).

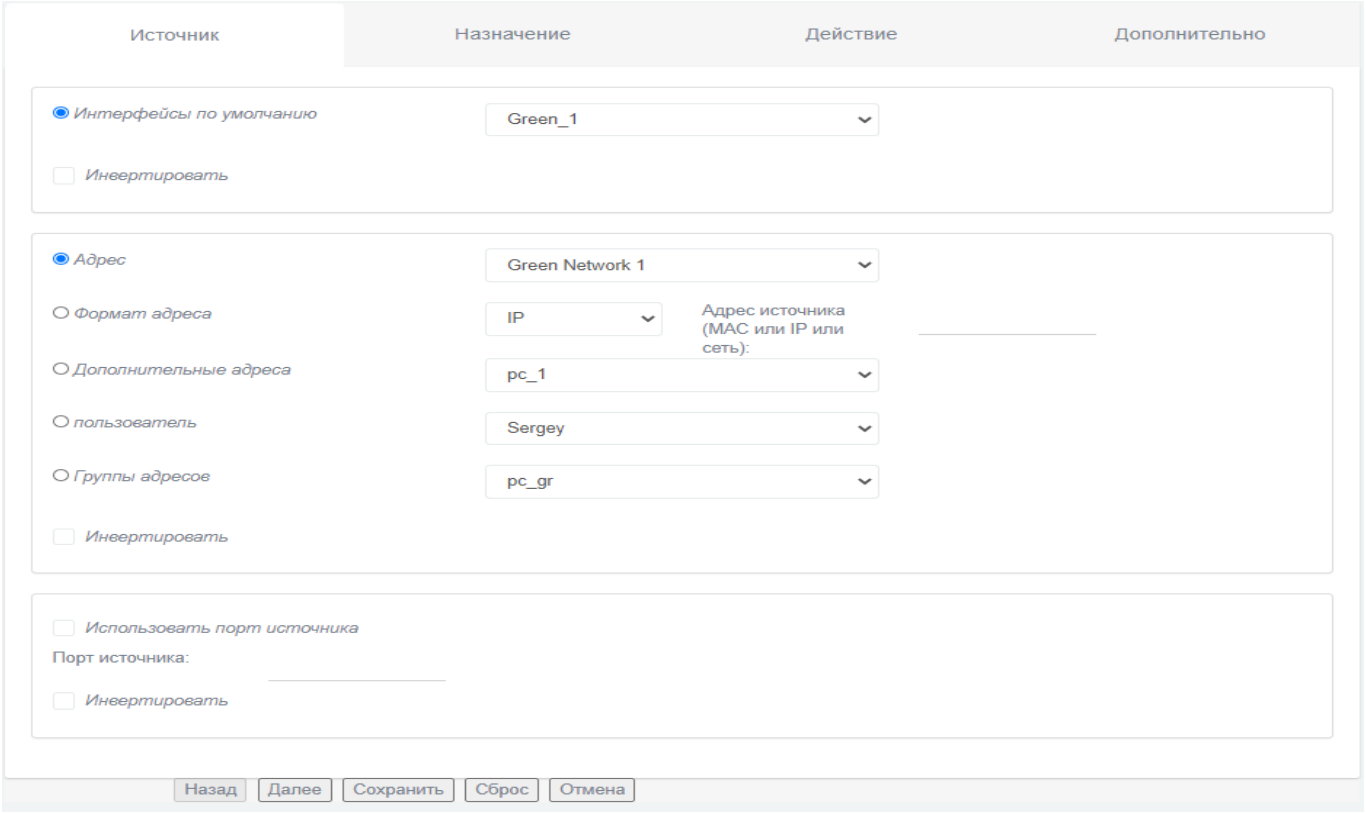


Рисунок 150 – Вкладка «Другие из внутренней сети во внешнюю»

Добавление правил фильтрации состоит из ввода следующих полей:

– «Источник»;

– «Назначение»;

– «Действие»;

– «Дополнительно».

2.7.9.1.1 Поле «Источник»

Поле «Источник» (рисунок 150) предназначено для настройки источника правила МЭ и содержит элементы, указанные в таблице 92.

Таблица 92 – Описание элементов поля «Источник»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Параметр и ниспадающий список «Интерфейсы по умолчанию»	Параметр активирует ниспадающий список «Интерфейсы по умолчанию» и позволяет выбрать один из интерфейсов
Параметр и ниспадающий список «Адрес»	Параметр активирует ниспадающий список «Адрес» и позволяет выбрать адрес источника
Параметр и ниспадающий список «Формат адреса»	Параметр активирует ниспадающий список «Формат адреса» и позволяет выбрать адрес
Поле «Адрес источника (MAC или IP или сеть)»	Предназначено для указания адреса источника обрабатываемых пакетов. Может задаваться вручную в соответствующем поле или выбираться из заданных заранее списков сетей
Параметр и ниспадающий список «Пользователь»	Параметр активирует ниспадающий список «Пользователь» и позволяет выбрать пользователя
Параметр и ниспадающий список «Группы адресов»	Параметр активирует ниспадающий список «Группы адресов» и позволяет выбрать группу адресов
Параметр «Использовать порт источника»	Предназначен для режима, при котором можно указывать порт, с которого поступают сетевые пакеты

Элемент	Описание
Поле «Порт источника»	Предназначено для указания порта
Параметр «Инвертировать»	Данный параметр в условии правила меняет действие условия на противоположное
Кнопка «Назад»	Кнопка перехода на предыдущую страницу
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.1.2 Поле «Назначение»

Поле «Назначение» (рисунок 151) используется для назначения служб, сервисов и цветов интерфейса.

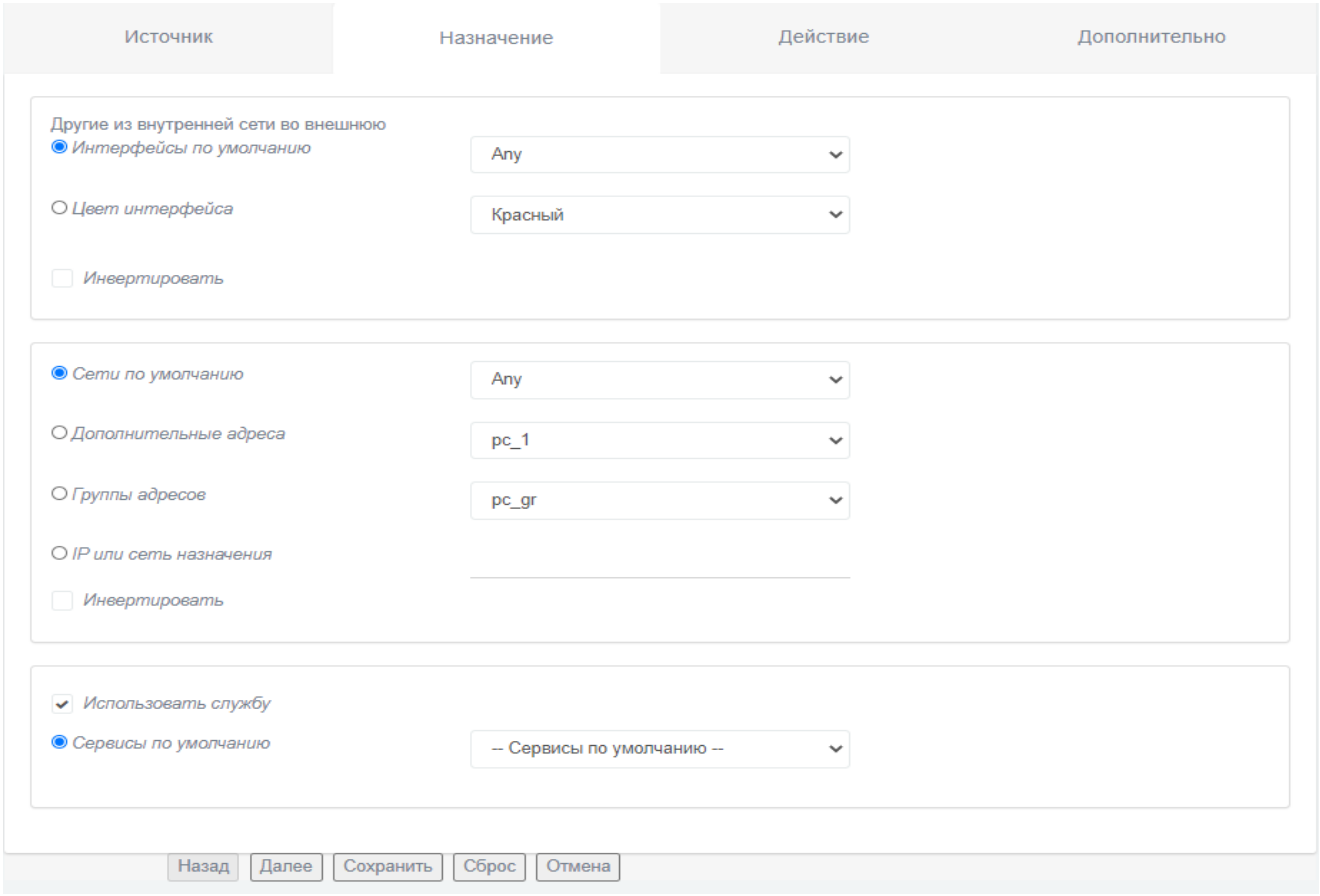


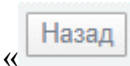
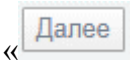
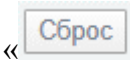
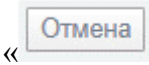
Рисунок 151 – Поле «Назначение»

Поле «Назначение» содержит элементы, указанные в таблице 93.

Таблица 93 – Описание элементов поля «Назначение»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)

Элемент	Описание
Параметр «Интерфейсы по умолчанию»	Параметр активирует ниспадающий список «Интерфейсы по умолчанию»
Ниспадающий список «Интерфейсы по умолчанию»	Предназначен для указания одного из определенных в системе интерфейсов
Параметр «Цвет интерфейса»	Параметр активирует ниспадающий список «Цвет интерфейса»
Ниспадающий список «Цвет интерфейса»	Предназначен для указания одного из определенных в системе цветов интерфейсов
Параметр «Сети по умолчанию»	Параметр активирует ниспадающий список «Сети по умолчанию»
Ниспадающий список «Сети по умолчанию»	Предназначен для указания одной из определенных в системе сетей
Параметр и ниспадающий список «Дополнительные адреса»	Параметр активирует ниспадающий список «Дополнительные адреса» и позволяет выбрать дополнительные адреса
Параметр и ниспадающий список «Группы адресов»	Параметр активирует ниспадающий список «Группы адресов» и позволяет выбрать группу адресов
Параметр и поле «IP или сеть назначения»	Предназначен для активации параметра. Поле предназначено для указания IP адреса или сети для узла назначения (целевого узла обрабатываемого пакета)
Параметр «Использовать службу»	Параметр активирует возможность использования службы
Параметр и ниспадающий список «Сервисы по умолчанию»	Параметр активирует ниспадающий список «Сервисы по умолчанию». Применяется для выбора службы (порта) «Рубикон», которой предназначается обрабатываемый пакет. Может быть выбран из списка стандартных сервисов (опция

Элемент	Описание
	«сервисы по умолчанию»), а также из списка заданных администратором служб
Параметр «Инвертировать»	Данный параметр в условии правила меняет действие условия на противоположное
Кнопка «  »	Кнопка перехода на предыдущую страницу
Кнопка «  »	Кнопка перехода на следующую страницу
Кнопка «  »	Кнопка сохранения введенной информации
Кнопка «  »	Кнопка сброса всех данных формы
Кнопка «  »	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.1.3 Поле «Действие»

Поле «Действие» (рисунок 152) предназначено для настройки действий при срабатывании правил.

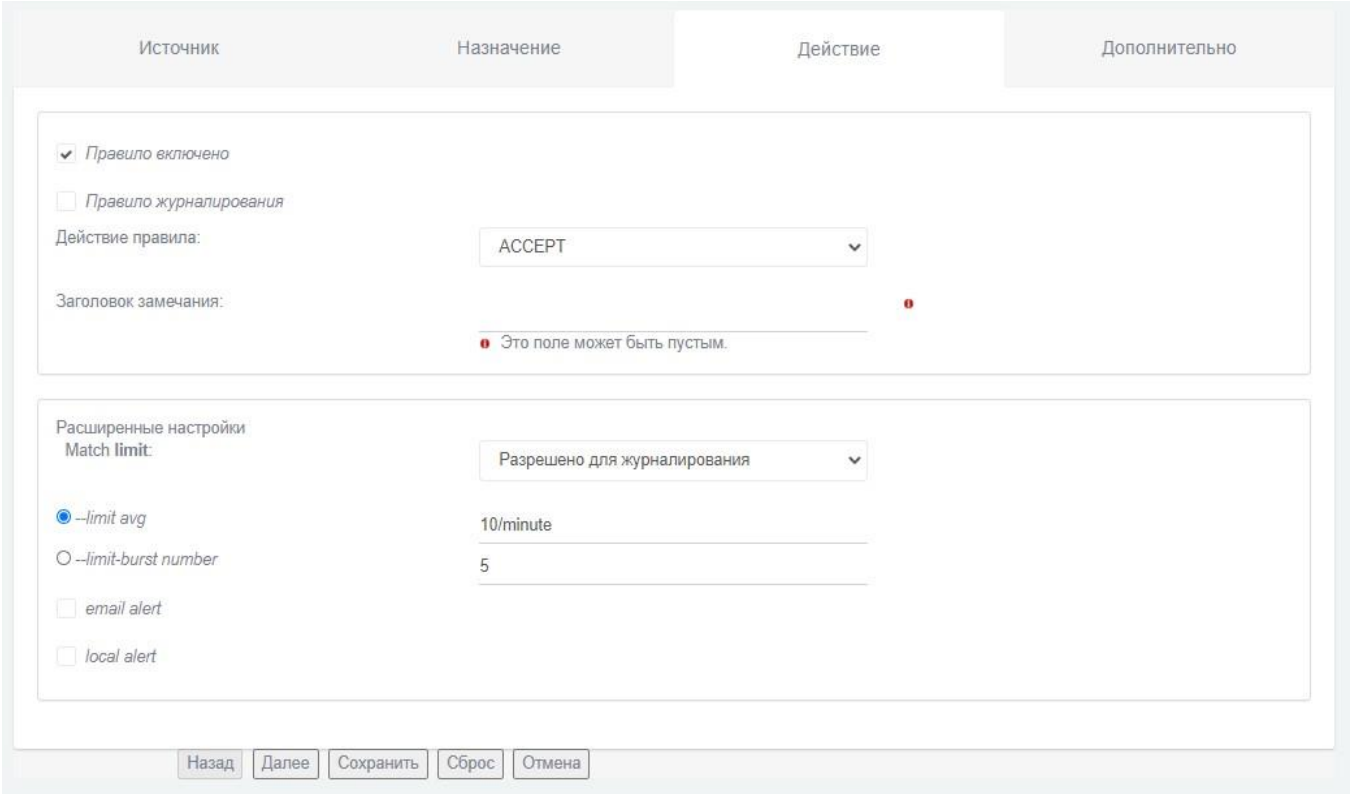
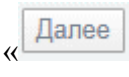


Рисунок 152 – Поле «Действие»

Поле «Действие» содержит элементы, указанные в таблице 94.

Таблица 94 – Описание элементов поля «Действие»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле необязательно для заполнения
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)

Элемент	Описание
Параметр «Правило включено»	Предназначен для указания необходимости включения/выключения правила
Параметр «Правило журналирования»	Предназначен для указания необходимости журналирования прохождения пакетов по данному правилу
Ниспадающий список «Действие правила»	Предназначен для указания действия при срабатывании правила
Поле «Заголовок замечания»	Предназначено для указания заголовка, помещаемого в строку журналирования по данному правилу
Ниспадающий список «Расширенные настройки Match limit»	Предназначен для включения расширенных настроек действия при срабатывании правил: – Возможность отключена; – Разрешено для журналирования; – Разрешено для политики принятия и сбрасывания; – Разрешено для политик обоих видов
Параметр «limit avg»	Предназначен для ограничения записи событий в журнал. Параметр «limit avg» задает среднюю частоту событий и указывается в формате число событий / единица времени
Параметр «limit-burst number»	Предназначен для ограничения записи событий в журнал. Параметр «limit-burst number» определяет пик «разовой» доставки пакетов. Значение по умолчанию «5»
Параметр «email alert»	Для получения оповещения о сработавшем правиле на электронную почту необходимо включить параметр «email alert»
Параметр «local alert»	Активация параметра включает локальные оповещения
Кнопка «  »	Кнопка перехода на следующую страницу
Кнопка «  »	Кнопка сохранения введенной информации

Элемент	Описание
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.1.4 Поле «Дополнительно»

Поле «Дополнительно» (рисунок 153) предназначена для настройки дополнительных критериев фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам. Кроме того, при срабатывании правила возможно присвоение числовой метки, применяемой для дальнейшей обработки сетевого пакета в целях маршрутизации.

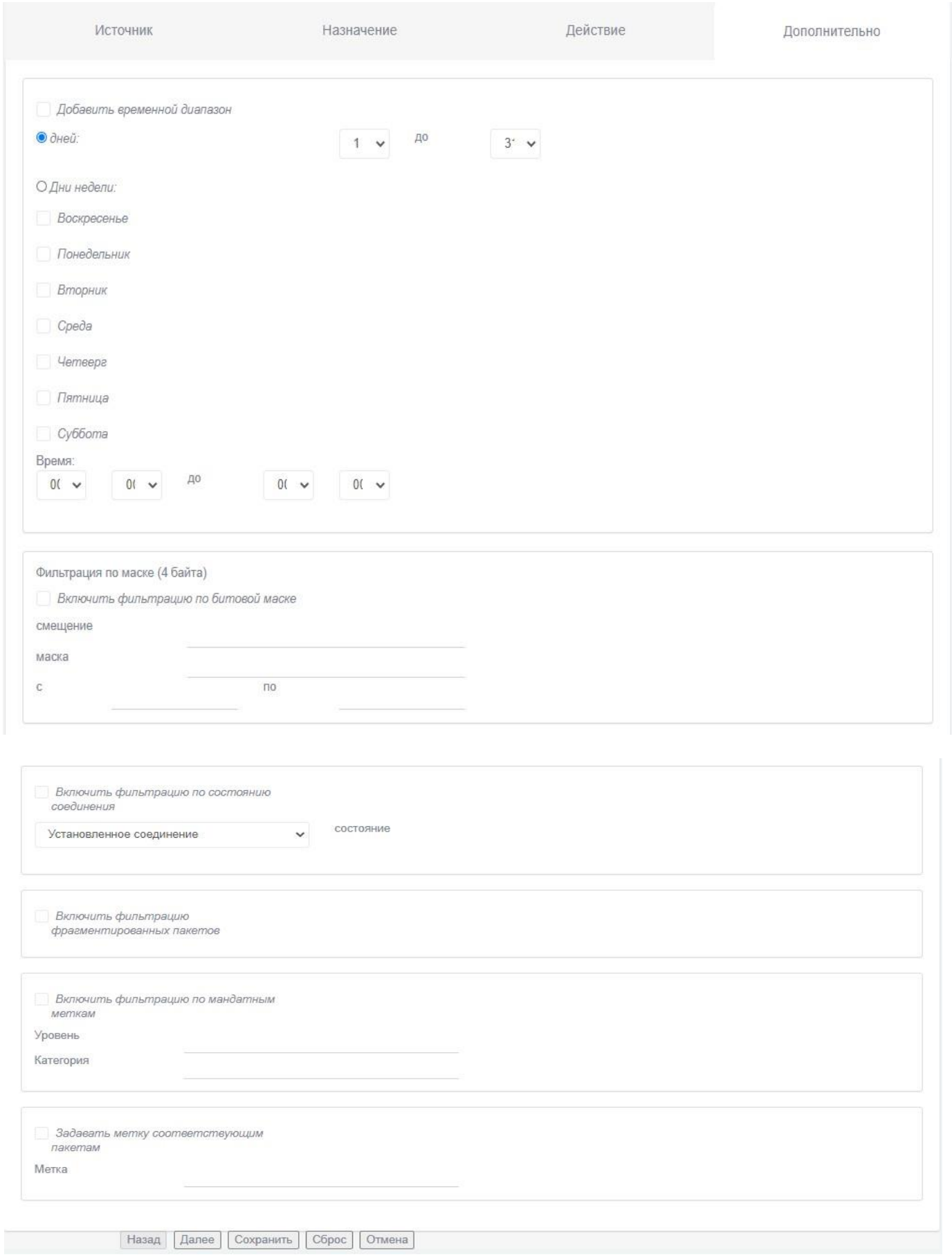


Рисунок 153 – Поле «Дополнительно»

Поле «Дополнительно» содержит элементы, указанные в таблице 95.

Таблица 95 – Описание элементов поля «Дополнительно»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Добавить временной диапазон»	Включение параметра дает возможность добавления временного диапазона для правил фильтрации сетевых пакетов из внутренней сети во внешнюю
Параметр и ниспадающие списки «Дней»	Предназначен для уточнения временного диапазона в днях
Параметр и перечень «Дни недели»	Активация параметра «Дни недели» дает возможность выбрать из перечня дни недели
Настройка «Фильтрация по маске (4 байта)»	Предназначена для включения фильтрации по битовой маске с внесением параметров «Смещение», «Маска», с указанием временного диапазона
Параметр «Включить фильтрацию по состоянию соединения»	Предназначен для активации параметра
Ниспадающий список «Состояние»	Предназначен для выбора соединения: – Установленное соединение; – Новое соединение

Элемент	Описание
Параметр «Включить фильтрацию фрагментированных пакетов»	Предназначен для включения фильтрации на уровне пакетов, что позволяет контролировать доступ к сети вне зависимости от программ, инициирующих подключение
Параметр «Включить фильтрацию по мандатным меткам»	При активации параметра созданное правило МЭ проверяет наличие мандатной метки согласно RFC 1108 (ГОСТ Р 58256-2018)
Поле «Уровень»	Предназначено для описания уровня данных (доступно всем, С, СС), задается в десятичном формате 1,2,3 и т.д.
Поле «Категория»	Предназначено для описания категории, к которой относятся данные, задается в двоичной форме 1 10 11 и т.д.
Параметр «Задавать метку соответствующим пакетам»	При активации параметра сетевые пакеты, попадающие под правило МЭ, будут промаркированы метками для обработки в «Рубикон». Данный механизм используется для статической маршрутизации по меткам
Поле «Метка»	Предназначено для задания метки, начиная с 1001 (например, 1001, 1002, 1003 и т.д.)
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.2 Вкладка «Доступ к устройству Рубикон»

Вкладка «Доступ к устройству Рубикон» (рисунок 154) предназначена дли 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).

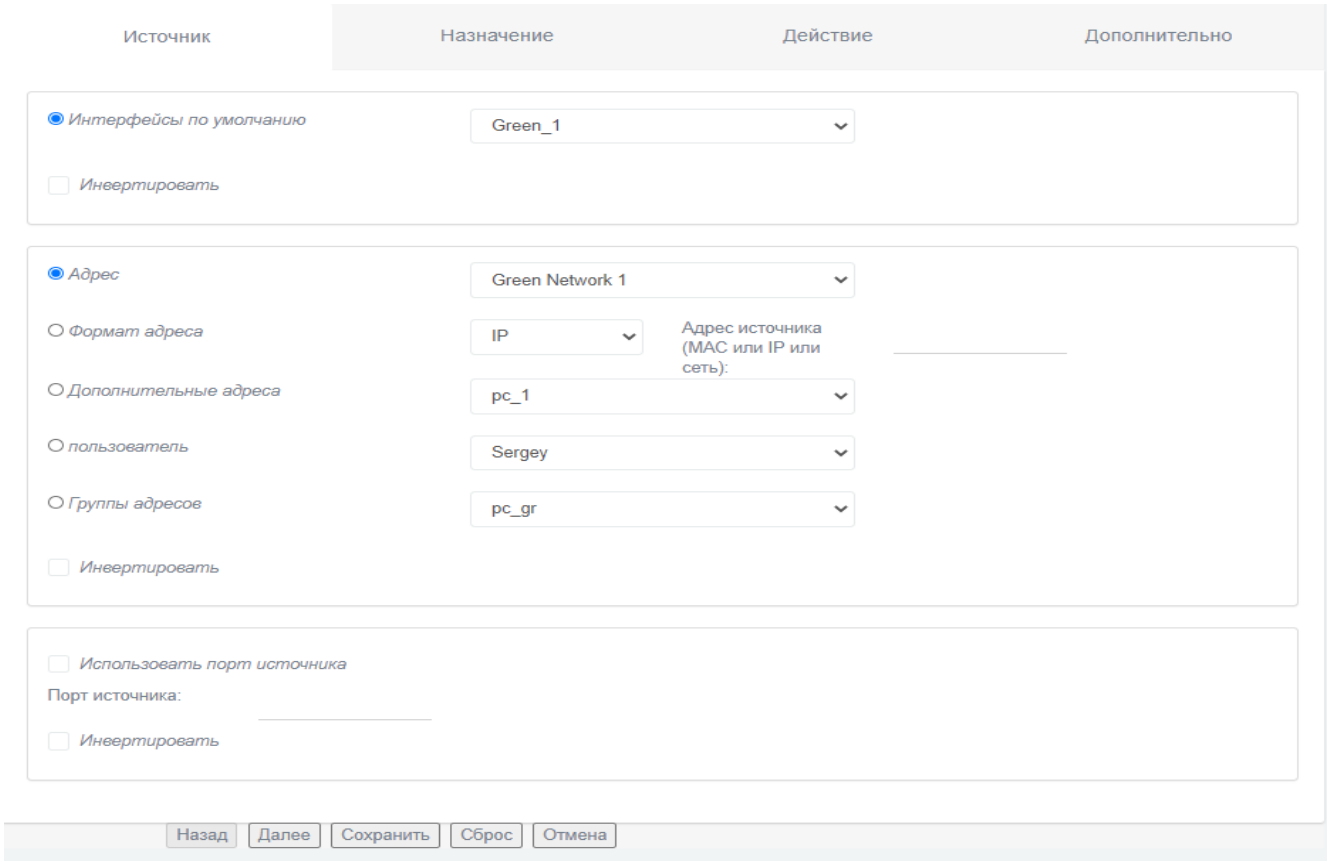


Рисунок 154 – Вкладка «Доступ к устройству Рубикон»

Добавление правил доступа состоит из полей:

– «Источник»;

– «Назначение»;

– «Действие»;

– «Дополнительно».

2.7.9.2.1 Поле «Источник»

Поле «Источник» (рисунок 154) предназначено для настройки источника правила МЭ и содержит элементы, указанные в таблице 96.

Таблица 96 – Описание элементов поля «Источник»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Интерфейсы по умолчанию»	Параметр активирует ниспадающий список «Интерфейсы по умолчанию»
Ниспадающий список «Интерфейсы по умолчанию»	Ниспадающий список позволяет выбрать один из интерфейсов
Параметр «Адрес»	Параметр активирует ниспадающий список «Адрес»
Ниспадающий список «Адрес»	Предназначен для указания адреса источника
Параметр «Формат адреса»	Параметр активирует ниспадающий список «Формат адреса»
Ниспадающий список «Формат адреса»	Указывает параметр адреса для строки ввода «Адрес источника (MAC или IP)»
Поле «Адрес источника (MAC или IP или сеть)»	Предназначено для указания адреса источника обрабатываемых пакетов. Может задаваться вручную в соответствующем поле или выбираться из заданных заранее списков сетей

Элемент	Описание
Параметр и ниспадающий список «Пользователь»	Параметр активирует ниспадающий список «Пользователь» и позволяет выбрать пользователя
Параметр и ниспадающий список «Группы адресов»	Параметр активирует ниспадающий список «Группы адресов» и позволяет выбрать группу адресов
Параметр «Использовать порт источника»	Предназначен для режима, при котором можно указывать порт, с которого поступают сетевые пакеты
Поле «Порт источника»	Предназначено для указания порта
Параметр «Инвертировать»	Данный параметр в условии правила меняет действие условия на противоположное
Кнопка «Назад»	Кнопка перехода на предыдущую страницу
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.2.2 Поле «Назначение»

Поле «Назначение» (рисунок 155) предназначено для задания порта назначения службы, которая будет использоваться для доступа к МЭ.

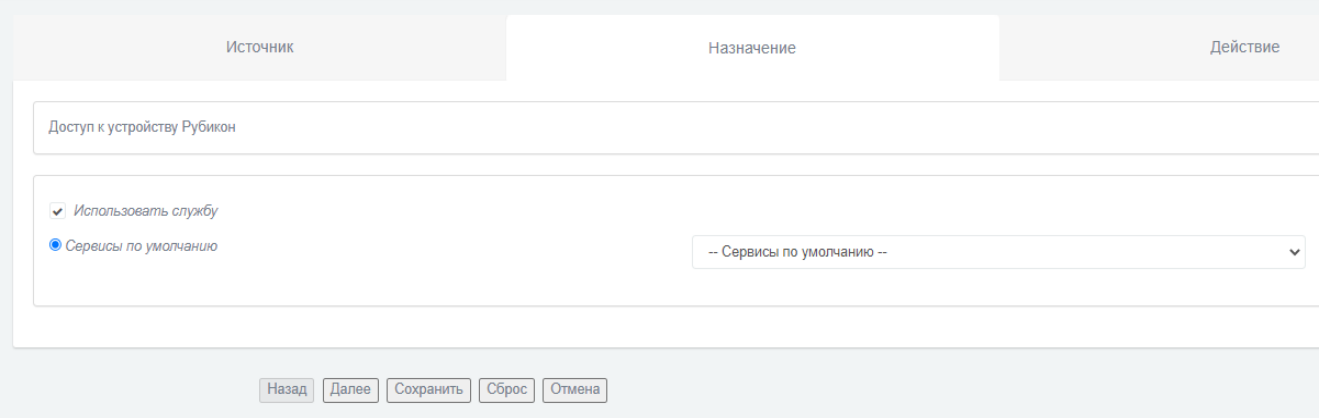
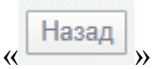
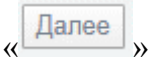


Рисунок 155 – Поле «Назначение»

Поле «Назначение» содержит элементы, указанные в таблице 97.

Таблица 97 – Описание элементов поля «Назначение»

Элемент	Описание
	Значок активации ниспадающего списка
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Параметр «Использовать службу»	Параметр включает службу для данного правила
Параметр «Сервисы по умолчанию»	Применяется для выбора службы (порта), которой предназначается обрабатываемый пакет. Может быть выбран из списка стандартных сервисов (опция «сервисы по умолчанию»), а также из списка заданных администратором служб
Ниспадающий список «Сервисы по умолчанию»	
Кнопка «  »	Кнопка перехода на предыдущую страницу
Кнопка «  »	Кнопка перехода на следующую страницу

Элемент	Описание
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.2.3 Поле «Действие»

Поле «Действие» (рисунок 156) предназначено для настройки действий при срабатывании правил.

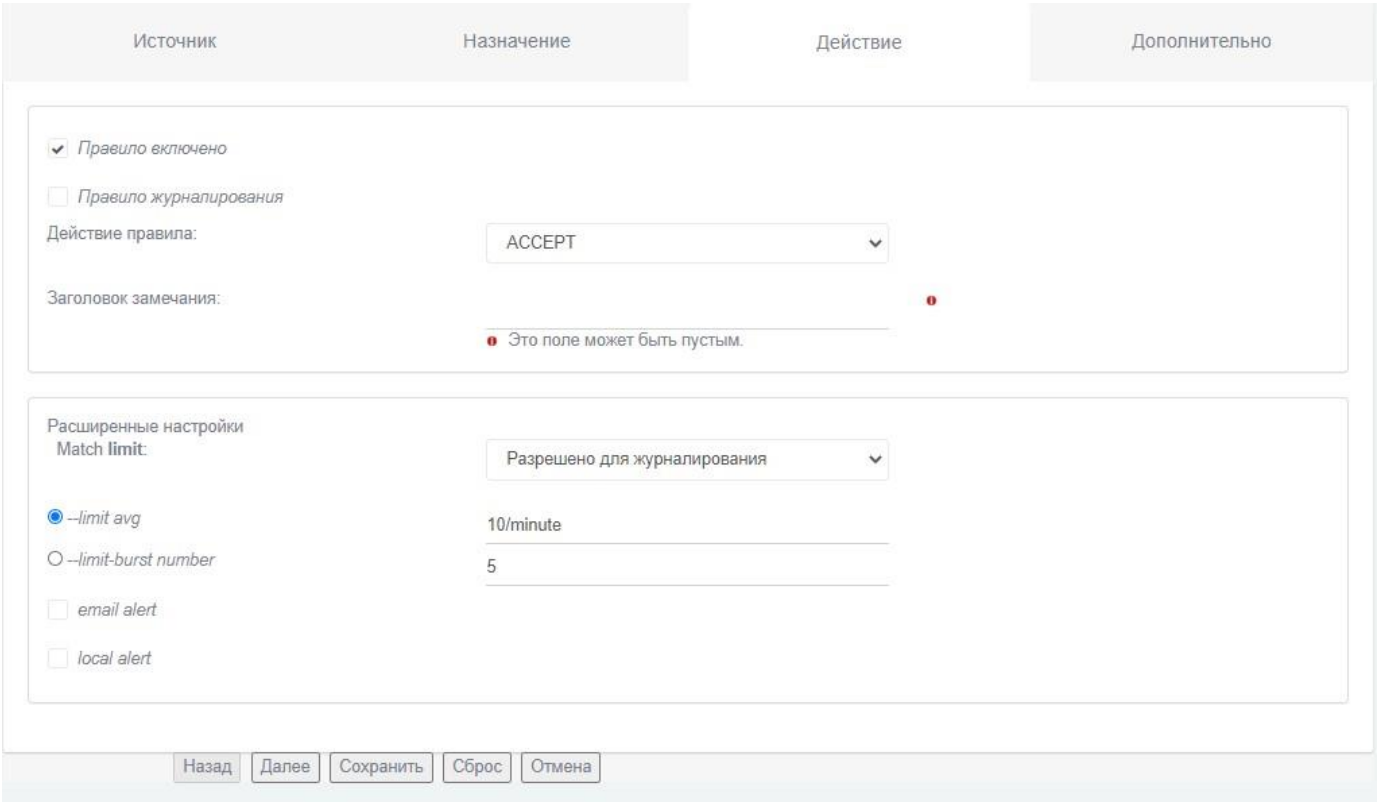


Рисунок 156 – Поле «Действие»

Поле «Действие» содержит элементы, указанные в таблице 98.

Таблица 98 – Описание элементов поля «Действие»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле необязательно для заполнения
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)

Элемент	Описание
Параметр «Правило включено»	Предназначен для указания необходимости включения/выключения правила
Параметр «Правило журналирования»	Предназначен для указания необходимости журналирования прохождения пакетов по данному правилу
Ниспадающий список «Действие правила»	Предназначен для указания действия при срабатывании правила
Поле «Заголовок замечания»	Предназначено для указания заголовка, помещаемого в строку журналирования по данному правилу
Параметр «limit avg»	Предназначен для ограничения записи событий в журнал. Параметр «limit avg» задает среднюю частоту событий и указывается в формате число событий / единица времени
Параметр «limit-burst number»	Предназначен для ограничения записи событий в журнал. Параметр «limit-burst number» определяет пик «разовой» доставки пакетов. Значение по умолчанию «5»
Параметр «email alert»	Для получения оповещения о сработавшем правиле на электронную почту необходимо включить параметр «email alert»
Параметр «local alert»	Активация параметра включает локальные оповещения
Кнопка «Назад»	Кнопка перехода на предыдущую страницу
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.2.4 Поле «Дополнительно»

Поле «Действие» (рисунок 157) предназначено для назначения дополнительных критериев фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам. Кроме того, при срабатывании правила возможно присвоение числовой метки, применяемой для дальнейшей обработки сетевого пакета в целях маршрутизации.

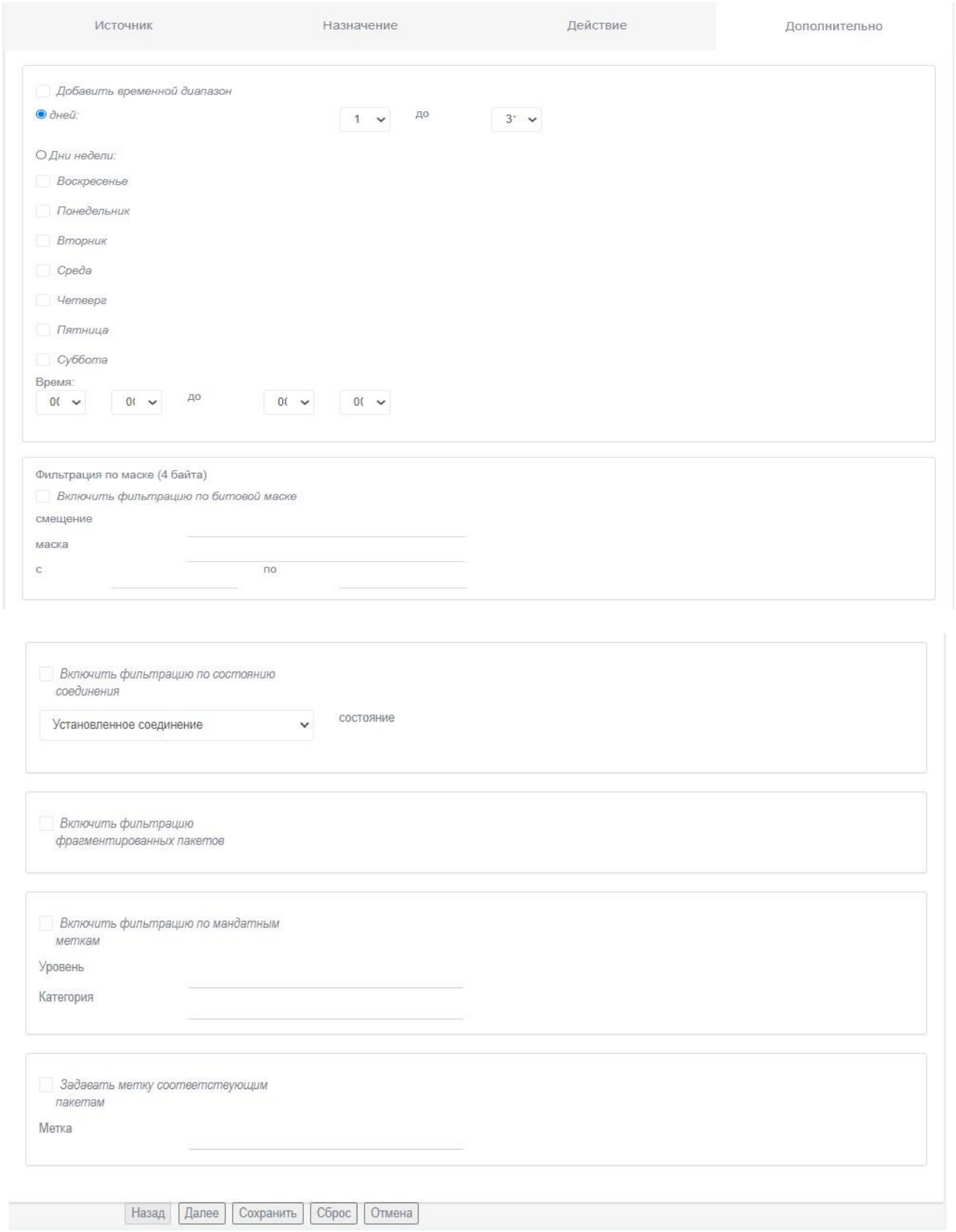


Рисунок 157 – Поле «Дополнительно»

Поле «Дополнительно» содержит элементы, указанные в таблице 99.

Таблица 99 – Описание элементов поля «Дополнительно»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Добавить временной диапазон»	Включение параметра дает возможность добавления временного диапазона для правил фильтрации сетевых пакетов из внутренней сети во внешнюю
Параметр и ниспадающие списки «Дней»	Предназначен для уточнения временного диапазона в днях
Параметр и перечень «Дни недели»	Активация параметра «Дни недели» дает возможность выбрать из перечня дни недели
Настройка «Фильтрация по маске (4 байта)»	Предназначена для включения фильтрации по битовой маске с внесением параметров «Смещение», «Маска», с указанием временного диапазона
Параметр «Включить фильтрацию по состоянию соединения»	Предназначен для активации параметра
Ниспадающий список «Состояние»	Предназначен для выбора соединения: – Установленное соединение;

Элемент	Описание
	– Новое соединение
Параметр «Включить фильтрацию фрагментированных пакетов»	Предназначен для включения фильтрации на уровне пакетов, что позволяет контролировать доступ к сети вне зависимости от программ, инициирующих подключение
Параметр «Включить фильтрацию по мандатным меткам»	При активации параметра созданное правило МЭ проверяет наличие мандатной метки согласно RFC 1108 (ГОСТ Р 58256-2018)
Поле «Уровень»	Предназначено для описания уровня данных (доступно всем, С, СС), задается в десятичном формате 1,2,3 и т.д.
Поле «Категория»	Предназначено для описания категории, к которой относятся данные, задается в двоичной форме 1 10 11 и т.д.
Параметр «Задавать метку соответствующим пакетам»	При активации параметра сетевые пакеты, попадающие под правило МЭ, будут промаркированы метками для обработки в «Рубикон». Данный механизм используется для статической маршрутизации по меткам
Поле «Метка»	Предназначено для задания метки, начиная с 1001 (например, 1001, 1002, 1003 и т.д.)
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.3 Подраздел «Перенаправление портов»

Подраздел «Перенаправление портов» (рисунок 158) предназначен для обработки сетевых пакетов, для которых реальный адрес и порт назначения подставляется при получении МЭ пакета с определенными администратором параметрами назначения (например, для организации доступа к серверам в ДМЗ).

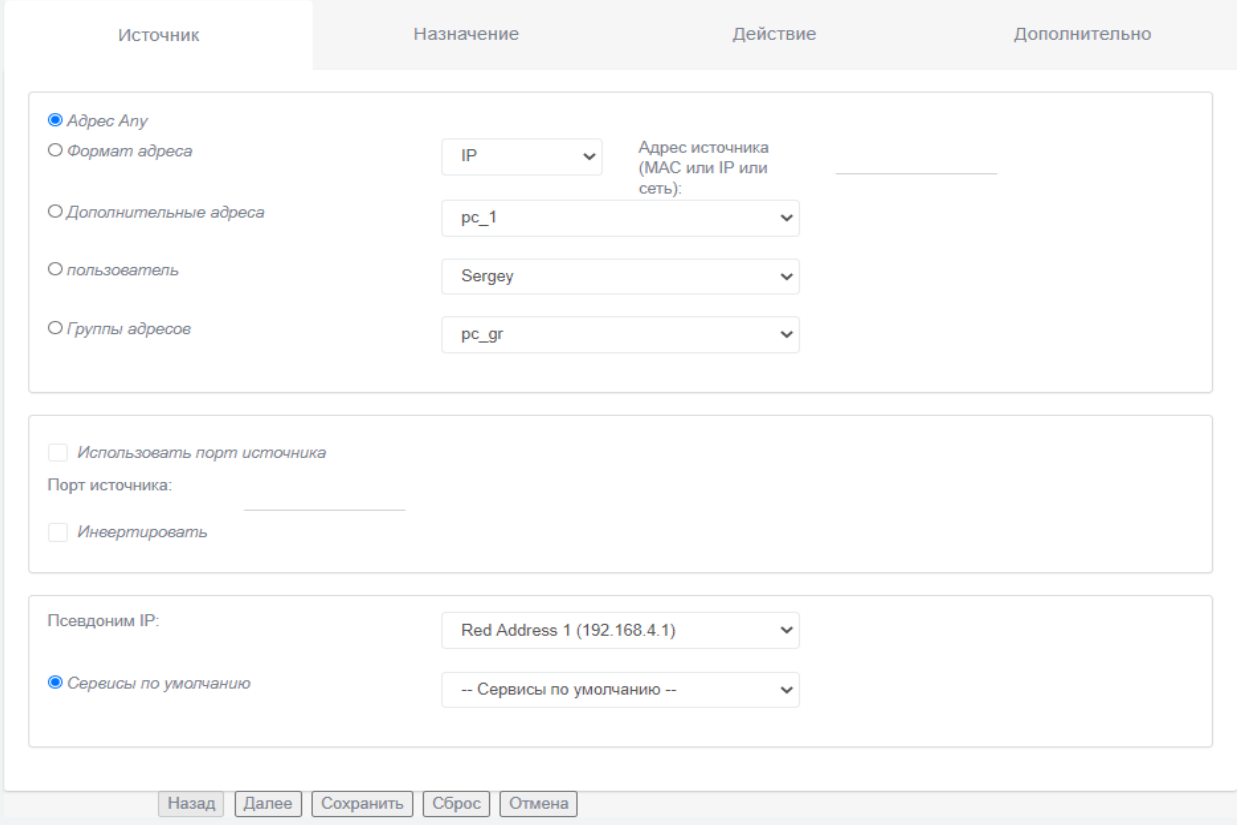


Рисунок 158 – Вкладка «Перенаправление портов»

Подраздел «Перенаправление портов» состоит из следующих полей:

– «Источник»;

– «Назначение»;

– «Действие»;

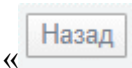
– «Дополнительно».

2.7.9.3.1 Поле «Источник»

Поле «Источник» (рисунок 158) предназначено для настройки источника пакета, получаемого МЭ и сетевых параметров, по которым принимается решение о перенаправлении. Настройка данного поля содержит элементы, указанные в таблице 100.

Таблица 100 – Описание элементов поля «Источник»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Адрес Any»	Активирует доступ со всех адресов
Параметр «Формат адреса»	Активирует IP или MAC
Поле «Адрес источника (MAC или IP или сеть)»	Предназначено для указания адреса источника обрабатываемых пакетов. Может задаваться вручную в соответствующем поле или выбираться из заданных заранее списков сетей
Параметр и ниспадающий список «Пользователь»	Параметр активирует ниспадающий список «Пользователь» и позволяет выбрать пользователя
Параметр и ниспадающий список «Группы адресов»	Параметр активирует ниспадающий список «Группы адресов» и позволяет выбрать группу адресов

Элемент	Описание
Параметр «Использовать порт источника»	Предназначен для указания при необходимости дополнительно использовать номер порта источника, находящегося в красной сети
Поле «Порт источника»	Предназначено для указания номера порта источника. Фильтрация по порту источника осуществляется только если установлен
Параметр «Инвертировать»	Данный параметр в условии правила меняет действие условия на противоположное
Параметр «Псевдоним IP»	Активирует ниспадающий список «Псевдоним IP»
Ниспадающий список «Псевдоним IP»	Предназначен для выбора IP-адреса красного интерфейса, на котором будет принят сетевой пакет МЭ. Заданный адрес является одним из параметров принятия решения о преобразовании адреса и порта назначения.
Параметр «Сервисы по умолчанию»	Активирует ниспадающий список «Сервисы по умолчанию»
Ниспадающий список «Сервисы по умолчанию»	Предназначен для выбора службы (порта) «Рубикон», на котором будет принят сетевой пакет МЭ. порт может быть выбран из списка стандартных сервисов (опция «сервисы по умолчанию»), а также из списка заданных администратором служб. Заданный порт является одним из параметров принятия решения о преобразовании адреса и порта назначения
Кнопка «  »	Кнопка перехода на предыдущую страницу

Элемент	Описание
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.3.2 Поле «Назначение»

Поле «Назначение» (рисунок 159) предназначено для выбора параметров преобразования адреса назначения, служб, сервисов и цветов интерфейса.

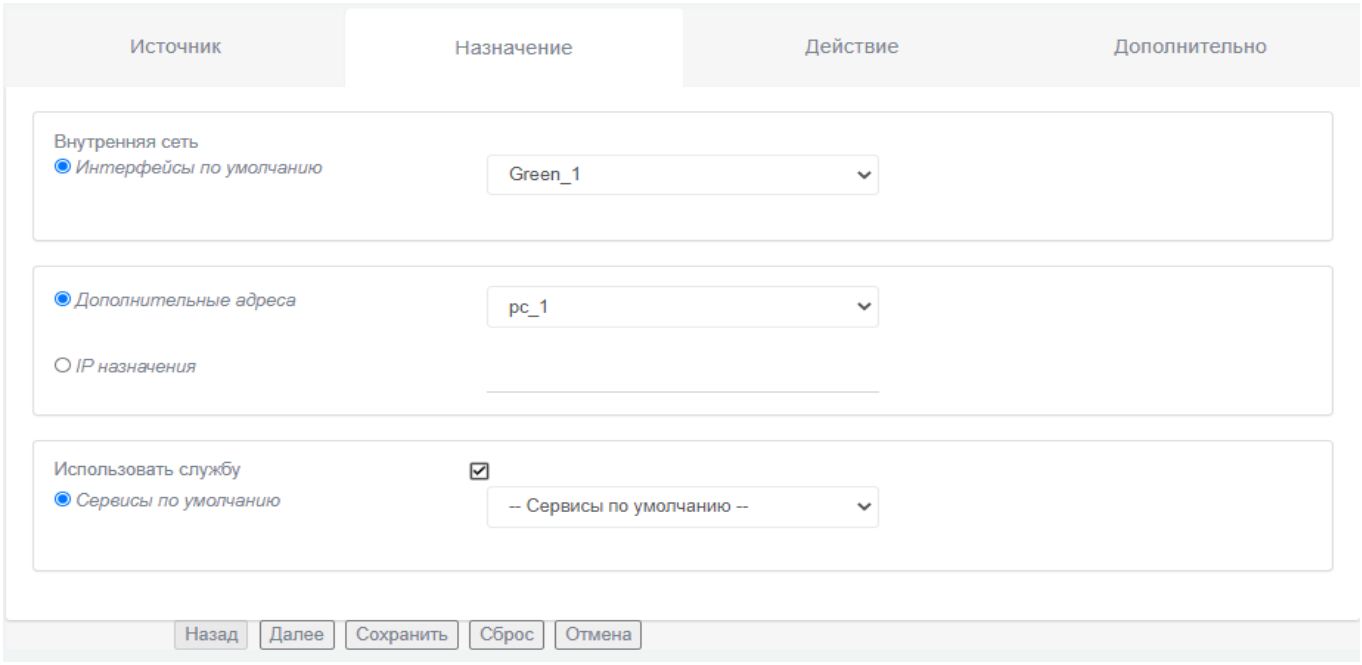
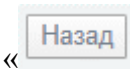
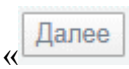


Рисунок 159 – Поле «Назначение»

Поле «Назначение» содержит элементы, указанные в таблице 101.

Таблица 101 – Описание элементов поля «Назначение»

Элемент	Описание
	Значок активации ниспадающего списка
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Параметр «Интерфейсы по умолчанию»	Ниспадающий список позволяет выбрать один из интерфейсов
Ниспадающий список «Интерфейсы по умолчанию»	
Параметр и поле «IP назначения»	Поле для указания адреса назначения, на который будет заменен адрес назначения исходного сетевого пакета
Параметр и ниспадающий список «Дополнительные адреса»	Параметр активирует ниспадающий список «Дополнительные адреса» и позволяет выбрать дополнительные адреса
Параметр «Сервисы по умолчанию»	Применяется для выбора службы (порта) «Рубикон», на который будет замене порт назначения исходного сетевого пакета. Может быть выбран из списка стандартных сервисов (опция «сервисы по умолчанию»), а также из списка заданных администратором служб
Ниспадающий список «Сервисы по умолчанию»	
Кнопка «  »	Кнопка перехода на предыдущую страницу
Кнопка «  »	Кнопка перехода на следующую страницу

Элемент	Описание
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.3.3 Поле «Действие»

Поле «Действие» (рисунок 160) предназначено для настройки действий при срабатывании правил.

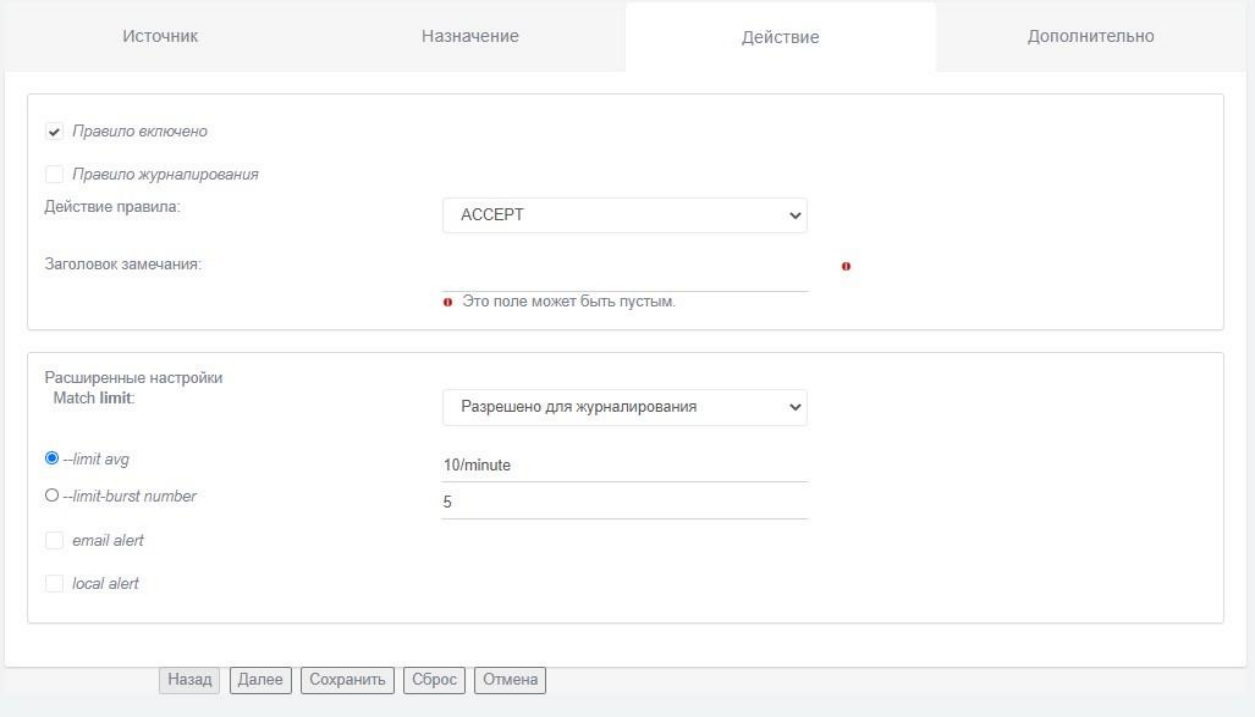


Рисунок 160 – Поле «Действие»

Поле «Действие» содержит элементы, указанные в таблице 102.

Таблица 102 – Описание элементов поля «Действие»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле необязательно для заполнения
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Правило включено»	Предназначен для указания необходимости включения/выключения правила
Параметр «Правило журналирования»	Предназначен для указания необходимости журналирования прохождения пакетов по данному правилу
Ниспадающий список «Действие правила»	Предназначен для указания действия при срабатывании правила
Поле «Заголовок замечания»	Предназначено для указания заголовка, помещаемого в строку журналирования по данному правилу
Параметр «limit avg»	Предназначен для ограничения записи событий в журнал. Параметр «limit avg» задает среднюю частоту событий и указывается в формате число событий / единица времени
Параметр «limit-burst number»	Предназначен для ограничения записи событий в журнал. Параметр «limit-burst number» определяет пик «разовой» доставки пакетов. Значение по умолчанию «5»
Параметр «email alert»	Для получения оповещения о сработавшем правиле на электронную почту необходимо включить параметр «email alert»

Элемент	Описание
Параметр «local alert»	Активация параметра включает локальные оповещения
Кнопка «Назад»	Кнопка перехода на предыдущую страницу
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.3.4 Настройка поля «Дополнительно»

Поле «Дополнительно» (рисунок 161) предназначено для назначения дополнительных критериев фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам. Кроме того, при срабатывании правила возможно присвоение числовой метки, применяемой для дальнейшей обработки сетевого пакета в целях маршрутизации.

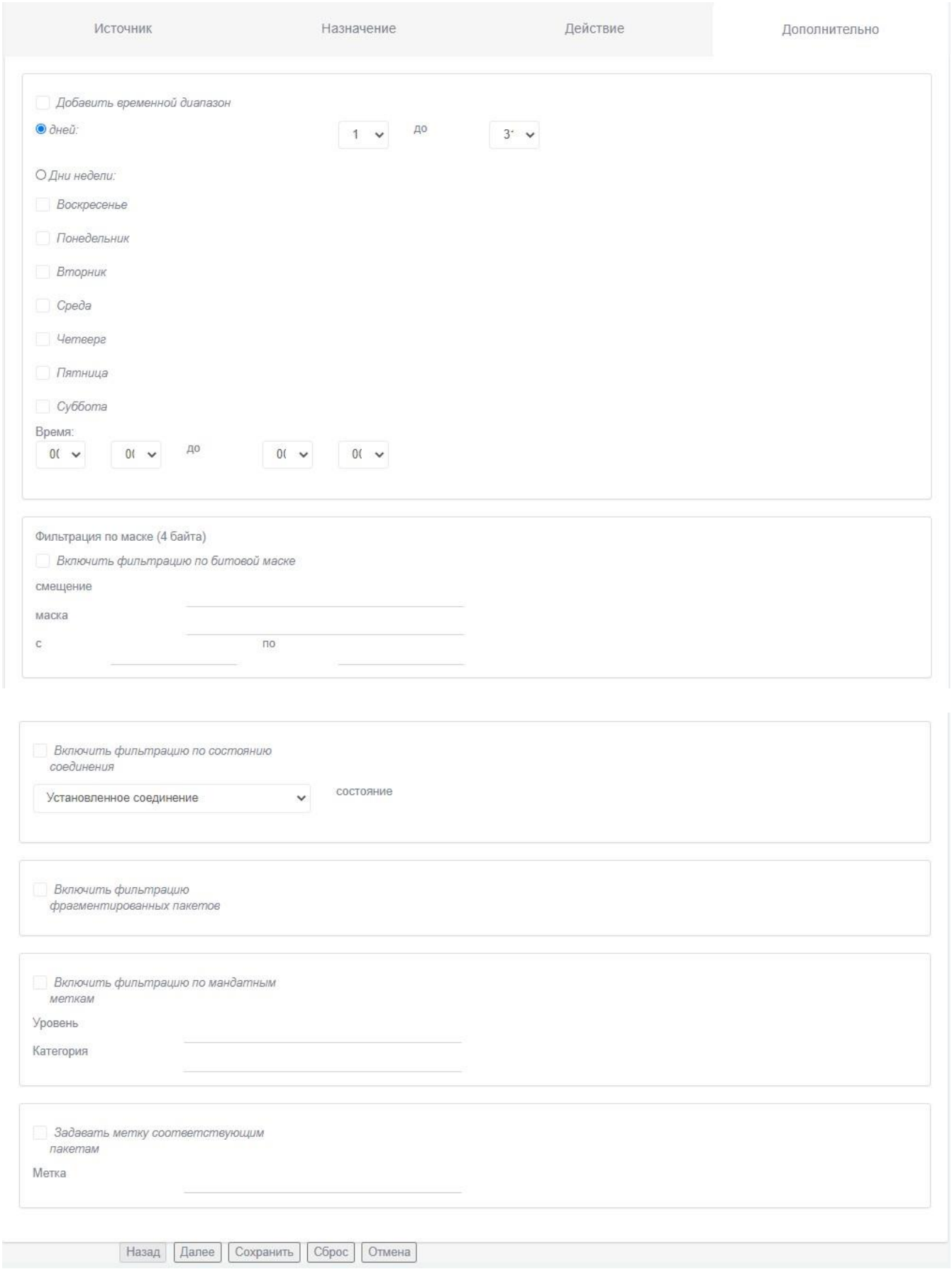
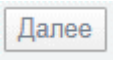
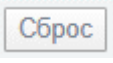
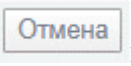


Рисунок 161 – Поле «Дополнительно»

Поле «Дополнительно» содержит элементы, указанные в таблице 103.

Таблица 103 – Описание элементов поля «Дополнительно»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Добавить временной диапазон»	Включение параметра дает возможность добавления временного диапазона для правил фильтрации сетевых пакетов из внутренней сети во внешнюю
Параметр и ниспадающие списки «Дней»	Предназначен для уточнения временного диапазона в днях
Параметр и перечень «Дни недели»	Активация параметра «Дни недели» дает возможность выбрать из перечня дни недели
Настройка «Фильтрация по маске (4 байта)»	Предназначена для включения фильтрации по битовой маске с внесением параметров «Смещение», «Маска», с указанием временного диапазона
Параметр «Включить фильтрацию по состоянию соединения»	Предназначен для активации параметра
Ниспадающий список «Состояние»	Предназначен для выбора соединения: – Установленное соединение;

Элемент	Описание
	– Новое соединение
Параметр «Включить фильтрацию фрагментированных пакетов»	Предназначен для включения фильтрации на уровне пакетов, что позволяет контролировать доступ к сети вне зависимости от программ, инициирующих подключение
Параметр «Включить фильтрацию по мандатным меткам»	При активации параметра созданное правило МЭ проверяет наличие мандатной метки согласно RFC 1108 (ГОСТ Р 58256-2018)
Поле «Уровень»	Предназначено для описания уровня данных (доступно всем, С, СС), задается в десятичном формате 1,2,3 и т.д.
Поле «Категория»	Предназначено для описания категории, к которой относятся данные, задается в двоичной форме 1 10 11 и т.д.
Параметр «Задавать метку соответствующим пакетам»	При активации параметра сетевые пакеты, попадающие под правило МЭ, будут промаркированы метками для обработки в «Рубикон». Данный механизм используется для статической маршрутизации по меткам
Поле «Метка»	Предназначено для задания метки, начиная с 1001 (например, 1001, 1002, 1003 и т.д.)
Кнопка «  »	Кнопка перехода на следующую страницу
Кнопка «  »	Кнопка сохранения введенной информации
Кнопка «  »	Кнопка сброса всех данных формы
Кнопка «  »	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.4 Вкладка «Прокси»

Вкладка «Прокси» (рисунок 162) – предназначена для ассоциации трафика, поступающего на определенный порт, с одним из обрабатываемых типов (HTTP, FTP). Обработка этого трафика осуществляется с помощью программы-посредника.

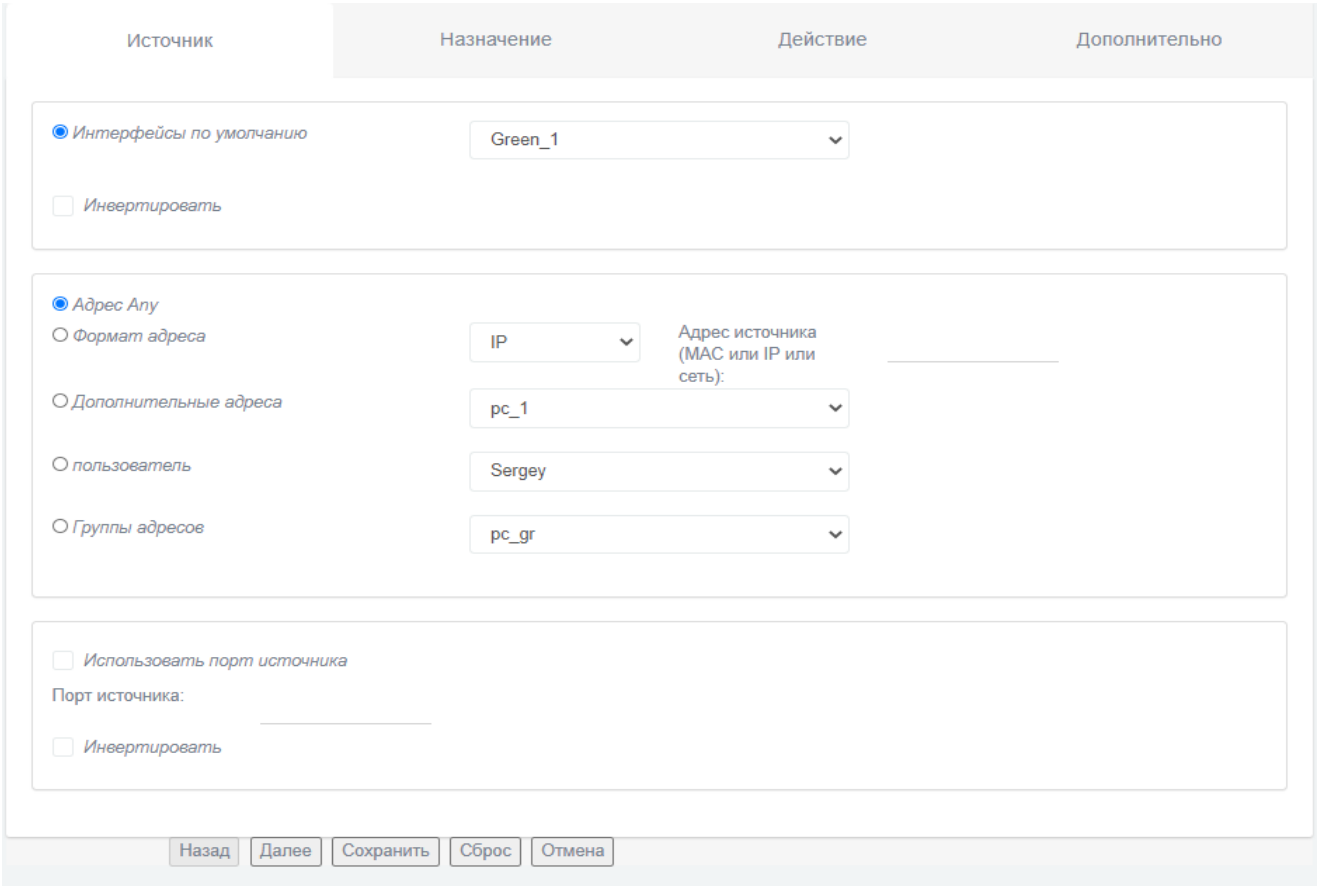


Рисунок 162 – Вкладка «Прокси»

Вкладка «Прокси» состоит из следующих настроек:

– «Источник»;

– «Назначение»;

– «Действие»;

– «Дополнительно».

2.7.9.4.1 Поле «Источник»

Поле «Источник» (рисунок 163) предназначено для настройки источника правила МЭ.

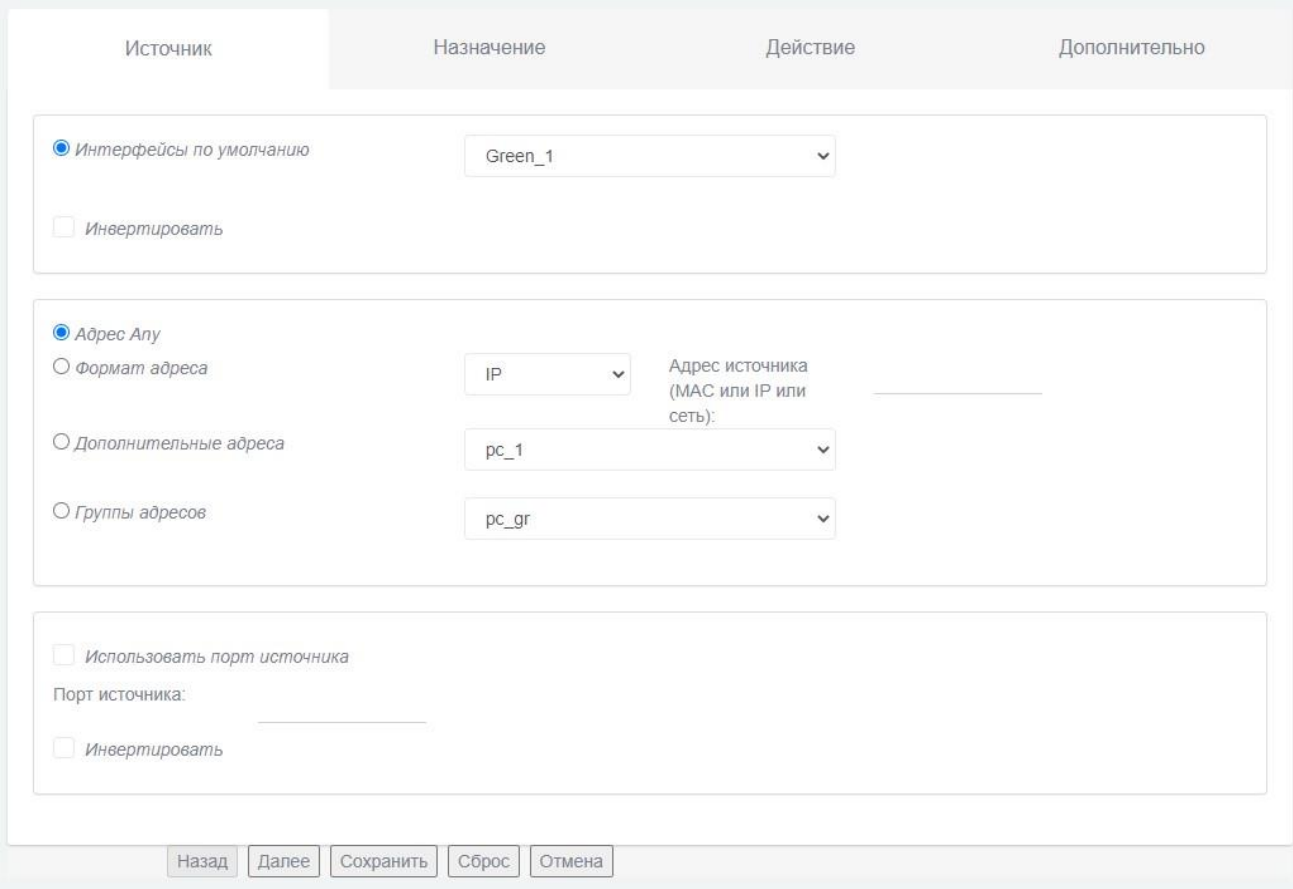
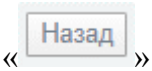


Рисунок 163 – Настройка «Источник»

Поле «Источник» содержит элементы, указанные в таблице 104.

Таблица 104 – Описание элементов поля «Источник»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)

Элемент	Описание
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр и ниспадающий список «Интерфейсы по умолчанию»	Ниспадающий список позволяет выбрать один из интерфейсов
Параметр «Адрес Any»	Активирует доступ со всех адресов
Параметр «Формат адреса»	Активирует ниспадающий список «Формат адреса»
Ниспадающий список «Формат адреса»	Указывает параметр адреса для строки ввода «Адрес источника (MAC или IP или сеть)»
Поле «Адрес источника (MAC или IP или сеть)»	Предназначено для указания адреса источника обрабатываемых пакетов. Может задаваться вручную в соответствующем поле или выбираться из заданных заранее списков сетей
Параметр и ниспадающий список «Дополнительные адреса»	Параметр активирует ниспадающий список «Дополнительные адреса» и позволяет выбрать дополнительные адреса
Параметр и ниспадающий список «Группы адресов»	Параметр активирует ниспадающий список «Группы адресов» и позволяет выбрать группу адресов
Параметр «Использовать порт источника»	Предназначен для режима, при котором можно указывать порт, с которого поступают сетевые пакеты
Поле «Порт источника»	Предназначено для указания порта
Параметр «Инвертировать»	Данный параметр в условии правила меняет действие условия на противоположное
Кнопка «  »	Кнопка перехода на предыдущую страницу

Элемент	Описание
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.4.2 Поле «Назначение»

Поле «Назначение» (рисунок 164) предназначено для назначения служб и сервисов.

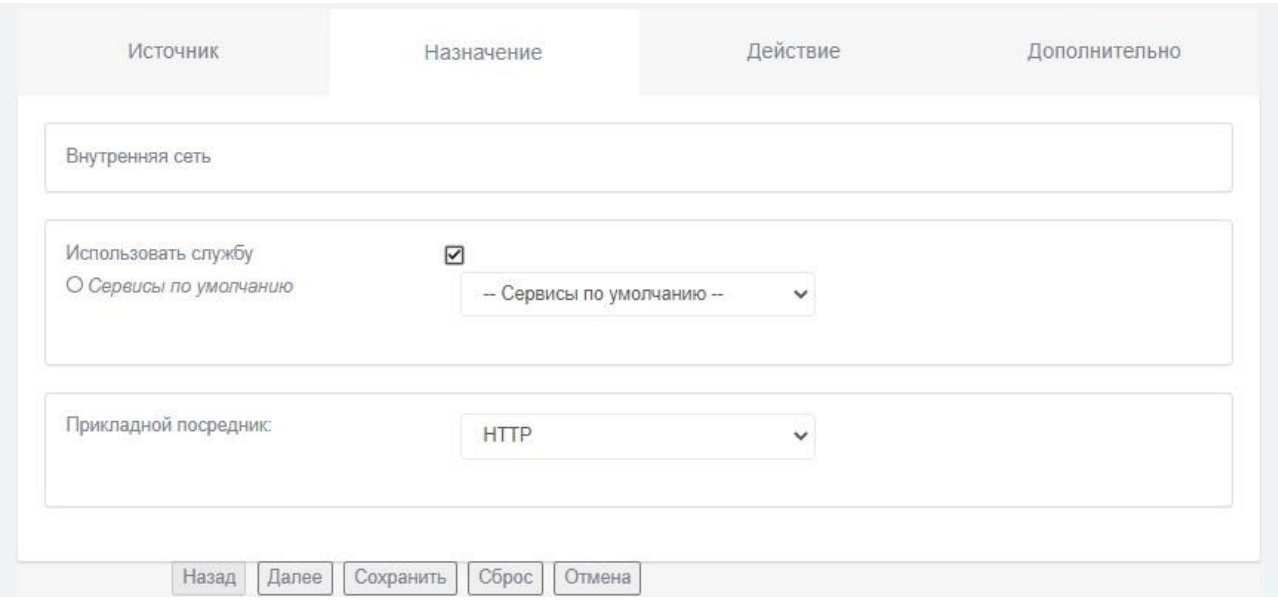
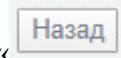
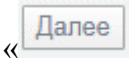
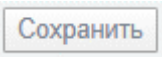
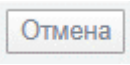


Рисунок 164 – Настройка «Назначение»

Поле «Назначение» содержит элементы, указанные в таблице 105.

Таблица 105 – Описание элементов поля «Назначение»

Элемент	Описание
	Значок активации ниспадающего списка
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Параметр «Использовать службу»	Параметр включает службу для данного правила
Параметр «Сервисы по умолчанию»	Применяется для выбора службы (порта) «Рубикон», на которой поступает трафик, требующий ассоциации с прикладным протоколом. Служба (порт) может быть выбрана из списка стандартных сервисов (опция «сервисы по умолчанию»), а также из списка заданных администратором служб
Ниспадающий список «Сервисы по умолчанию»	
Ниспадающий список «Прикладной посредник»	Прикладной посредник предоставляет выбор прикладного протокола (HTTP, FTP) для ассоциации и обработки трафика, определенного пользователем. Ниспадающий список позволяет выбрать протокол
Кнопка «  »	Кнопка перехода на предыдущую страницу
Кнопка «  »	Кнопка перехода на следующую страницу
Кнопка «  »	Кнопка сохранения введенной информации
Кнопка «  »	Кнопка сброса всех данных формы

Элемент	Описание
Кнопка «  »	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.4.3 Поле «Действие»

Поле «Действие» (рисунок 165) предназначено для настройки действий при срабатывании правил.

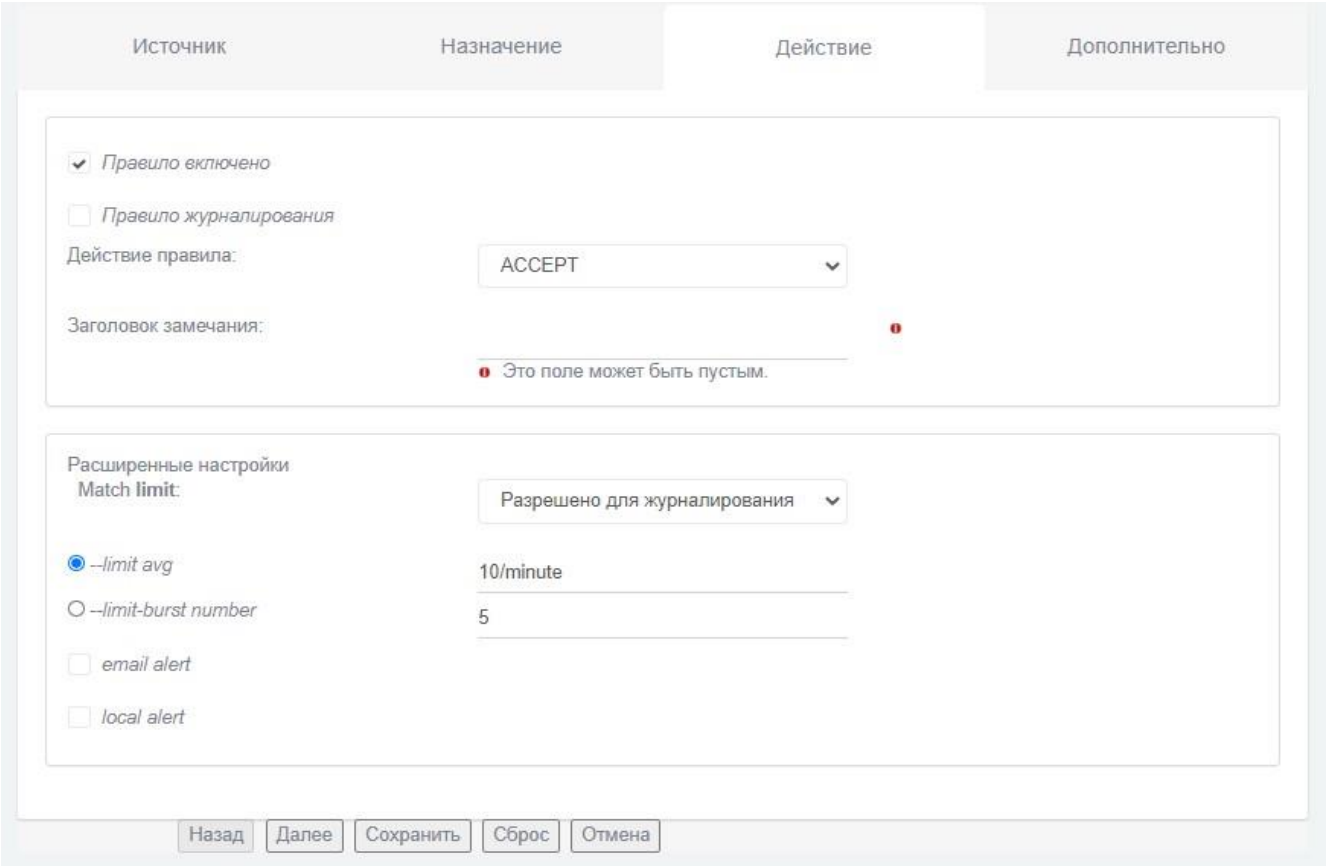
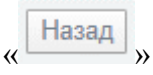


Рисунок 165 – Настройка «Действие»

Поле «Действие» содержит элементы, указанные в таблице 106.

Таблица 106 – Описание элементов поля «Действие»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации

Элемент	Описание
	Поле необязательно для заполнения
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Правило включено»	Предназначен для указания необходимости включения/выключения правила
Параметр «Правило журналирования»	Предназначен для указания необходимости журналирования прохождения пакетов по данному правилу
Ниспадающий список «Действие правила»	Предназначен для указания действия при срабатывании правила
Поле «Заголовок замечания»	Предназначено для указания заголовка, помещаемого в строку журналирования по данному правилу
Параметр «limit avg»	Предназначен для ограничения записи событий в журнал. Параметр «limit avg» задает среднюю частоту событий и указывается в формате число событий / единица времени
Параметр «limit-burst number»	Предназначен для ограничения записи событий в журнал. Параметр «limit-burst number» определяет пик «разовой» доставки пакетов. Значение по умолчанию «5»
Параметр «email alert»	Для получения оповещения о сработавшем правиле на электронную почту необходимо включить параметр «email alert»
Параметр «local alert»	Активация параметра включает локальные оповещения
Кнопка «  »	Кнопка перехода на предыдущую страницу

Элемент	Описание
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.4.4 Поле «Дополнительно»

Поле «Дополнительно» (рисунок 166) предназначено для назначения дополнительных критериев фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам. Кроме того, при срабатывании правила возможно присвоение числовой метки, применяемой для дальнейшей обработки сетевого пакета в целях маршрутизации.

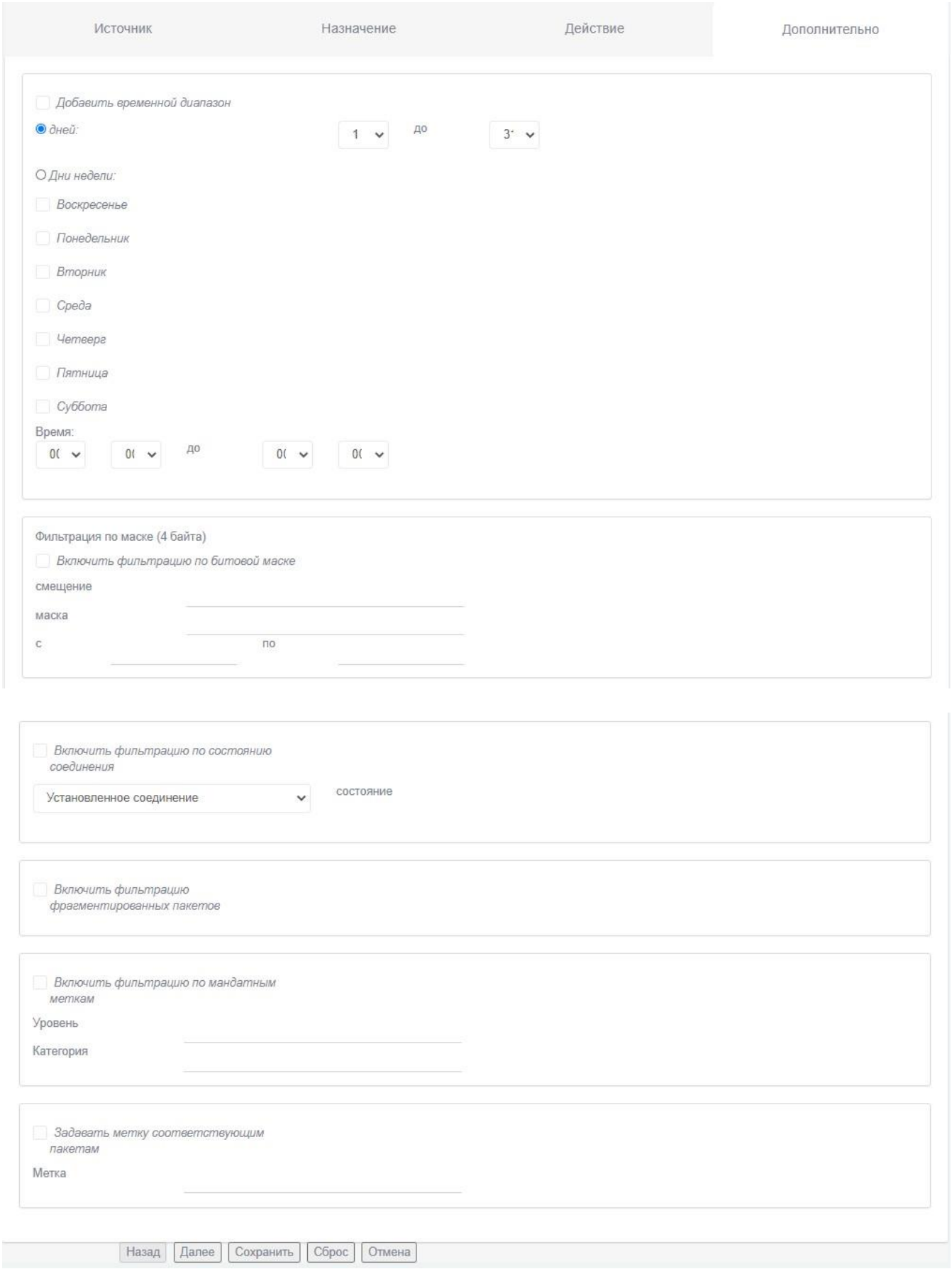


Рисунок 166 – Поле «Дополнительно»

Поле «Дополнительно» содержит элементы, указанные в таблице 107.

Таблица 107 – Описание элементов поля «Дополнительно»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Добавить временной диапазон»	Включение параметра дает возможность добавления временного диапазона для правил фильтрации сетевых пакетов из внутренней сети во внешнюю
Параметр и ниспадающие списки «Дней»	Предназначен для уточнения временного диапазона в днях
Параметр и перечень «Дни недели»	Активация параметра «Дни недели» дает возможность выбрать из перечня дни недели
Настройка «Фильтрация по маске (4 байта)»	Предназначена для включения фильтрации по битовой маске с внесением параметров «Смещение», «Маска», с указанием временного диапазона
Параметр «Включить фильтрацию по состоянию соединения»	Предназначен для активации параметра
Ниспадающий список «Состояние»	Предназначен для выбора соединения: – Установленное соединение;

Элемент	Описание
	– Новое соединение
Параметр «Включить фильтрацию фрагментированных пакетов»	Предназначен для включения фильтрации на уровне пакетов, что позволяет контролировать доступ к сети вне зависимости от программ, инициирующих подключение
Параметр «Включить фильтрацию по мандатным меткам»	При активации параметра созданное правило МЭ проверяет наличие мандатной метки согласно RFC 1108 (ГОСТ Р 58256-2018)
Поле «Уровень»	Предназначено для описания уровня данных (доступно всем, С, СС), задается в десятичном формате 1,2,3 и т.д.
Поле «Категория»	Предназначено для описания категории, к которой относятся данные, задается в двоичной форме 1 10 11 и т.д.
Параметр «Задавать метку соответствующим пакетам»	При активации параметра сетевые пакеты, попадающие под правило МЭ, будут промаркированы метками для обработки в «Рубикон». Данный механизм используется для статической маршрутизации по меткам
Поле «Метка»	Предназначено для задания метки, начиная с 1001 (например, 1001, 1002, 1003 и т.д.)
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.5 Вкладка «Доступ извне»

Вкладка «Доступ извне» (рисунок 167) предназначена для создания правил организации административного доступа к МЭ из красной сети.

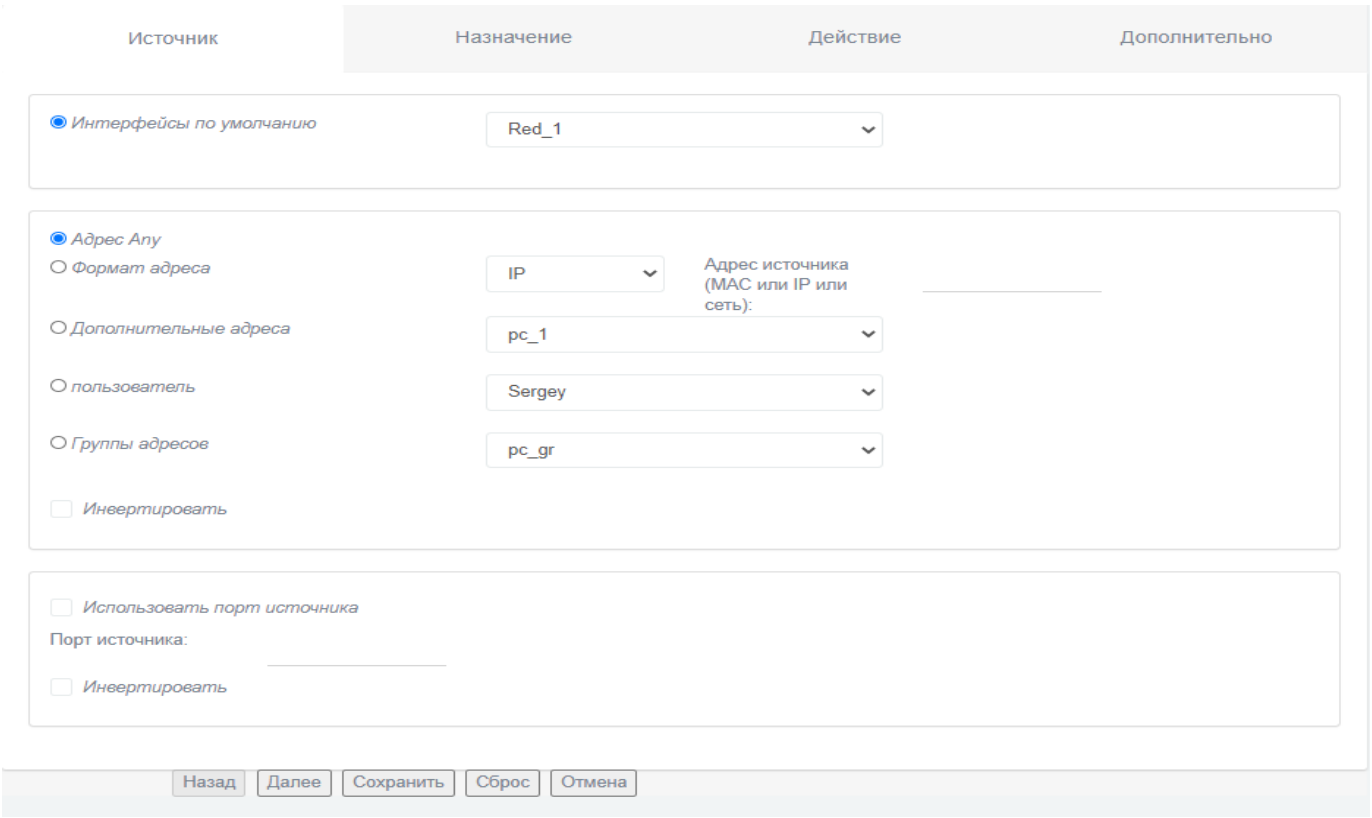


Рисунок 167 – Вкладка «Доступ извне»

Вкладка «Доступ извне» состоит из следующих полей:

– «Источник»;

– «Назначение»;

– «Действие»;

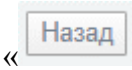
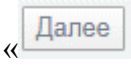
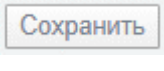
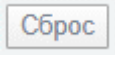
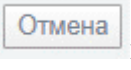
– «Дополнительно».

2.7.9.5.1 Поле «Источник»

Поле «Источник» (рисунок 168) предназначено для настройки источника правила МЭ и содержит элементы, указанные в таблице 108.

Таблица 108 – Описание элементов поля «Источник»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Интерфейсы по умолчанию»	Параметр активирует ниспадающий список «Интерфейсы по умолчанию»
Ниспадающий список «Интерфейсы по умолчанию»	Ниспадающий список позволяет выбрать один из интерфейсов
Параметр «Адрес Any»	Активирует доступ со всех адресов
Параметр «Формат адреса»	Активирует ниспадающий список «Формат адреса»
Ниспадающий список «Формат адреса»	Указывает параметр адреса для строки ввода «Адрес источника (MAC или IP или сеть)»
Поле «Адрес источника (MAC или IP или сеть)»	Предназначено для указания адреса источника обрабатываемых пакетов. Может задаваться вручную в

Элемент	Описание
	соответствующем поле или выбираться из заданных заранее списков сетей
Параметр и ниспадающий список «Дополнительные адреса»	Параметр активирует ниспадающий список «Дополнительные адреса» и позволяет выбрать дополнительные адреса
Параметр и ниспадающий список «Пользователь»	Параметр активирует ниспадающий список «Пользователь» и позволяет выбрать пользователя
Параметр и ниспадающий список «Группы адресов»	Параметр активирует ниспадающий список «Группы адресов» и позволяет выбрать группу адресов
Параметр «Использовать порт источника»	Предназначен для режима, при котором можно указывать порт, с которого поступают сетевые пакеты
Поле «Порт источника»	Предназначено для указания порта
Параметр «Инвертировать»	Данный параметр в условии правила меняет действие условия на противоположное
Кнопка «  »	Кнопка перехода на предыдущую страницу
Кнопка «  »	Кнопка перехода на следующую страницу
Кнопка «  »	Кнопка сохранения введенной информации
Кнопка «  »	Кнопка сброса всех данных формы
Кнопка «  »	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.5.2 Поле «Назначение»

Поле «Назначение» (рисунок 169) определяет порт доступа для указанного в поле «Источник» интерфейса.

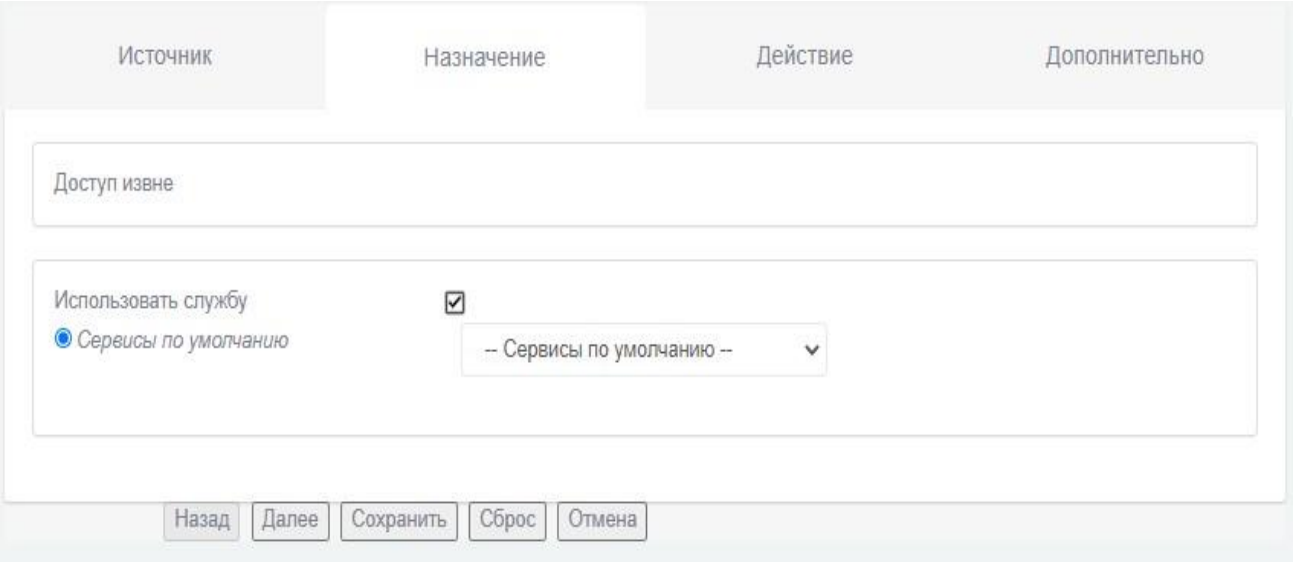


Рисунок 169 – Поле «Назначение»

Поле «Назначение» содержит элементы, указанные в таблице 109.

Таблица 109 – Описание элементов поля «Назначение»

Элемент	Описание
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок активации ниспадающего списка
Параметр «Сервисы по умолчанию»	Активирует сервисы по умолчанию
Ниспадающий список «Сервисы по умолчанию»	Применяется для выбора службы (порта) «Рубикон», которой предназначается обрабатываемый пакет. Может

Элемент	Описание
	быть выбран из списка стандартных сервисов (опция «сервисы по умолчанию»), а также из списка заданных администратором служб
Кнопка «Назад»	Кнопка перехода на предыдущую страницу
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.5.3 Поле «Действие»

Поле «Действие» (рисунок 170) предназначено для настройки действий при срабатывании правил.

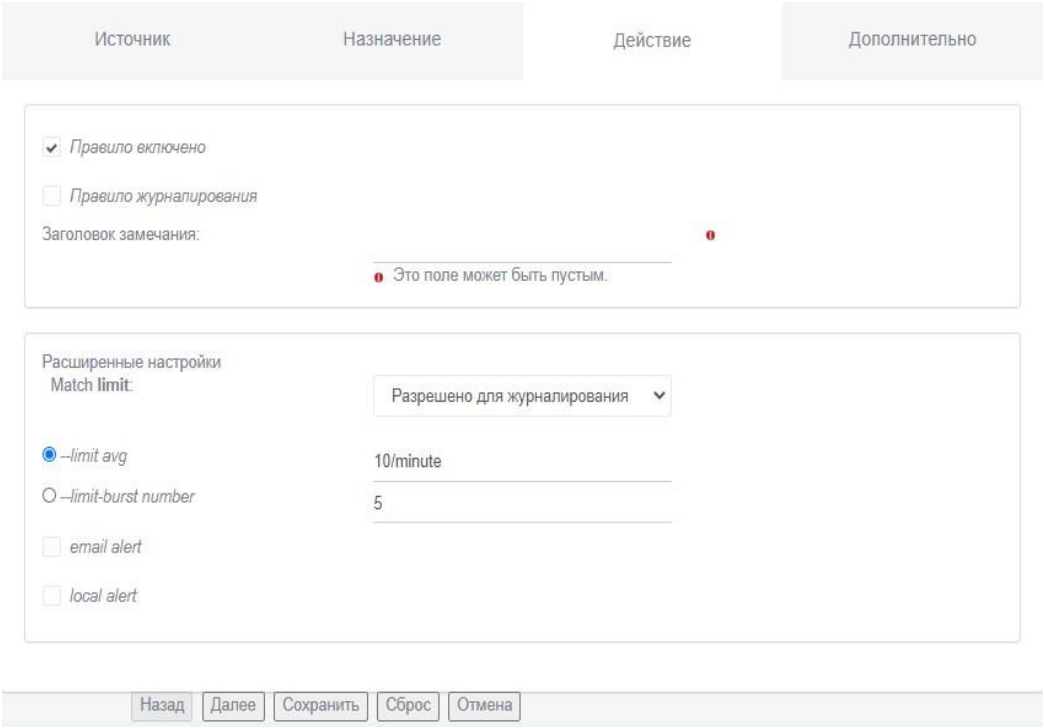


Рисунок 170 – Поле «Действие»

Поле «Действие» содержит элементы, указанные в таблице 110.

Таблица 110 – Описание элементов поля «Действие»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле необязательно для заполнения
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Правило включено»	Предназначен для указания необходимости включения/выключения правила
Параметр «Правило журналирования»	Предназначен для указания необходимости журналирования прохождения пакетов по данному правилу
Поле «Заголовок замечания»	Предназначено для указания заголовка, помещаемого в строку журналирования по данному правилу
Параметр «limit avg»	Предназначен для ограничения записи событий в журнал. Параметр «limit avg» задает среднюю частоту событий и указывается в формате число событий / единица времени
Параметр «limit-burst number»	Предназначен для ограничения записи событий в журнал. Параметр «limit-burst number» определяет пик «разовой» доставки пакетов. Значение по умолчанию «5»
Параметр «email alert»	Для получения оповещения о сработавшем правиле на электронную почту необходимо включить параметр «email alert»
Параметр «local alert»	Активация параметра включает локальные оповещения

Элемент	Описание
Кнопка «Назад»	Кнопка перехода на предыдущую страницу
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.5.4 Поле «Дополнительно»

Поле «Дополнительно» (рисунок 171) предназначено для назначения дополнительных критериев фильтрации: по времени, по битовой маске, по состоянию соединения, по фрагментированным пакетам, по мандатным меткам. Кроме того, при срабатывании правила возможно присвоение числовой метки, применяемой для дальнейшей обработки сетевого пакета в целях маршрутизации.

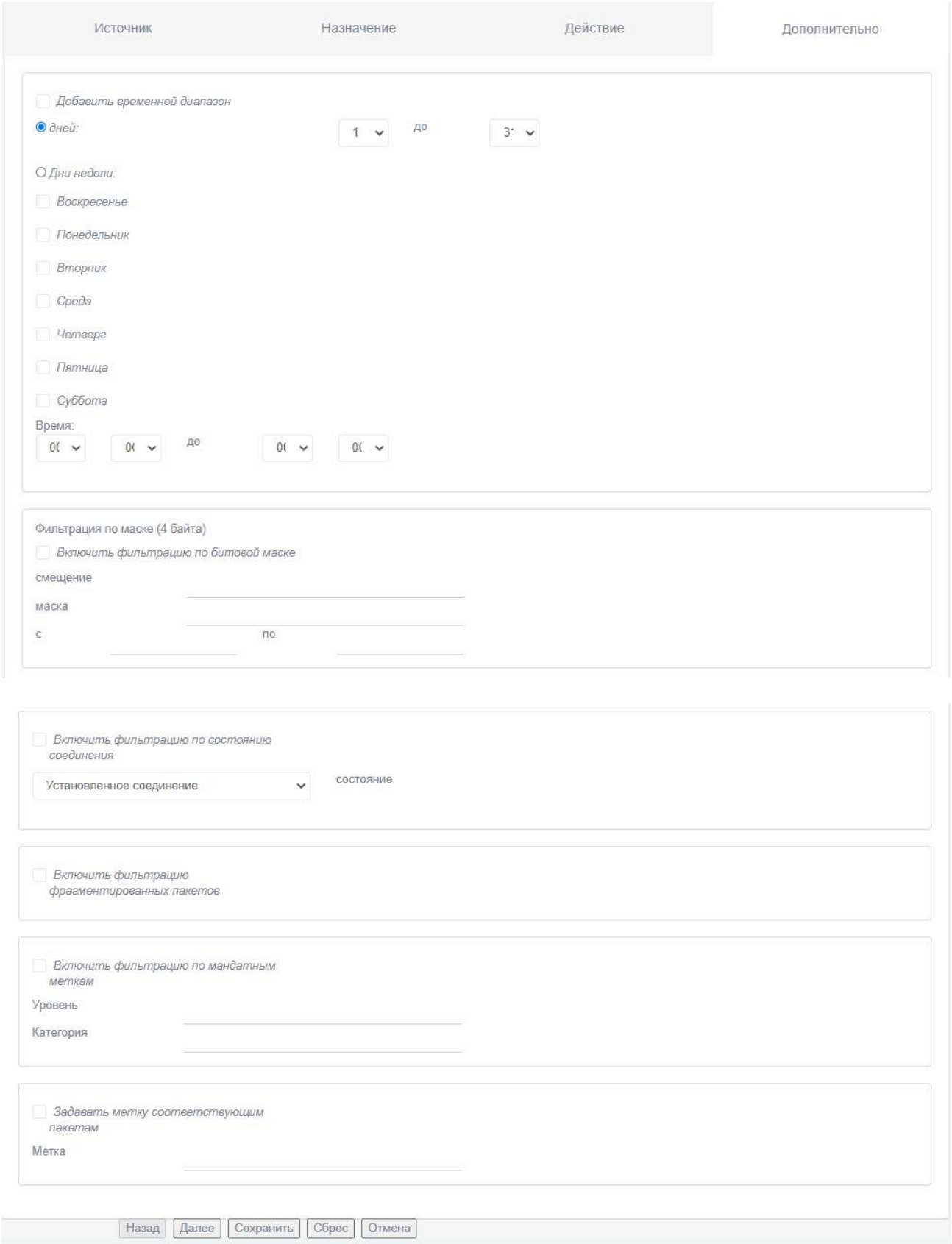
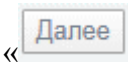
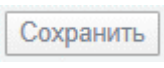
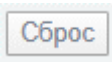


Рисунок 171 – Поле «Дополнительно»

Поле «Дополнительно» содержит элементы, указанные в таблице 111.

Таблица 111 – Описание элементов поля «Дополнительно»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Добавить временной диапазон»	Включение параметра дает возможность добавления временного диапазона для правил фильтрации сетевых пакетов из внутренней сети во внешнюю
Параметр и ниспадающие списки «Дней»	Предназначен для уточнения временного диапазона в днях
Параметр и перечень «Дни недели»	Активация параметра «Дни недели» дает возможность выбрать из перечня дни недели
Настройка «Фильтрация по маске (4 байта)»	Предназначена для включения фильтрации по битовой маске с внесением параметров «Смещение», «Маска», с указанием временного диапазона
Параметр «Включить фильтрацию по состоянию соединения»	Предназначен для активации параметра

Элемент	Описание
Ниспадающий список «Состояние»	Предназначен для выбора соединения: – Установленное соединение; – Новое соединение
Параметр «Включить фильтрацию фрагментированных пакетов»	Предназначен для включения фильтрации на уровне пакетов, что позволяет контролировать доступ к сети вне зависимости от программ, инициирующих подключение
Параметр «Включить фильтрацию по мандатным меткам»	При активации параметра созданное правило МЭ проверяет наличие мандатной метки согласно RFC 1108 (ГОСТ Р 58256-2018)
Поле «Уровень»	Предназначено для описания уровня данных (доступно всем, С, СС), задается в десятичном формате 1,2,3 и т.д.
Поле «Категория»	Предназначено для описания категории, к которой относятся данные, задается в двоичной форме 1 10 11 и т.д.
Параметр «Задавать метку соответствующим пакетам»	При активации параметра сетевые пакеты, попадающие под правило МЭ, будут промаркированы метками для обработки в «Рубикон». Данный механизм используется для статической маршрутизации по меткам
Поле «Метка»	Предназначено для задания метки, начиная с 1001 (например, 1001, 1002, 1003 и т.д.)
Кнопка «  »	Кнопка перехода на следующую страницу
Кнопка «  »	Кнопка сохранения введенной информации
Кнопка «  »	Кнопка сброса всех данных формы

Элемент	Описание
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.6 Вкладка «L2»

Вкладка «L2» (рисунок 172) предназначена для создания правил фильтрации МЭ на канальном уровне (L2).

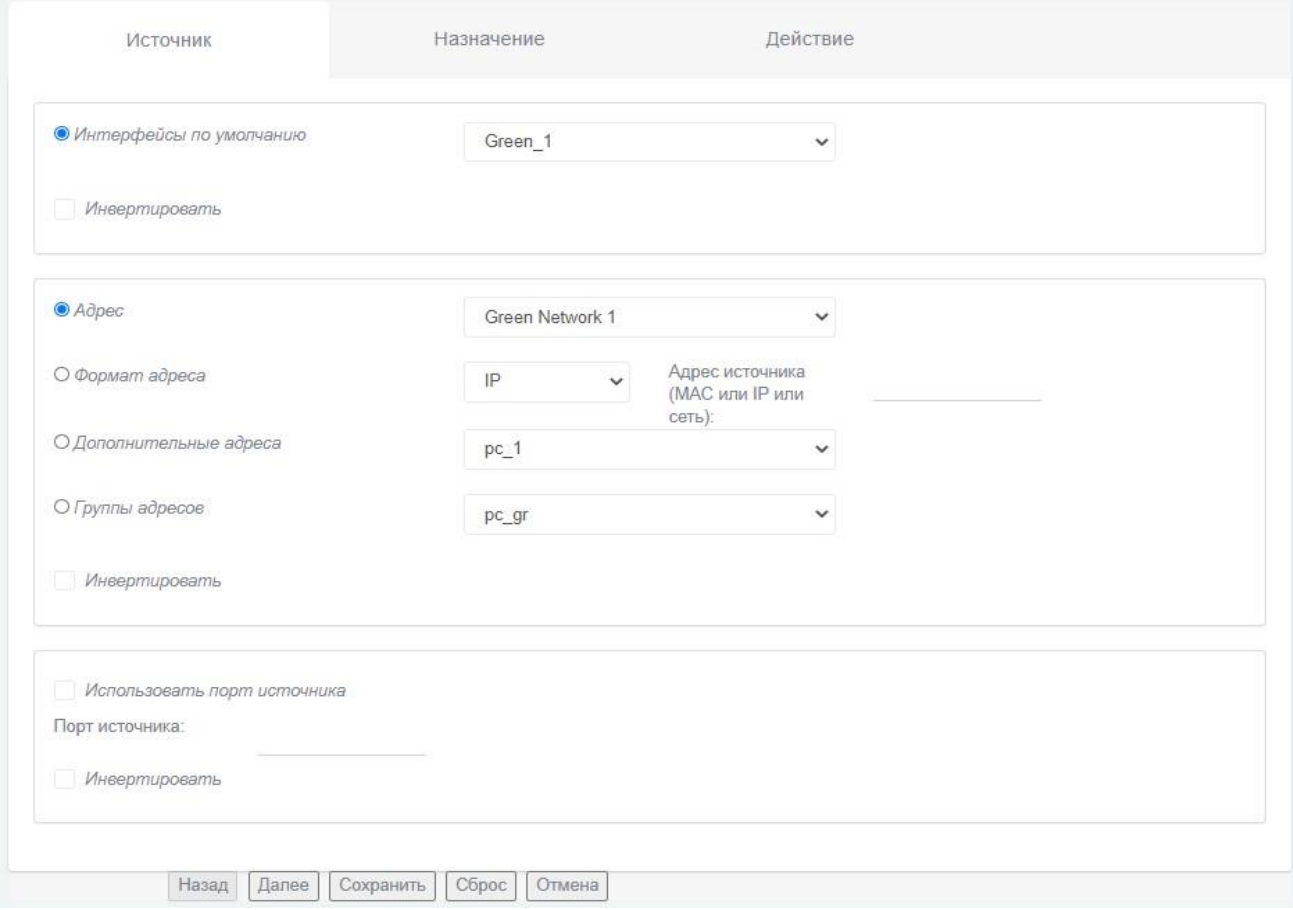


Рисунок 172 – Вкладка «L2»

Вкладка «L2» состоит из следующих полей:

– «Источник»;

– «Назначение»;

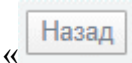
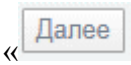
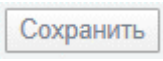
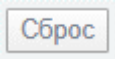
– «Действие».

2.7.9.6.1 Поле «Источник»

Поле «Источник» (рисунок 172) предназначено для настройки параметров фильтрации. Описание элементов указаны в таблице 112.

Таблица 112 – Описание элементов поля «Источник»

Элемент	**Описание**
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Интерфейсы по умолчанию»	Параметр активирует ниспадающий список «Интерфейсы по умолчанию»
Ниспадающий список «Интерфейсы по умолчанию»	Ниспадающий список позволяет выбрать один из интерфейсов
Параметр «Адрес»	Активирует доступ со всех адресов
Ниспадающий список «Адрес»	Активирует ниспадающий список «Формат адреса»

Элемент	Описание
Параметр «Формат адреса»	Активирует ниспадающий список «Формат адреса»
Ниспадающий список «Формат адреса»	Указывает параметр адреса для строки ввода «Адрес источника (MAC или IP)»
Поле «Адрес источника (MAC или IP или сеть)»	Предназначено для указания адреса источника обрабатываемых пакетов. Может задаваться вручную в соответствующем поле или выбираться из заданных заранее списков сетей
Параметр и ниспадающий список «Дополнительные адреса»	Параметр активирует ниспадающий список «Дополнительные адреса» и позволяет выбрать дополнительные адреса
Параметр и ниспадающий список «Группы адресов»	Параметр активирует ниспадающий список «Группы адресов» и позволяет выбрать группу адресов
Параметр «Использовать порт источника»	Предназначен для режима, при котором можно указывать порт, с которого поступают сетевые пакеты
Поле «Порт источника»	Предназначено для указания порта
Параметр «Инвертировать»	Данный параметр в условии правила меняет действие условия на противоположное
Кнопка «  »	Кнопка перехода на предыдущую страницу
Кнопка «  »	Кнопка перехода на следующую страницу
Кнопка «  »	Кнопка сохранения введенной информации
Кнопка «  »	Кнопка сброса всех данных формы

Элемент	Описание
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.6.2 Поле «Назначение»

Поле «Назначение» (рисунок 173) предназначено для настройки параметров фильтрации.

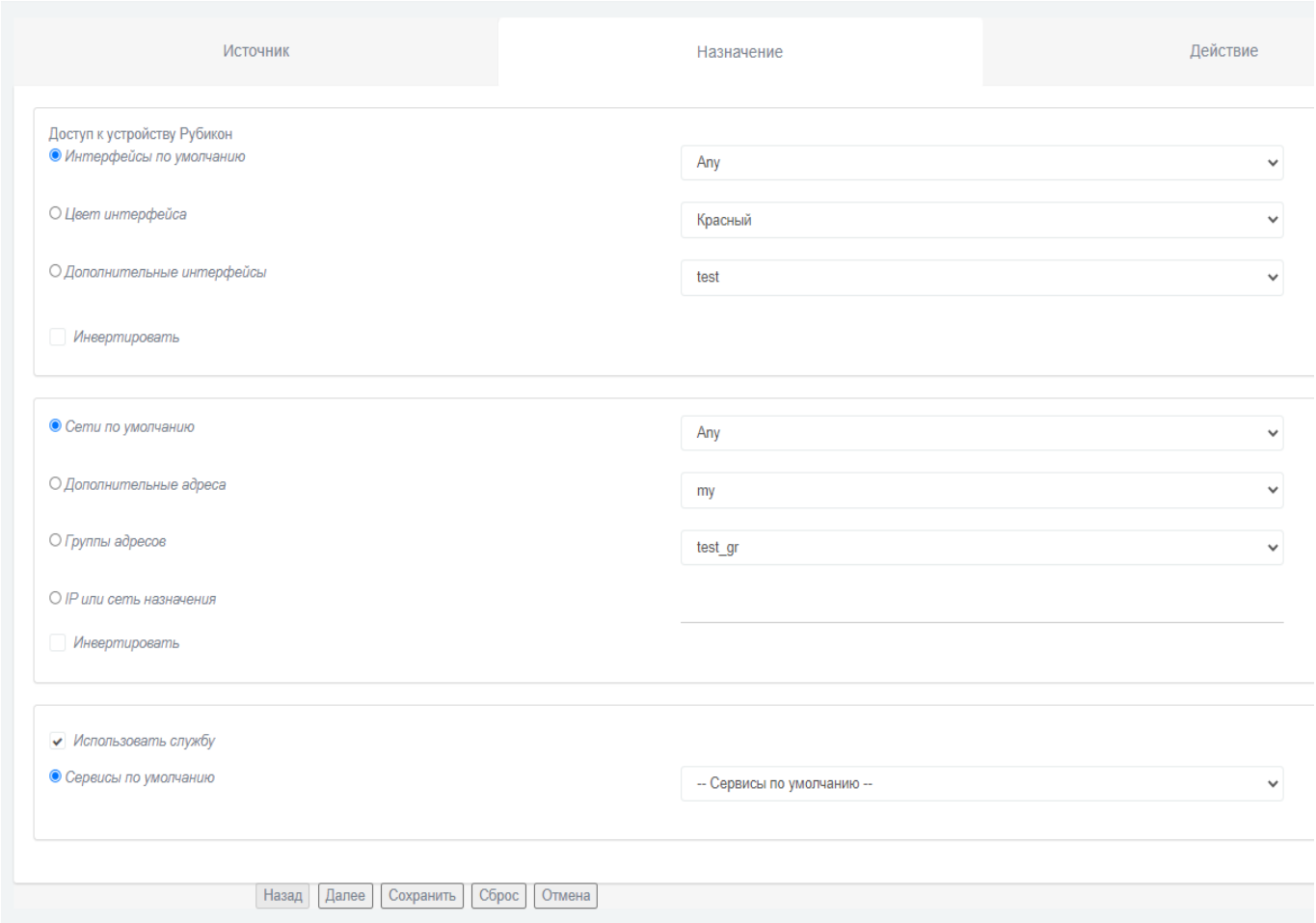


Рисунок 173 – Поле «Назначение»

Поле «Назначение» содержит элементы, указанные в таблице 113.

Таблица 113 – Описание элементов поля «Назначение»

Элемент	Описание
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
Параметр и ниспадающий список «Интерфейсы по умолчанию»	Параметр активирует ниспадающий список «Интерфейсы по умолчанию» и позволяет выбрать один из интерфейсов
Параметр и ниспадающий список «Цвет интерфейса»	Параметр активирует ниспадающий список «Цвет интерфейса» и предназначен для указания одного из определенных в системе цветов интерфейсов
Параметр и ниспадающий список «Сети по умолчанию»	Параметр активирует ниспадающий список «Сети по умолчанию» и предназначен для указания одной из определенных в системе сетей
Параметр и поле «IP или сеть назначения»	Предназначен для активации параметра. Поле предназначено для указания IP адреса или сети для узла назначения (целевого узла обрабатываемого пакета)
Параметр «Использовать службу»	Параметр активирует возможность использования службы
Параметр и ниспадающий список «Сервисы по умолчанию»	Активирует сервисы по умолчанию и применяется для выбора службы (порта) «Рубикон», которой предназначается обрабатываемый пакет. Может быть

Элемент	Описание
	выбран из списка стандартных сервисов (опция «сервисы по умолчанию»), а также из списка заданных администратором служб
Кнопка «Назад»	Кнопка перехода на предыдущую страницу
Кнопка «Далее»	Кнопка перехода на следующую страницу
Кнопка «Сохранить»	Кнопка сохранения введенной информации
Кнопка «Сброс»	Кнопка сброса всех данных формы
Кнопка «Отмена»	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.9.6.3 Поле «Действие»

Поле «Действие» (рисунок 174) предназначено для настройки действий при срабатывании правил.

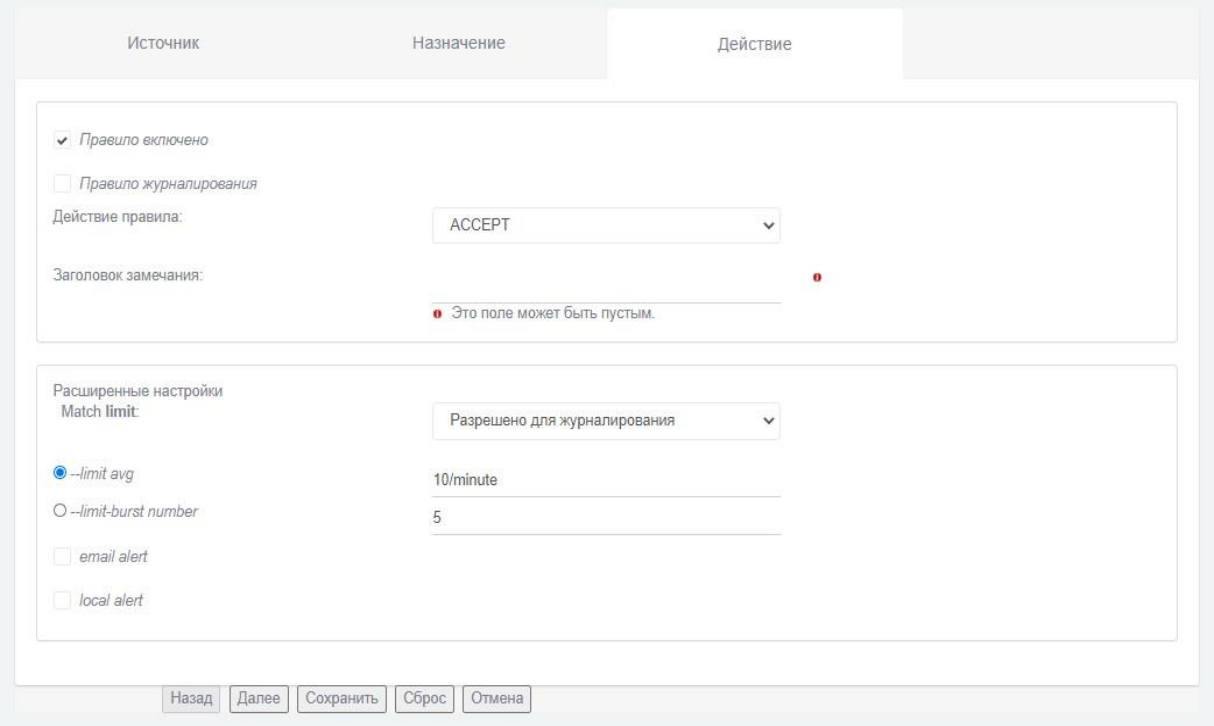
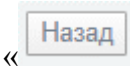
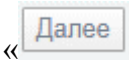
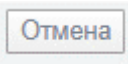


Рисунок 174 – Поле «Действие»

Поле «Действие» содержит элементы, указанные в таблице 114.

Таблица 114 – Описание элементов поля «Действие»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле необязательно для заполнения
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
Параметр «Правило включено»	Предназначен для указания необходимости включения/выключения правила
Параметр «Правило журналирования»	Предназначен для указания необходимости журналирования прохождения пакетов по данному правилу
Ниспадающий список «Действие правила»	Предназначен для указания действия при срабатывании правила
Поле «Заголовок замечания»	Предназначено для указания заголовка, помещаемого в строку журналирования по данному правилу
Ниспадающий список «Расширенные настройки Match limit»	Предназначен для включения расширенных настроек действия при срабатывании правил: – Возможность отключена; – Разрешено для журналирования; – Разрешено для политики принятия и сбрасывания; – Разрешено для политик обоих видов

Элемент	Описание
Параметр «limit avg»	Предназначен для ограничения записи событий в журнал. Параметр «limit avg» задает среднюю частоту событий и указывается в формате число событий / единица времени
Параметр «limit-burst number»	Предназначен для ограничения записи событий в журнал. Параметр «limit-burst number» определяет пик «разовой» доставки пакетов. Значение по умолчанию «5»
Параметр «email alert»	Для получения оповещения о сработавшем правиле на электронную почту необходимо включить параметр «email alert»
Параметр «local alert»	Активация параметра включает локальные оповещения
Кнопка «  »	Кнопка перехода на предыдущую страницу
Кнопка «  »	Кнопка перехода на следующую страницу
Кнопка «  »	Кнопка сохранения введенной информации
Кнопка «  »	Кнопка сброса всех данных формы
Кнопка «  »	Кнопка отмены заполнения формы и возврата на страницу «Правила межсетевого экрана» без сохранения введенных данных

2.7.10 Подраздел «Конфигурация DMZ»

Подраздел «Конфигурация DMZ» (рисунок 175) предназначен для создания правил DMZ для межсетевого экрана.

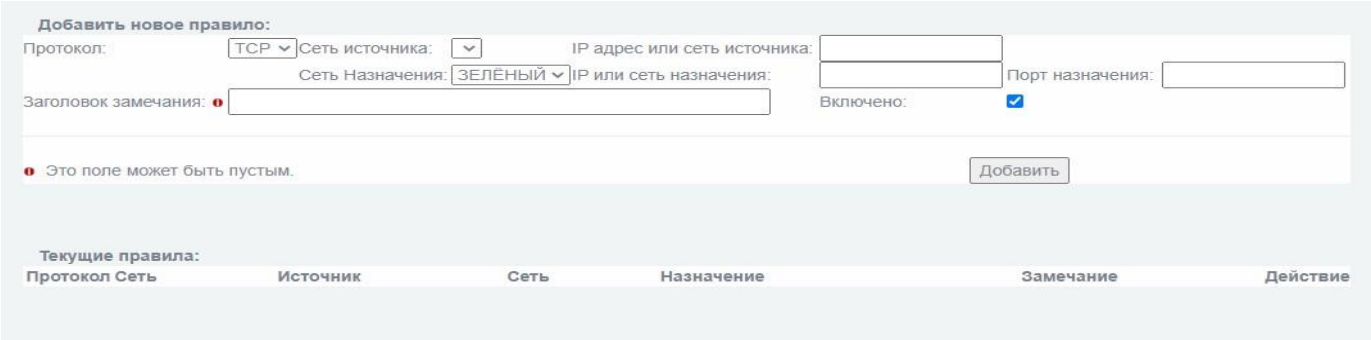


Рисунок 175 – Подраздел «Конфигурация DMZ»

Подраздел «Конфигурация DMZ» содержит элементы, указанные в таблице 115.

Таблица 115 – Описание элементов подраздела «Конфигурация DMZ»

Элемент	Описание
	Значок активации ниспадающего списка
	Поле для ввода необходимой информации
	Поле необязательно для заполнения
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
Ниспадающий список «Протокол»	Ниспадающий список предлагает выбрать из протоколов: – TCP; – UDP
Поле «Заголовок замечания»	Предназначено для указания заголовка, помещаемого в строку журналирования по данному правилу
Ниспадающий список «Сеть источника»	Предназначен для указания сети источника пакета из ранее определенного списка красных интерфейсов

Элемент	Описание
Ниспадающий список «Сеть Назначения»	Предназначен для указания сети назначения пакета из ранее определенного списка красных интерфейсов
Поле «IP адрес или сеть источника»	Предназначено для указания IP-адреса или сети источника пакета
Поле «IP или сеть назначения»	Предназначено для указания IP-адреса или сети назначения пакета
Параметр «Включено»	Данный параметр включает правило DMZ
Поле «Порт назначения»	Предназначено для указания порта назначения пакета
Кнопка «Добавить»	Сохраняет информацию и добавляет правило в список правил DMZ

2.8 Раздел «VPN»

Раздел «VPN» содержит подразделы:

– «Настройка IPSec»;

– «Настройка VPN»;

– «GRE»;

– «Выпуск сертификатов».

2.8.1 Подраздел «Настройка IPSec»

Подраздел «Настройка IPSec» предназначен для организации сетевого туннеля и настройки взаимодействия по протоколу IPSec.

Подраздел «Настройка IPSec» состоит из следующих полей:

– «Глобальные настройки»;

– «Статус и управление соединением».

Поле «Глобальные настройки» представлено на рисунке 176.

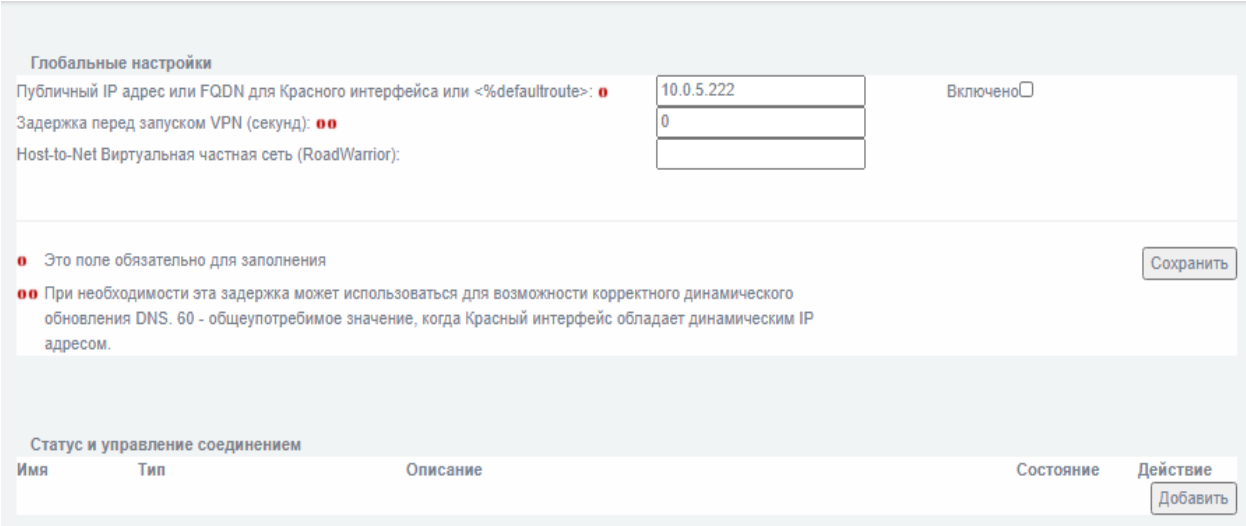


Рисунок 176 – Поле «Глобальные настройки»

Описание элементов поля «Глобальные настройки» представлены в таблице 116.

Таблица 116 – Описание элементов поля «Глобальные настройки»

Элемент	Описание
Параметр «Публичный IP адрес или FQDN для Красного интерфейса или <%defaultroute>»	Внешний IP адрес или FQDN сетевого интерфейса, использующегося для установления туннеля IPSec либо параметр <%defaultroute> для использования интерфейса, для которого определен маршрут по умолчанию.
Чекбокс «Включено»	Предназначен для включения или выключения службы создания туннеля IPSec
Параметр «Задержка перед запуском VPN (секунд)»	Предназначен для указания времени задержки перед стартом процесса организации туннеля при старте подсистемы захвата и разбора пакетов.
Параметр «Host-to-Net Виртуальная частная сеть (RoadWarrior)»	Указывает способ организации туннеля IPSec, при котором туннель создается между отдельным узлом и устройством, осуществляющим маршрутизацию между несколькими сетями.
Параметр «Виртуальная частная сеть типа сеть-сеть»	Указывает способ организации туннеля IPSec, при котором туннель создается между двумя устройствами, осуществляющими маршрутизацию между несколькими сетями.
Кнопка «Сохранить»	Сохраняет информацию о настройках IPSec.

Поле «Статус и управление соединением» предназначено для создания нового соединения (рисунок 176). Для создания нового соединения следует нажать кнопку «Добавить». В результате откроется поле выбора типа соединения (рисунок 177).

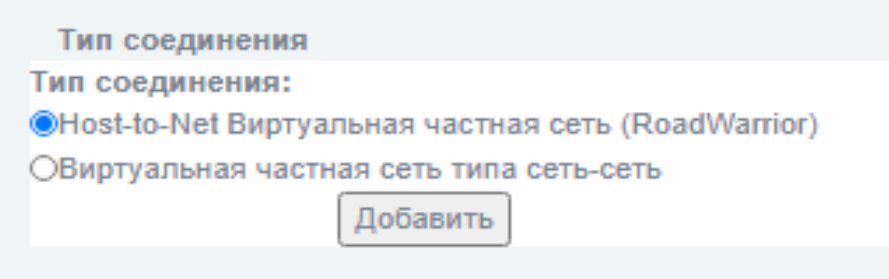


Рисунок 177 – Поле выбора типа соединения «Тип соединения»

После выбора типа соединения следует нажать кнопку «Добавить». В результате откроется вкладка с двумя полями:

– поле «Имя соединения»;
– поле «Аутентификация».

Описание элементов поля «Имя соединения» представлены в таблице 117.

Таблица 117 – Описание элементов поля «Имя соединения»

Элемент	Описание
Параметр «Имя»	Предназначен для ввода имени туннеля.
Чекбокс «Включено»	Предназначен для включения или выключения соединения.
Параметр «Удалённый узел / IP»	IP-адрес удаленного узла, участвующий в организации туннеля IPSec.
Параметр «Локальный идентификатор (ID)»	Идентификатор локального узла.
Параметр «Локальная подсеть»	IP-адрес локальной подсети, которая взаимодействует через туннель IPSec.
Параметр «Удалённая подсеть»	IP-адрес локальной подсети-адрес удаленной подсети, которая взаимодействует через туннель IPSec.
Параметр «Удаленный идентификатор (ID)»	Идентификатор удаленного узла.
Параметр «Заголовок замечания»	Дополнительная информация для отображения пользователю.

Элемент	Описание
Чекбокс «По окончании задать дополнительные настройки»	Предназначен для выбора дополнительных настроек алгоритмов организации туннеля IPSec после заполнения информации о настройках туннеля.

Описание элементов поля «Аутентификация» представлены в таблице 118.

Таблица 118 – Описание элементов поля «Аутентификация»

Элемент	Описание
Опция и поле «Использовать общий ключ»	Предназначена для задания общего PSK-ключа для организации туннеля IPSec.
Опция «Загрузить сертификат PKCS12»	Предназначена для выбора организации туннеля при использовании аутентификации с помощью сертификата.
Кнопка «Выберите файл»	Предназначена для выбора файла сертификата PKCS12.
Поле «Пароль файла PKCS12»	Ввод пароля файла сертификата PKCS12.
Опция «Клиент идентифицируется по строкам IPV4_ADDR, FQDN, USER_FQDN или DER_ASN1_DN в поле Remote ID»	Предназначена для аутентификации клиента по IP-адресу, доменному имени или полю Remote ID в сертификате.

Для сохранения настроек соединения необходимо нажать кнопку «Сохранить». Для отмены введенных настроек следует нажать кнопку «Отмена».

2.8.2 Подраздел «Настройка VPN»

Подраздел «Настройка VPN» используется для создания экземпляров серверов и клиентов VPN (рисунок 178).

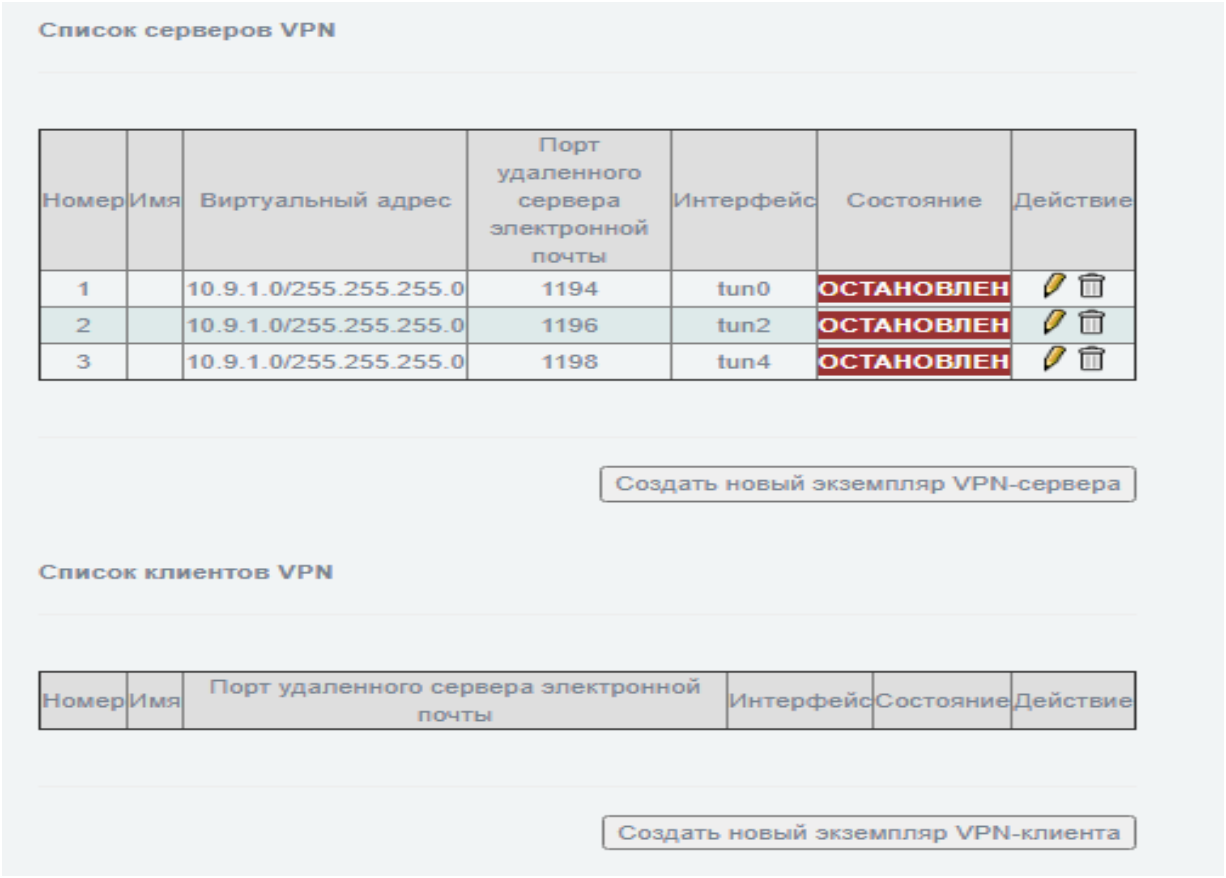


Рисунок 178 – Подраздел «Настройка VPN»

2.8.2.1 Вкладка «Настройка сервера VPN»

При нажатии на кнопку «Создать новый экземпляр VPN-сервера» откроется вкладка «Настройка сервера VPN», содержащая следующие поля (рисунок 179):

- поле «Настройка сервера VPN 2»;
- поле «Управление локальными сетями»;
- поле «Управление сетями клиентов VPN».

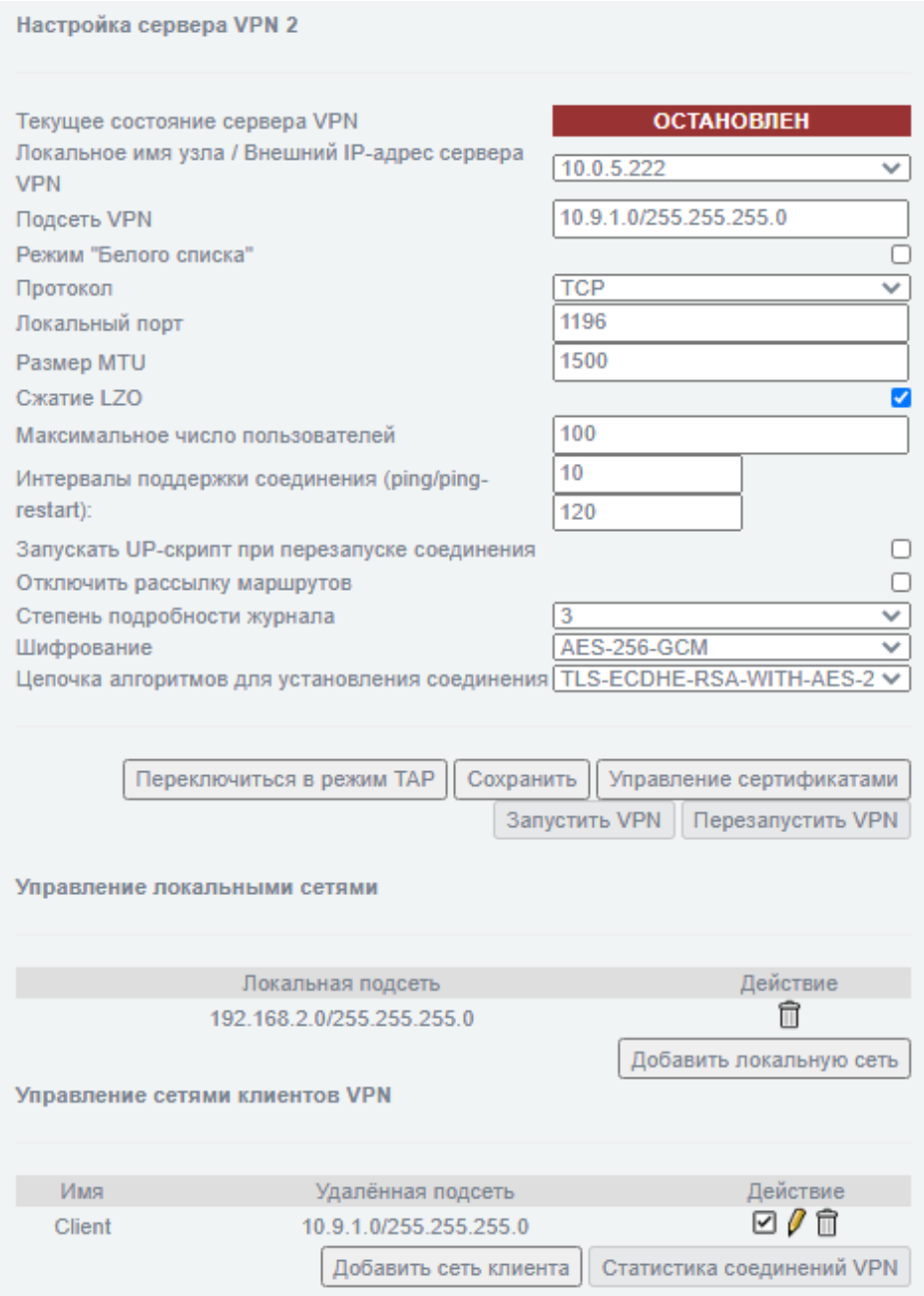


Рисунок 179 – Вкладка «Настройка сервера VPN»

2.8.2.1.1 Поле «Настройка сервера VPN 2»

Описание элементов поля «Настройка сервера VPN 2» представлено в таблице 119.

Таблица 119 – Описание элементов поля «Настройка сервера VPN 2»

Элемент	Описание
Параметр «Текущее состояние сервера VPN»	Предназначен для отображения состояния сервера VPN (запущен или остановлен)
Параметр «Локальное имя узла / Внешний IP-адрес сервера VPN»	Предназначен для ввода имени или внешнего IP-адреса сервера VPN
Параметр «Подсеть VPN»	Предназначен для ввода подсети, которая будет использоваться в туннеле VPN
Чекбокс «Режим "Белого списка"»	Предназначен для включения режима «Белого списка», когда к соединению через туннель VPN допускаются только клиенты из явно разрешенных сетей
Параметр «Протокол»	Предназначен для выбора протокола, используемого для установления VPN-туннеля
Параметр «Локальный порт»	Предназначен для ввода информации о локальном порте, на который приходят запросы на установление VPN-соединения
Параметр «Размер MTU»	Предназначен для ввода информации о размере MTU в туннеле VPN
Чекбокс «Сжатие LZO»	Предназначен для указания использования сжатия LZO при передаче информации в туннеле
Параметр «Максимальное число пользователей»	Предназначен для указания максимального числа пользователей сервера VPN
Параметры «Интервалы поддержки соединения (ping/ping-restart)»	Первый параметр определяет интервал в секундах между выполнениями команды «ping» соответствующего сервера VPN, второй параметр задает интервал между выполнениями команды «ping» сервера VPN в режиме ожидания его возможного рестарта при обнаружении отсутствия откликов на ping

Элемент	Описание
Чекбокс «Запускать UP-скрипт при перезапуске соединения»	Предназначен для включения/выключения запуска внутреннего скрипта обработки ситуации перезапуска соединения
Чекбокс «Отключить рассылку маршрутов»	Предназначен для включения/выключения необходимости рассылки маршрутов сетей, настроенных в сервисе VPN
Параметр «Степень подробности журнала»	Предназначен для указания подробности журнала: 1 – минимальная степень, 6 – максимальная
Параметр «Шифрование»	Предназначен для указания алгоритма, применяемого для передачи данных в создаваемом туннеле VPN
Параметр «Цепочка алгоритмов для установления соединения»	Предназначен для указания цепочки (последовательности) алгоритмов, применяемых при установлении соединения VPN.
Кнопка «Переключиться в режим TAP»	Переключиться в режим TAP из TUN (по умолчанию и наоборот)
Кнопка «Сохранить»	Сохранить введённые настройки сервера VPN
Кнопка «Управление сертификатами»	Открывает вкладку «Управление сертификатами»
Кнопка «Запустить VPN»	Предназначена для запуска сервера VPN с указанными настройками
Кнопка «Перезапустить VPN»	Предназначена для перезапуска сервера VPN с указанными настройками

2.8.2.1.1.1 Вкладка «Управление сертификатами 2»

Вкладка «Управление сертификатами 2» открывается при нажатии кнопки «Управление сертификатами» в поле «Настройка сервера VPN 2» (рисунок 180).

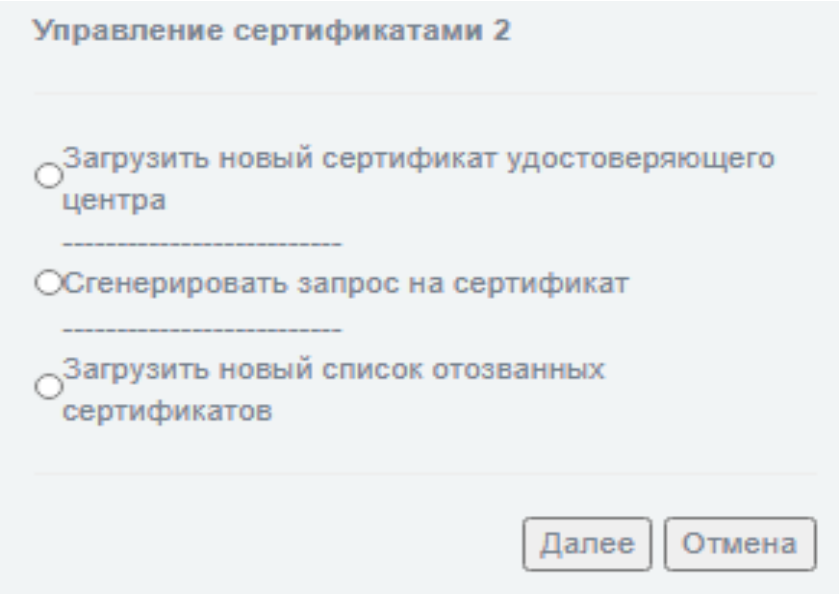


Рисунок 180 – Вкладка «Управление сертификатами 2»

Описание элементов вкладки «Управление сертификатами 2» представлено в таблице 120.

Таблица 120 – Описание элементов поля «Управление сертификатами 2»

Элемент	Описание
Опция «Загрузить новый сертификат удостоверяющего центра»	При выборе данной опции и нажатии кнопки «Далее» открывается вкладка «Загрузка нового сертификата удостоверяющего центра 3». На этой вкладке предлагается выбрать на компьютере файл сертификата, предварительно полученный в удостоверяющем центре и загрузить его в «Рубикон», используя кнопки «Выберите файл» и «Загрузить новый сертификат удостоверяющего центра» (рисунок 180)
Опция «Сгенерировать запрос на сертификат»	При выборе данной опции и нажатии кнопки «Далее» открывается вкладка «Загрузка нового сертификата удостоверяющего центра 3» (рисунок 181)

Элемент	Описание
Опция «Загрузить новый список отозванных сертификатов»	При выборе данной опции и нажатии кнопки «Далее» открывается вкладка «Загрузка нового списка отозванных сертификатов 3». Далее следует выбрать файл нового списка отозванных сертификатов и загрузить его (рисунок 182)
Кнопка «Далее»	Инициировать процедуру загрузки сертификата
Кнопка «Отмена»	Отменить процедуру загрузки сертификата

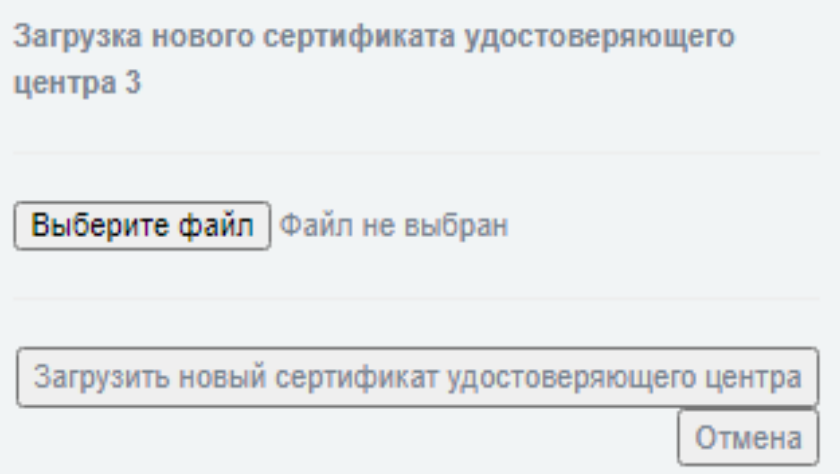


Рисунок 181 – Вкладка «Загрузка нового сертификата удостоверяющего центра 3»

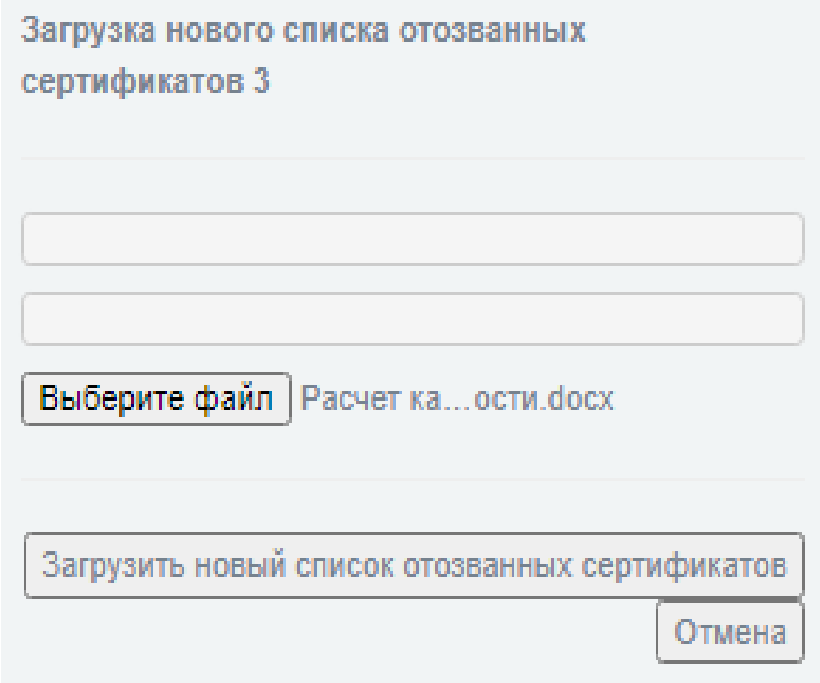


Рисунок 182 – Вкладка «Загрузка нового списка отозванных сертификатов 3»

2.8.2.1.1.2 Вкладка «Запрос сертификата 3»

Вкладка «Запрос сертификата 3» открывается из вкладки «Управление сертификатами 2», предназначена для формирования запроса на сертификат путем введения реквизитов пользователя в текстовую форму и его отправки в удостоверяющий центр (рисунок 183).

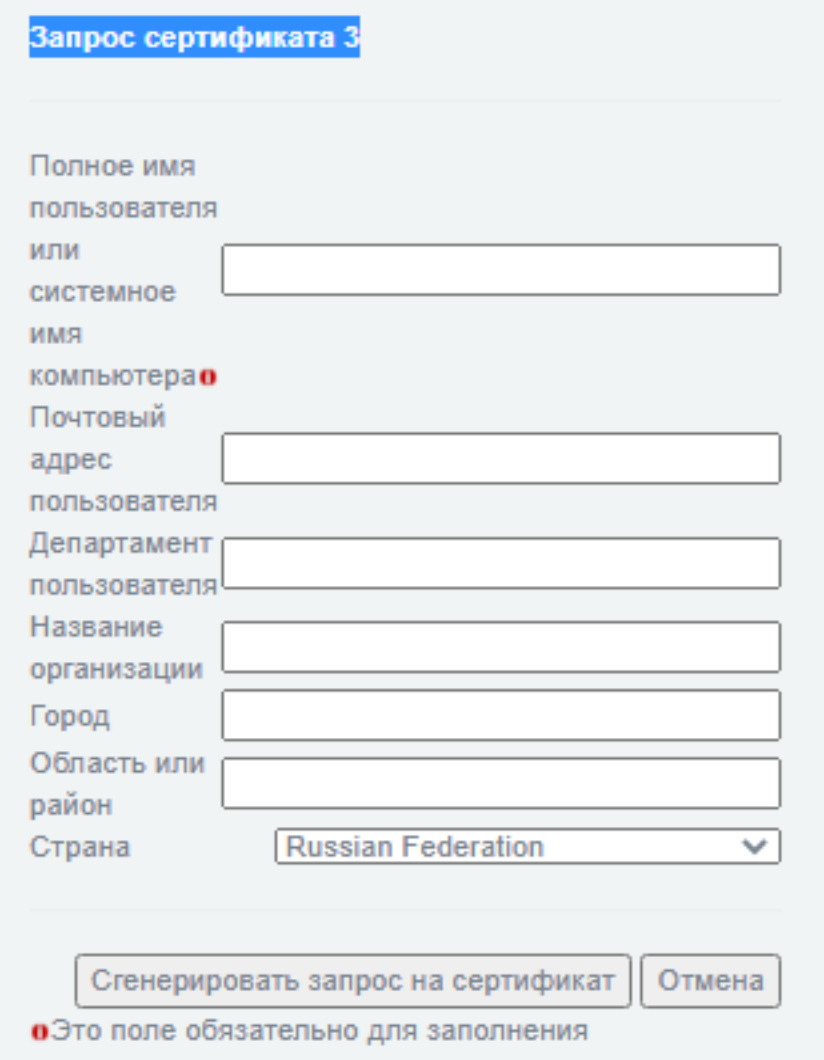


Рисунок 183 – Вкладка «Запрос сертификата 3»

По окончанию заполнения формы запроса на сертификат следует нажать кнопку «Сгенерировать запрос на сертификат». В результате откроется вкладка «Обработка запроса на сертификат 3», в которой можно скачать экземпляр запроса на сертификат, выбрать файл сертификата на компьютере и загрузить его в «Рубикон» (рисунок 184).

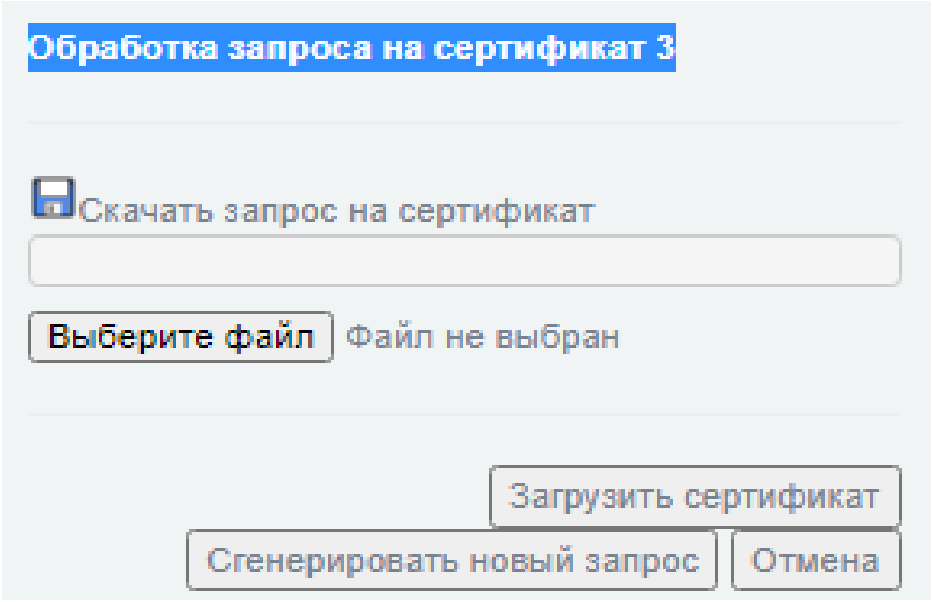


Рисунок 184 – Вкладка «Обработка запроса на сертификат 3»

2.8.2.1.2 Поле «Управление локальными сетями»

Поле «Управление локальными сетями» предназначено добавления и удаления локальных сетей. Для добавления локальной сети следует воспользоваться кнопкой «Добавить локальную сеть», по нажатии которой откроется вкладка «Добавление локальной подсети 3» (рисунок 185).

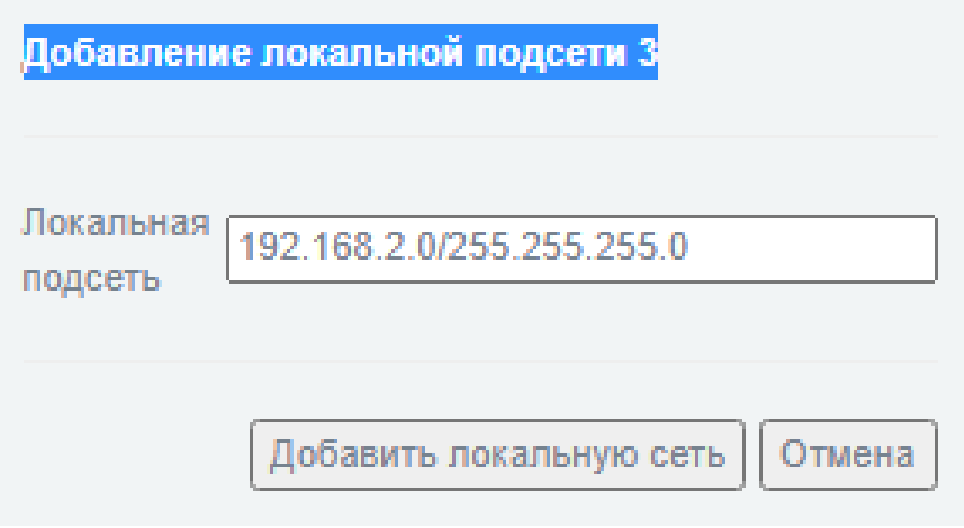


Рисунок 185 – Вкладка «Добавление локальной подсети 3»

Для добавления локальной подсети следует ввести IP-адрес/маску подсети и нажать кнопку «Добавить локальную сеть».

2.8.2.1.3 Поле «Управление сетями клиентов VPN»

Поле «Управление сетями клиентов VPN» предназначено для добавления, удаления, подключения/отключения сети клиента VPN. Для включения/отключения сети клиента VPN

используется чекбокс, редактирования/удаления, соответствующие символы «карандаш» и «корзина», для добавления сети следует нажать кнопку «Добавить сеть клиента», в результате чего откроется вкладка «Добавление подсети клиента3» (рисунок 186).

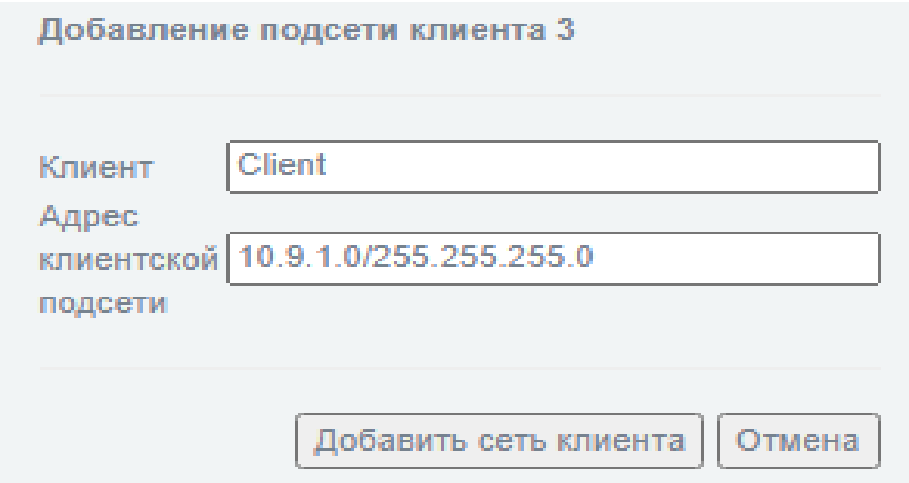


Рисунок 186 – Вкладка «Добавление подсети клиента3»

На вкладке следует задать имя клиента и IP-адрес/маску клиентской подсети, далее нажать кнопку «Добавить сеть клиента». Добавленная сеть отобразится в списке клиентов VPN в поле «Управление сетями клиентов VPN».

2.8.2.2 Создание нового экземпляра VPN-клиента

Создание нового экземпляра VPN-клиента инициируется кнопкой «Создать новый экземпляр VPN-клиента» на вкладке «Настройка VPN» в поле «Список клиентов VPN». В результате откроется вкладка, содержащая поля «Настройка клиента VPN 2» и «Список удаленных узлов VPN» (рисунок 187).

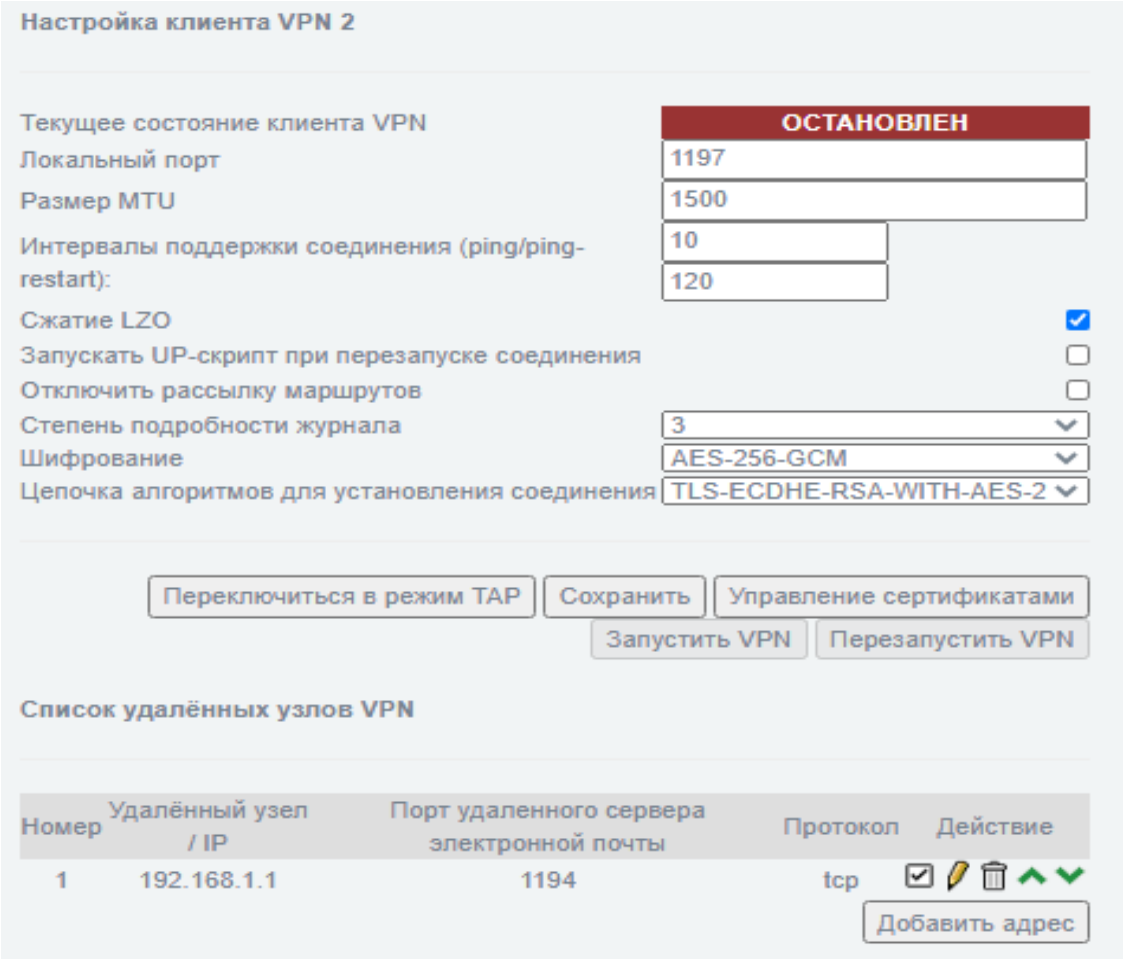


Рисунок 187 – Вкладка «Настройка клиента VPN 2»

Описание элементов вкладки «Настройка клиента VPN 2» представлено в таблице 121.

Таблица 121 – Описание элементов поля «Настройка клиента VPN 2»

Элемент	Описание
Параметр «Текущее состояние клиента VPN»	Предназначен для отображения текущего состояния клиента VPN (запущен или остановлен)
Параметр «Локальный порт»	Предназначен для ввода информации о локальном порте, на который приходят запросы на установление VPN-соединения
Параметр «Размер MTU»	Предназначен для ввода информации о размере MTU в туннеле VPN
Чекбокс «Сжатие LZO»	Предназначен для указания использования сжатия LZO при передаче информации в туннеле
Чекбокс «Запускать UP-скрипт при перезапуске соединения»	Предназначен для включения/выключения запуска внутреннего скрипта обработки ситуации перезапуска соединения.

Элемент	Описание
Чекбокс «Отключить рассылку маршрутов»	Предназначен для включения/выключения необходимости рассылки маршрутов сетей, настроенных в сервисе VPN
Параметр «Степень подробности журнала»	Предназначен для указания подробности журнала: 1 – минимальная степень, 6 – максимальная.
Параметр «Шифрование»	Предназначен для указания алгоритма, применяемого для передачи данных в создаваемом туннеле VPN.
Параметр «Цепочка алгоритмов для установления соединения»	Предназначен для указания цепочки (последовательности) алгоритмов, применяемых при установлении соединения VPN.
Кнопка «Переключиться в режим TAP»	Переключиться в режим TAP из TUN (по умолчанию и наоборот)
Кнопка «Сохранить»	Сохранить введённые настройки клиента VPN
Кнопка «Управление сертификатами»	Открывает вкладку «Управление сертификатами»
Кнопка «Запустить VPN»	Предназначена для запуска сервера VPN с указанными настройками.
Кнопка «Перезапустить VPN»	Предназначена для перезапуска сервера VPN с указанными настройками.

2.8.2.2.1 Поле «Список удаленных узлов VPN»

Поле «Список удаленных узлов VPN» предназначено для добавления, удаления, подключения/отключения удаленных узлов VPN. Для включения/отключения удаленного узла VPN используется чекбокс, редактирования/удаления, соответствующие символы « » «карандаш» и « » «корзина», для добавления узла следует нажать кнопку «Добавить адрес», в результате чего откроется вкладка «Удаленный узел 2» (рисунок 188).

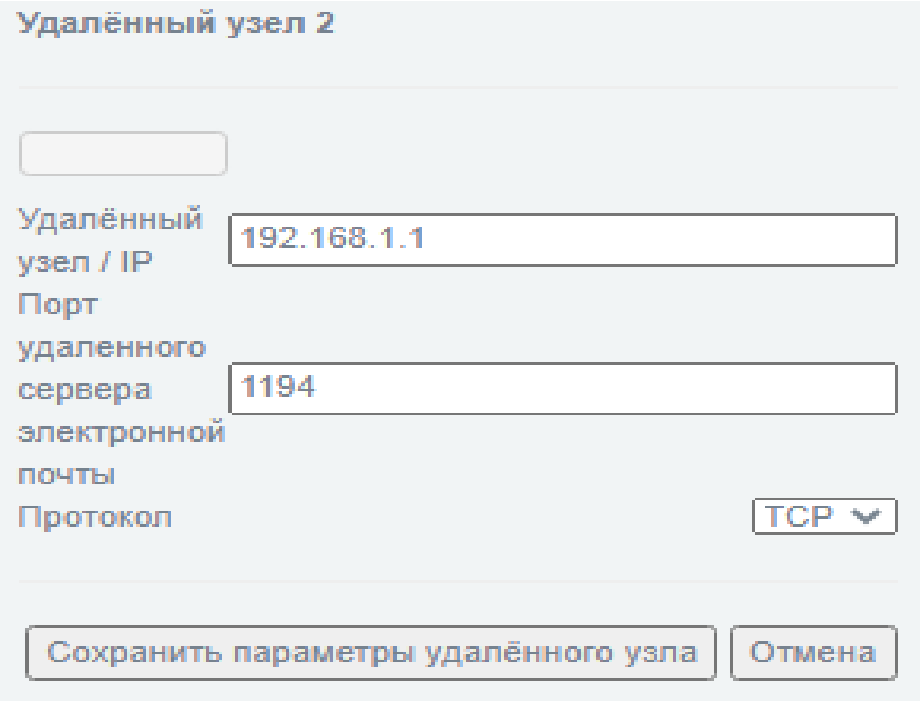


Рисунок 188 – Вкладка «Удаленный узел 2»

На вкладке следует задать IP-адрес, порт и сетевой протокол удаленного узла, далее нажать кнопку «Сохранить параметры удаленного узла». Добавленный узел отобразится в списке удаленных узлов VPN в поле «Список удаленных узлов VPN».

2.8.3 Подраздел «GRE»

Подраздел «GRE» (рисунок 189) предназначен для создания GRE-туннелей.

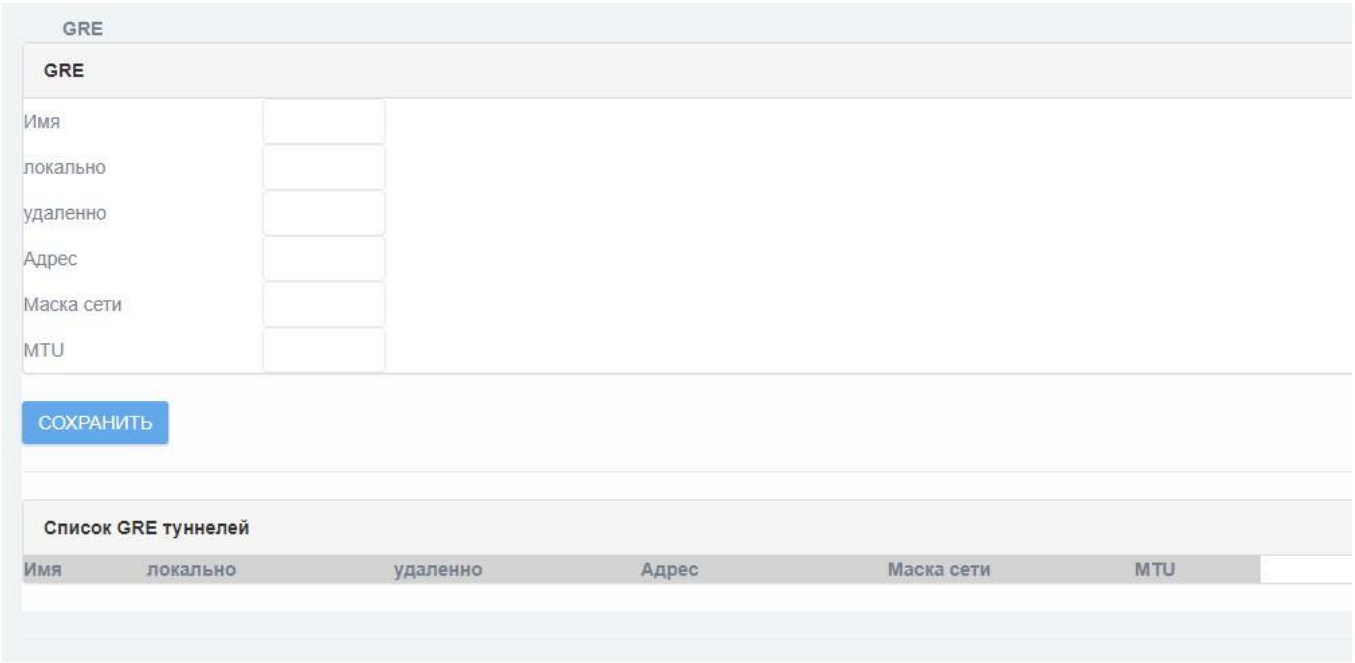


Рисунок 189 – Подраздел «GRE»

Подраздел «GRE» содержит элементы, указанные в таблице 122.

Таблица 122 – Описание элементов подраздела «GRE»

Элемент	Описание
	Поле для ввода необходимой информации
Поле «Имя»	Предназначено для указания имени GRE-туннеля
Поле «локально»	Предназначено для указания IP-адреса устройства, от которого будет устанавливаться GRE-туннель
Поле «удаленно»	Предназначено для указания IP-адрес удаленного устройства, с которым будет устанавливаться GRE-туннель
Поле «Адрес»	Предназначено для указания виртуального локального IP-адреса GRE-туннеля
Поле «Маска сети»	Предназначено для указания IP-маски для GRE-туннеля
Поле «MTU»	Предназначено для указания MTU для GRE-туннеля
Кнопка «  »	Сохранение введенной информации

Для настройки виртуального интерфейса GRE-туннеля на странице «VPN → GRE» пользователю необходимо ввести значения следующих параметров:

a) «Имя» – имя интерфейса GRE. Допускается имя, состоящее из латинских букв верхнего и нижнего регистра и цифр от 0 до 9;

b) «локально», «удаленно» – локальный и удаленный адреса (адреса сетевых адаптеров локального и удаленного узлов, которые принимают сетевые пакеты, инициализирующие туннель, и сетевые пакеты протокола GRE, инкапсулирующие сетевые пакеты внутри туннеля после его установки). В качестве локального допустим корректный IP-адрес, принадлежащий одному из сетевых интерфейсов комплекса «Рубикон», в качестве удаленного — корректный IP-адрес (туннель будет установлен только если удаленный адрес доступен по сети);

c) «Адрес» – IP-адрес виртуального интерфейса GRE внутри установленного туннеля. Допустим корректный IP-адрес, не входящий ни в какой другой сетевой диапазон адресов комплекса «Рубикон»;

d) «Маска сети» – IP-маска, определяющая диапазон сетевых адресов виртуального туннеля GRE. Допустима корректная IP-маска в формате десятичной записи четырех байт маски, разделенных точками;

e) «MTU» – необязательный параметр MTU для виртуального интерфейса GRE.

Пример ввода значений параметров представлен на рисунке 190.

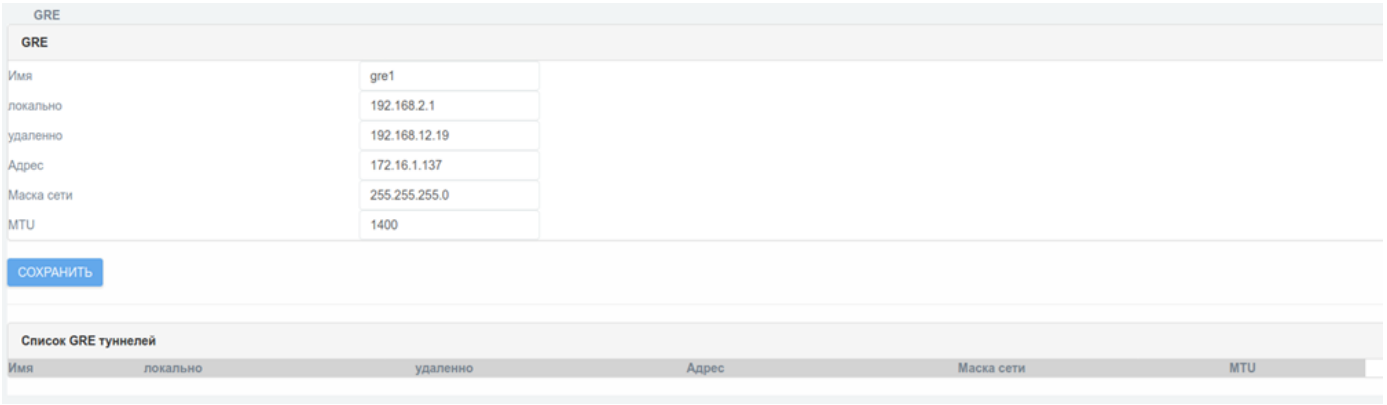


Рисунок 190 – Подраздел «GRE». Пример ввода значений параметров

Для применения введенных параметров необходимо нажать кнопку «Сохранить».

Если все исходные данные корректны, то созданный интерфейс отобразится в списке GRE туннелей (рисунок 191).

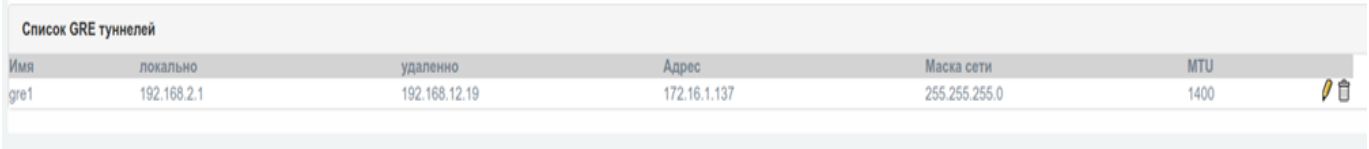


Рисунок 191 – Список туннелей GRE

Также интерфейс будет отображен на вкладке «Состояние → Состояние сети» (рисунок 192).

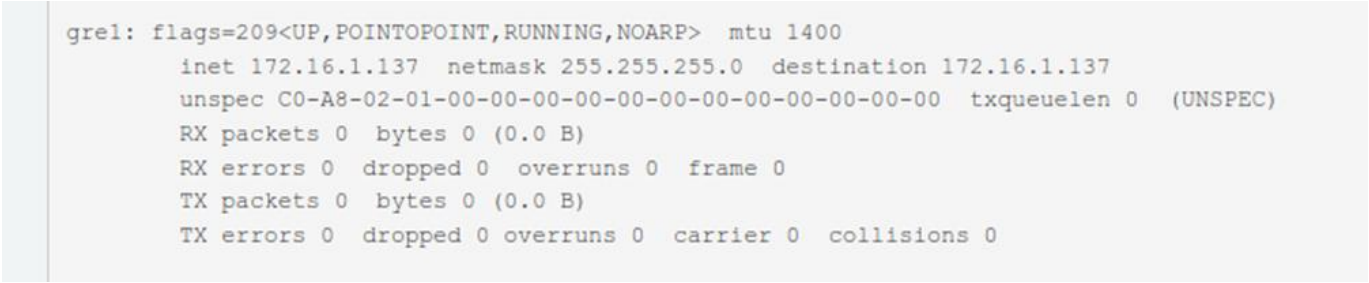


Рисунок 192 – Отображение интерфейса на вкладке «Состояние → Состояние сети»

Для организации туннеля GRE с использованием созданного интерфейса необходимо:

a) обеспечить доступность по сети IP-адреса узла, указанного в поле «удаленно»;

b) обеспечить прохождение пакетов протокола GRE от удаленного узла к локальному по указанным IP-адресам;

c) добавить правило, разрешающее прием комплексом «Рубикон» пакетов протокола GRE от удаленного узла на локальный по указанным IP-адресам.

Для этого необходимо на странице «Межсетевой экран → Службы» добавить соответствующую службу с используемым протоколом GRE (рисунок 193):

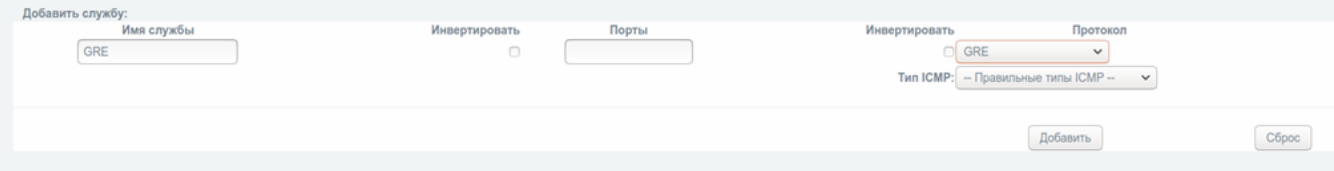


Рисунок 193 – Добавление службы с используемым протоколом GRE

После нажатия на кнопку «Добавить» протокол GRE будет внесен в список служб, используемых межсетевым экраном (рисунок 194).

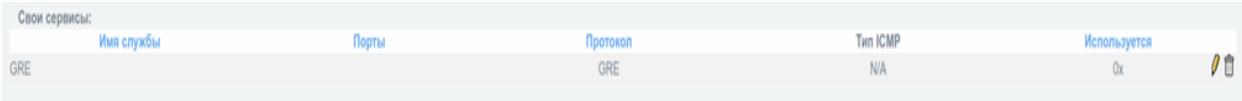


Рисунок 194 – Служба GRE

Далее, на вкладке «Межсетевой экран → правила межсетевого экрана → Другие из внутренней сети во внешнюю», необходимо добавить правило, разрешающее прохождение пакетов протокола GRE от IP-адреса удаленного узла к IP-адресу локального интерфейса (рисунки 195 - 197).

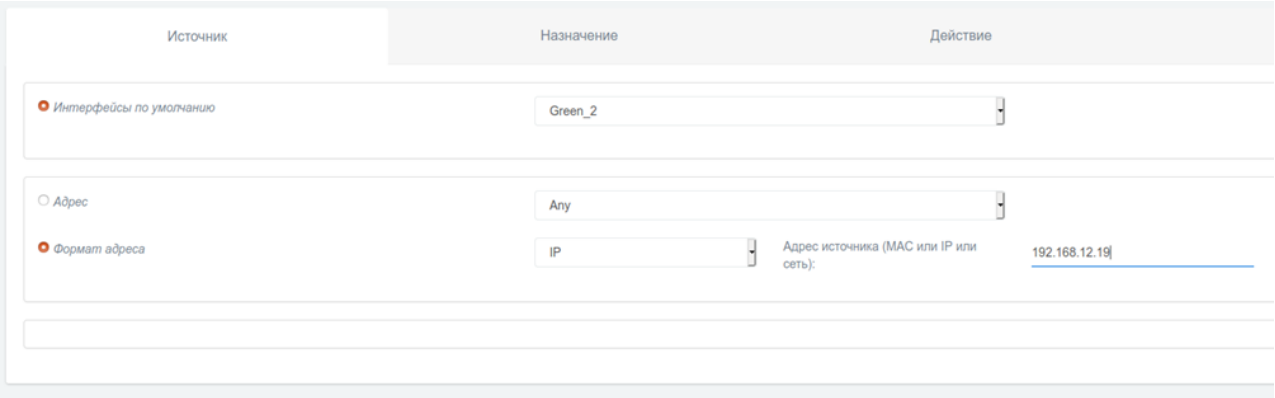


Рисунок 195 – Добавление правила, разрешающего прохождение пакетов протокола GRE от IP-адреса удаленного узла к IP-адресу локального интерфейса. Вкладка «Источник»

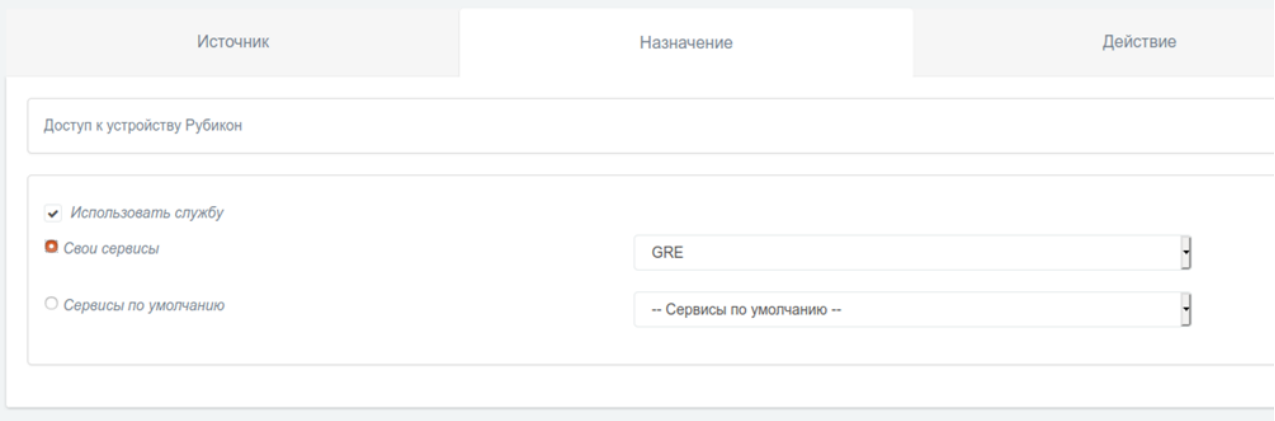


Рисунок 196 – Добавление правила, разрешающего прохождение пакетов протокола GRE от IP-адреса удаленного узла к IP-адресу локального интерфейса. Вкладка «Назначение»

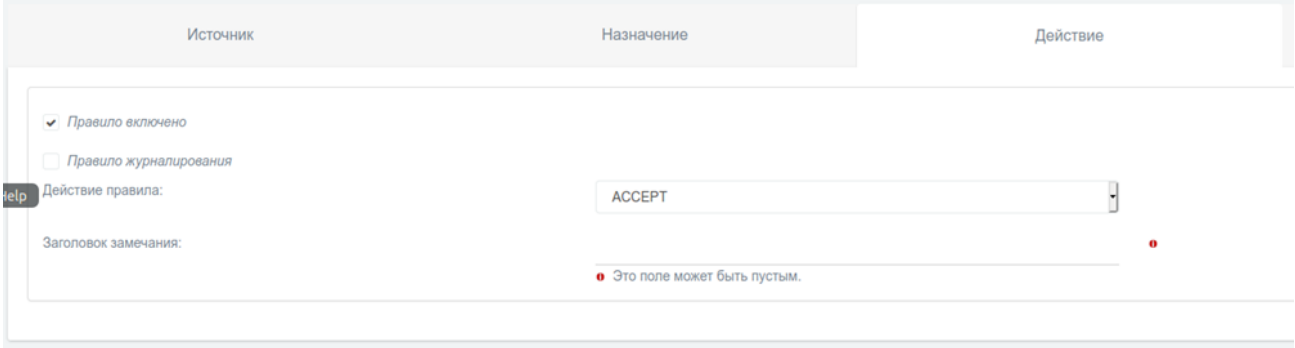


Рисунок 197 – Добавление правила, разрешающего прохождение пакетов протокола GRE от IP-адреса удаленного узла к IP-адресу локального интерфейса. Вкладка «Действие»

После применения настроек, правило будет отображено в списке правил «Доступ к устройству Рубикон» (рисунок 198).

Рисунок 198 – Отображение правила в списке правил

Далее следует добавить правила фильтрации на интерфейсе GRE трафика в соответствии с заданной политикой. Для этого необходимо на странице «Межсетевой экран → Настройки межсетевого экрана» установить расширенный режим настройки и применить конфигурации кнопкой «Сохранить» (рисунок 199).

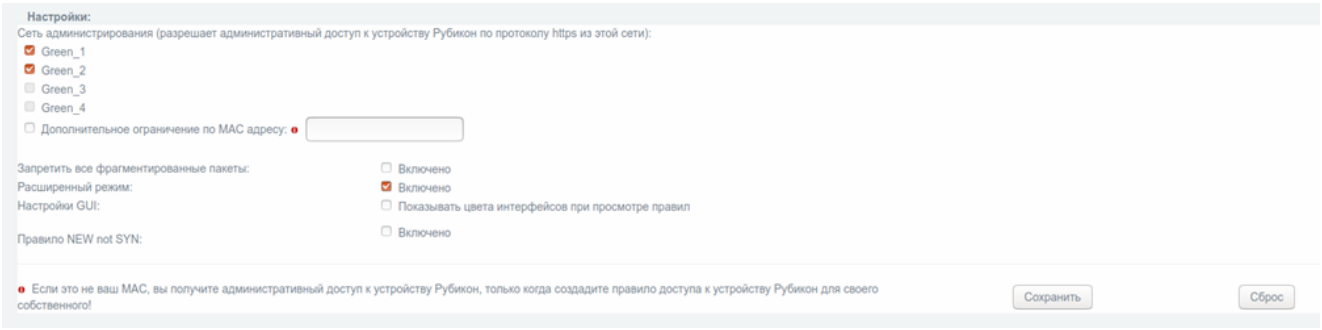


Рисунок 199 – Установка расширенного режима настройки

Далее, на странице «Межсетевой экран → Интерфейсы», следует внести созданный интерфейс GRE в список интерфейсов межсетевого экрана (Рисунок 200).

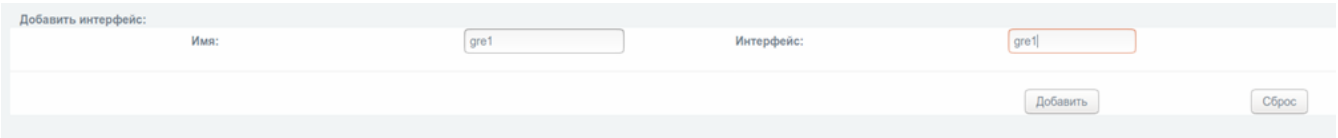


Рисунок 200 – Внесение созданного интерфейса GRE в список интерфейсов межсетевого экрана

Применить конфигурацию кнопкой «Добавить», после чего интерфейс отобразится в списке используемых межсетевым экраном (рисунок 201).

Рисунок 201 – Отображение интерфейса в списке используемых межсетевым экраном

Далее следует создать правила в соответствии с политикой фильтрации пакетов с использованием созданного интерфейса.

2.8.4 Подраздел «Выпуск сертификатов»

Подраздел «Выпуск сертификатов» предназначен для управления сертификатами (рисунок 202).

Рисунок 202 – Подраздел «Выпуск сертификатов»

2.8.4.1 Поле «Удостоверяющий центр»

Поле «Удостоверяющий центр» предназначено для выпуска сертификата удостоверяющего центра и загрузки списка отозванных сертификатов. Элементы поля «Удостоверяющий центр» представлены в таблице 123.

Таблица 123 – Элементы поля «Удостоверяющий центр»

Элемент	Описание
Кнопка «Сгенерировать новый сертификат»	Предназначена для перехода в диалоговое окно выпуска самоподписанного сертификата удостоверяющего центра.
Кнопка «Скачать список отозванных сертификатов»	Предназначена для скачивания списка отозванных сертификатов.

Для выпуска сертификата удостоверяющего центра необходимо нажать кнопку «Сгенерировать новый сертификат». В появившемся диалоговом окне требуется заполнить поля, характеризующие удостоверяющий центр. Обязательными являются поля «Имя или адрес хоста» и «Название организации». Эта информация должна быть уникальна для сертификатов данного удостоверяющего центра (рисунок 203).

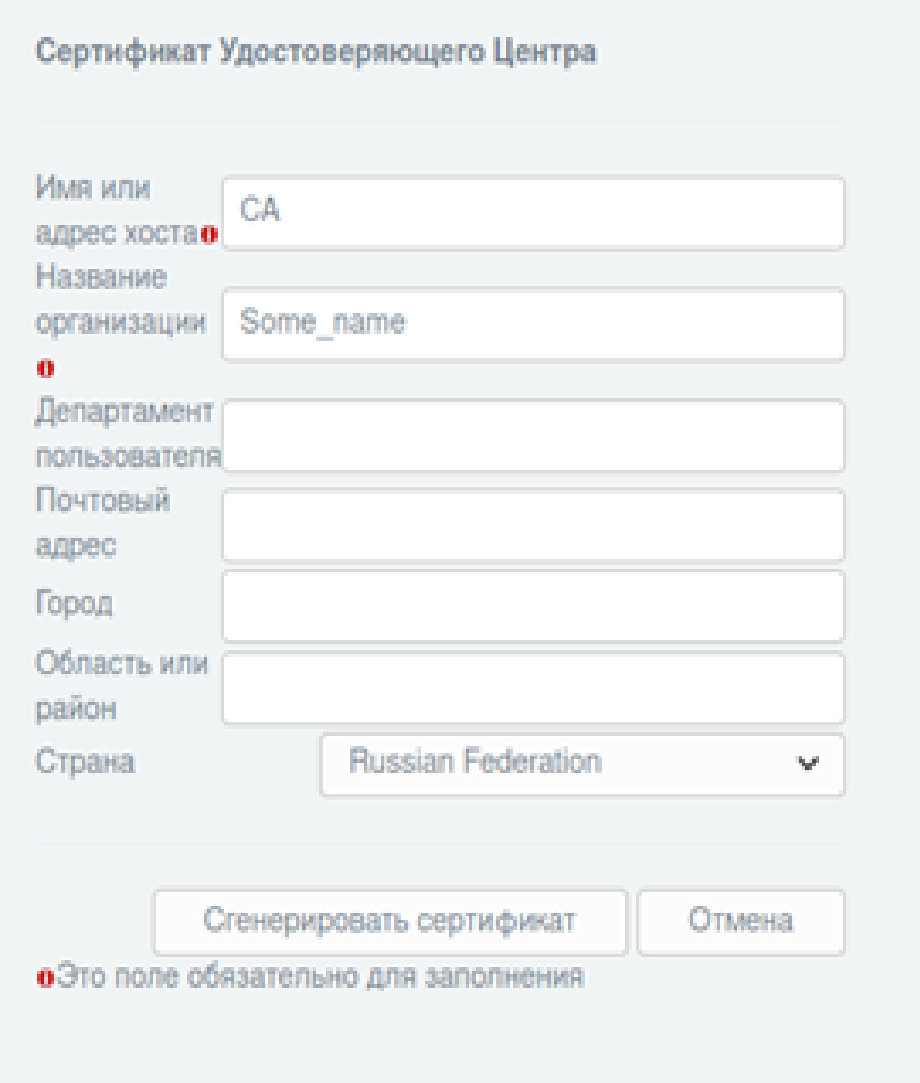


Рисунок 203 – Генерация сертификата управляющего центра

Поля формы «Сертификат удостоверяющего центра» представлены в таблице 124.

Таблица 124 – Поля формы «Сертификат удостоверяющего центра»

Элемент	Описание
Поле «Имя или адрес хоста» (поле обязательно для заполнения)	Предназначено для указания имени или адреса узла удостоверяющего центра
Поле «Название организации» (поле обязательно для заполнения)	Предназначено для указания названия организации, идентифицирующей удостоверяющий центр.
Поле «Департамент пользователя»	Предназначено для указания информации о департаменте, идентифицирующем удостоверяющий центр.
Поле «Почтовый адрес»	Предназначено для указания почтового адреса, идентифицирующем администратора удостоверяющий центр.
Поле «Город»	Предназначено для указания информации о городе, идентифицирующем удостоверяющий центр.
Поле «Область или район»	Предназначено для указания информации об области или районе, идентифицирующих удостоверяющий центр.
Ниспадающий список «Страна»	Предназначен для выбора информации о стране, идентифицирующей удостоверяющий центр.
Кнопка «Сгенерировать сертификат»	Предназначена для выпуска сертификата удостоверяющего центра согласно заполненным полям.
Кнопка «Отмена»	Предназначена для отмены действий по выпуску сертификата удостоверяющего центра.

После выпуска сертификата удостоверяющего центра в списке появится информация о сертификате: имя сертификата, серийный номер, дата выпуска, дата истечения срока и действия, которые возможны для работы с сертификатом (рисунок 204).

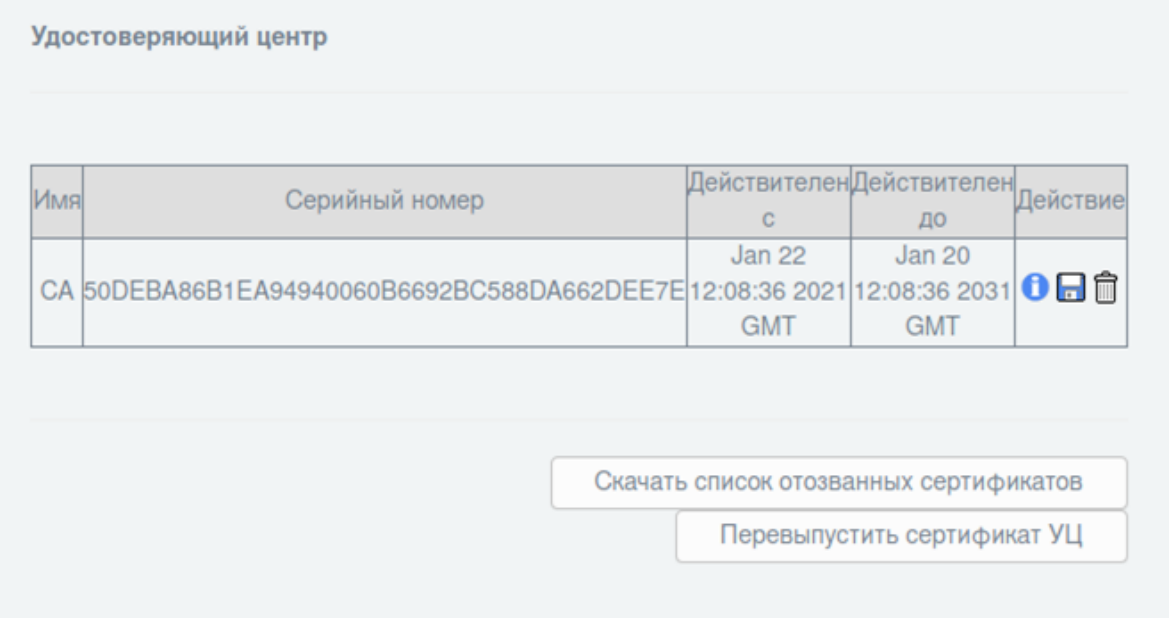


Рисунок 204 – Информация о сертификате

Элементы поля «Удостоверяющий центр» представлены в таблице 125.

Таблица 125 – Элементы поля «Удостоверяющий центр»

Элемент	Описание
	Предназначен для получения информации о сертификате
	Предназначен для загрузки сертификата на локальный диск пользователя
	Предназначен для удаления сертификата удостоверяющего центра

Скачивание отозванных сертификатов производится с помощью кнопки «Скачать список отозванных сертификатов».

2.8.4.2 Поле «Запросы на выдачу сертификата»

Поле «Запросы на выдачу сертификата» предназначено для обработки запросов на выдачу сертификатов. Для обработки запроса необходимо файл запроса поместить в список для подписи с помощью кнопок «Выберите файл» и «Загрузить запрос сертификата» (рисунок 205).

Рисунок 205 – Поле «Запросы на выдачу сертификата»

Элементы поля «Запросы на выдачу сертификата» представлены в таблице 124.

Таблица 124 – Элементы поля «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 список интерфейса для последующей подписи

Загруженный запрос на выдачу сертификата помещается в список запросов. В списке указывается: субъект (запись CommonName из сертификата) и действия, возможные для данного субъекта (рисунок 206).

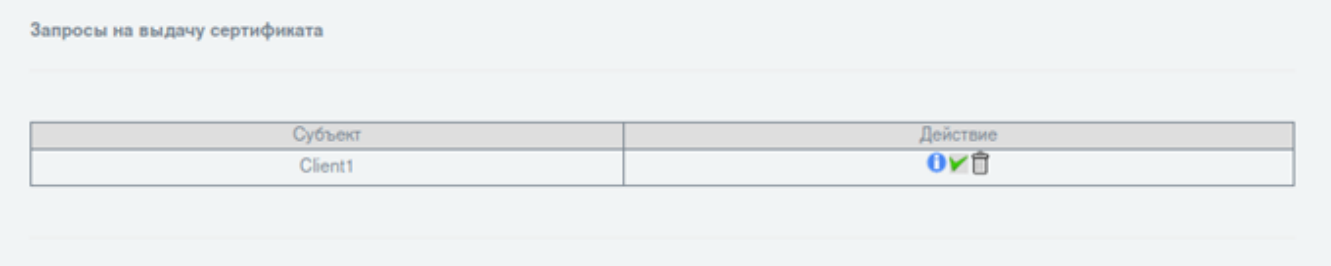


Рисунок 206 – Поле «Запросы на выдачу сертификата»

Элементы поля «Запросы на выдачу сертификата» представлены в таблице 127.

Таблица 127 – Элементы поля «Запросы на выдачу сертификата»

Элемент	Описание
	Предназначен для получения информации о запросе на получение сертификата
	Предназначен для выдачи сертификата по запросу на получение сертификата
	Предназначен для удаления запроса на получение сертификата

При нажатии на 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 список в поле «Выданные сертификаты».

2.8.4.3 Поле «Выданные сертификаты»

Поле «Выданные сертификаты» содержит список выданных удостоверяющим центром сертификатов с указанием информации о выданных сертификатах. Указанный список содержит информацию о выданном сертификате: имя сертификата, серийный номер, дата выпуска, дата истечения срока и действия, которые возможны для работы с сертификатом (рисунок 207).

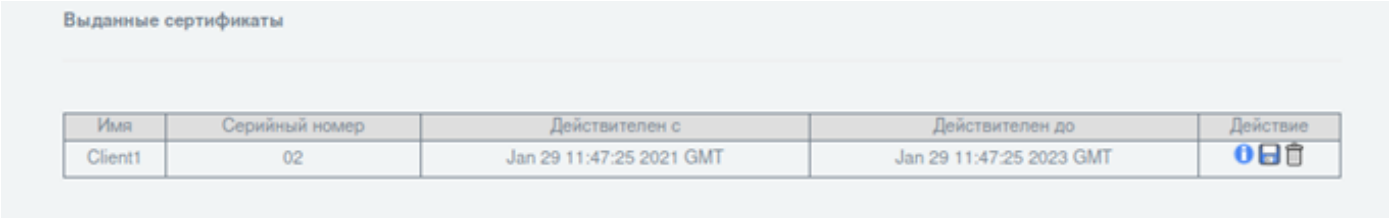


Рисунок 207 – Поле «Выданные сертификаты»

Элементы поля «Выданные сертификаты» представлены в таблице 128.

Таблица 128 – Элементы поля «Выданные сертификаты»

Элемент	Описание
	Предназначен для получения информации о сертификате
	Предназначен для загрузки сертификата на локальный диск пользователя
	Предназначен для удаления сертификата удостоверяющего центра

2.9 Раздел «Журналы»

Раздел «Журналы» содержит следующие подразделы:

– Подраздел «Настройки журналирования»;

– Подраздел «Журнал межсетевого экрана»;

– Подраздел «Журнал обнаружения атак»;

– Подраздел «Системный протокол».

2.9.1 Подраздел «Настройки журналирования»

Подраздел «Настройки журналирования» (рисунок 208) предназначен для установки параметров отображения и ведения журналов.

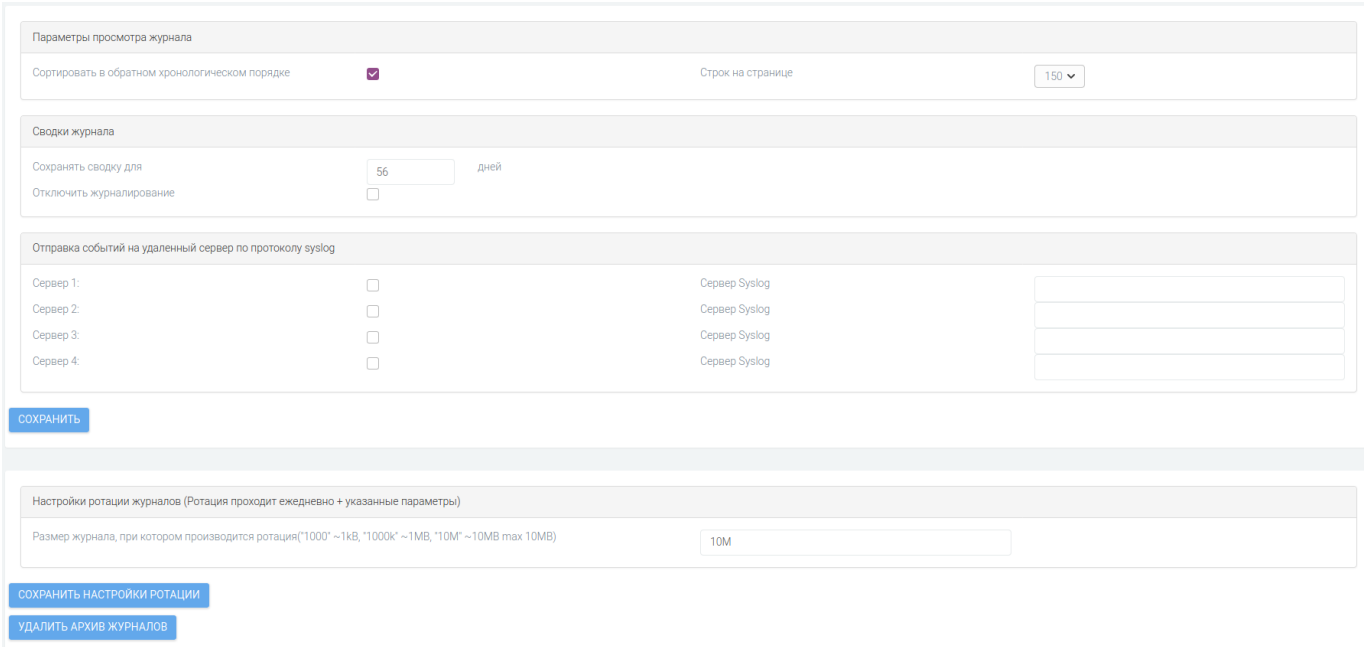


Рисунок 208 – Подраздел «Настройки журналирования»

Подраздел «Настройки журналирования» содержит элементы, указанные в таблице 129.

Таблица 129 – Описание элементов подраздела «Настройки журналирования»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок активации ниспадающего списка
Параметр «Сортировать в обратном хронологическом порядке»	Включение сортировки в обратном хронологическом порядке
Ниспадающее меню «Строк на странице»	Указание количества строк на странице
Поле «Сохранять сводку для»	Количество дней, за которые сохраняется сводка
Параметр «Отключить журналирование»	Включение / отключение журналирования
Параметр «Сервер 1»	Включение сервера Syslog 1
Поле «Сервер Syslog»	Адрес сервера Syslog
Параметр «Сервер 2»	Включение сервера Syslog 2
Поле «Сервер Syslog»	Адрес сервера Syslog
Параметр «Сервер 3»	Включение сервера Syslog 3
Поле «Сервер Syslog»	Адрес сервера Syslog
Параметр «Сервер 4»	Включение сервера Syslog 4
Поле «Сервер Syslog»	Адрес сервера Syslog

Элемент	Описание
Поле «Размер журнала, при котором производится ротация ("1000" ~1kB, "1000k" ~1MB, "10M" ~10MB max 10MB)»	Максимальный размер журнала, при котором происходит его перезапись
Кнопка «СОХРАНИТЬ»	Сохранение выбранных параметров
Кнопка «СОХРАНИТЬ НАСТРОЙКИ РОТАЦИИ»	Сохранение настроек ротации
Кнопка «УДАЛИТЬ АРХИВ ЖУРНАЛОВ»	Удаление архивов журналов

2.9.2 Подраздел «Журнал межсетевого экрана»

Подраздел «Журнал межсетевого экрана» (рисунок 209) предназначен для вывода общего отчета о системе за определенный период.

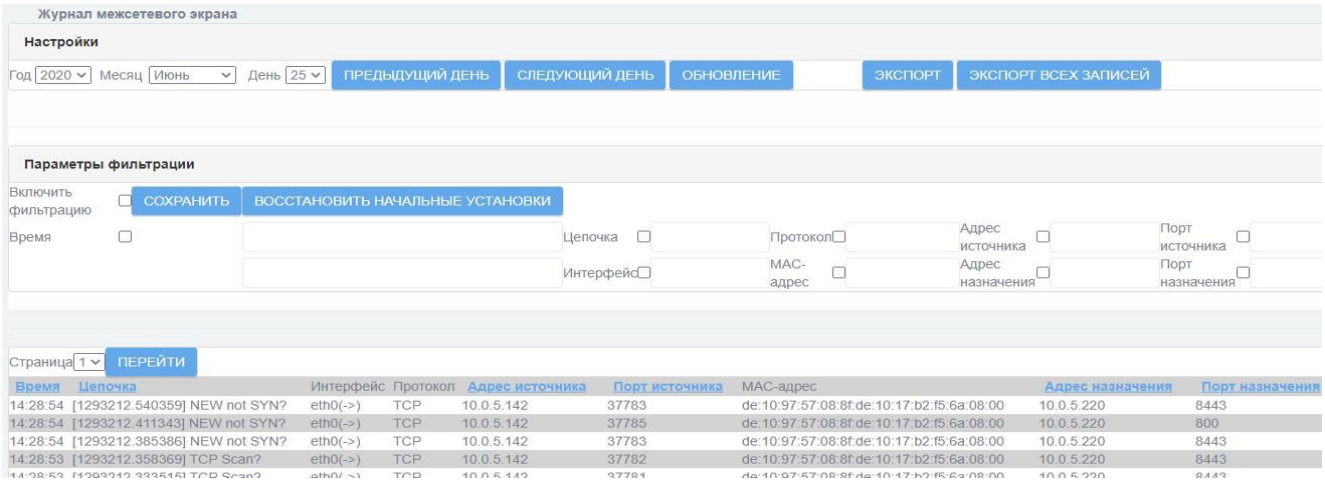
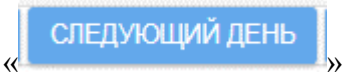
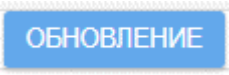
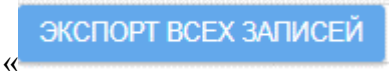
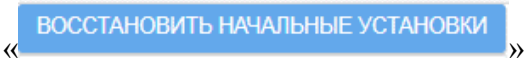


Рисунок 209 – Подраздел «Журнал межсетевого экрана»

Подраздел «Журнал межсетевого экрана» содержит элементы, указанные в таблице 130.

Таблица 130 – Описание элементов подраздела «Журнал межсетевого экрана»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок активации ниспадающего списка
Ниспадающее поле «Год»	Указание отображения информации за указанный год
Ниспадающее поле «Месяц»	Указание отображения информации за указанный месяц
Ниспадающее поле «День»	Указание отображения информации за указанный день
Кнопка «  »	Предназначена для перехода к странице информации на один день раньше
Кнопка «  »	Предназначена для перехода к странице информации на один день позже
Кнопка «  »	Предназначена для обновления информации для выбранного периода времени

Элемент	Описание
Кнопка «  »	Предназначена для экспорта отсортированных данных в текстовом виде
Кнопка «  »	Предназначена для экспорта всех данных в виде архива
Параметр «Включить фильтрацию»	Параметр включает фильтрацию по заданным категориям
Кнопка «  »	Сохранение текущих настроек фильтрации
Кнопка «  »	Восстановление первоначальных настроек фильтрации
Параметр «Время»	Включение фильтрации по указанному времени
Поле «Время»	Поле для указания времени фильтрации
Параметр «Цепочка»	Включение фильтрации по указанной цепочке
Поле «Цепочка»	Поле для указания цепочки фильтрации
Параметр «Интерфейс»	Включение фильтрации по заданному интерфейсу
Поле «Интерфейс»	Поле указания интерфейса для фильтрации
Параметр «Протокол»	Включение фильтрации по заданному протоколу

Элемент	Описание
Поле «Протокол»	Поле указания протокола для фильтрации
Параметр «MAC-адрес»	Включение фильтрации по определенному MAC-адресу
Поле «MAC-адрес»	Поле указания MAC-адреса для фильтрации
Параметр «Адрес источника»	Включение фильтрации по адресу источника
Поле «Адрес источника»	Поле указания адреса источника для фильтрации
Параметр «Адрес назначения»	Включение фильтрации по адресу назначения
Поле «Адрес назначения»	Поле указания адреса назначения для фильтрации
Параметр «Порт источника»	Включение фильтрации по порту источника
Поле «Порт источника»	Поле указания порта источника для фильтрации
Параметр «Порт назначения»	Включение фильтрации по порту назначения
Поле «Порт назначения»	Поле указания порта назначения для фильтрации
Ниспадающий список «Страница»	Ниспадающее поле выбора страницы для перехода

Элемент	Описание
Кнопка «ПЕРЕЙТИ»	Кнопка перехода на выбранную страницу

2.9.3 Подраздел «Журнал обнаружения атак»

Подраздел «Журнал обнаружения атак» (рисунок 210) предназначен для отображения журнала СОВ.

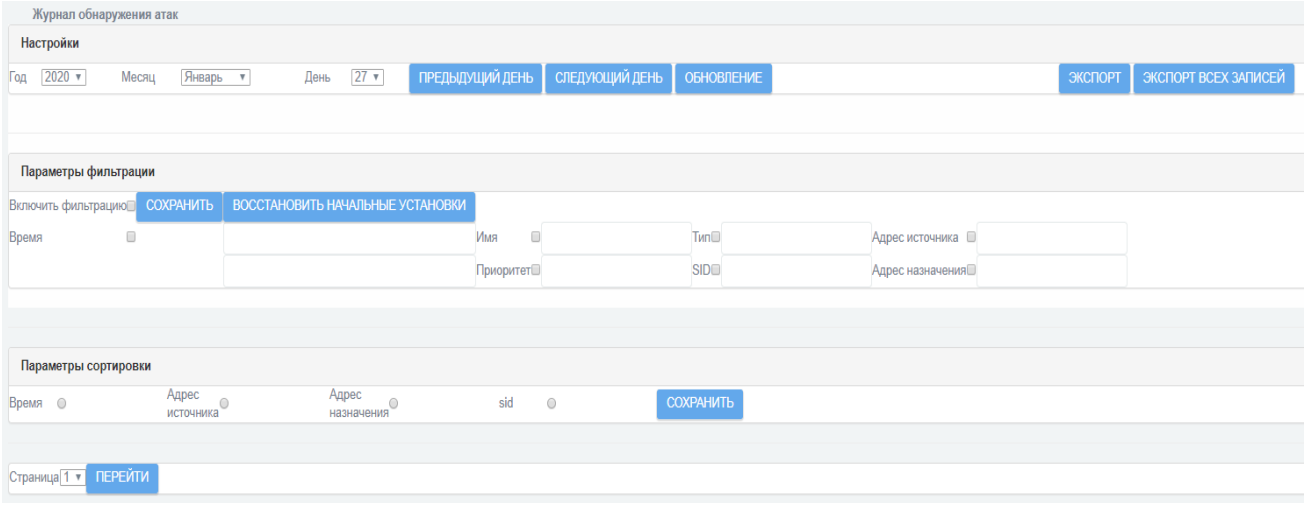
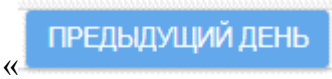
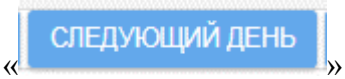
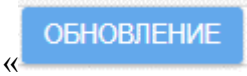
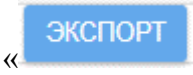
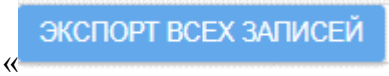


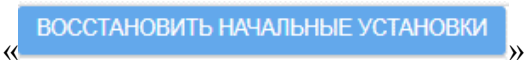
Рисунок 210 – Подраздел «Журнал обнаружения атак»

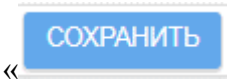
Подраздел «Журнал обнаружения атак» содержит элементы, указанные в таблице 131.

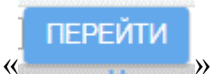
Таблица 131 – Описание элементов подраздела «Журнал обнаружения атак»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)

Элемент	Описание
	Пустое поле для проставления флажка (параметр выключен)
	Поле с проставленным флажком (параметр включен)
	Значок активации ниспадающего списка
Ниспадающее поле «Год»	Указание отображения информации за указанный год
Ниспадающее поле «Месяц»	Указание отображения информации за указанный месяц
Ниспадающее поле «День»	Указание отображения информации за указанный день
Кнопка «  »	Предназначена для перехода к странице информации на один день раньше
Кнопка «  »	Предназначена для перехода к странице информации на один день позже
Кнопка «  »	Предназначена для обновления информации для выбранного периода времени
Кнопка «  »	Предназначена для экспорта отсортированных данных в текстовом виде
Кнопка «  »	Предназначена для экспорта всех данных в виде архива

Элемент	Описание
Параметр «Включить фильтрацию»	Параметр включает фильтрацию по заданным категориям
Кнопка «  »	Сохранение текущих настроек фильтрации
Кнопка «  »	Восстановление первоначальных настроек фильтрации
Параметр «Время»	Включение фильтрации по указанному времени
Поле «Время»	Поле для указания времени фильтрации
Параметр «Имя»	Включение фильтрации по имени правила
Поле «Имя»	Поле указания имени для фильтрации
Параметр «Приоритет»	Включение фильтрации по приоритету
Поле «Приоритет»	Поле указания приоритета для фильтрации
Параметр «Тип»	Включение фильтрации по типу, к которому относится правило
Поле «Тип»	Поле указания типа для фильтрации
Параметр «SID»	Включение фильтрации по SID
Поле «SID»	Поле указания SID для фильтрации
Параметр «Адрес источника»	Включение фильтрации по адресу источника
Поле «Адрес источника»	Поле указания адреса источника для фильтрации

Элемент	Описание
Параметр «Адрес назначения»	Включение фильтрации по адресу назначения
Поле «Адрес назначения»	Поле указания адреса назначения для фильтрации
Параметр «Параметры сортировки»	Параметры сортировки: время, адрес источника, адрес назначения, sid
Параметр «Время»	Параметр включения сортировки по времени
Параметр «Адрес источника»	Параметр включения сортировки по адресу источника
Параметр «Адрес назначения»	Параметр включения сортировки по адресу назначения
Параметр «sid»	Параметр включения сортировки по sid (Security Identifier)
Кнопка « 

» | Кнопка сохранения типа сортировки |
| Ниспадающий список «Страница» | Ниспадающее поле выбора страницы для перехода |
| Кнопка « 

» | Кнопка перехода на выбранную страницу |

2.9.4 Подраздел «Системный протокол»

Подраздел «Системный протокол» (рисунок 211) предназначен для отображения сообщений об ошибках в «Рубикон», а также отображения всех событий функционирования «Рубикон».

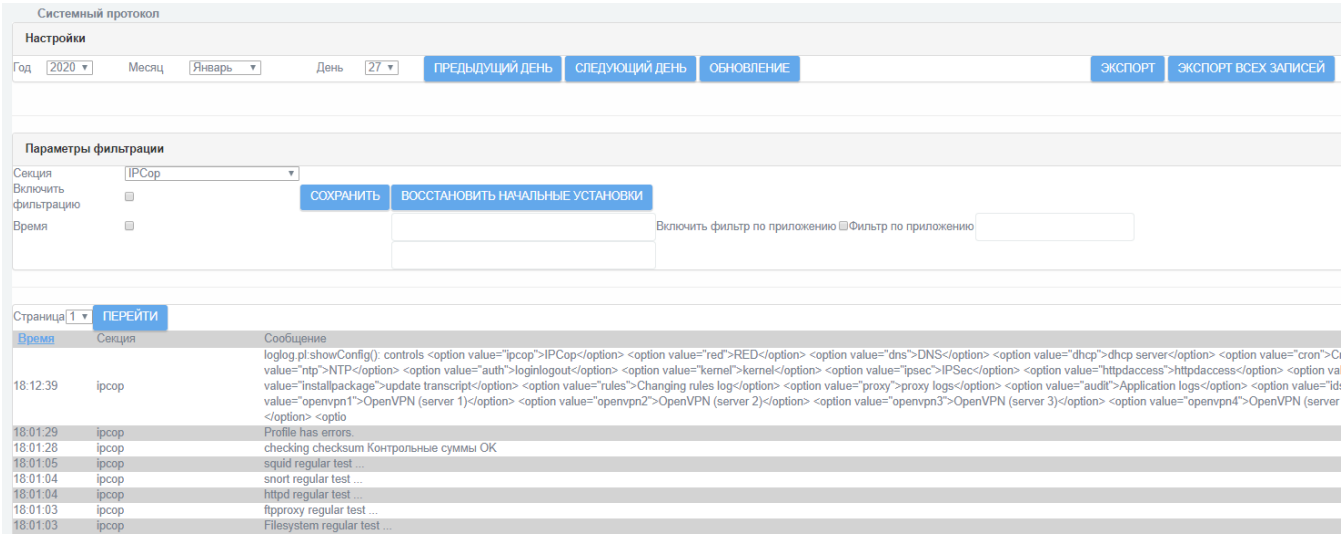
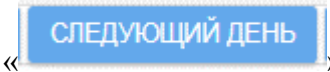
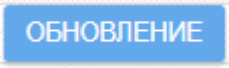
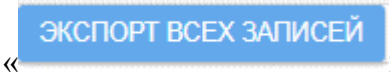
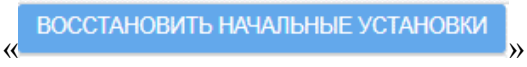


Рисунок 211 – Подраздел «Системный протокол»

Подраздел «Системный протокол» содержит элементы, указанные в таблице 132.

Таблица 132 – Описание элементов подраздела «Системный протокол»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Значок активации ниспадающего списка
Ниспадающее поле «Год»	Указание отображения информации за указанный год

Элемент	Описание
Ниспадающее поле «Месяц»	Указание отображения информации за указанный месяц
Ниспадающее поле «День»	Указание отображения информации за указанный день
Кнопка «  »	Предназначена для перехода к странице информации на один день раньше
Кнопка «  »	Предназначена для перехода к странице информации на один день позже
Кнопка «  »	Предназначена для обновления информации для выбранного периода времени
Кнопка «  »	Предназначена для экспорта отсортированных данных в текстовом виде
Кнопка «  »	Предназначена для экспорта всех данных в виде архива
Ниспадающий список «Секция»	Предназначен для выбора параметров фильтрации
Параметр «Включить фильтрацию»	Параметр включает фильтрацию по заданным категориям
Кнопка «  »	Сохранение текущих настроек фильтрации
Кнопка «  »	Восстановление первоначальных настроек фильтрации
Параметр «Время»	Включение фильтрации по указанному времени

Элемент	Описание
Поле «Время»	Поле для указания времени фильтрации
Параметр «Включить фильтр по приложению»	Параметр включает фильтрацию по указанному приложению
Поле «Фильтр по приложению»	Поле указания приложения для фильтрации
Ниспадающий список «Страница»	Ниспадающее поле выбора страницы для перехода
Кнопка «  »	Кнопка перехода на выбранную страницу

3 ОПИСАНИЕ ОПЕРАЦИЙ

3.1 Присвоение ролей

ПО «Рубикон» поддерживает присвоение пользователям следующих ролей:

a) «Администратор» – имеет доступ к просмотру веб-интерфейса и настройке «Рубикон»;

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

c) «Пользователь» – не имеет доступа к просмотру веб-интерфейса (кроме стартовой страницы) и страницы установки соединения «https://<ip-address>:8443/cgi-bin/connect.cgi». Параметр «ip-address» при первоначальной установке имеет значение 192.168.1.1 и может быть изменен администратором. На странице установки соединения после нажатия кнопки «Установить соединение» ПО «Рубикон» фиксирует IP-адрес пользователя и предоставляет соответствующие права, назначенные данному пользователю администратором в разделе «Межсетевой экран» подраздела «Правила межсетевого экрана».

Для того, чтобы добавить новых пользователей в подразделе «Пользователи» раздела «Система», в ниспадающем списке «Роль» выберите роль («Администратор», «Аудитор», «Пользователь»), затем заполните следующие текстовые поля (рисунок 212):

a) «Имя»;

b) «Пароль»;

c) «подтверждение».

Далее следует нажать кнопку «Сохранить».

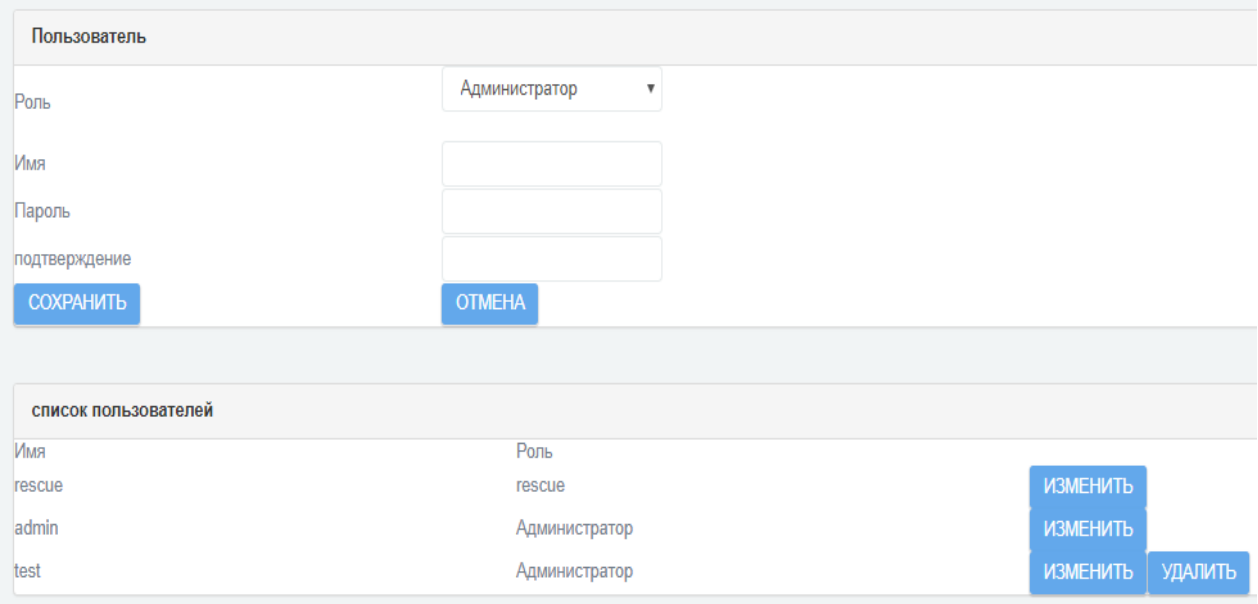


Рисунок 212 – Подраздел «Пользователи» раздела «Система»

Список пользователей отображается в блоке «Список пользователей». При необходимости, можно удалить пользователя или внести изменения в учетную запись.

Авторизация роли «Аудитор» и роли «Пользователь» выполняется аналогично авторизации роли «Администратор». Для работы с «Рубикон» пользователю необходимо получить логин и пароль у администратора безопасности.

3.2 Просмотр сведений о программе

После успешного прохождения процедуры авторизации администратор может вывести на экран сведения о «Рубикон» (версию, производителя и т.п.), перейдя в подраздел «О программе» раздела «Система» (рисунок 213).

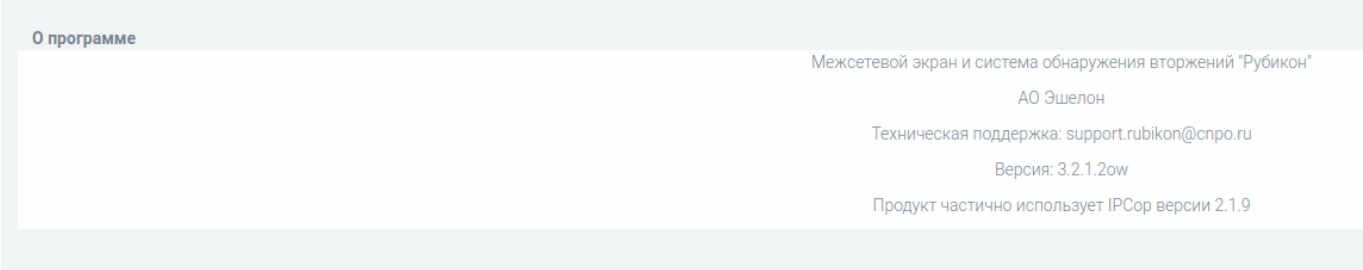


Рисунок 213 – Подраздел «О программе» раздела «Система»

3.3 Настройка резервирования

3.3.1 Горячее резервирование

Функция горячего резервирования устройства «Рубикон» обеспечивает бесперебойную реализацию функций межсетевого экрана и СОВ в случае возможного выхода из строя устройства «Рубикон».

Горячее резервирование реализуется посредством двух идентично настроенных устройств «Рубикон», подключенными к одним и тем же сегментам сети одноименными интерфейсами. При этом один из комплексов назначается главным, а другой — резервным. Главное устройство при этом полноценно работает и выполняет функции МЭ и СОВ, а резервное находится в режиме ожидания и получает от главного пакеты о работоспособности. На каждом из одноименных сетевых интерфейсов главного и резервного устройств назначается одинаковый виртуальный IP-адрес, так, чтобы при выходе из строя главного устройства резервное сохраняло конфигурацию сети. Таким образом, пара устройств «Рубикон» представляется в сети как одиночное устройство «Рубикон», сетевые адреса которого совпадают с настроенными виртуальными адресами.

При выходе из строя главного устройства резервное перестает получать сетевые пакеты о работоспособности главного устройства, и, через определенный администратором в поле «задержка» промежуток времени принимает на себя функции главного: активирует функции приема, передачи и обработки сетевых пакетов на виртуальных адресах.

В случае восстановления функций главного устройства в сети оно рассылает сетевые пакеты о своей работоспособности. Резервное, получая указанные пакеты, возвращается в режим ожидания и перестает обрабатывать сетевые пакеты на виртуальных адресах.

Пример: резервирование устройств при организации взаимодействия «зеленой» и «красной» сети (рисунок 214).

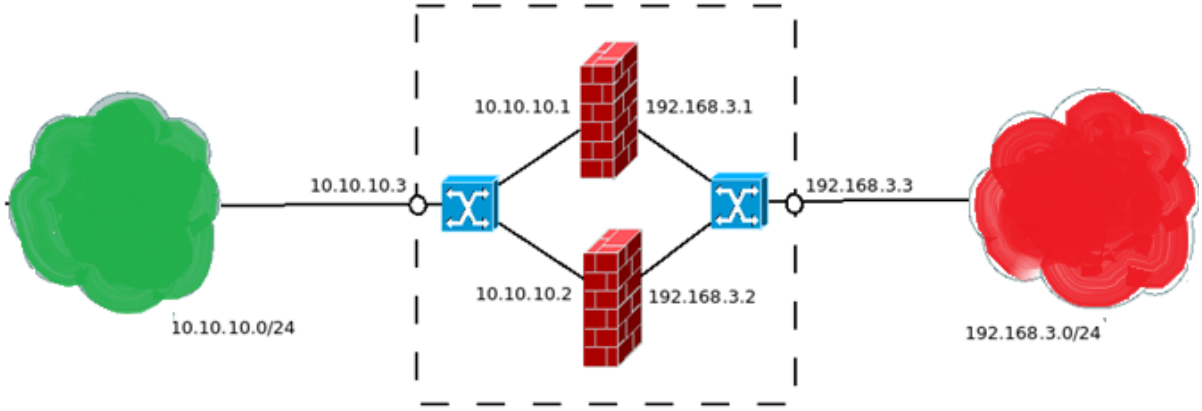


Рисунок 214 – Резервирование устройств при организации взаимодействия «зеленой» и «красной» сети

В представленной схеме верхнее устройство «Рубикон» настроено в качестве главного, нижнее устройство «Рубикон» настроено в качестве резервного. Адреса «зеленой» сети принадлежат диапазону 10.10.10.0/24, главному устройству «Рубикон» присвоен адрес в этой сети: 10.10.10.1, резервному устройству: 10.10.10.2. Виртуальный адрес резервирования в «зеленой» сети: 10.10.10.3. Адреса «красной» сети принадлежат диапазону 192.168.3.0/24, главному устройству присвоен адрес в этой сети: 192.168.3.1, резервному: 192.168.3.2. Виртуальный адрес резервирования в «красной» сети: 192.168.3.3.

Для настройки функции горячего резервирования необходимо:

1) настроить виртуальный адрес «зеленого» интерфейса. Для этого следует в подразделе «Горячее резервирование CARP (VRRP)» раздела «Сеть» нажать кнопку редактирования интерфейса (GREEN_1) (рисунок 215);

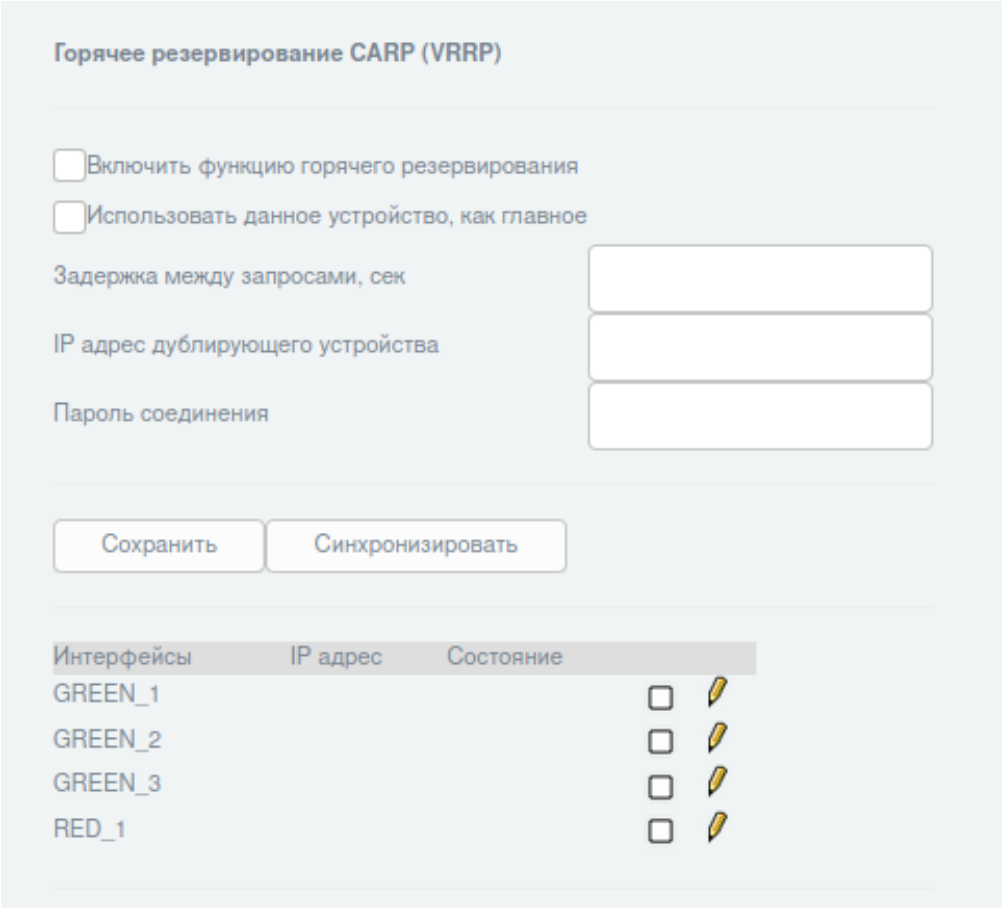


Рисунок 215 – Подраздел «Горячее резервирование CARP (VRRP)» раздела «Сеть»

2) в отобразившемся окне редактирования указать общий виртуальный IP адрес и нажать кнопку «Сохранить» (рисунок 216);

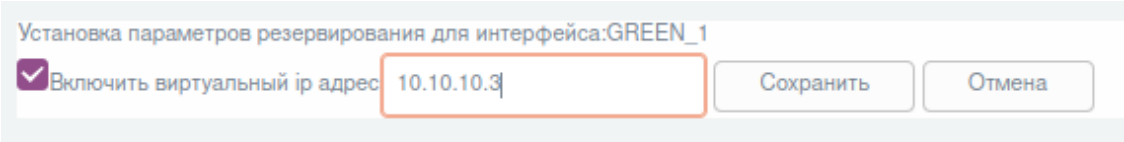


Рисунок 216 – Общий виртуальный IP-адрес для «зеленого» интерфейса

3) настроить виртуальный адрес «красного» интерфейса. Для этого в подразделе «Горячее резервирование CARP (VRRP)» раздела «Сеть» нажать кнопку редактирования интерфейса (RED_1) (рисунок 215);

4) в отобразившемся окне редактирования указать общий виртуальный IP адрес и нажать кнопку «Сохранить» (рисунок 217);

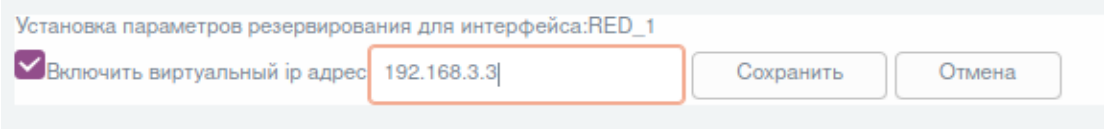


Рисунок 217 – Общий виртуальный IP-адрес для «красного» интерфейса

5) для главного устройства установить элемент управления «Использовать данное устройство, как главное» (рисунок 218);

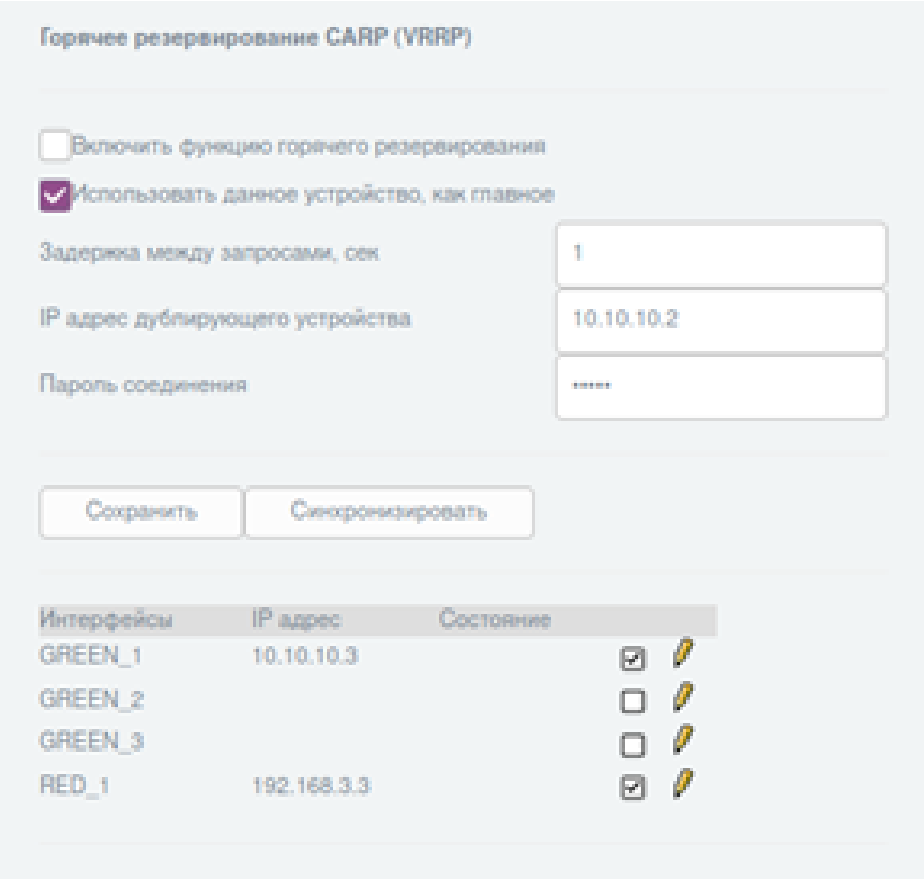


Рисунок 218 – Настройка резервного устройства «Рубикон»

6) для главного и резервного устройств заполнить поля «Задержка», «IP адрес дублирующего устройства» и «Пароль соединения» следующими значениями:

a) задержки между запросами;

b) IP-адреса дублирующего устройства (если настраивается главное, то указывается IP-адрес резервного и наоборот);

c) пароля для протокола обмена (пароли, заданные на главном и резервном устройстве, должны совпадать);

7) для главного и резервного устройств установить элемент управления «Включить функцию горячего резервирования» (рисунок 219);

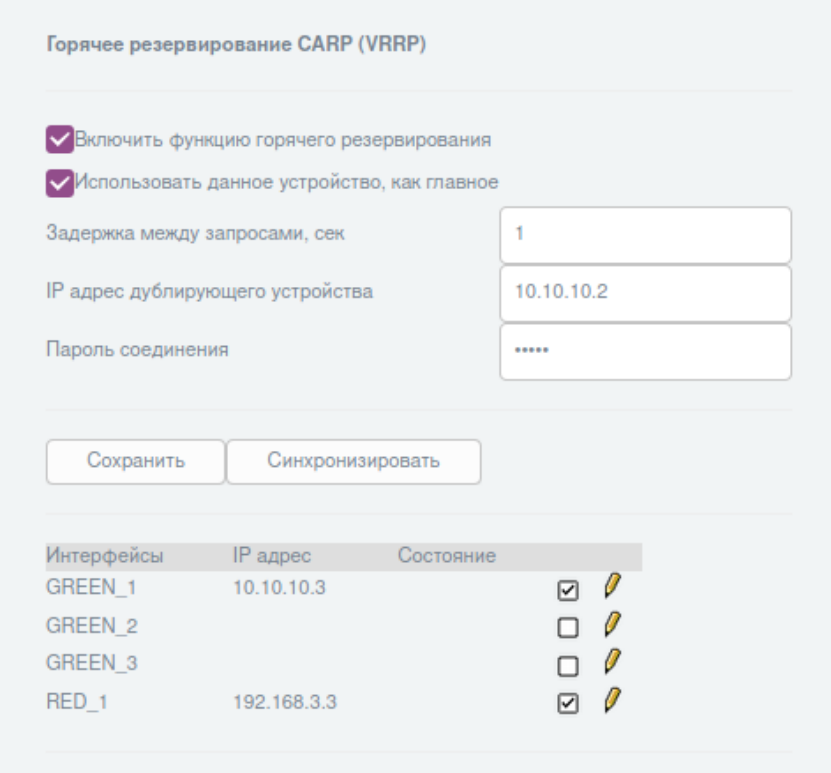


Рисунок 219 – Включение функции горячего резервирования

8) для проверки правильности настройки горячего резервирования необходимо выполнить команду ping с адресом виртуального интерфейса: $ ping 10.10.10.3.

3.4 Работа с журналами событий

3.4.1 Общие положения

В «Рубикон» предусмотрены следующие журналы:

1) журнал МЭ;

2) журнал обнаружения атак (вторжений);

3) системный протокол

Системный протокол содержит информацию обо всех действиях, производимых в «Рубикон». Регистрируемые события:

1) запуск выполнения функций аудита;

2) попытка авторизации;

3) успешная авторизация;

4) неудачная авторизация;

5) действия, предпринимаемые в ответ на возможные нарушения безопасности;

6) чтение информации из записей аудита;

7) параметры, используемые при просмотре;

8) все модификации конфигурации аудита, происходящие во время сбора данных аудита;

9) разрешения на запрашиваемые информационные потоки;

10) все попытки импортировать данные пользователя;

11) все попытки экспортировать информацию;

12) все модификации режима выполнения функций;

13) все модификации значений данных;

14) использование функций управления;

15) модификация группы пользователей – исполнителей роли;

16) каждое использование прав, представленных ролью;

17) все модификации значений атрибутов безопасности;

18) обнаружение сбоя функций безопасности, если аудит возможен;

19) факт возникновения сбоя или прерывания обслуживания;

20) возобновление нормальной работы;

21) тип сбоя или прерывания обслуживания;

22) невозможность возврата к безопасному состоянию после сбоя функций безопасности, если аудит возможен;

23) изменения внутреннего представления времени;

24) предоставление меток времени;

25) выполнение тестирования внешних сущностей и протоколирование результатов тестирования;

26) выполнение и результаты самотестирования функций безопасности;

27) успешное использование механизмов согласования данных функций безопасности;

28) использование механизмов согласования данных функций безопасности;

29) идентификация функций безопасности, данные которых интерпретируются;

30) обнаружение модифицированных данных функций безопасности;

31) любой сбой, обнаруженный функциями безопасности;

32) завершение выполнения функций аудита.

Журналы можно хранить локально или отправлять на удаленный сервер.

3.4.2 Настройка параметров отображения и ведения журналов

Для настройки параметров отображения и ведения журналов необходимо перейти в подраздел «Настройки журналирования» раздела «Журналы» (рисунок 220).

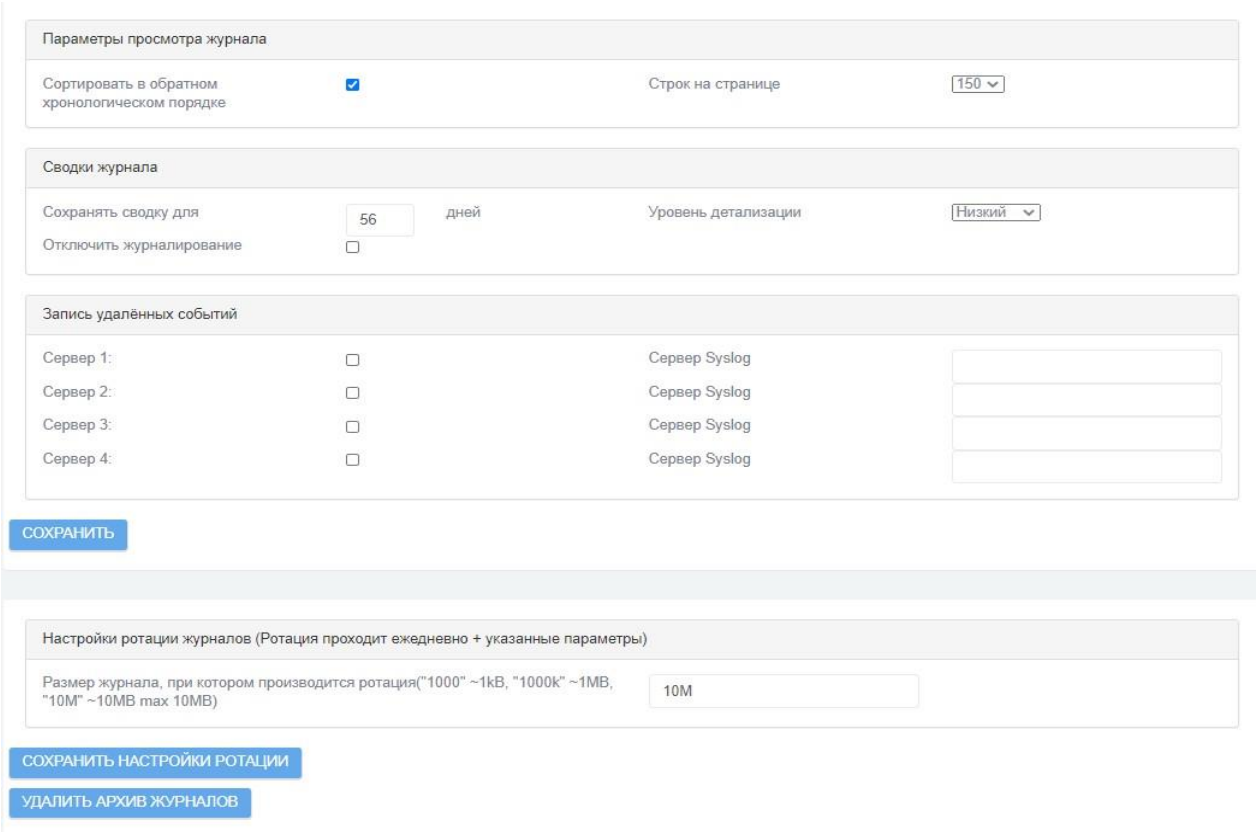


Рисунок 220 – Страница настройки параметров отображения журналов

Для настройки администратору доступны следующие поля:

1) «Параметры просмотра журнала»;
2) «Сводки журнала»;
3) «Запись удаленных событий»;
4) «Настройки ротации журнала».

3.4.2.1 Параметры просмотра журнала

Параметр «Сортировать в обратном хронологическом порядке» предназначен для установления отображения записей журналов в обратном хронологическом порядке.

Параметр «Строк на странице» предназначен для установления количества строк, отображаемых на одной странице журнала.

3.4.2.2 Сводки журнала

Параметр «Сохранять сводку для» предназначен для указания временного периода хранения сводки журнала (в днях). После истечения указанного срока записи удаляются из журнала.

Параметр «Уровень детализации» может принимать следующие значения:

a) низкий;

b) средний;

c) высокий.

Отметка напротив поля «Отключить журналирование» позволяет отключить запись всех системных событий и обнаруженных атак, а также отправку записей на удаленный сервер (если эта опция была включена ранее).

3.4.2.3 Запись удаленных событий

Параметр «Включено» предназначен для включения возможности журналирования событий на удаленном сервере.

Поле «Сервер Syslog» предназначено для указания адреса удаленного syslog-сервера.

3.4.2.4 Настройки ротации журналов

Для настройки ротации журналов необходимо выполнить следующие действия:

1) задать «Количество файлов старых журналов, которые необходимо сохранить на устройстве» в текстовом поле;

2) задать «Размер журнала, при котором производится ротация («1000» ~1kB, «1000k» ~1MB, «10M» ~10MB, max 10MB)» в текстовом поле;

3) перейти по ссылке «Посмотреть статистику ротированных журналов» для просмотра статистики;

4) для сохранения внесенных изменений в настройки параметров отображения и ведения журналов нажать кнопку «Сохранить».

3.4.3 Сервер времени

Для настройки сервера времени необходимо перейти в подраздел «Сервер времени» раздела «Службы» (рисунок 221).

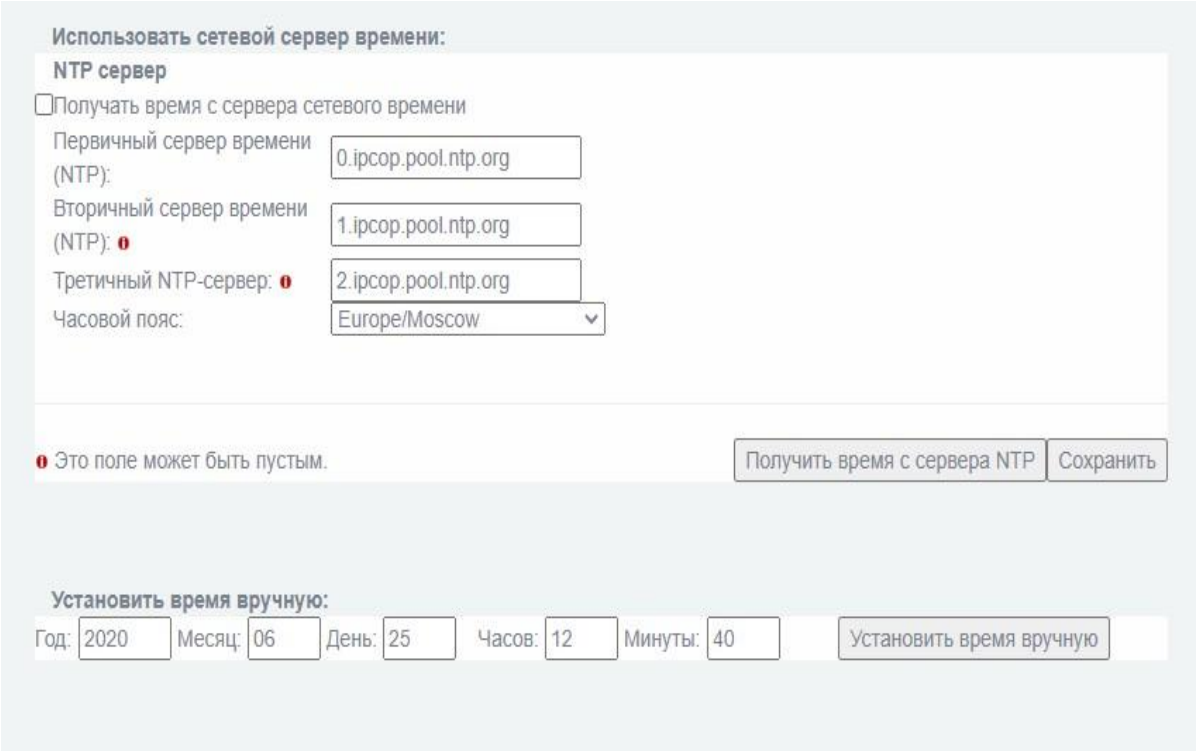


Рисунок 221 – Подраздел «Сервер времени» раздела «Службы»

В разделе следует указать сервер, который будет передавать временные метки для журналирования, для этого необходимо выполнить следующие действия:

1) поставить флажок напротив параметра «Получать время с сервера сетевого времени»;
2) заполнить текстовое поле «Первичный сервер времени (NTP)»;
3) заполнить текстовое поле «Вторичный сервер времени (NTP)» (необязательное поле);
4) заполнить текстовое поле «Третичный NTP-сервер»;
5) в ниспадающем списке «Часовой пояс» выберите город;
6) нажать кнопку «Сохранить».

Для установки времени вручную необходимо перейти в секцию «Установить время вручную» (рисунок 221).

3.4.4 Журнал межсетевого экрана

Для работы с журналом межсетевого экрана следует перейти в подраздел «Журнал межсетевого экрана» раздела «Журналы (рисунок 222).

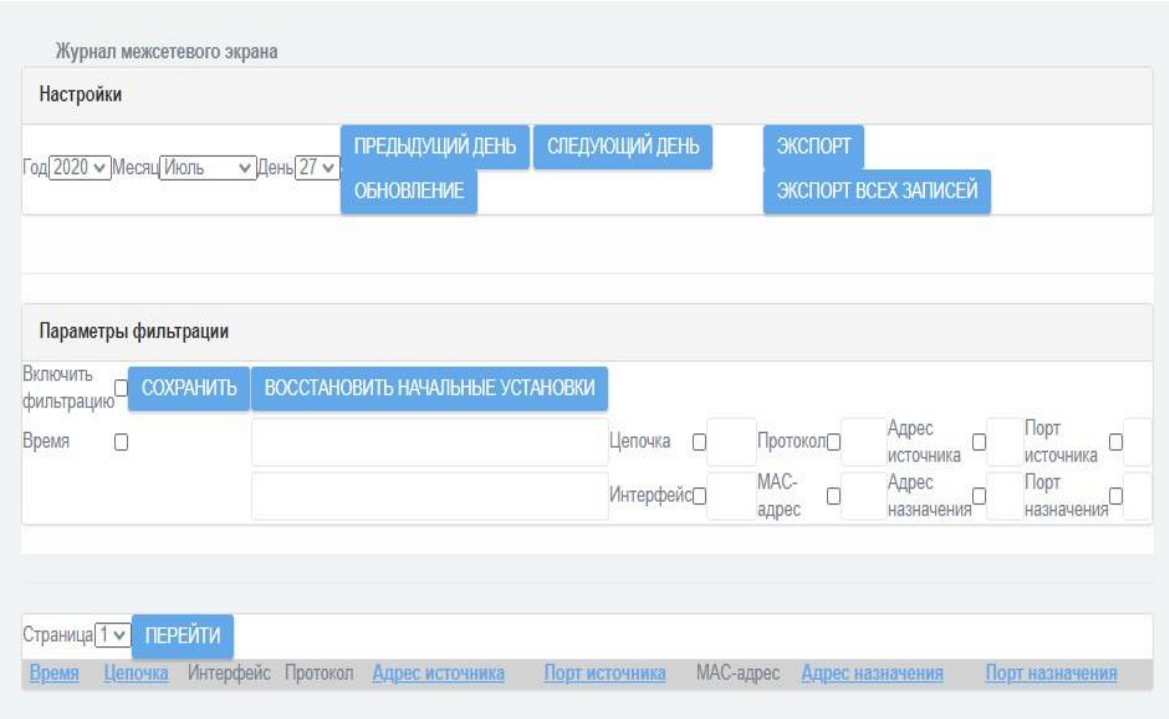


Рисунок 222 – Подраздел «Журнал межсетевого экрана» раздел «Журналы»

На странице журнала межсетевого экрана предусмотрена возможность выборочного просмотра записей. Для просмотра информации журнала, отсортированной по какому-либо параметру, необходимо включить фильтрацию. Для этого следует отметить соответствующие пункты и нажать кнопку «Сохранить».

Загрузить события из журнала можно за период, равный одним суткам. Для этого необходимо указать день и месяц текущего года (рисунок 222).

Имеется возможность ограничить промежуток времени, за который будут отображены события выбранных суток, путем выставления конкретных временных рамок (рисунок 222).

На странице журнала межсетевого экрана отображен ряд кнопок:

СЛЕДУЮЩИЙ ДЕНЬ	предназначена для перехода к странице информации на один день раньше
ПРЕДЫДУЩИЙ ДЕНЬ	предназначена для перехода к странице информации на один день позже

ОБНОВЛЕНИЕ	предназначена для обновления информации для выбранного периода времени
ЭКСПОРТ	предназначена для экспорта отсортированных данных в текстовом виде
ЭКСПОРТ ВСЕХ ЗАПИСЕЙ	предназначена для экспорта всех данных в виде архива
ВОССТАНОВИТЬ НАЧАЛЬНЫЕ УСТАНОВКИ	предназначена для сброса всех параметров фильтров

Доступны следующие параметры для настройки фильтрации журнала МЭ:

a) время;

b) цепочка;

c) интерфейс;

d) протокол;

e) адрес источника;

f) порт источника;

g) MAC-адрес;

h) адрес назначения;

i) порт назначения.

Журналы МЭ сортируются по адресу источника, порту источника и MAC-адресу.

3.4.5 Журнал обнаружения атак

Для просмотра журнала обнаружения атак СОВ необходимо перейти в подраздел «Журнал обнаружения атак» раздела «Журналы» (рисунок 223).

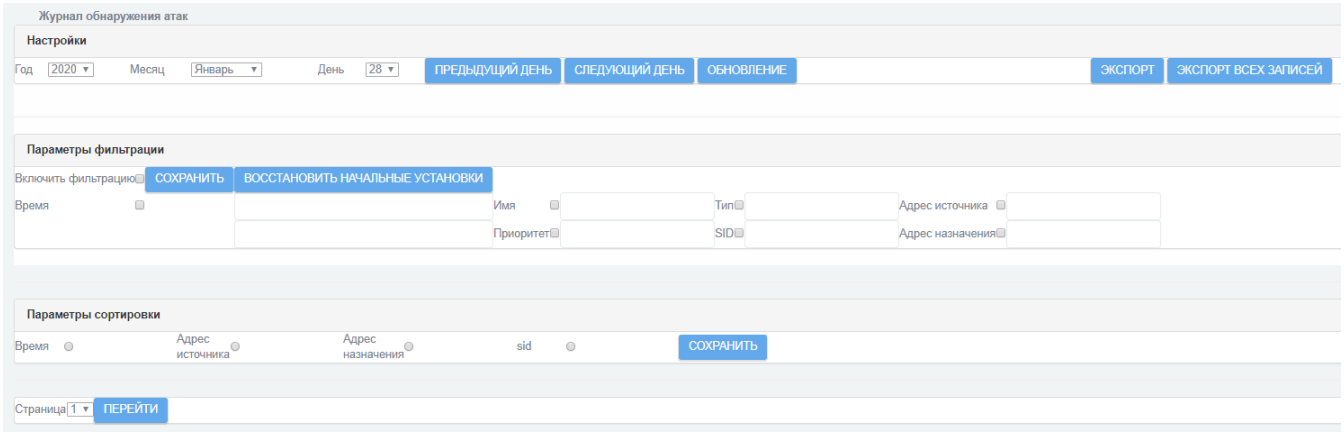


Рисунок 223 – Подраздел «Журнал обнаружения атак» раздела «Журналы»

На странице журнала обнаружения атак предусмотрена возможность выборочного просмотра записей. Для просмотра записей журнала, отсортированных по какому-либо параметру, необходимо включить фильтрацию. Для этого необходимо выбрать соответствующий параметр в поле «Параметры сортировки» и нажать кнопку «Сохранить».

Загрузить события из журнала можно по умолчанию за период, равный одним суткам. Для этого необходимо указать день и месяц текущего года (рисунок 222).

Есть возможность выбрать промежуток времени, за который будут отображены события выбранных суток, путем выставления конкретных временных рамок (рисунок 222).

На странице журнала обнаружения атак представлен ряд кнопок:

ПРЕДЫДУЩИЙ ДЕНЬ	предназначена для перехода к странице информации на один день раньше
СЛЕДУЮЩИЙ ДЕНЬ	предназначена для перехода к странице информации на один день позже
ОБНОВЛЕНИЕ	предназначена для обновления информации для выбранного периода времени
ЭКСПОРТ	предназначена для экспорта отсортированных данных в текстовом виде
ЭКСПОРТ ВСЕХ ЗАПИСЕЙ	предназначена для экспорта всех данных в виде архива
СОХРАНИТЬ	предназначена для сброса всех параметров фильтров

Доступны следующие параметры для настройки фильтрации журнала обнаружения атак:

1) имя;
2) приоритет;
3) тип;
4) SID (Security Identifier);
5) адрес источника;
6) адрес назначения.

3.4.6 Системный протокол

Для просмотра системного протокола необходимо перейти в подраздел «Системный протокол» раздел «Журналы» (рисунок 224).

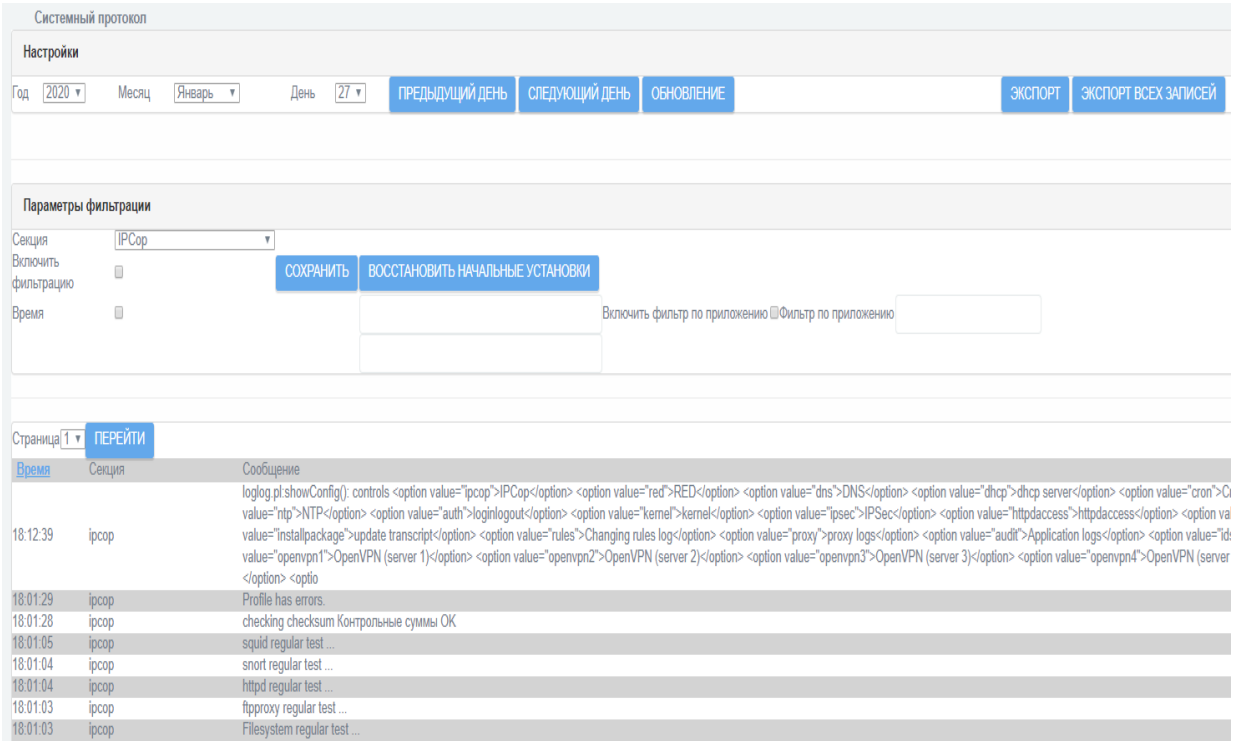
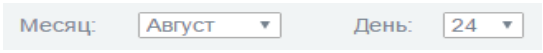
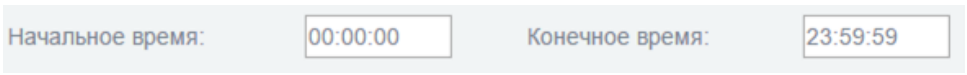
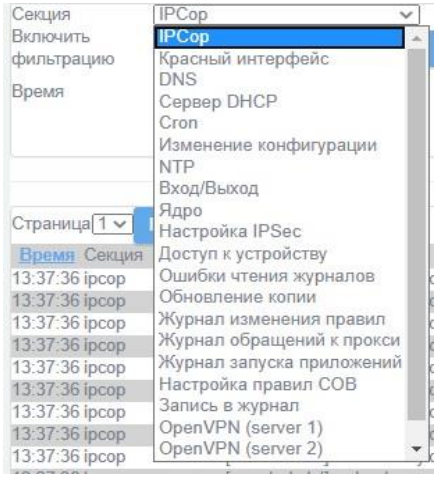


Рисунок 224 – Подраздел «Системный протокол» раздел «Журналы»

Доступны следующие параметры для настройки фильтрации системного протокола:

По дате:	
По времени:	
По секции:	

По приложению:	Фильтр по приложению: /cgi-bin/logs.cgi/config.dat

На странице системного протокола расположен ряд кнопок:

ПРЕДЫДУЩИЙ ДЕНЬ	предназначена для перехода к странице информации на один день раньше
СЛЕДУЮЩИЙ ДЕНЬ	предназначена для перехода к странице информации на один день позже
ОБНОВЛЕНИЕ	предназначена для обновления информации для выбранного периода времени
ЭКСПОРТ	предназначена для экспорта отсортированных данных в текстовом виде
ЭКСПОРТ ВСЕХ ЗАПИСЕЙ	предназначена для экспорта всех данных в виде архива
ВОССТАНОВИТЬ НАЧАЛЬНЫЕ УСТАНОВКИ	предназначена для сброса всех параметров фильтров

На рисунках 225 – 226 приведены примеры фильтрации системного протокола по секции «IPCop» и журналу запуска приложений соответственно.

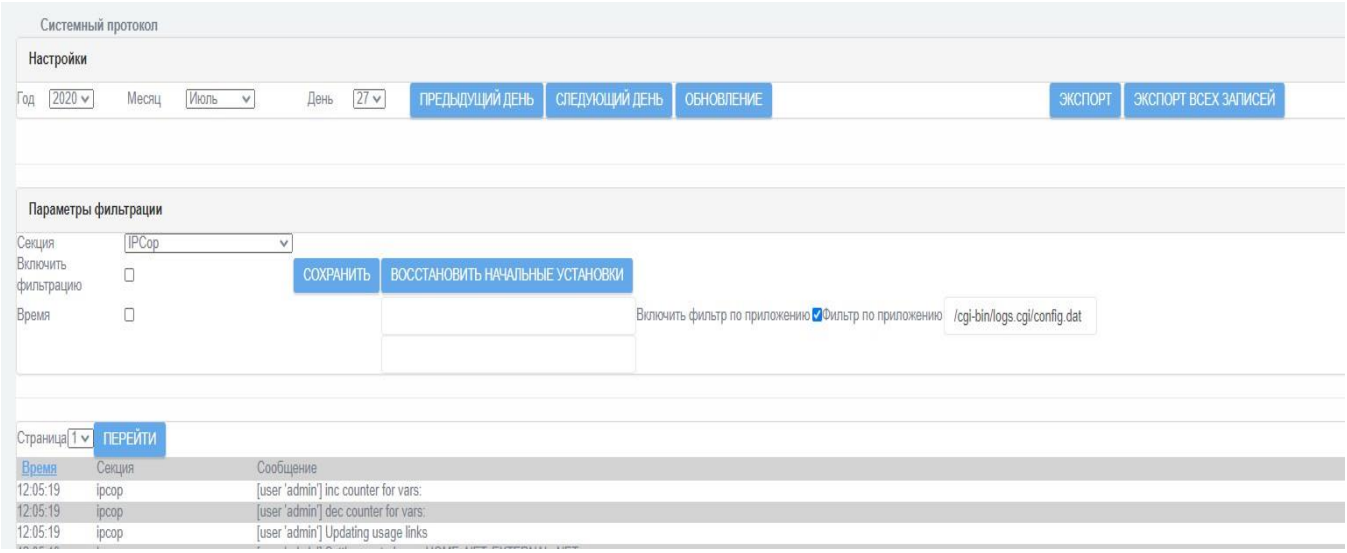


Рисунок 225 – Пример фильтрации системного протокола по секции «IPCop»

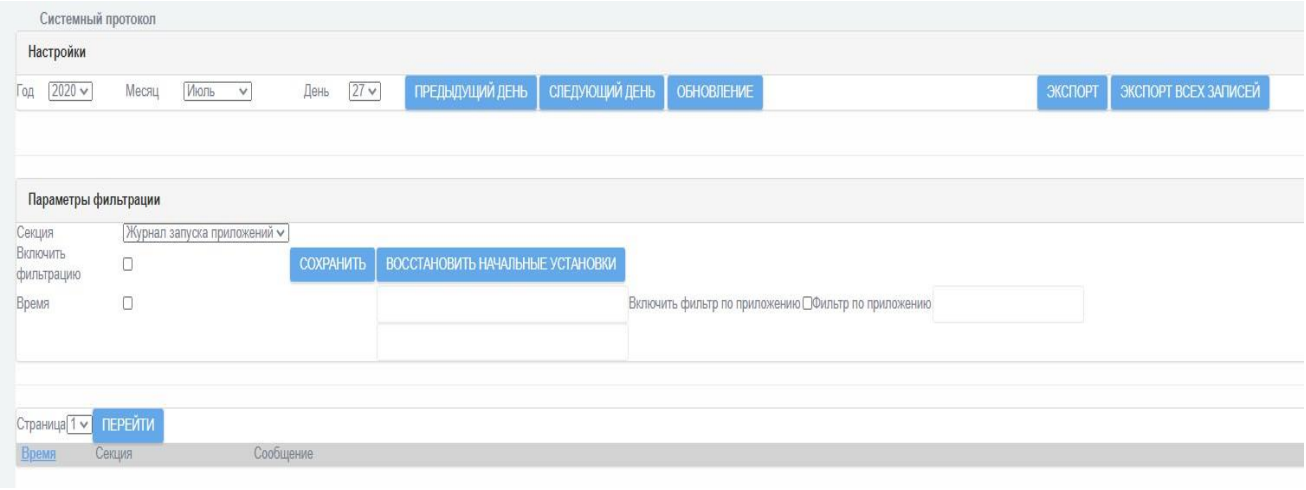


Рисунок 226 – Пример фильтрации системного протокола по секции «Журнал запуска приложений»

3.4.7 Работа с уведомлениями

В случае попыток нарушения правил и при обнаружении критичных событий безопасности в шапке веб-интерфейса отображается соответствующее сообщение. При нажатии на кнопку вы можете получить более подробную информацию о возникшей проблеме в виде всплывающего окна (рисунок 227).

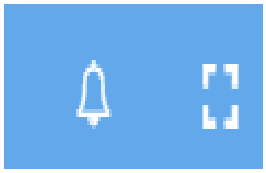


Рисунок 227 – Новые уведомления «Рубикон»

Также «Рубикон» позволяет настроить уведомление администратора об обнаруженных атаках и нарушениях правил МЭ по электронной почте. Для настройки уведомления по электронной почте необходимо перейти в подраздел «Почта» раздела «Система» (рисунок 228).

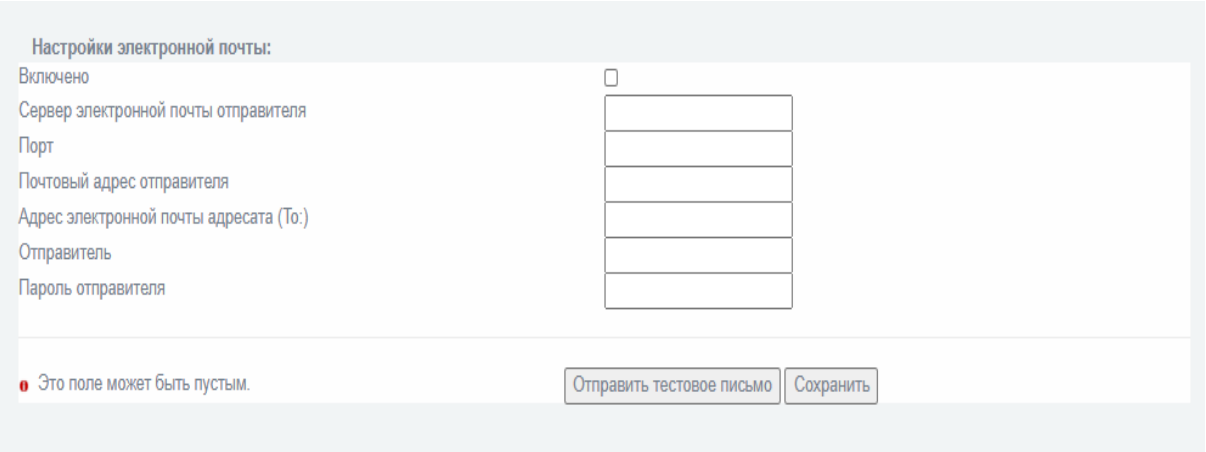


Рисунок 228 – Подраздел «Почта» раздела «Система»

Также необходимо включить параметр «email alert» в правиле МЭ для получения оповещения на электронную почту (рисунок 229).

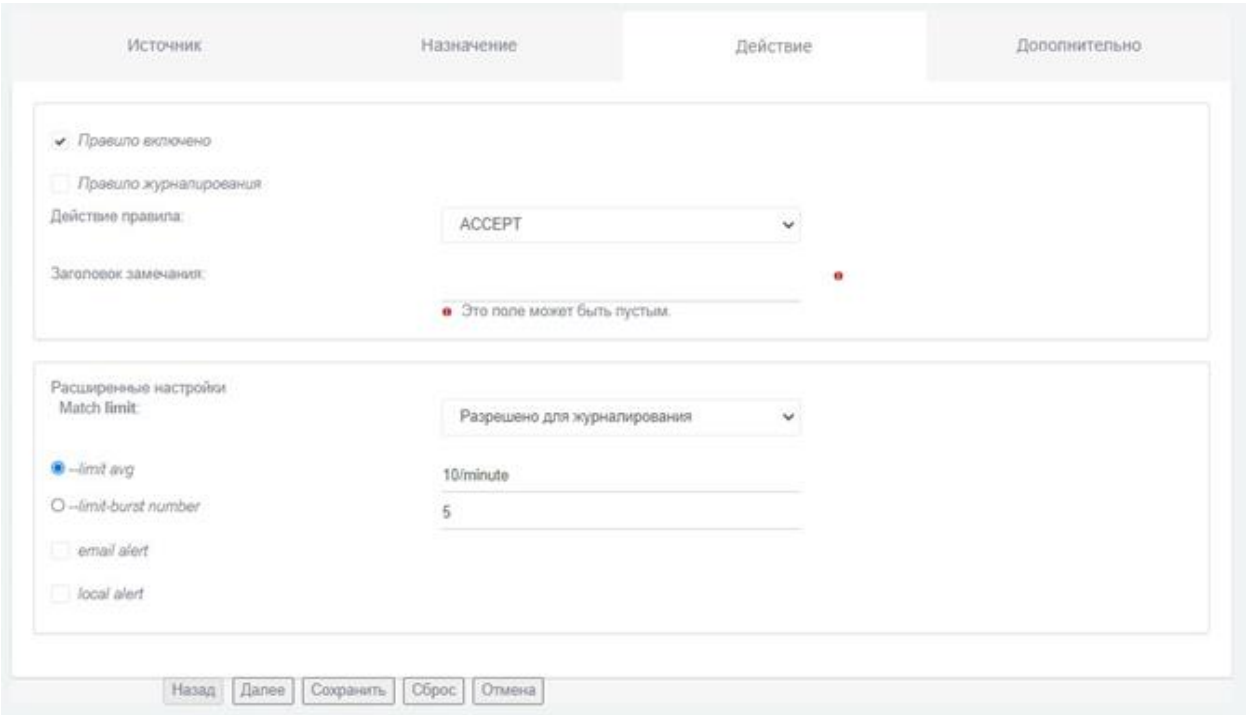


Рисунок 229 – Поле включения параметра «email alert»

Для подтверждения внесенной информации следует нажать кнопку «Сохранить». После этого уведомления об обнаруженных атаках будут приходить на электронную почту.

3.5 Настройка однонаправленного шлюза

Комплект однонаправленного шлюза состоит из двух полукомплектов, один из которых выполняет функции передатчика (далее ОШ-Tx), а второй приемника (далее ОШ-Rx). Односторонняя передача данных обеспечивается аппаратными сетевыми адаптерами соединенные между собой оптическим кабелем.

Однонаправленный шлюз может функционировать в двух режимах:

- в режиме маршрутизатора для передачи сетевых пакетов в одну сторону по средствам маршрутизации от ОШ-Tx к ОШ-Rx (данный режим работы применим к сетевому взаимодействию, который **не требует ответов на отправленные сетевые пакеты, либо установления соединения**);
- передачи файлов с одного ftp-сервера (далее ftp-сервер-Tx) подключенного к ОШ-Tx на второй ftp-сервер (далее ftp-сервер-Rx) подключенного к ОШ-Rx.

Для настройки однонаправленного шлюза **в режиме маршрутизации сетевых пакетов**, необходимо выполнить следующие действия:

1. на странице **«Система» → «Интерфейсы»** для ОШ-Tx и ОШ-Rx произвести настройку сетевой адресации для корректной маршрутизации сетевых пакетов, для этого необходимо задать **IP-адреса сетевым интерфейсам**, включая и интерфейс однонаправленного шлюза (имя сетевого интерфейса в системе — **diode0**) (рисунок 230);

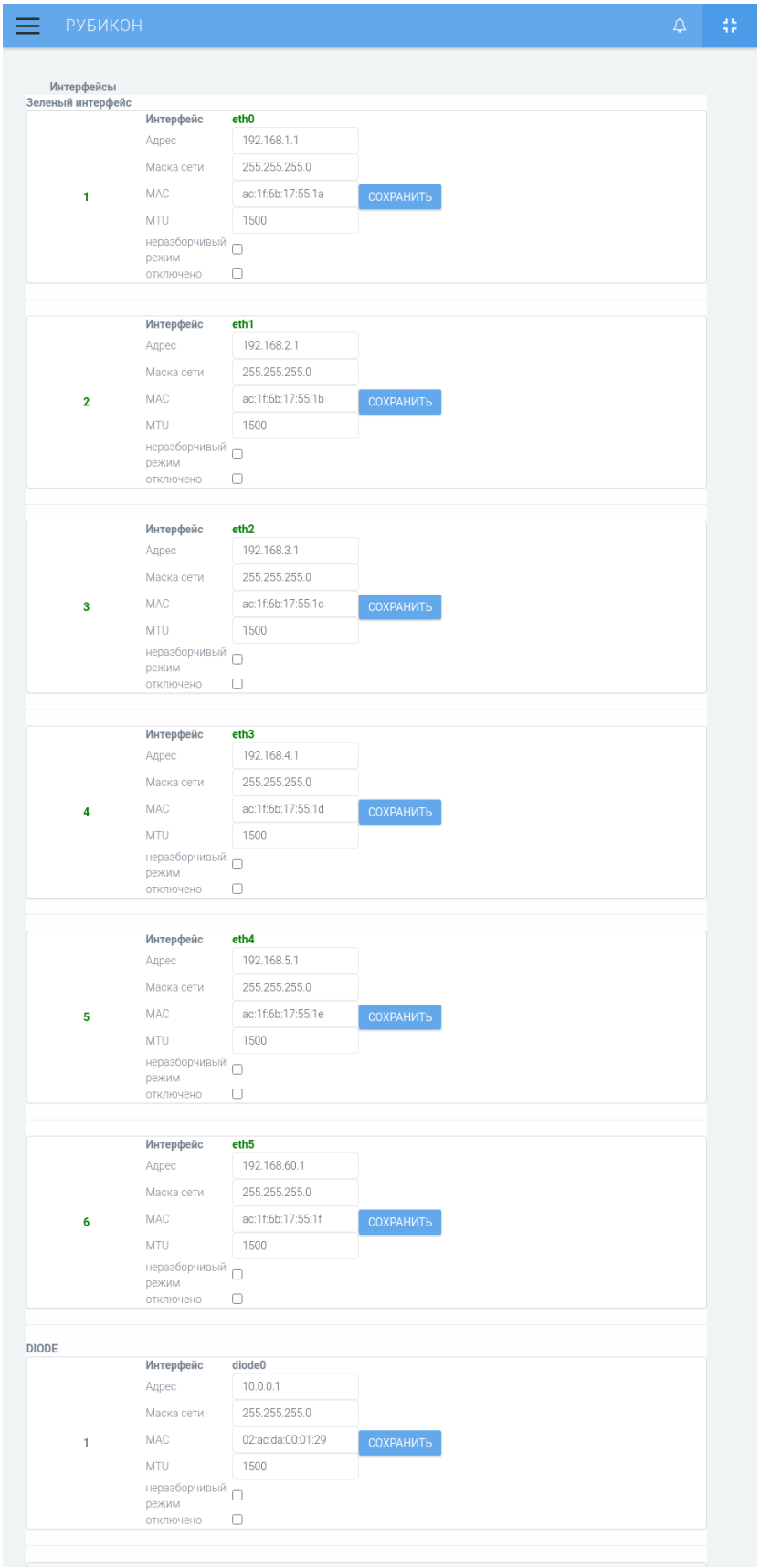


Рисунок 230 – настройка IP-адресов сетевого адаптера

2. включить **расширенный режим** настройки межсетевого экрана (рисунок 231)

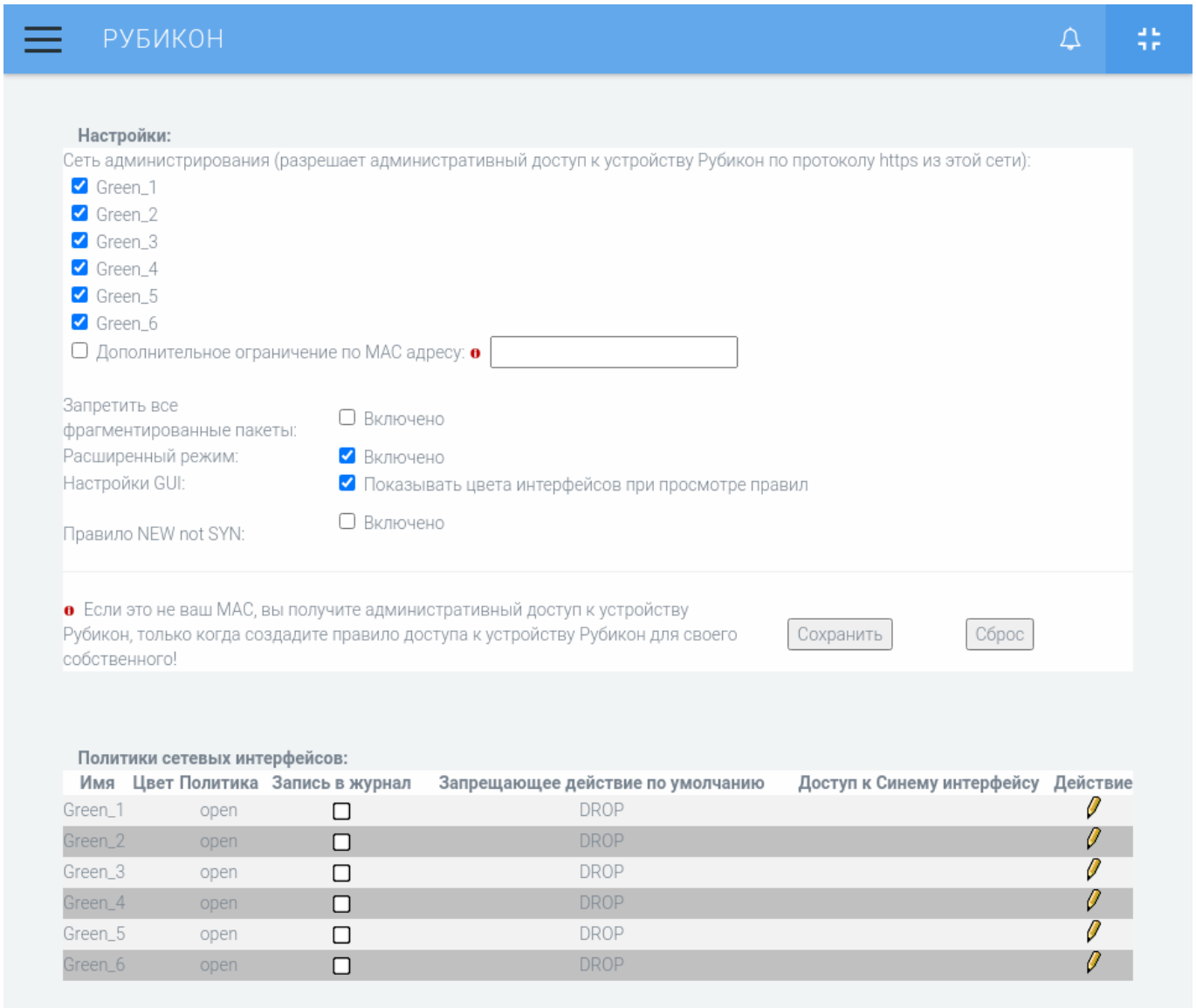


Рисунок 231 – Включение расширенного режима настройки межсетевого экрана

3. на странице **«Межсетевой экран» → «Интерфейсы по умолчанию» добавить** для ОШ-Tx и ОШ-Rx **сетевой интерфейс однонаправленного шлюза** (имя сетевого интерфейса в системе — **diode0**) в список интерфейсов, используемых в составлении правил межсетевого экрана и марш-рутизации (рисунок 232);

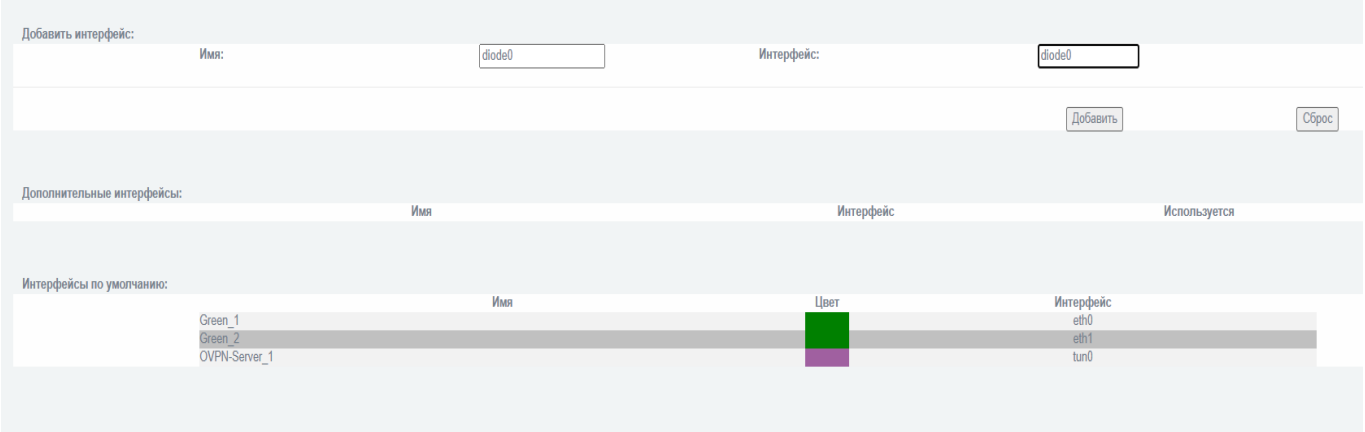


Рисунок 232 – Добавление сетевого интерфейса в список интерфейсов

4. **добавить** на странице **«Сеть» → «Конфигурация ARP»** ОШ-Tx и ОШ-Rx **MAC-адрес противоположного устройства** (для ОШ-Tx — MAC-адрес сетевого интерфейса diode0 ОШ-Rx, а для ОШ-Rx — MAC-адрес сетевого интерфейса diode0 ОШ-Tx) в **ARP-таблицу** (рисунок 233);

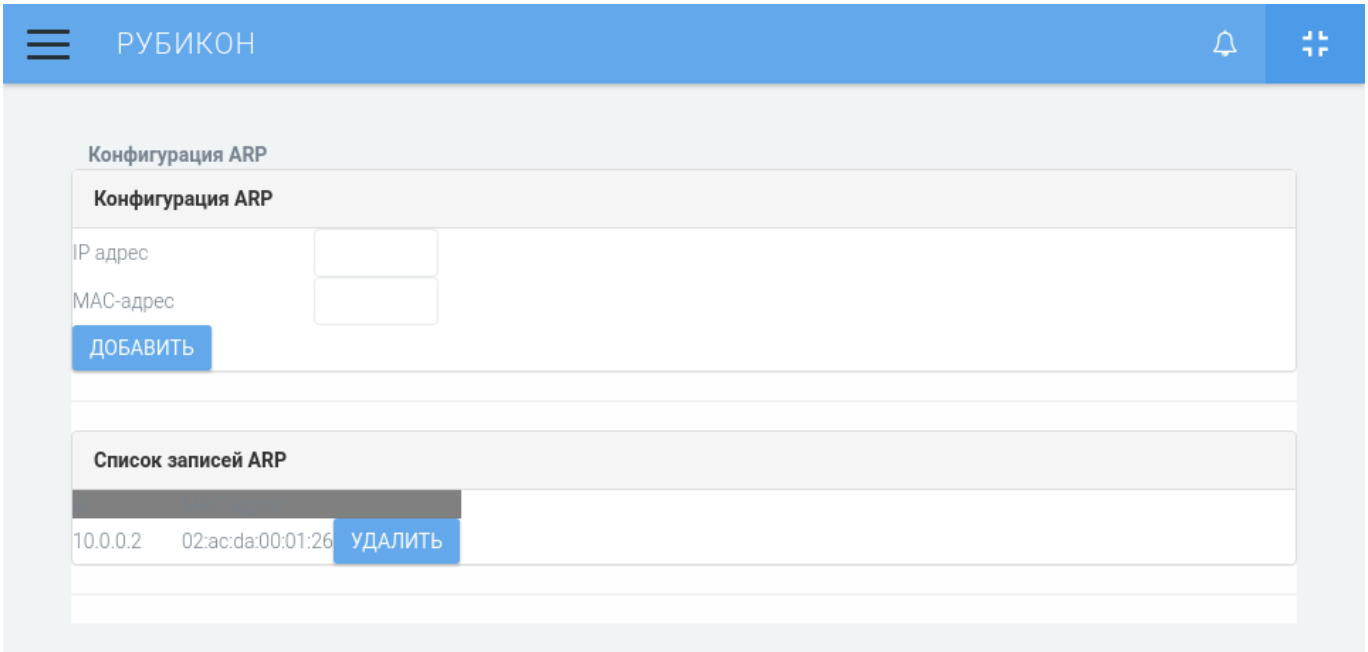


Рисунок 233 – Добавление MAC-адреса противоположного устройства

5. **добавить** на странице **«Сеть» → «Маршруты»** ОШ-Tx маршрут до удаленной сети/узла через однонаправленный шлюз, для ОШ-Rx добавлять маршрут в обратном направлении не нужно, поскольку сетевые пакеты не будут проходить в обратном направлении (рисунок 234);

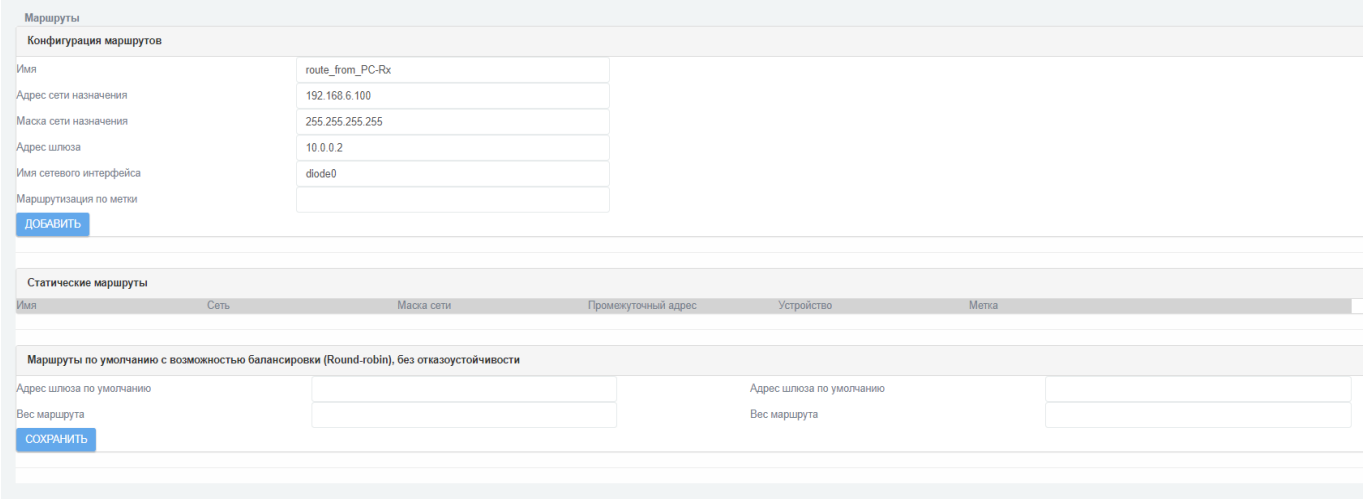


Рисунок 234 – Добавление маршрута до удаленного узла

6. на странице **«Состояние» → «Состояние сети»** для ОШ-Tx и ОШ-Rx проверить корректность сетевых настроек (IP-адресации сетевых интерфейсов, маршрутизации и ARP-таблицы) (рисунок 235);

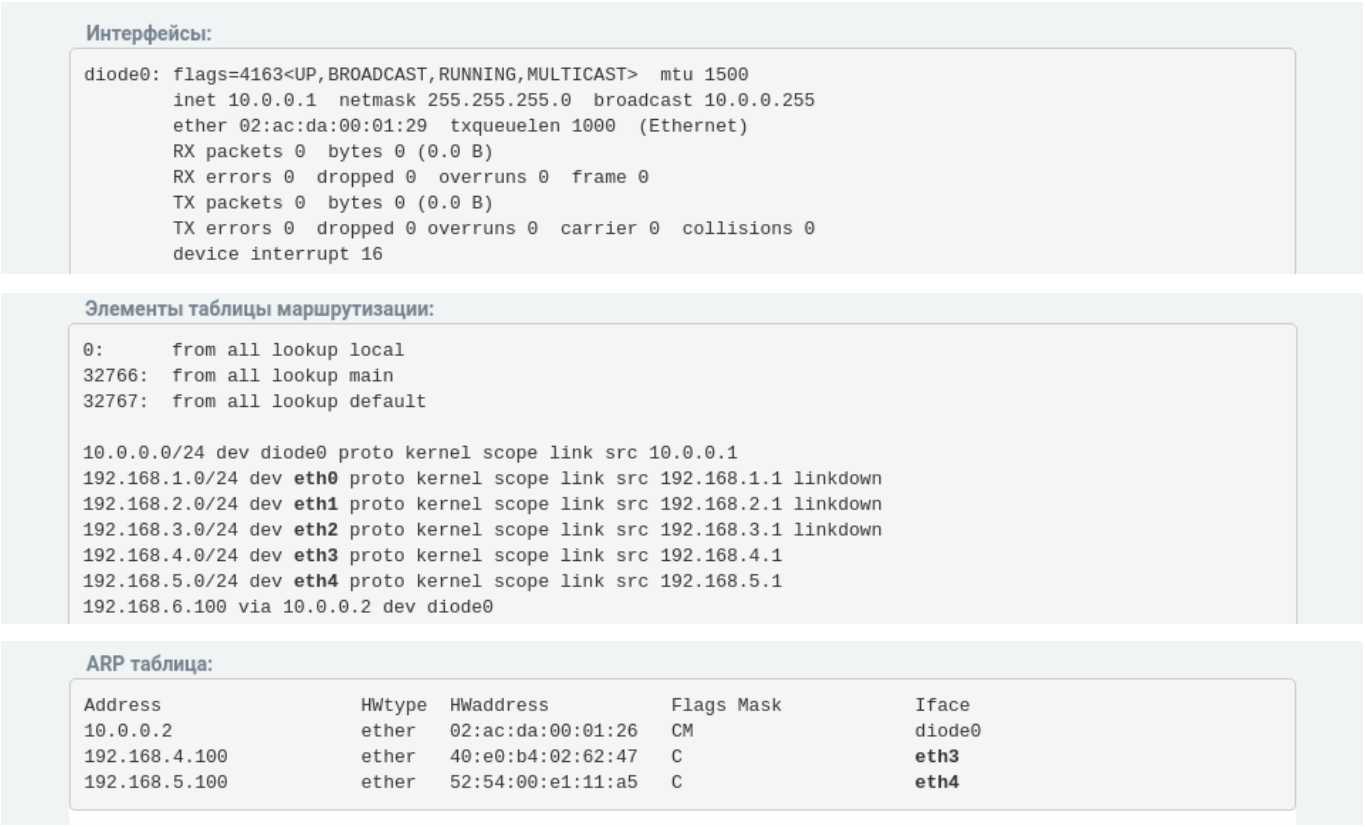


Рисунок 235 – Проверка сетевых настроек

7. для прохождения сетевых пакетов необходимо **добавить правила межсетевого экрана**:

- на **ОШ-Tx правило межсетевого экрана** в разделе **«Другие из внутренней сети во внешнюю»**, **разрешающее прохождение сетевых пакетов**, приходящих на сетевой интерфейс

ОШ-Tx и маршрутизируемых на сетевой интерфейс однонаправленной передачи данных, **согласно соответствующим параметрам сетевого пакета** (параметры зависят от политики безопасности прохождения пакетов) (рисунок 242);

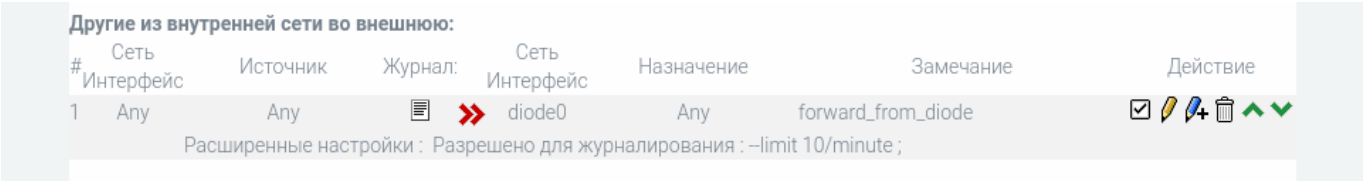


Рисунок 236 – Добавление на ОШ-Tx правила межсетевого экрана

- на **ОШ-Rx правило межсетевого экрана** в разделе **«Другие из внутренней сети во внешнюю»**, **разрешающее прохождение сетевых пакетов**, приходящих на интерфейс однонаправленной передачи данных ОШ-Rx и маршрутизируемых на сетевой интерфейс, **согласно соответствующим параметрам сетевого пакета** (параметры зависят от политики безопасности прохождения пакетов) (рисунок 237);

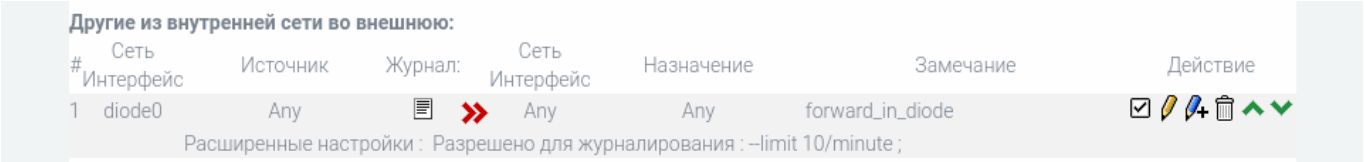


Рисунок 237 – Добавление на ОШ-Rx правила межсетевого экрана

8. на странице **«Состояние» → «Настройки IPTables»** проверить корректность настройки правил межсетевого экрана (рисунок 238, рисунок 239);

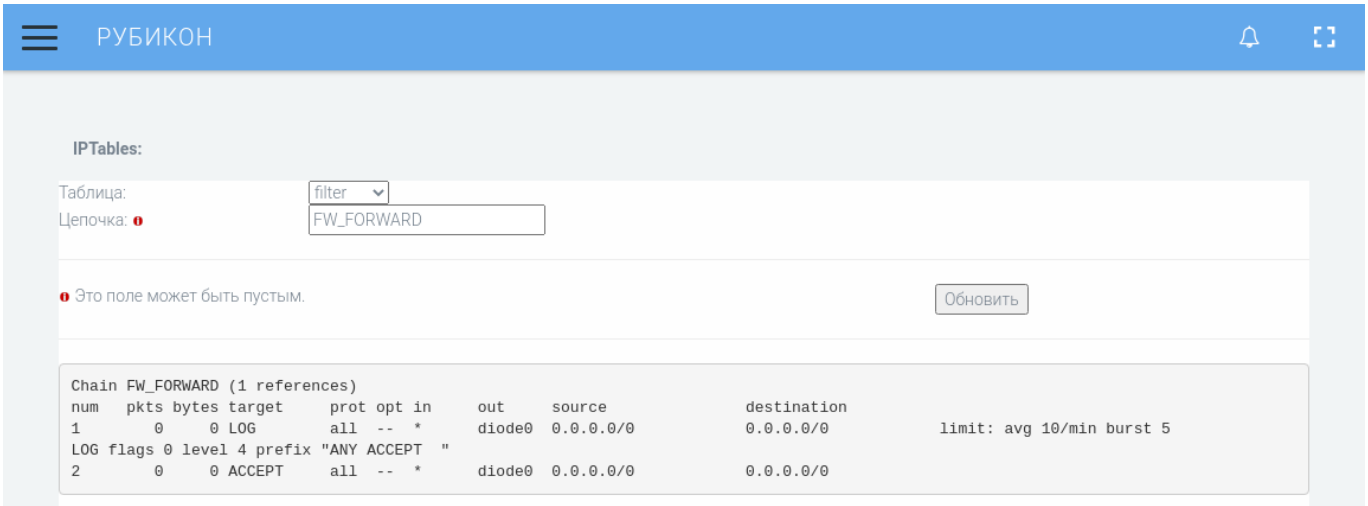


Рисунок 238 – настройка правил межсетевого экрана ОШ-Tx

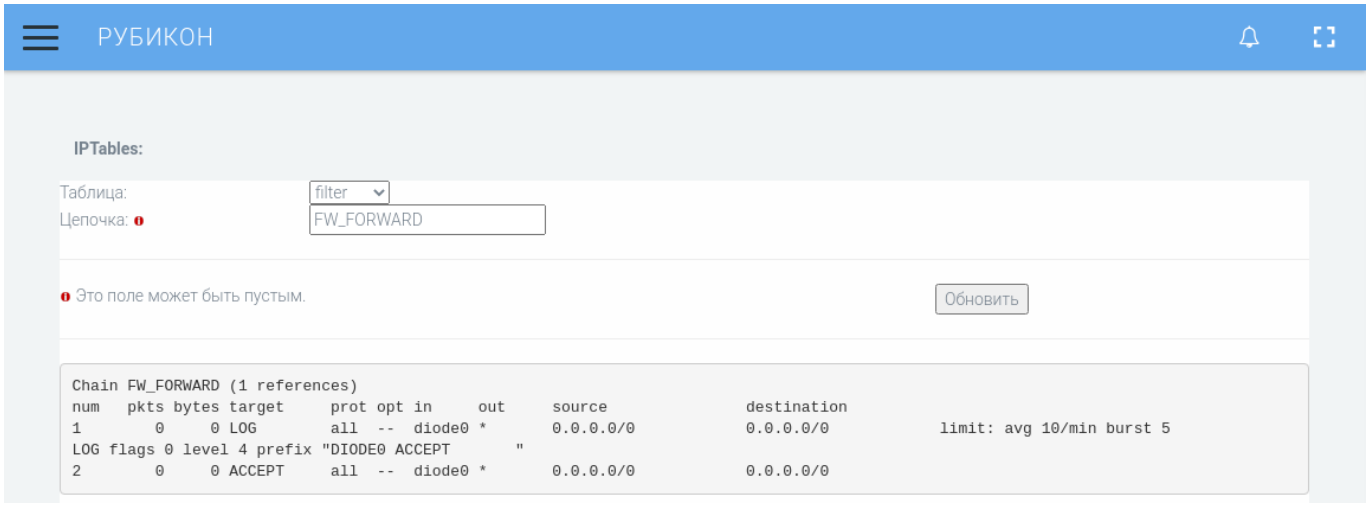


Рисунок 239 – настройка правил межсетевого экрана ОШ-Rx

Для настройки однонаправленного шлюза **в режиме передачи файлов от ftp-сервера-Tx до ftp-сервера-Rx**, необходимо выполнить следующие действия:

1. на странице **«Система» → «Интерфейсы»** для ОШ-Tx и ОШ-Rx произвести настройку сетевой адресации, для этого необходимо задать **IP-адреса сетевым интерфейсам**, включая и интерфейс однонаправленного шлюза (имя сетевого интерфейса в системе — **diode0**) (рисунок 240);

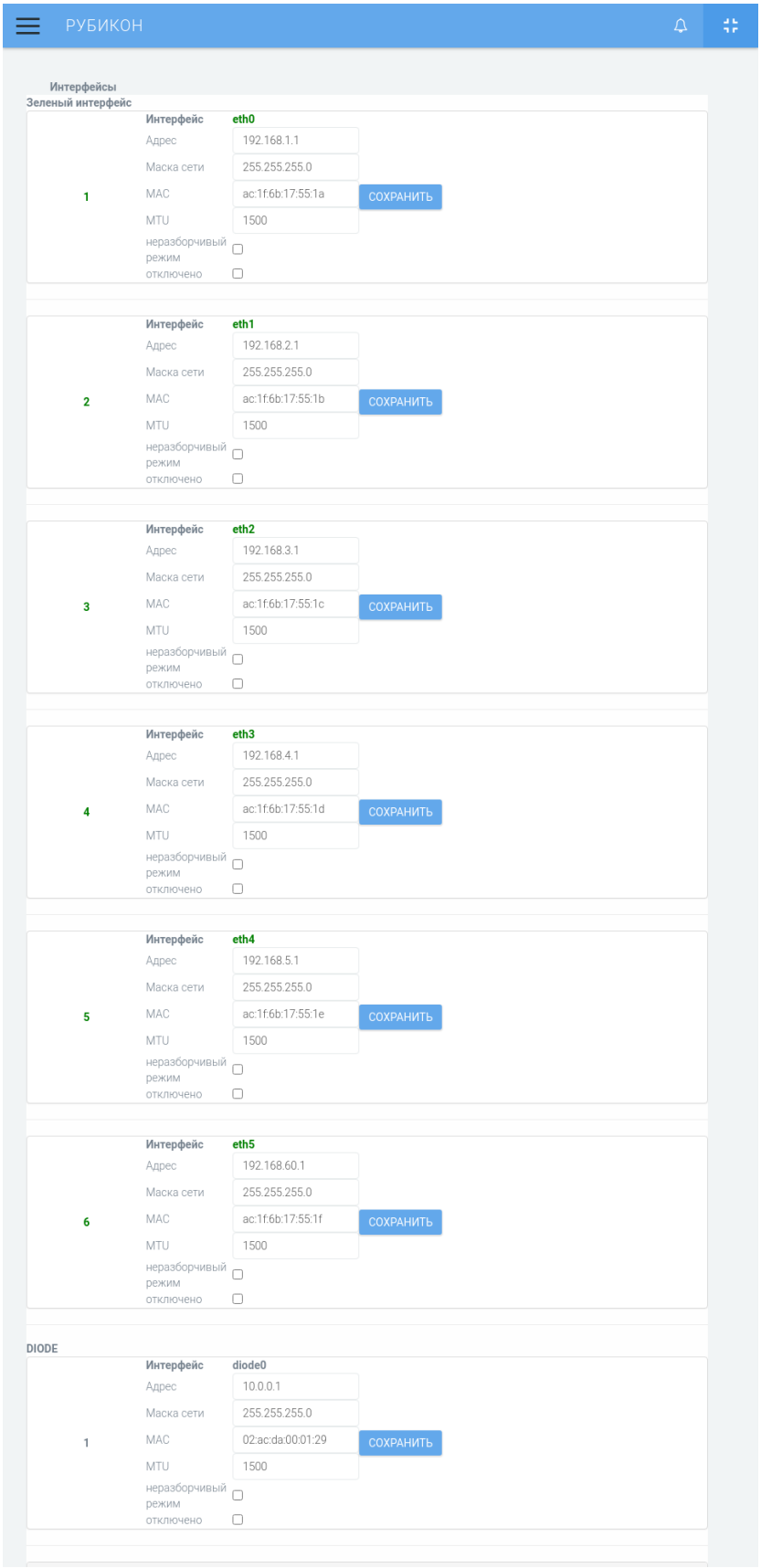


Рисунок 240 – настройка IP-адресов сетевого адаптера

2. включить **расширенный режим** настройки межсетевого экрана (рисунок 241)

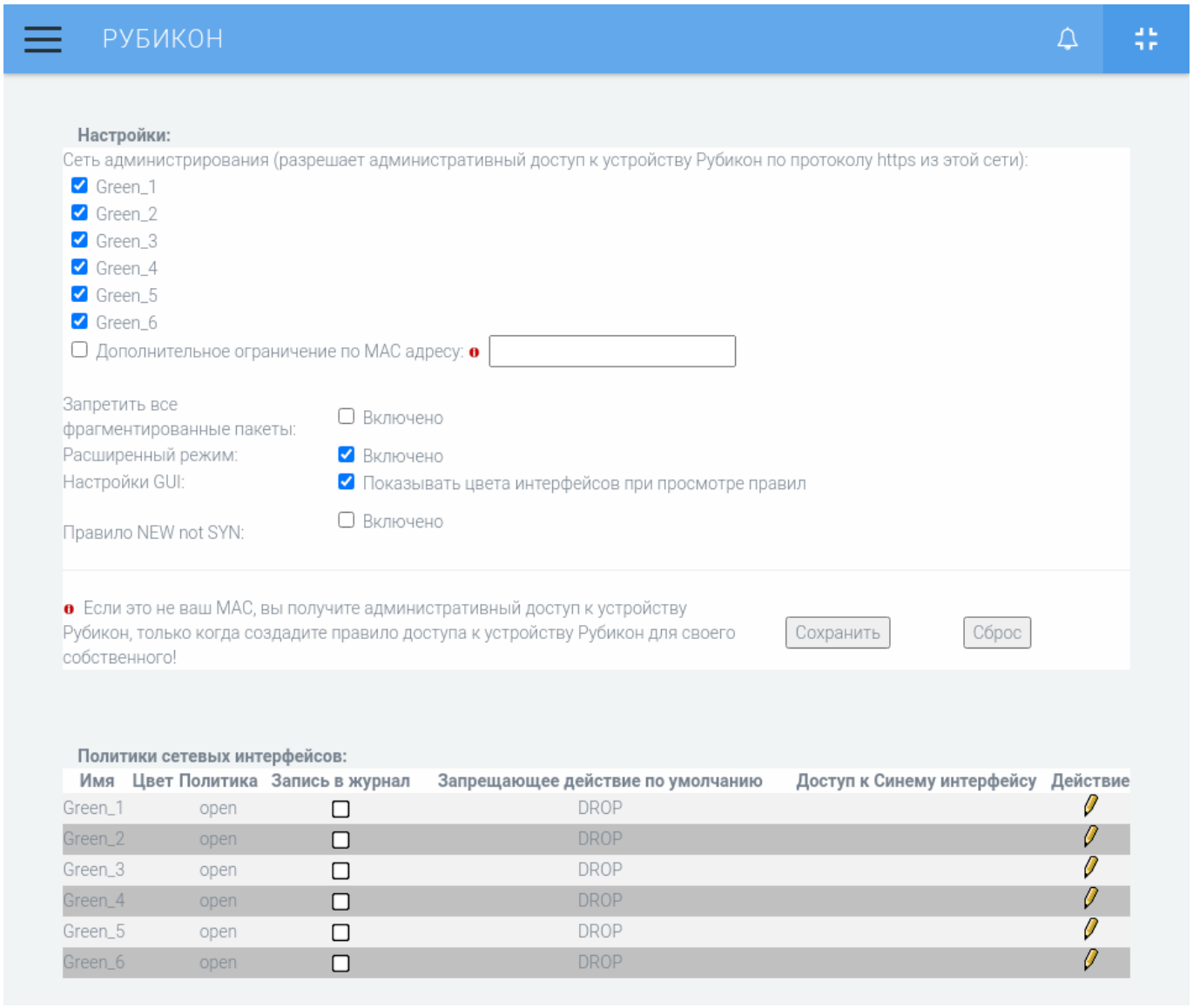


Рисунок 241 – Включение расширенного режима настройки межсетевого экрана

3. на странице **«Межсетевой экран» → «Интерфейсы» добавить** для ОШ-Rx **сетевой интерфейс однонаправленного шлюза** (имя сетевого интерфейса в системе **— diode0**) в список интерфейсов, используемых в составлении правил межсетевого экрана (рисунок 242);

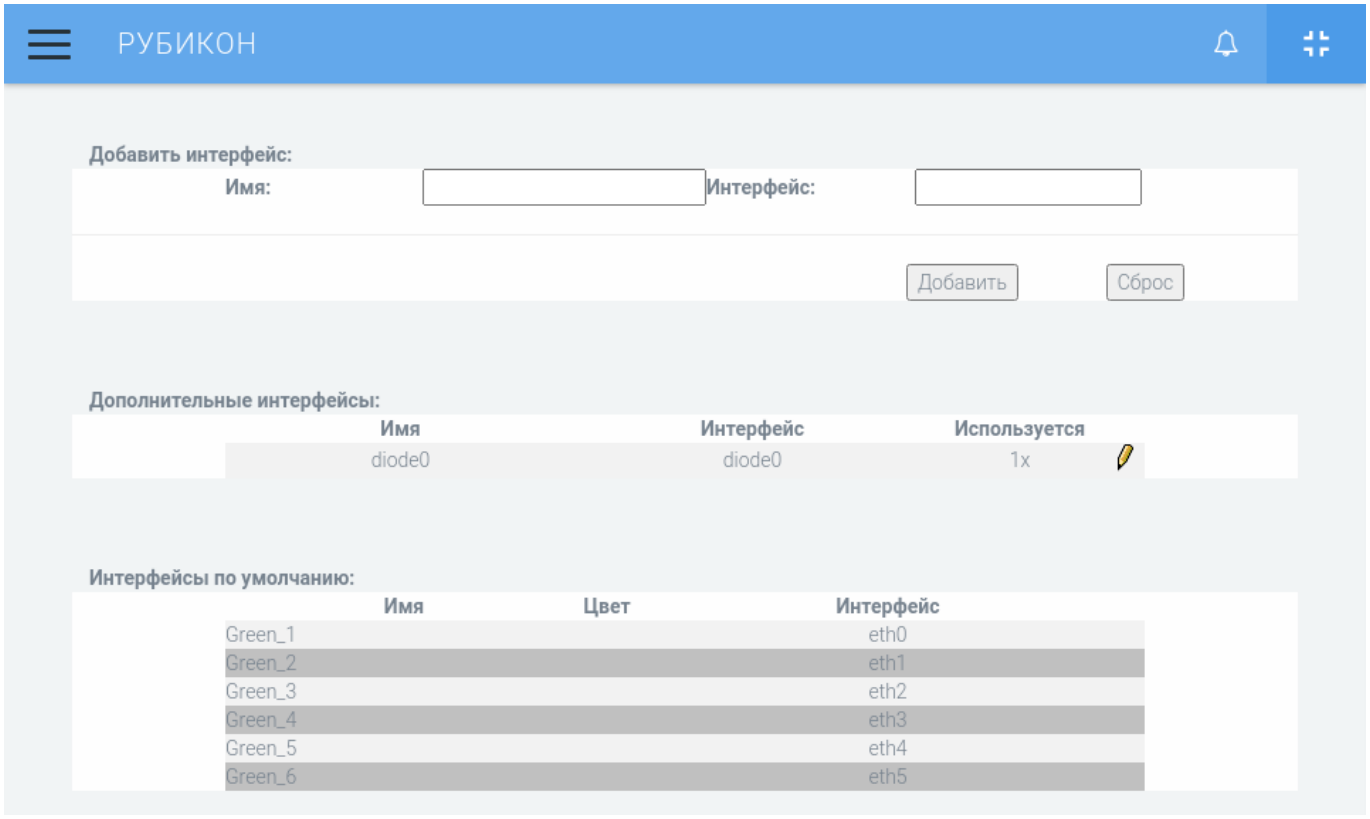


Рисунок 242 – Добавление сетевого интерфейса в список интерфейсов

4. **добавить** на странице **«Сеть» → «Конфигурация ARP»** ОШ-Tx и ОШ-Rx **MAC-адрес дополнительного устройства** (для ОШ-Tx — MAC-адрес сетевого интерфейса diode0 ОШ-Rx, а для ОШ-Rx — MAC-адрес сетевого интерфейса diode0 ОШ-Tx) в **ARP-таблицу** (рисунок 243);

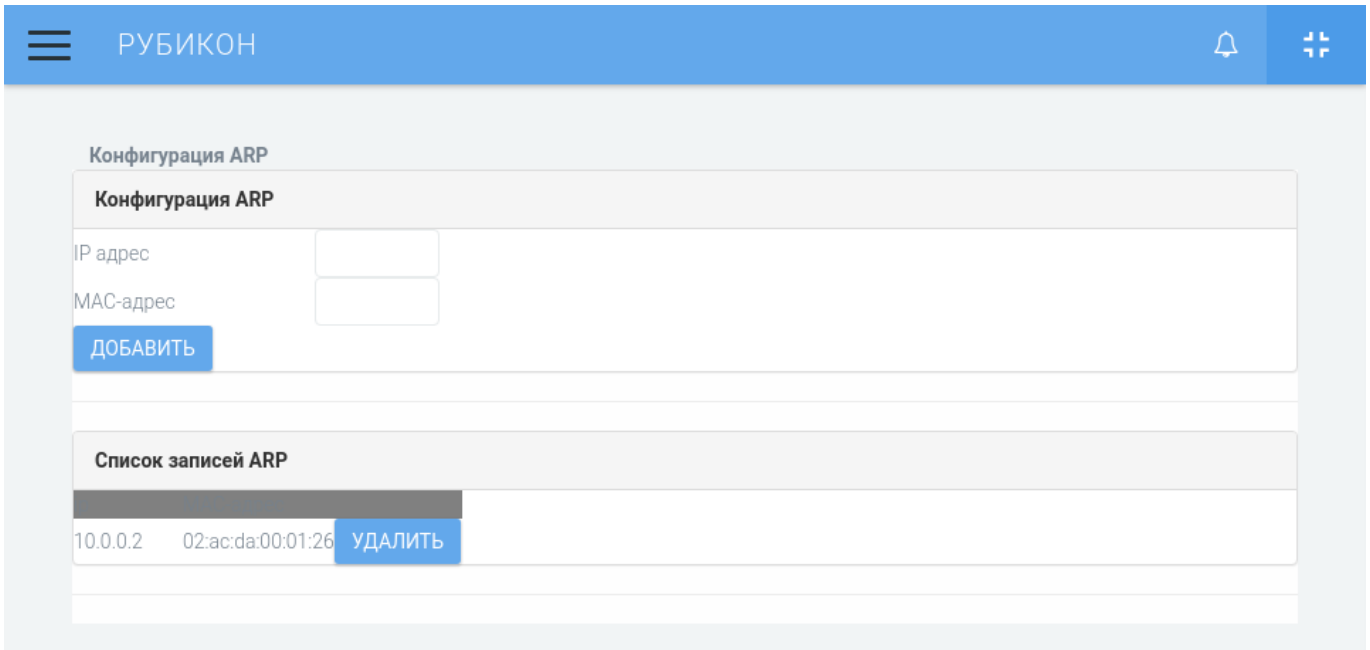


Рисунок 243 – Добавление MAC-адреса дополнительного устройства

5. на странице **«Состояние» → «Состояние сети»** для ОШ-Tx и ОШ-Rx проверить корректность сетевых настроек (IP-адресации сетевых интерфейсов, маршрутизации и ARP-таблицы) (рисунок 244);

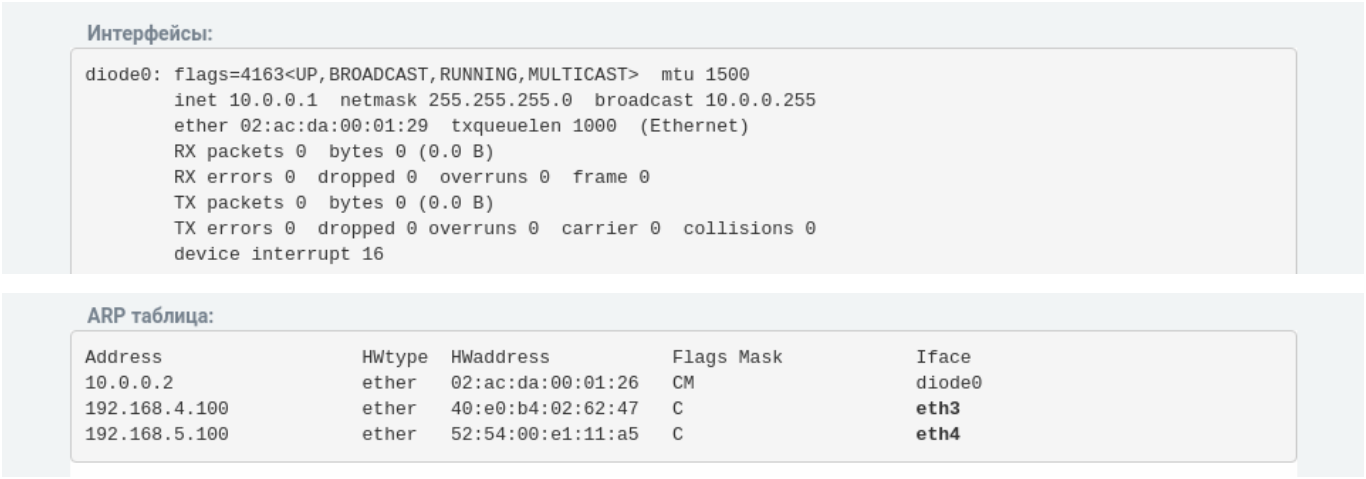


Рисунок 244 – Проверка сетевых настроек

6. для приема сетевых пакетов необходимо **добавить правило межсетевого экрана**:

- на **ОШ-Rx правило межсетевого экрана** в разделе **«Доступ к устройству»**, **разрешающее прием сетевых пакетов**, приходящих на интерфейс однонаправленной передачи данных ОШ-Rx, **согласно соответствующим параметрам сетевого пакета** (параметры зависят от политики безопасности прохождения пакетов) (рисунок 245);

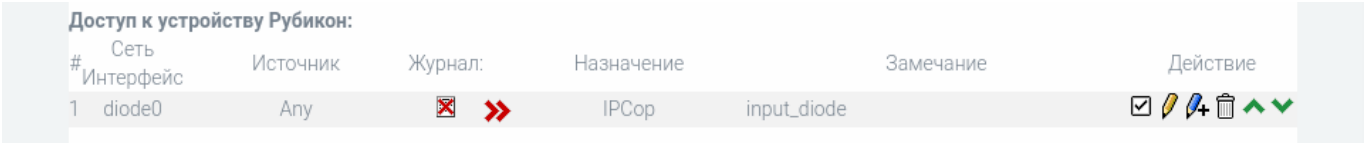


Рисунок 245 – Добавление на ОШ-Rx правила сетевого экрана

7. на странице **«Состояние» → «Настройки IPTables»** проверить корректность настройки правил межсетевого экрана (рисунок 246);

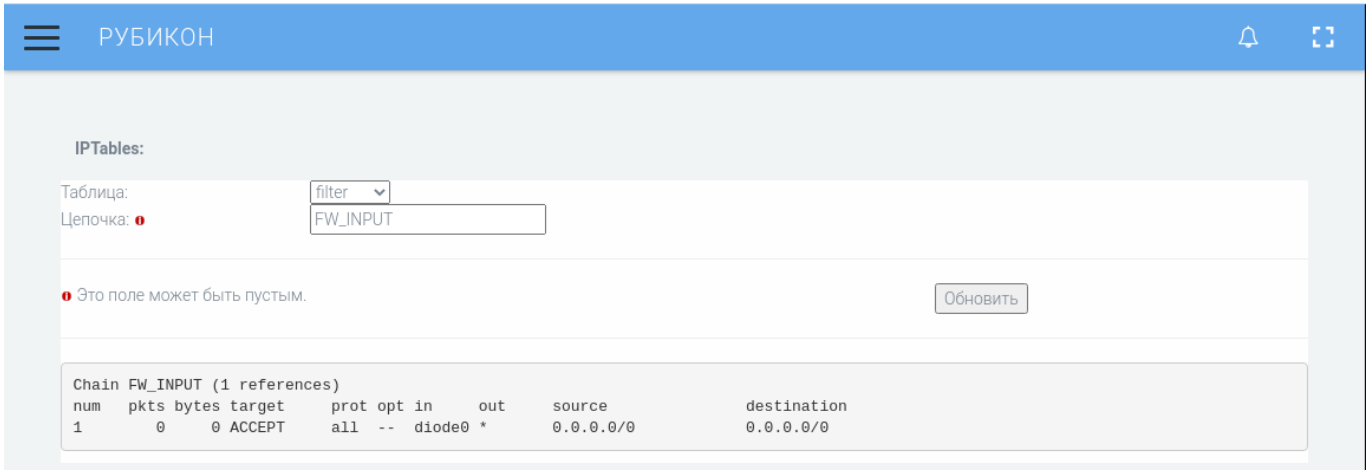


Рисунок 246 – настройка правил межсетевого экрана ОШ-Rx

8. Согласно документации на используемый ftp-сервер, произвести настройку ftp-сервера-Tx и ftp-сервера-Rx для подключения ОШ-Tx и ОШ-Rx к ним**. Пример настройки ftp-сервера vsftpd:**

```
# Example config file /etc/vsftpd.conf
listen=YES
listen_ipv6=NO
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in  your  local  time  zone.  The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# You may fully customise the login banner string:
ftpd_banner=Welcome to blah FTP service.
#
# This option should be the name of a directory which is empty.  Also, the
```

```
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
```

В качестве учетной записи будем использовать учетную запись пользователя с домашней директорией в /home/user

9. для взаимодействия с ftp-сервером-Tx и ftp-сервером-Rx необходимо **выполнить следующую настройку**:

- на странице **ОШ-Tx «Сеть» → «Однонаправленный шлюз»** произвести настройку взаимодействия с **ftp-сервером-Tx** (рисунок 247);

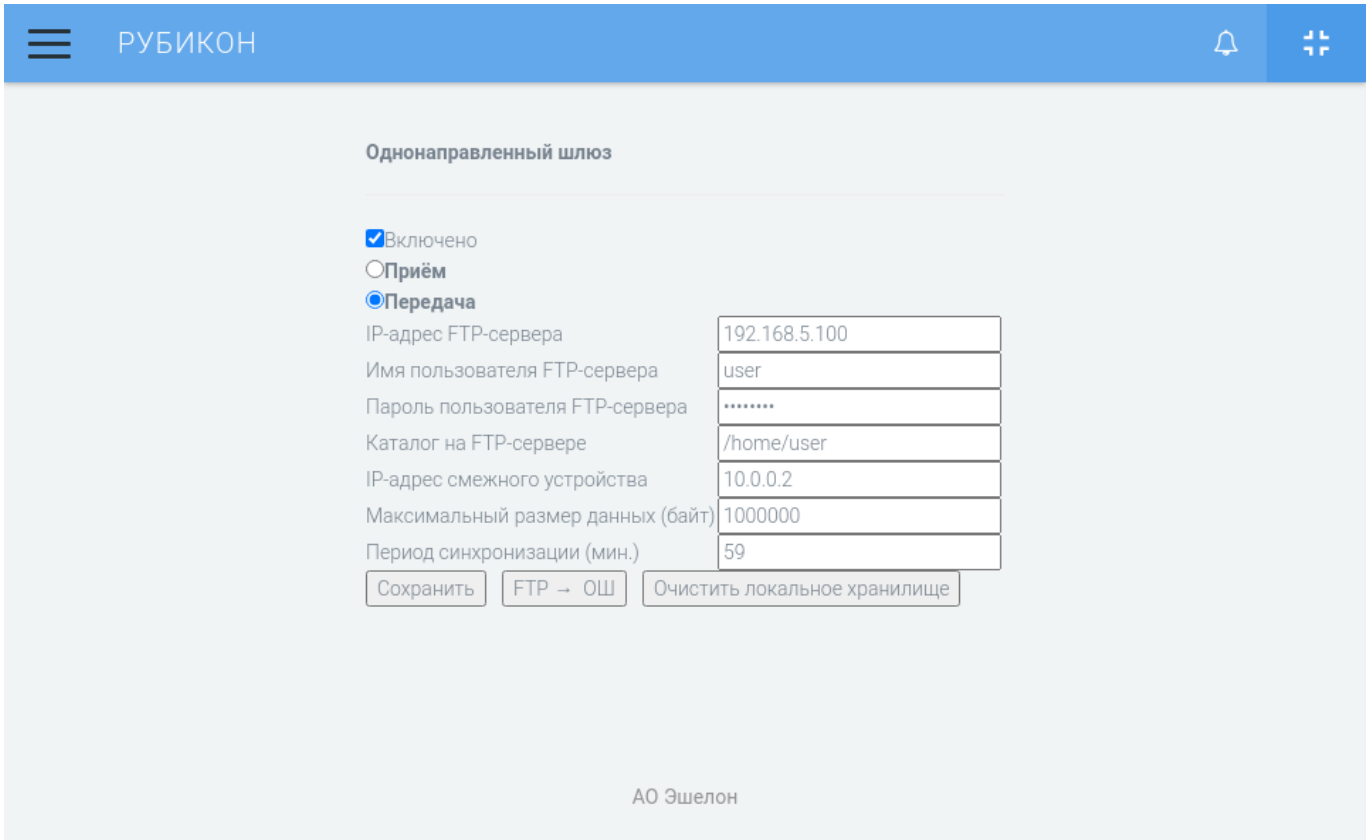


Рисунок 247 – настройка взаимодействия ОШ-Tx с ftp-сервером-Tx

Параметр	Описание
Включено	Для **включения** функции передачи файлов установить элемент **«Включено»**, для **выключения** функции передачи файлов — **сбросить данный элемент**
Тип сетевого адаптера	**установить тип** сетевого адаптера (**приемник (ОШ-Tx)** или **передатчик (ОШ-Rx)**) для однонаправленной передачи
IP-адрес сервера	**указать адрес FTP-сервера** с которого (для передающего устройства) или на который (для приемного устройства) будут скачены или загружены файлы
Имя пользователя сервера	**указать параметры учетной записи** (имя учетной записи и пароль) **соответствующего FTP-сервера** для подключения к ftp-серверу с целью скачивания файлов (для передающего устройства) и загрузки файлов (для принимающего устройства)
Пароль пользователя	**указать адрес FTP-сервера** с которого (для передающего устройства) или на который (для приемного устройства) будут скачены или загружены файлы
Каталог на сервере	**указать каталог FTP-сервера**, из которого (для передающего устройства) или в который (для приемного) будут скачены или загружены файлы **указать IP-адрес дополнительного устройства** (для ОШ-Tx — IP-адрес ОШ-Rx, а для ОШ-Rx — IP-адрес ОШ-Tx)
IP-адрес дополнительного устройства	
Максимальный размер данных (байт)	для **ОШ-Tx** указать **максимальный размер одного файла для передачи** (зависит от размера каталога **«/store»** в разделе **«Использование диска»** страницы **«Состояние» → «Состояние системы»** и не должно превышать этот размер). На **ОШ-Rx** этот параметр **не указывается**. При **смене типа устройства** (с приемного на передающее), **данные о максимальном размере данных не заполняются автоматически и требуют ручного ввода**
Период синхронизации (мин.)	указать **временной интервал для периодического обращения ОШ-Tx к FTP-серверу-Tx** в целях определения наличия новых файлов для передачи. **Период синхронизации — целое число минут в диапазоне от 1 до 59 минут**. На **ОШ-Rx** этот параметр **не указывается**. При **смене типа устройства** (с приемного на передающее), **данные о периоде синхронизации не заполняются автоматически и требуют ручного ввода**

Сохранить	для **применения введенных данных** необходимо нажать кнопку **«Сохранить»**
Скачать	для принудительного **обращения ОШ-Тх к FTP-серверу-Тх** необходимо нажать кнопку **«Скачать»**
Очистить локальный хранилище	Для **очистки локального хранилища файлов («/store») и истории загруженных файлов** (по которой определяется необходимость получения новых файлов с FTP-сервера) необходимо нажать кнопку **«Очистить локальное хранилище»**

- на странице **ОШ-Rx «Сеть» → «Однонаправленный шлюз»** произвести настройку взаимодействия с **ftp-сервером-Rx** (рисунок 248);

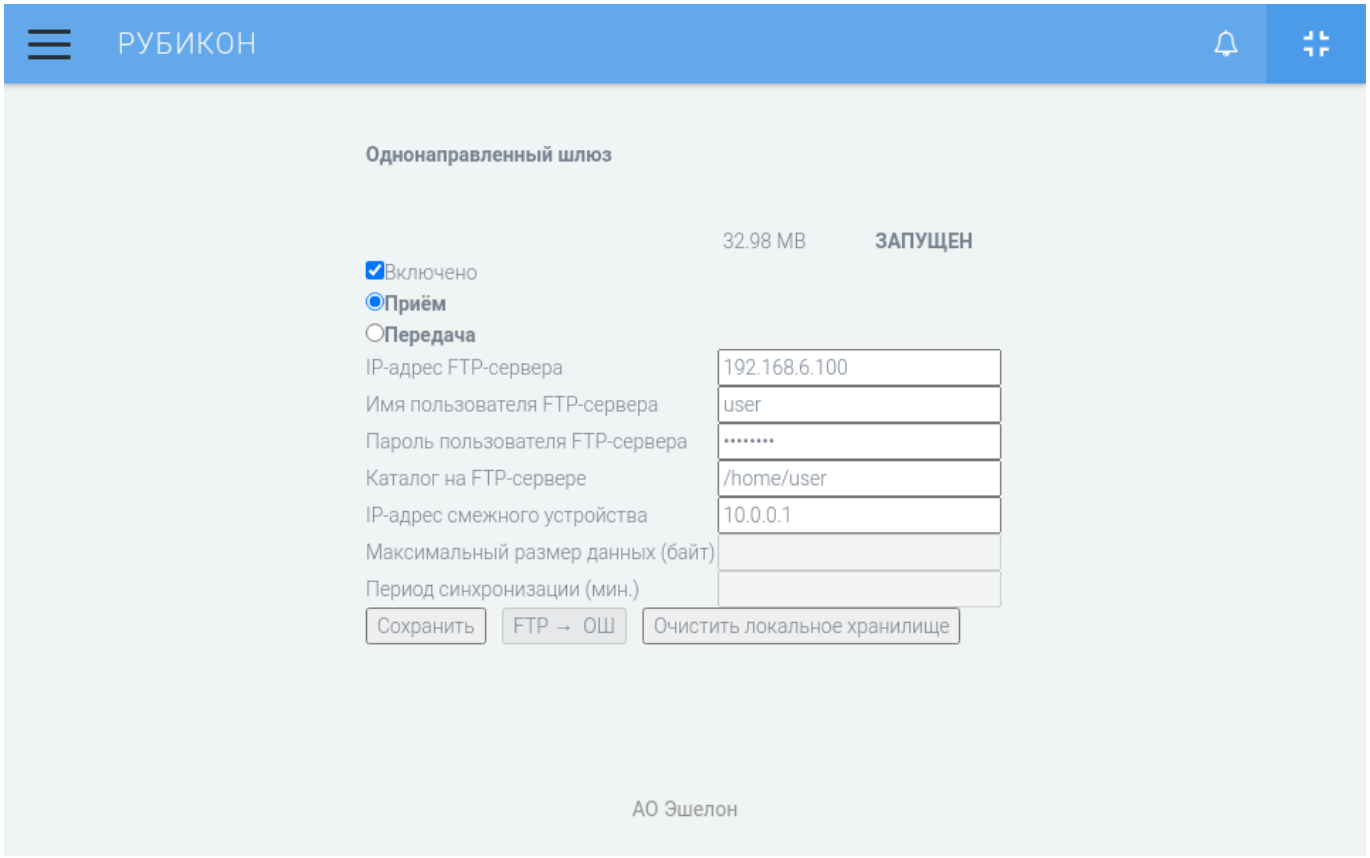


Рисунок 248 – настройка взаимодействия ОШ-Rx с ftp-сервером-Rx

10. проверить факт подключения к ftp-серверу и загрузку файлов можно в самом ftp-сервере (рисунок 249, рисунок 250)

```
#: cat /var/log/vsftpd.log | grep -E "CONNECT|LOGIN|DOWNLOAD"

Thu Apr  1 15:40:03 2021 [pid 6295] CONNECT: Client "192.168.5.1"
Thu Apr  1 15:40:03 2021 [pid 6294] [user] OK LOGIN: Client "192.168.5.1"
Thu Apr  1 15:40:03 2021 [pid 6296] [user] OK DOWNLOAD: Client "192.168.5.1",
"/home/user/test-1", 1048576 bytes, 58277.84Kbyte/sec
Thu Apr  1 15:41:03 2021 [pid 6300] CONNECT: Client "192.168.5.1"
Thu Apr  1 15:41:03 2021 [pid 6299] [user] OK LOGIN: Client "192.168.5.1"
Thu Apr  1 15:41:03 2021 [pid 6301] [user] OK DOWNLOAD: Client "192.168.5.1",
"/home/user/test-2", 1048576 bytes, 52707.43Kbyte/sec
Thu Apr  1 15:42:02 2021 [pid 6323] CONNECT: Client "192.168.5.1"
Thu Apr  1 15:42:02 2021 [pid 6322] [user] OK LOGIN: Client "192.168.5.1"
Thu Apr  1 15:42:02 2021 [pid 6324] [user] OK DOWNLOAD: Client "192.168.5.1",
"/home/user/test-3", 1048576 bytes, 53205.86Kbyte/sec
Thu Apr  1 15:43:02 2021 [pid 6328] CONNECT: Client "192.168.5.1"
Thu Apr  1 15:43:02 2021 [pid 6327] [user] OK LOGIN: Client "192.168.5.1"
Thu Apr  1 15:43:02 2021 [pid 6329] [user] OK DOWNLOAD: Client "192.168.5.1",
"/home/user/test-4", 1048576 bytes, 50760.92Kbyte/sec
Thu Apr  1 15:44:02 2021 [pid 6333] CONNECT: Client "192.168.5.1"
Thu Apr  1 15:44:02 2021 [pid 6332] [user] OK LOGIN: Client "192.168.5.1"
Thu Apr  1 15:44:03 2021 [pid 6334] [user] OK DOWNLOAD: Client "192.168.5.1",
"/home/user/test-5", 1048576 bytes, 58304.39Kbyte/sec
Thu Apr  1 15:45:03 2021 [pid 6337] CONNECT: Client "192.168.5.1"
Thu Apr  1 15:45:03 2021 [pid 6336] [user] OK LOGIN: Client "192.168.5.1"
Thu Apr  1 15:46:03 2021 [pid 6340] CONNECT: Client "192.168.5.1"
Thu Apr  1 15:46:03 2021 [pid 6339] [user] OK LOGIN: Client "192.168.5.1"
Thu Apr  1 15:47:03 2021 [pid 6343] CONNECT: Client "192.168.5.1"
Thu Apr  1 15:47:03 2021 [pid 6342] [user] OK LOGIN: Client "192.168.5.1"
Thu Apr  1 15:48:03 2021 [pid 6346] CONNECT: Client "192.168.5.1"
Thu Apr  1 15:48:03 2021 [pid 6345] [user] OK LOGIN: Client "192.168.5.1"
```

Рисунок 249 – журнал ftp-сервера-Tx

```
#: cat /var/log/vsftpd.log | grep -E "CONNECT|LOGIN|UPLOAD"

Thu Apr  1 15:40:04 2021 [pid 3029] CONNECT: Client "192.168.6.1"
Thu Apr  1 15:40:04 2021 [pid 3028] [user] OK LOGIN: Client "192.168.6.1"
Thu Apr  1 15:40:04 2021 [pid 3030] [user] OK UPLOAD: Client "192.168.6.1",
"/home/user/test-1", 1048576 bytes, 76304.02Kbyte/sec
Thu Apr  1 15:41:04 2021 [pid 3032] CONNECT: Client "192.168.6.1"
Thu Apr  1 15:41:04 2021 [pid 3031] [user] OK LOGIN: Client "192.168.6.1"
Thu Apr  1 15:41:04 2021 [pid 3033] [user] OK UPLOAD: Client "192.168.6.1",
"/home/user/test-2", 1048576 bytes, 77248.04Kbyte/sec
Thu Apr  1 15:42:03 2021 [pid 3053] CONNECT: Client "192.168.6.1"
Thu Apr  1 15:42:03 2021 [pid 3052] [user] OK LOGIN: Client "192.168.6.1"
Thu Apr  1 15:42:03 2021 [pid 3054] [user] OK UPLOAD: Client "192.168.6.1",
"/home/user/test-3", 1048576 bytes, 66636.30Kbyte/sec
Thu Apr  1 15:43:03 2021 [pid 3056] CONNECT: Client "192.168.6.1"
Thu Apr  1 15:43:03 2021 [pid 3055] [user] OK LOGIN: Client "192.168.6.1"
Thu Apr  1 15:43:03 2021 [pid 3057] [user] OK UPLOAD: Client "192.168.6.1",
"/home/user/test-4", 1048576 bytes, 72965.65Kbyte/sec
Thu Apr  1 15:44:03 2021 [pid 3059] CONNECT: Client "192.168.6.1"
Thu Apr  1 15:44:03 2021 [pid 3058] [user] OK LOGIN: Client "192.168.6.1"
Thu Apr  1 15:44:03 2021 [pid 3060] [user] OK UPLOAD: Client "192.168.6.1",
"/home/user/test-5", 1048576 bytes, 67046.42Kbyte/sec
```

Рисунок 250 – журнал ftp-сервера-Rx

или в системном журнале однонаправленного шлюза (рисунок 251, рисунок 252)

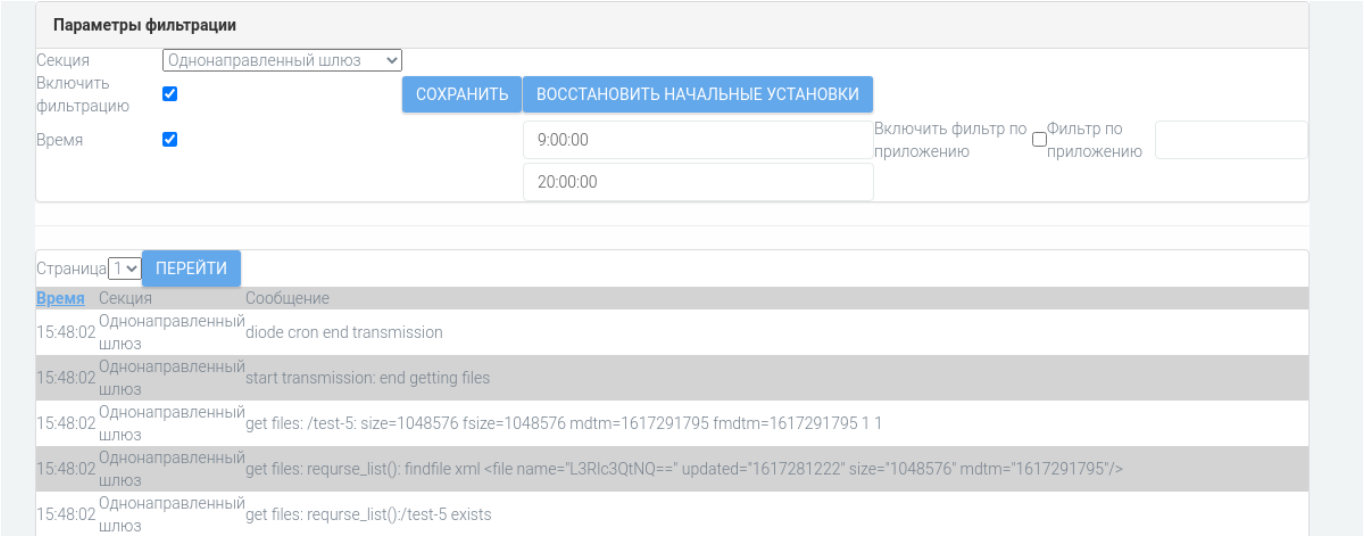


Рисунок 251 – журнал однонаправленного шлюза ОШ-Tx

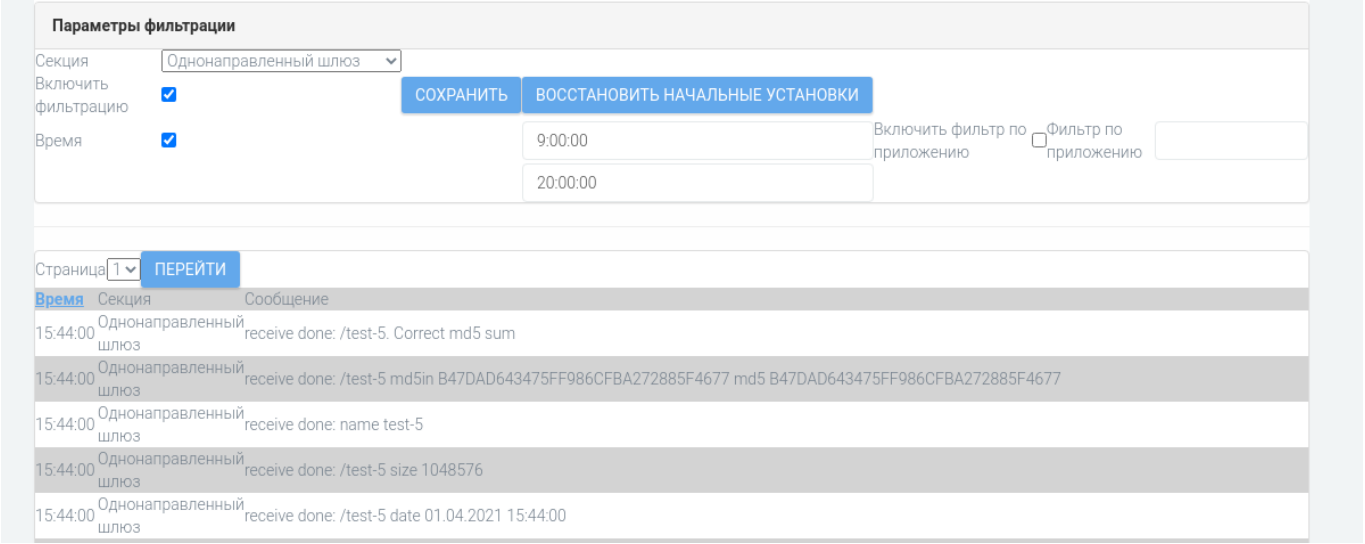


Рисунок 252 – журнал однонаправленного шлюза ОШ-Rx

11. Передача файлов состоит из следующих действий:
    - ОШ-Tx обращается к ftp-серверу-Tx для получения списка файлов (автоматически, через указанный промежуток времени, либо вручную при нажатии на кнопку «Скачать»);
    - ОШ-Tx проверяет по внутреннему журналу производилась ли передача данных файлов (по имени файла и времени его изменения, если один из этих параметров не совпадает, то данный файл будет передан);
    - ОШ-Tx скачивает во внутреннее хранилище («/store») файлы с ftp-сервера-Tx;
    - При скачивании файла с ftp-сервер-Tx, у ОШ-Tx будет активно моргать светодиод сетевого адаптера, подключенного к ftp-серверу-Tx и светодиод активности жесткого диска;

- После скачивания первого же файла, ОШ-Tx подсчитывает для него контрольную сумму и начинает передавать файл из внутреннего хранилища («/store») и служебную информацию по однонаправленному каналу связи;
- ОШ-Rx находится в режиме ожидания данных от ОШ-Tx;
- ОШ-Rx при получении сетевых пакетов от ОШ-Tx начинает собирать файл в локальном хранилище («/store»);
- При передаче файлов по однонаправленному каналу связи у ОШ-Rx светодиод на адаптере приемника должен активно моргать;
- После получения всего файла, ОШ-Rx проверяет контрольную сумму файла;
- Если контрольная сумма верна, то ОШ-Rx подключается к ftp-серверу-Rx и начинает загрузку файла на него;
- При загрузке файла на ftp-сервер-Rx, у ОШ-Rx будет активно моргать светодиод сетевого адаптера, подключенного к ftp-серверу-Rx и светодиод активности жесткого диска;
- Если файл находится в директории, то ОШ-Rx создает дерево директории на ftp-сервере-Rx и после этого загрузит в него файл (рисунок 253);
- Имена файлов и директории могут быть только допустимые в FTP-протоколе.

```
#: cat /var/log/vsftpd.log | grep -E "CONNECT|OK LOGIN|OK UPLOAD|OK MKDIR"

Thu Apr  1 15:13:22 2021 [pid 2819] CONNECT: Client "192.168.6.1"
Thu Apr  1 15:13:22 2021 [pid 2818] [user] OK LOGIN: Client "192.168.6.1"
Thu Apr  1 15:13:22 2021 [pid 2820] [user] OK MKDIR: Client "192.168.6.1",
"/home/user/test/"
Thu Apr  1 15:13:22 2021 [pid 2820] [user] OK UPLOAD: Client "192.168.6.1",
"/home/user/test/test-1", 102400 bytes, 15888.15Kbyte/sec
```

Рисунок 253 – журнал ftp-сервера-Rx с созданием директории и загрузкой в него файла

12. Поскольку передача файлов состоит из нескольких итерации, возможен следующий вариант развития событий, который необходимо контролировать пользователю – если файлы будут создаваться на ftp-сервере-Tx быстрее чем, однонаправленный шлюз может их передать, то возникнет ресинхронизация между ftp-сервере-Tx и ftp-сервере-Rx. Если при этом на ftp-сервере-Tx перестать создавать файлы, то содержимое ftp-сервере-Tx и ftp-сервере-Rx через некоторое время синхронизируются. Также необходимо учитывать, что **передача новых файлов не начнется, пока не будут до конца переданы файлы, находящиеся в очереди на передачу**.

13. Для сброса передачи необходимо выполнить следующие действия:
    - Остановить сервис передачи файлов на ОШ-Тх
    - Удалить файлы с ftp-сервер-Тх
    - На ОШ-Тх нажать кнопку «Очистить локальное хранилище»
    - Заново запустить сервис передачи файлов на ОШ-Тх
14. Оптимальный размер файлов необходимо выбирать исходя из следующих ограничений:
    - Чем больше файлов малого размера, тем дольше будет суммарная передача (т.е. один файл большого размера передастся быстрее, чем много мелких с таким же суммарным размером)
    - Чем больше размер файла, тем больше вероятность его повреждения

Оптимальным размером файла считается размер от 10Мб - 1000Мб, но при этом однонаправленный шлюз может передавать файлы как меньших, так и больших размеров.

3.6 Настройка автовосстановления

3.6.1 Действия системы в случае сбоя

Перейдите в подраздел «Автоматическое восстановление» раздел «Система» (рисунок 254).

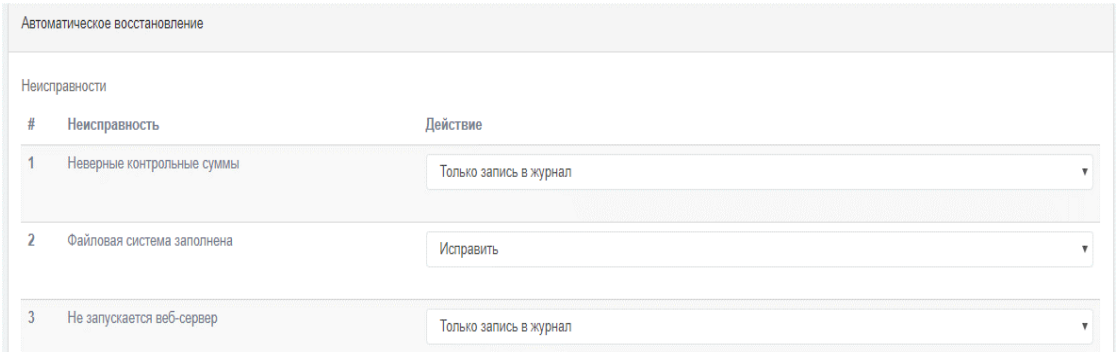


Рисунок 254 – Подраздел «Автоматическое восстановление» раздела «Система»

В разделе представлено 6 типов сбоев и в выпадающих списках приведены опции восстановления при разных неисправностях:

1) неверные контрольные суммы:

a) только запись в журнал;

b) выключение;

c) восстановить последнюю резервную копию настроек;

2) файловая система заполнена:

a) выключение;

b) исправить;

3) не запускается веб-сервер:

a) только запись в журнал;

b) выключение;

c) исправить;

d) восстановить последнюю резервную копию настроек;

4) не запускается СОВ:

a) только запись в журнал;

b) выключение;

c) исправить;

d) восстановить последнюю резервную копию настроек;

5) не запускается http-прокси:

a) только запись в журнал;

b) выключение;

c) исправить;

d) восстановить последнюю резервную копию настроек;

6) не запускается ftp-прокси:

a) только запись в журнал;

b) выключение;

c) исправить;

d) восстановить последнюю резервную копию настроек.

В случае сбоя в журнале аудита регистрируются соответствующие события (рисунок 255):

1) «файл конфигурации системы автоматического восстановления не найден» – запись появляется при ошибке чтения файла конфигурации механизма автоматического восстановления;

2) «неверные контрольные суммы» – индикация ошибки;

3) «не удалось восстановить конфигурацию из резервной копии» – запись появляется при ошибке восстановления из резервной копии (самой новой из имеющихся);

4) «не удалось выключить Рубикон» – запись появляется при ошибке выключения «Рубикон»;

5) «критически мало места на жестком диске» – индикация ошибки;

6) «не удалось очистить /var/log/archives» – запись появляется в случае ошибки действия «Исправить» при неисправности «мало места на ЖД»;

7) «директория /var/log/archive очищена, но места на жестком диске недостаточно для стабильной работы» – запись появляется в случае, если старые логи очищены, но места на диске все равно мало;

8) «не удалось перезапустить веб-сервер» – запись появляется в случае ошибки действия «Исправить» при неисправности «веб-сервер не запущен»;

9) «СОВ не запущена для интерфейса» – индикация ошибки;

10) «не удалось перезапустить СОВ для интерфейса»;

11) «http-прокси не запущен» – индикация ошибки;

12) «не удалось перезапустить http-прокси» – индикация ошибки;

13) «ftp-прокси не запущен» – индикация ошибки;

14) «не удалось перезапустить ftp-прокси» – индикация ошибки.

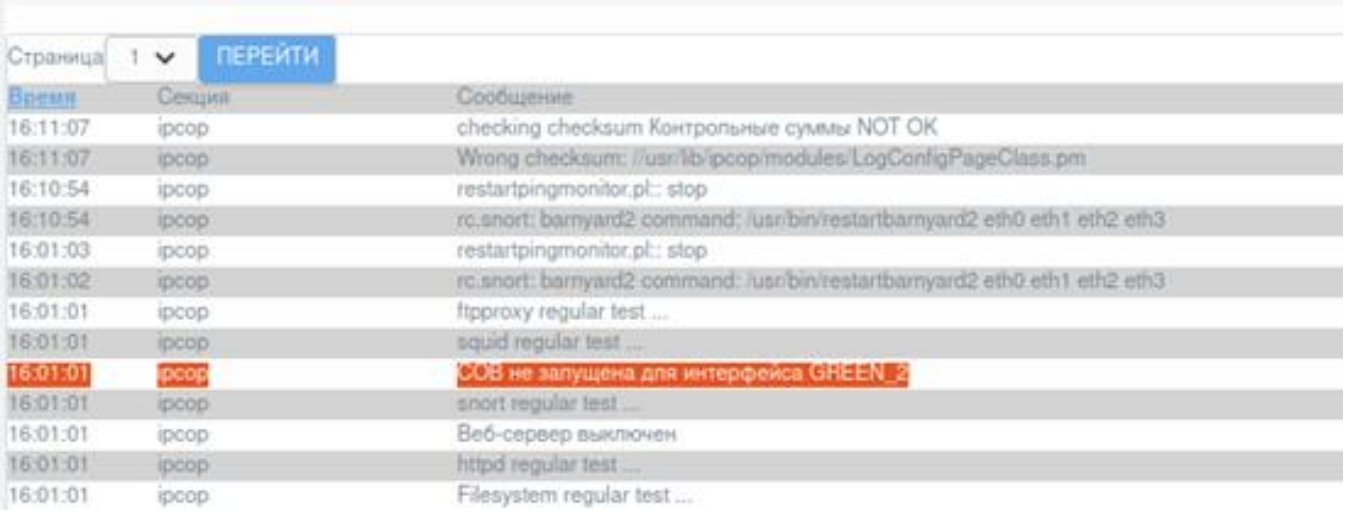


Рисунок 255 – Запись в журнале от механизма восстановления

3.6.2 Консоль восстановления

Консоль восстановления предназначена для возможности восстановления функционирования «Рубикон» в случае неработоспособности или отсутствия доступа к веб-интерфейсу. Для того чтобы запустить консоль восстановления выполните следующие действия:

1) войти в консоль «Рубикон»;

2) ввести логин пользователя «rescue» (по умолчанию);

3) ввести пароль пользователя «rescue» (по умолчанию).

После выполнения указанных выше шагов, появится строка:

```
Welcome to rubish - rubicon rescue shell.
Press '?' or type help to see possible commands.
rubiconish:~/configs>
```

Введите команду help, чтобы посмотреть список команд с описанием:

```
rubiconish:~/configs>help
  cd                change directory.
  cls               Clean screen
  exit              Exit menu 'rubiconsh'
  help              Get help
  ls                Prints containing of directory.
  ping               packets to host
  quit              Quit
  read              Read system configuration files.
  restore_cfg       Restore rubicon configuration from file
  traceroute        Print the route packets trace to network host
  reboot            Reboot the system
  shutdown          Shutdown the system
  passwd            Set password of rescue
  rs_web_passwd     Set web-admin's password
  ifconfig          Read network settings
rubiconish:~/configs>
```

cd «опционально path name» — команда позволяет осуществить переход в папку /home, /var/logs, /configs, cd без параметров осуществляет переход в папку /configs.

cls — команда очистки экрана.

exit (а также «q» и «ctrl-d» «quit») — выход.

ls «опциональные параметры» — команда выводит список файлов и папок в указанном каталоге. Принимает до 10 параметров, например:

```
rubiconish:~/>ls -l
drwxrwxr-x   2 root root  4096     28 13:50 bin
drwxr-xr-x   4 root root  1024     26 18:21 boot
```

Для просмотра доступных параметров введите команду «ls –help».

ping «опциональные параметры» «хост» — команда запускает пинг указанного хоста (по имени или по хосту). Принимает до 10 параметров, например:

```
rubiconish:~/configs>ping -c 2 8.8.8.8
  PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
  64 bytes from 8.8.8.8: icmp_seq=1 ttl=54 time=69.5 ms
  64 bytes from 8.8.8.8: icmp_seq=2 ttl=54 time=67.7 ms
```

--- 8.8.8.8 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 1001ms

rtt min/avg/max/mdev = 67.775/68.683/69.591/0.908 ms

rubiconish:~/configs>

Для просмотра доступных параметров введите команду «ping –help».

read «filename» — позволяет посмотреть содержимое файла, выход по нажатию кнопки «q».

restore_cfg «файл» (опционально «--hadrware») — команда позволяет восстановить конфигурацию «Рубикон». Если добавить параметр «--hardware», то также будут восстановлены настройки физических интерфейсов. Файлы в формате *.dat находятся в папке /home/httpd/html/backup.

traceroute «опциональные параметры» «хост» — команда позволяет определить маршрут до хоста. Принимает до 9 параметров.

reboot — команда перезагрузки изделия.

shutdown — команда выключения изделия.

passwd — команда позволяет сменить пароль для пользователя rescue.

rs_web_passwd — команда позволяет сбросить пароль администратора для web-интерфейса «Рубикон». Пароль по умолчанию: radmin.

ifconfig «опционально -a» — команда выводит конфигурацию интерфейсов. Доступен один опциональный параметр -a.

Все команды, введенные пользователем, сохраняются в текстовый файл /var/log/rubicon_shell_log.

При старте консоли пишется строка:

New session started. «имя пользователя» «дата» «время»

Все команды пишутся в формате:

«команда с параметрами» «пользователь» «время»

Файл rubicon_shell_log недоступен для редактирования.

3.7 Проверка целостности программного обеспечения

3.7.1 Контроль целостности исполняемых файлов и файлов конфигурации

Для контроля целостности исполняемых файлов и файлов конфигурации необходимо зайти в подраздел «Контрольные суммы» раздел «Состояние» и нажать кнопку «Проверить контрольные суммы».

При наличии ошибок контрольных сумм исполняемых файлов и файлов конфигурации, результаты проверки будут отображены в поле «Ошибки» (рисунок 256).

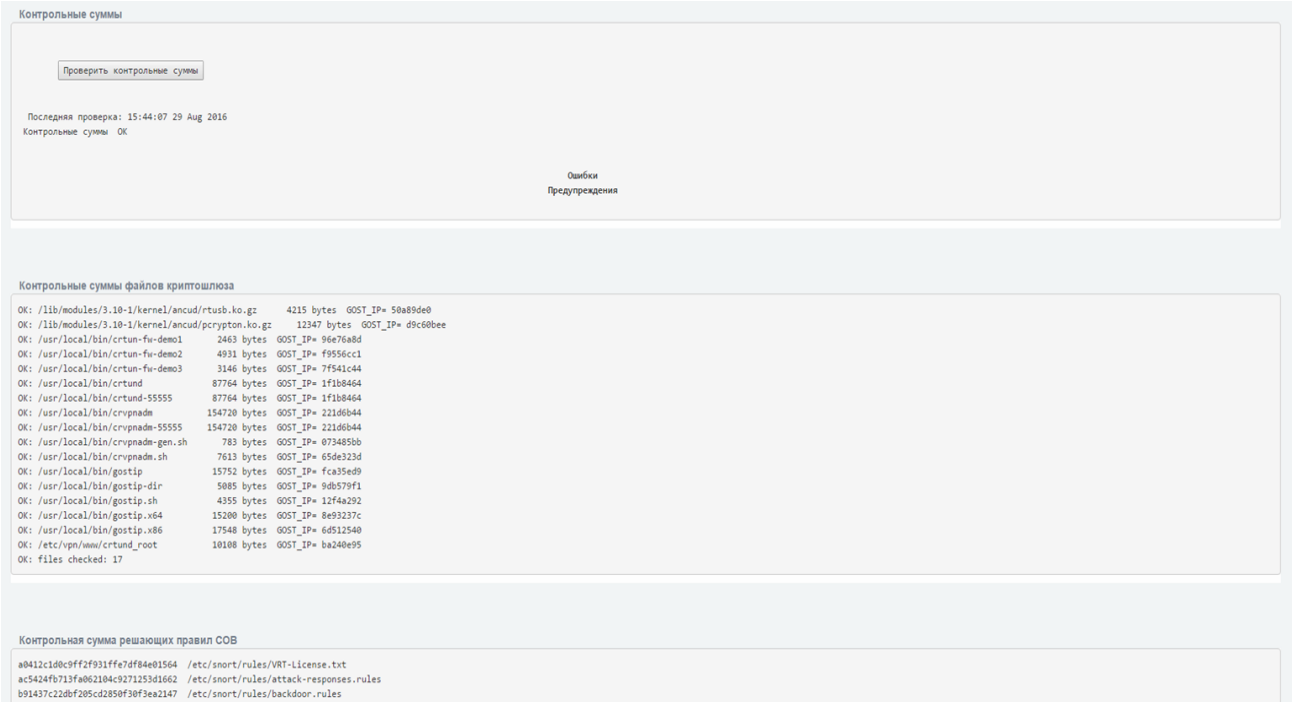


Рисунок 256 – Результаты верификации контрольных сумм файлов

3.8 Тестирование САВЗ

Тестирование САВЗ выполняется следующим образом:

1) перейти в подраздел «Прокси» раздел «Службы» (рисунок 257);

2) поставить флажок «Включить взаимодействие с сервером ICAP»;

3) Задать параметр «Адрес сервера ICAP». В текстовом поле необходимо ввести адрес средства антивирусной защиты. Он будет использован при осуществлении функции прокси;

4) Перейдите по ссылке «test eicar».

После перехода по ссылке, будет выполнено тестирование САВЗ.

Рисунок 257 – Тестирование САВЗ

3.9 Процедуры обновления «Рубикон»

3.9.1 Общий порядок поставки обновлений

Доставка обновлений ПО «Рубикон» осуществляется с использованием сетевых протоколов передачи данных (загрузка с сервера производителя «Рубикон» – АО «Научно-производственное объединение «Эшелон» – далее: «Разработчик»), параметры сервера обновлений: https://brp.cnpo.ru/brp/upd_rubicon_owgw_rules.tar.gz .

Процедура выпуска обновлений ПО «Рубикон» состоит из следующих мероприятий:

a) анализ сообщений о недостатках и потребностей пользователей;

b) проектирование и разработка обновления продукта с учетом проведенного анализа;

c) тестирование обновленного «Рубикон»;

d) оценка влияния обновлений на функции безопасности «Рубикон»;

e) выпуск документа «release notes», содержащего информацию об обновлении, процедур его получения, установки и верификации;

f) при необходимости выпуск новой версии эксплуатационной документации;

g) получение одобрения регулятора на внесение изменений в сертифицированное средство защиты информации;

h) отгрузка файлов на сервер обновлений;

i) предоставление обновлений пользователям для загрузки.

3.9.2 Процедуры и меры безопасности при доставке обновлений «Рубикон»

Разработчик ведет учет покупателей «Рубикон». Выполняется регистрация следующей информации: наименование организации, адрес организации, номер знака соответствия, контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование «Рубикон»). Уведомление пользователей о выпуске обновления ПО «Рубикон» выполняется с использованием рассылки электронных почтовых сообщений с адреса электронной почты support.rubikon@cnpo.ru. Разработчик направляет документ «release notes» в адрес зарегистрированных пользователей. Данный документ содержит описание обновления, процедур получения и контроля целостности обновления, процедур тестирования, установки, применения и верификации.

3.9.2.1 Доставка и контроль целостности обновлений «Рубикон»

Обновления программного обеспечения «Рубикон» публикуются в закрытой части сервера разработчика. Доступ пользователей к закрытой части сервера осуществляется с использованием учетной записи и пароля, указанного в электронном почтовом сообщении, уведомляющем о наличии обновления. При публикации обновлений «Рубикон» также публикуется файл сертификата его подписи. После получения обновления пользователь имеет возможность выполнить проверку его легитимности.

3.9.2.2 Контроль установки обновления

Критерием правильности установки обновления программного обеспечения является доступность веб-интерфейса «Рубикон» и отображение информации о новой версии программного обеспечения в разделе «Система» подразделе «О программе».

3.10 Процедуры обновления БРП

3.10.1 Общий порядок поставки БРП

Доставка обновлений БРП осуществляется с использованием сетевых протоколов передачи данных (загрузка с сервера разработчика), параметры сервера обновлений: https://brp.cnpo.ru/brp/upd_rubicon_owgw_rules.tar.gz .

Разработчик осуществляет проверку, адаптацию обновлений от различных компаний-поставщиков обновлений БРП (далее – поставщик БРП).

3.10.2 Локализация и противодействие новому типу вторжения (атаки)

3.10.2.1 Фиксация появления нового типа вторжения

Обновление БРП является важным аспектом эффективного функционирования системы обнаружения вторжения.

Поставщик БРП осуществляют постоянный мониторинг появления новых сетевых атак. Обнаруженные атаки локализуются, и на их основе формируется ежемесячное обновление.

Разработчик на постоянной основе осуществляет загрузку, проверку и анализ обновлений от поставщика БРП.

Кроме того, разработчик независимо от поставщика БРП осуществляет постоянный мониторинг появления новых сетевых угроз. На основании проведенного мониторинга разработчик может пополнить обновленную БРП собственными правилами, а также модифицировать полученные от поставщика БРП правила.

3.10.2.2 Предоставление обновления покупателям

Процедура предоставления покупателям обновлений БРП в общем случае выполняется следующим образом:

1) загрузка обновлений с серверов поставщика БРП, предоставляющих обновления БРП для разработчика;
2) проверка целостности загруженных обновлений;
3) обработка БРП;
4) тестирование работоспособности СОВ с обновленными правилами;
5) оценка влияния обновленных БРП на функции безопасности СОВ;
6) подготовка к отгрузке обновленных БРП:
   a) формирование архива с БРП;
   b) формирование файла сертификата подписи;
7) отгрузка файлов на сервер обновлений;
8) предоставление обновлений БРП клиентам для загрузки.

3.10.3 Процедуры и меры безопасности при доставке обновлений БРП

3.10.3.1 Оповещение пользователей «Рубикон» об обновлении БРП

Уведомление пользователей о выпуске обновления БРП выполняется с использованием рассылки электронных почтовых сообщений. При необходимости получения консультации по тому или иному правилу в обновленной БРП пользователю следует обратиться в техническую поддержку предприятия-изготовителя

3.10.3.2 Доставка и контроль целостности БРП на стороне пользователя

Обновления БРП, успешно прошедшие контроль влияния на безопасность «Рубикон», публикуются в закрытой части сервера разработчика. Доступ пользователей к закрытой части сервера осуществляется с использованием учетной записи и пароля, указанного в электронном почтовом сообщении, уведомляющем о наличии обновления. При публикации обновления БРП публикуется файл подписи. После получение обновления БРП пользователь имеет возможность выполнить контроль его легитимности.

4 ТЕКСТОВЫЕ СООБЩЕНИЯ

В настоящем разделе описываются типовые сообщения при возникновении аварийных ситуаций.

Большинство аварийных ситуаций можно разделить на две группы:

1) ситуации, связанные с ошибками конфигурации:
   a) некорректные сетевые настройки;
   b) некорректные настройки фильтрации пакетов;
c) некорректные правила СОВ;
2) ситуации, связанные с ошибками оборудования:
   a) выход из строя сетевых контроллеров;
   b) выход из строя дисковых накопителей.

При некорректном заполнении полей «Рубикон» отобразит сообщение об ошибке следующего вида (рисунок 258). Сообщение об ошибке появляется вверху экрана и содержит описательную часть ошибки.

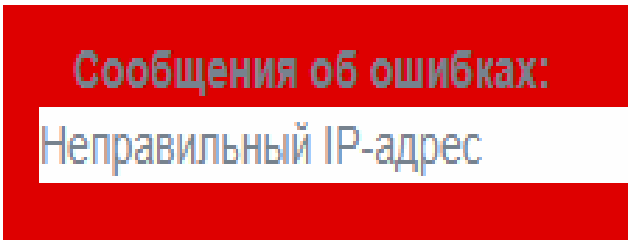


Рисунок 258 – Сообщение об ошибке

Чаще всего их можно исправить переконфигурированием изделия, либо восстановлением из ранее сделанной резервной копии, либо восстановлением с установочного носителя.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ И ТЕРМИНОВ

Сокращение / Термин	Расшифровка / Определение
DHCP	(англ. *Dynamic Host Configuration Protocol*) – сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP
DNS	(англ. *Domain Name System*) – компьютерная распределенная система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене (SRV-запись)
ICMP	(англ. *Internet Control Message Protocol* – протокол межсетевых управляющих сообщений) – сетевой протокол, входящий в стек протоколов TCP/IP
IP	(англ. *Internet Protocol Address*) – уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP
SID	(англ. *Security Identifier*) – структура данных переменной длины, которая идентифицирует учетную запись пользователя, группы, службы, домена или компьютера (в Windows на базе технологии NT (NT4, 2000, XP, 2003, Vista,7,8,10)
Squid	Программный пакет, реализующий функцию кэширующего прокси-сервера для протоколов HTTP, FTP, Gopher и HTTPS
VPN	(англ. *Virtual Private Network* – виртуальная частная сеть) – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет)
БРП	База решающих правил

Сокращение / Термин	Расшифровка / Определение
Задание по безопасности	Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного изделия
ЗБ	Задание по безопасности
ИС	Информационная система
ИТ	Информационная технология
МЭ	Межсетевой экран
ОС	Операционная система
ОУД	Оценочный уровень доверия
ПБО	Политика безопасности объекта оценки
ПЗ	Профиль защиты
ПО	Программное обеспечение
Политика безопасности «Рубикон»	Совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых «Рубикон»
Профиль защиты	Совокупность требований безопасности для «Рубикон»
Разработчик	АО «НПО «Эшелон»
САВЗ	Средства антивирусной защиты
СЗИ	Средство защиты информации
СОВ	Система обнаружения вторжений
ТДБ	Требования доверия к безопасности
Угроза безопасности информации	Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации
УЦ	Удостоверяющий центр

Лист регистрации изменений										
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводит. документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					