АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «ЭШЕЛОН»

УТВЕРЖДЕН

НПЕШ.465614.004 РА-ЛУ

МЕЖСЕТЕВОЙ ЭКРАН И СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ «РУБИКОН-К» НПЕШ.465614.004

Руководство администратора

НПЕШ.465614.004 РА

Версия документа 1.1

Оглавление

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Идентификация документа

Название документа	Межсетевой экран и система обнаружения вторжений «Рубикон-К». Руководство администратора
Версия документа	Версия 1.1
Обозначение документа	НПЕШ.465614.004 РА 01
Идентификация Рубикон-К	Межсетевой экран и система обнаружения вторжений «Рубикон-К». НПЕШ.465614.004 Версия 2.4.1.4.ab.
Идентификация разработчика	АО «НПО «Эшелон»
Уровень доверия	Оценочный уровень доверия ОУД3, усиленного компонентами ADV_FSP.4 «Полная функциональная спецификация», ADV_IMP.2 «Полное отображение представления реализации функциональных возможностей безопасности», ADV_LLD.1 «Описательный проект нижнего уровня», ADV_TDS.3 «Базовый модульный проект», ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация», ALC_FLR.1 «Базовое устранение недостатков», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», AVA_VLA.3 «Умеренно стойкий», AVA_VAN.5 «Усиленный методический анализ», расширенного компонентами ADV_IMP_EXT.3 «Реализация Рубикон-К», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения Рубикон-К», AMA_SIA_EXT.3(1) «Анализ влияния обновлений на безопасность Рубикон-К», ALC_UPI_EXT.1 Процедуры обновления базы решающих правил, AMA_SIA_EXT.3(2) Экспертиза анализа влияния обновлений базы решающих правил на безопасность системы обнаружения вторжений.
Идентификация ПЗ	Профиль защиты межсетевых экранов типа «А» четвертого класса защиты. ИТ.МЭ.А4.ПЗ. Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ. Профиль защиты систем обнаружения вторжений уровня сети второго класса защиты. ИТ.СОВ.С4.ПЗ
Идентификация ОК	Требования к межсетевым экранам, утвержденные приказом ФСТЭК России от 09 февраля 2016 г. № 9.

	ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Требования к системам обнаружения вторжений, утвержденные приказом ФСТЭК России от 6 декабря 2011 г. № 638. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
Ключевые слова	Межсетевой экран, система обнаружения вторжений, ОУД3

1.2 Аннотация документа

Документ предназначен для ознакомления потребителей с технической информацией о межсетевом экране и системе обнаружения вторжений «Рубикон-К» НПЕШ.465614.004 (далее по тексту - Рубикон-К) и содержит общие сведения об Рубикон-К, организационно-распорядительные меры, сведения о структуре Рубикон-К, описание настроек Рубикон-К и тексты сообщений, выдаваемых в ходе выполнения настройки, проверки, а также о процессе функционирования Рубикон-К.

Настоящий документ соответствует ТДБ «AGD_OPE.1 Руководство пользователя по эксплуатации», «AGD_PRE.1 Подготовительные процедуры» о чем свидетельствует следующая таблица.

Идентификатор требования	**Содержание требования**	**Раздел документа**
AGD_OPE.1 Руководство пользователя по эксплуатации		
AGD_OPE.1.1C	В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено описание доступных пользователям функций, возможных прав и обязанностей, которыми следует управлять в защищенной среде функционирования, а также уместных предупреждений.	2, 5.3
AGD_OPE.1.2C	В руководстве пользователя по эксплуатации в рамках каждой	5.3, 6, 7, 8, 9, 10, 11, 12

	пользовательской роли должно быть представлено описание принципов безопасной работы с предоставленными в Рубикон-К интерфейсами.	
AGD_OPE.1.3C	В руководстве пользователя по эксплуатации должно быть представлено описание доступных для каждой пользовательской роли функций и интерфейсов, особенно всех параметров безопасности под управлением пользователя, с указанием безопасных значений, если это уместно.	5.3
AGD_OPE.1.4C	В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено четкое представление каждого типа имеющих значение для безопасности событий, связанных с доступными пользователю обязательными для выполнения функциями, включая изменение характеристик безопасности сущностей, находящихся под управлением ФБО.	10.1
AGD_OPE.1.5C	В руководстве пользователя по эксплуатации должны быть идентифицированы все возможные режимы работы Рубикон-К (включая операции после сбоев и ошибок эксплуатации), их последствия и участие в обеспечении безопасного функционирования.	4, 13
AGD_OPE.1.6C	В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть **приведено** описание всех мер безопасности, предназначенных для выполнения целей безопасности для	3.2, 5.3

	среды функционирования согласно описанию в ЗБ**, имеющих отношение к пользователю**.	
AGD_OPE.1.7C	Руководство пользователя по эксплуатации должно быть четким и обоснованным.	-
AGD_PRE1.1C	В подготовительных процедурах должны описываться все шаги, необходимые для безопасной приемки поставленного Рубикон-К в соответствии с процедурами поставки заявителя (разработчика, производителя).	3.1
AGD_PRE1.2C	В подготовительных процедурах должны описываться все необходимые шаги для безопасной установки Рубикон-К, **реализации и оценки реализации всех функций безопасности среды функционирования Рубикон-К** в соответствии с целями безопасности для среды функционирования, описанными в ЗБ.	3.1, 5

1.3 Термины и определения

В настоящем документе используются термины и определения согласно ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» и ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств».

Squid	Программный пакет, реализующий функцию кэширующего прокси-сервера для протоколов HTTP, FTP, Gopher и HTTPS.
Администратор Рубикон-К	Уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию Рубикон-К (ОО)
Задание по безопасности	Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного Рубикон-К
Объект оценки	Подлежащий сертификации (оценке) Рубикон-К

Политика безопасности Рубикон-К	Совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых Рубикон-К
Профиль защиты	Совокупность требований безопасности для Рубикон-К
Разработчик	АО «НПО «Эшелон»
Угроза безопасности информации	Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации.
Функции безопасности Рубикон-К	Совокупность всех функций безопасности Рубикон-К, направленных на осуществление политики безопасности объекта оценки (ПБО).

Перечень сокращений

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

ICMP - Internet Control Message Protocol

IP - Internet Protocol

SID - Security Identifier

VPN - Virtual Private Network

БРП - база решающих правил

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

САВЗ - средства антивирусной защиты

СВТ - средство вычислительной техники

СЗИ - средство защиты информации

СОВ - система обнаружения вторжений

ТДБ - требования доверия к безопасности

УЦ - удостоверяющий центр

ФБО - функции безопасности объекта оценки

ФТБ - функциональные требования безопасности

2 ОБЩИЕ СВЕДЕНИЯ

РУБИКОН-К предназначен для выполнения следующих функций:

- 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.

Функции контроля и фильтрации сетевого трафика реализуются в соответствии с заданными правилами проходящих через него информационных потоков. Рубикон-К используется в целях обеспечения защиты (некриптографическими методами) информации ограниченного доступа.

3 ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫЕ МЕРЫ

3.1 Процедуры поставки

3.1.1 Общий порядок поставки

РУБИКОН-К поставляется в составе изделия межсетевой экран и система обнаружения вторжений «Рубикон-К». НПЕШ.465614.004. Версия 2.4.1.4.ab.

При поставке Рубикон-К заказчику от среды производства до среды установки АО «НПО «Эшелон» (далее Разработчик) выполняет следующие действия:

1) Расчет контрольных сумм файлов программного обеспечения Рубикон-К, установленного на аппаратную платформу.

2) Упаковка комплекта поставки.

3) Передача упакованного комплекта поставки на склад готовой продукции.

4) Выдача упакованного комплекта поставки уполномоченному представителю заказчика.

3.1.2 Комплектность упаковки

Упаковка в общем случае содержит следующие комплектующие:

1) Аппаратная платформа с установленным программными и аппаратными компонентами Рубикон-К.

2) Носитель с образом программного обеспечения, установленного на аппаратной платформе.

3) Задание по безопасности.

4) Формуляр на Рубикон-К.

5) Руководство администратора.

3.1.3 Процедуры и меры безопасности при распространении Рубикон-К к месту назначения

Процедуры и меры безопасности при распространении Рубикон-К к месту назначения решают следующие задачи:

– обеспечивают идентификацию и целостность Рубикон-К во время пересылки;

– обеспечивают обнаружение несанкционированных модификаций Рубикон-К;

– препятствуют попыткам подмены Рубикон-К от имени разработчика.

Контроль целостности программного обеспечения компонентов Рубикон-К, установленного на аппаратную платформу

Расчет эталонных контрольных сумм файлов программного обеспечения компонентов Рубикон-К, установленного на аппаратную платформу, осуществляется на этапе сборки и выполняется внутренними средствами Рубикон-К. Рассчитанные контрольные суммы хранятся в энергонезависимой памяти «Рубикон-К». При включении «Рубикон-К» выполняет контроль целостности установленных файлов до запуска программы. При выявлении несоответствия сохраненным значениям на монитор выводится уведомление об этом событии.

Контроль целостности файлов установочного диска

Перечень файлов, записанных на установочный компакт-диск, а также их контрольные суммы содержатся в формуляре на Рубикон-К, входящего в комплект поставки.

Контроль целостности аппаратной платформы

Корпус аппаратной платформы после установки программных и аппаратных компонентов Рубикон-К опечатывается уникальным одноразовым стикером. Вскрыть корпус без разрушения стикера невозможно.

Контроль сохранности упакованного комплекта

Комплект Рубикон-К упаковывают в пластиковый пакет, помещают в картонную коробку и заклеивают коробку скотчем с символикой АО «НПО «Эшелон». Упакованный комплект хранится на складе готовой продукции, оснащенном охранной сигнализацией.

Поддержка безопасности доставки

Доставка готовой продукции к месту назначения осуществляется силами разработчика. Выдача Рубикон-К уполномоченному представителю заказчика осуществляется на основании документов, удостоверяющих полномочия представителя.

Передача Рубикон-К заказчику подтверждается актом сдачи-приемки Рубикон-К, на котором проставляются подписи и печати сторон.

3.2 Требования безопасности к среде ИТ

РУБИКОН-К обеспечивает функциональное назначение при реализации пользователем следующих предварительных организационно-распорядительных мер:

– обеспечение сохранности оборудования и физической целостности системных блоков компьютеров;

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

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

К среде ИТ, в которой функционирует Рубикон-К, предъявляются следующие требования безопасности, относящиеся к пользователю:

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

– обеспечение физической сохранности технических средств (межсетевого экрана, СВТ, на котором он функционирует и терминалов, с которых выполняется его управление) и исключение возможности доступа к ним посторонних лиц;

– обеспечение установки, конфигурирования и управления Рубикон-К в соответствии с эксплуатационной документацией;

– обеспечение поддержки средств аудита, используемых в Рубикон-К.

4 СТРУКТУРА ПРОГРАММЫ

РУБИКОН-К состоит из подсистем, описанных в данном разделе.

4.1 Подсистема обеспечения сетевого взаимодействия

Данная подсистема состоит из нескольких модулей.

4.1.1 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:

- сетевой адрес узла отправителя и получателя;
- логический или физический сетевой интерфейс Рубикон-К, через который проходит пакет;
- сетевой протокол, который используется для взаимодействия;
- направление пакета (входящий/исходящий);
- транспортный протокол, который используется для взаимодействия;
- порты источника и получателя в рамках сеанса (сессии);
- флаг фрагментации;
- мандатная метка;
- команды (разрешенные/запрещенные), параметры команд; последовательности используемых команд - для FTP протокола;
- мобильный код (разрешенный/запрещенный) - для языков программирования Java и JavaScript;
- прикладное ПО (разрешенное/запрещенное) - для веб-браузеров (Internet Explorer, Mozilla Firefox, Google Chrome и др).

4.1.2 Модуль маршрутизации

Программный модуль Рубикон-К, предназначенный для выполнения статической маршрутизации.

4.1.3 Модуль преобразования адресов

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

4.1.4 Модуль приоритизации

Программный модуль Рубикон-К, обеспечивающий приоритизацию информационных потоков на основе установленных приоритетов значений сетевого адреса и используемого порта.

4.1.5 Модуль управления состояниями

Программный модуль Рубикон-К, предназначенный для проверки каждого пакета по таблице состояний для определения того, не противоречит ли состояние пакета ожидаемому состоянию.

4.1.6 Модуль сетевого посредника

Программный модуль Рубикон-К, осуществляющий посредничество в передаче информации сетевого трафика, основанное на следующих типах атрибутов безопасности:

- сетевой адрес и порт отправителя и получателя;
- сетевой трафик (FTP, SMTP, HTTP);
- разрешенные/ запрещенные атрибуты информации в заголовках пакетов.

4.1.7 Модуль настройки сетевых интерфейсов

Программный модуль Рубикон-К, осуществляет маскирование датчика СОВ на сетевом уровне и позволяет настраивать сетевые интерфейсы.

4.2 Подсистема идентификации / аутентификации

Данная подсистема состоит из одного модуля.

4.2.1 Модуль аутентификации веб-сервера

Модуль аутентификации веб-сервера обеспечивает идентификацию и аутентификацию администраторов Рубикон-К, а также идентификацию и аутентификацию

субъектов межсетевого взаимодействия до передачи межсетевым экраном информационного потока получателю.

4.3 Подсистема бесперебойного функционирования и восстановления

Данная подсистема состоит из нескольких модулей.

4.3.1 Модуль тестирования и контроля целостности

Программный модуль Рубикон-К, обеспечивающий контроль целостности исполняемых файлов Рубикон-К путем контрольного суммирования, а также проверку работоспособности служб Рубикон-К и сетевого соединения.

4.3.2 Модуль восстановления

Программный модуль Рубикон-К, обеспечивающий автоматическое восстановление устойчивых и безопасных состояний HTTP сервера, прокси сервера, VPN сервера, сервиса аудита, службы времени, службы СОВ и DHCP.

4.3.3 Модуль кластеризации

Программный модуль Рубикон-К, обеспечивающий кластеризацию Рубикон-К с помощью резервирования Рубикон-К.

4.4 Подсистема регистрации событий

Данная подсистема состоит из одного модуля.

4.4.1 Модуль работы с журналом

Программный модуль Рубикон-К, предназначенный для создания, хранения и просмотра записей аудита. Рубикон-К 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 Рубикон-К, аудитор Рубикон-К) возможность читать всю информацию из записей аудита, осуществлять поиск, сортировать записи аудита.

4.5 Подсистема взаимодействия с внешними системами

Данная подсистема состоит из нескольких модулей.

4.5.1 Модуль взаимодействия с внешними СЗИ

Программный модуль Рубикон-К, обеспечивающий взаимодействия Рубикон-К с САВЗ по протоколу адаптации Интернет-контента (ICAP).

4.5.2 Модуль связи с сервером журналирования

Программный модуль Рубикон-К, обеспечивающий взаимодействие с сервером журналирования.

4.6 Подсистема управления

Данная подсистема состоит из нескольких модулей.

4.6.1 Модуль веб-сервера

Программный модуль Рубикон-К, обеспечивающий выполнение запросов пользователей.

4.6.2 Модуль преобразования конфигурации - браузера

Программный модуль Рубикон-К, обеспечивающий представление информации для пользователей.

4.7 Подсистема обнаружения вторжений

Данная подсистема состоит из нескольких модулей.

4.7.1 Агент обновления

Программный модуль Рубикон-К, предназначен для получения актуальной базы решающих правил СОВ с сервера обновлений.

4.7.2 Модуль сигнатурного анализа сетевого трафика

Программный модуль Рубикон-К, использующийся для САВЗ, содержит сигнатуру, позволяющую блокировать сетевой трафик, если САВЗ обнаружил в нем вирусную активность.

4.7.3 Модуль эвристического анализа сетевого трафика

Программный модуль Рубикон-К, предназначен для обнаружения вторжений с помощью эвристического анализа.

4.7.4 Модуль реагирования

Программный модуль Рубикон-К, позволяет уведомлять администратора об обнаруженных вторжениях и выдачу управляющих сигналов межсетевому экрану.

4.8 Веб-интерфейс

Данная подсистема состоит из одного модуля.

4.8.1 Программа управления

Программный модуль Рубикон-К, позволяет решать задачи по администрированию СОВ.

4.9 Операционная система

Данная подсистема состоит из нескольких модулей.

4.9.1 Модуль выдачи меток времени

Программный модуль Рубикон-К, предоставляющий надежные метки времени для собственного использования (при генерации записей в журнале аудита).

4.9.2 Модуль захвата и разбора трафика

Программный модуль Рубикон-К, модуль предназначен для обнаружения вторжений на основе анализа протоколов.

4.10 Подсистема BIOS

Данная подсистема состоит из одного модуля.

4.10.1 Модуль BIOS

Программный модуль Рубикон-К, предоставляющий обнаружение, инициализацию и передачу загрузчику управления.

5 НАСТРОЙКА ПРОГРАММЫ

5.1 Установка Рубикон-К

Перед установкой Рубикон-К ознакомьтесь с требованиями к компьютеру, на котором функционирует ПО Рубикон-К, и с требованиями к ПО консоли управления (таблица 1).

Таблица 1 - Программно-аппаратные требования для консоли управления

Элемент среды функционирования	**Параметры**
Вычислительная платформа консоли управления Рубикон-К	процессор: Pentium III, 1.2 ГГц оперативная память: 8 Гб жесткий диск (свободное пространство): 150 МБ сетевая карта: 100 Мбит/с
ОС консоли управления	ОС семейства Linux\Unix 64 bit: Astra Linux Common Edition (Орел) 1.11, Special Edition (Смоленск) 1.5, МСВС 5.0, Ubuntu 16.04, Debian 7.11, 8.6 ОС семейства Microsoft Windows 64 bit: Windows Server 2003/2008, Windows версии 7, 8, 10

Для выполнения установки Рубикон-К произведите загрузку с установочного носителя Рубикон-К.

Установка представляет собой неинтерактивный процесс, в процессе которого устанавливается Рубикон-К, происходит настройка оборудования и задаются параметры системы по умолчанию.

После установки Рубикон-К имеет сетевой интерфейс с IP-адресом **192.168.1.1**. Сервер Рубикон-К обрабатывает запросы пользователей. А веб-интерфейс обеспечивает предоставление информации для администратора и аудитора в удобном виде. Через веб-интерфейс может производиться начальная настройка параметров Рубикон-К. При дальнейшей настройке параметры администрирования можно изменить.

5.2 Описание старта и процедура проверки правильности старта

Старт Рубикон-К начинается с загрузки операционной системы. По окончании загрузки работоспособность и правильность старта можно проверить, выполнив команду **«ping 192.168.1.1»** на любом из компьютеров, подключенных к внутренней защищаемой сети.

Для прохождения процедур идентификации и аутентификации выполните следующие действия:

1) установите соединение с графическим интерфейсом Рубикон-К, подключившись по защищенному https-соединению **https:// 192.168.1.1:8443**;

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

3) введите пароль пользователя с ролью Администратор в текстовое поле **«Пароль»** формы авторизации. По умолчанию **«radmin»**;

4) нажмите кнопку **«Вход»**.

При превышении трех неуспешных попыток ввода логина и пароля, доступ к Рубикон-К будет заблокирован.

При первом подключении к административному интерфейсу измените пароль на странице **«Система → Пароли»** (рисунок 1).

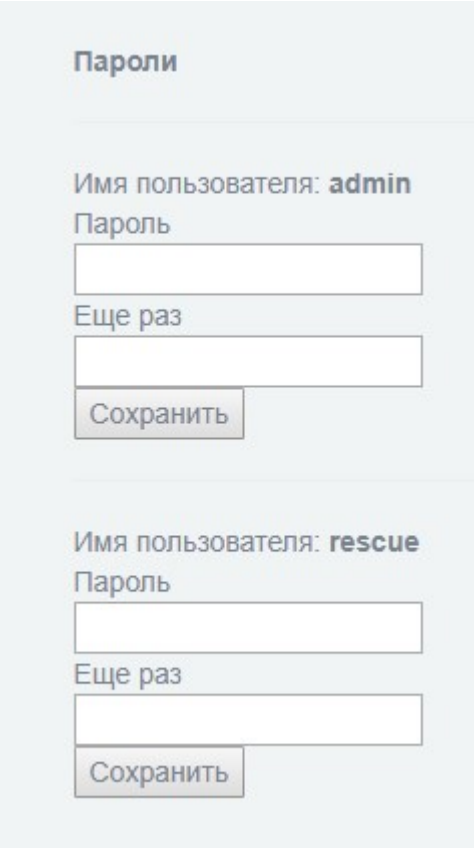


Рисунок 1 - Раздел «Система → Пароли»

После выполнения указанных выше шагов пользователь с полномочиями администратора будет перенаправлен на стартовую страницу.

5.3 Роли

РУБИКОН-К поддерживает следующие роли:

1) администратор - имеет доступ к просмотру веб-интерфейса и настройке Рубикон-К;

2) аудитор - имеет доступ к просмотру веб-интерфейса, без возможности внесения изменений в настройки Рубикон-К;

3) пользователь - не имеет доступа к просмотру веб-интерфейса (кроме стартовой страницы) и настройке Рубикон-К. После аутентификации Рубикон-К фиксирует IP-адрес пользователя и предоставляет соответствующие правила. Пользователь включает правила нажатием кнопки **«Запуск правил»** на стартовой странице Рубикон-К.

Для того чтобы добавить новых пользователей в разделе **«Система → Пользователи»** в выпадающем списке **«роль»** выберите роль (администратор, аудитор, пользователь), а затем заполните следующие текстовые поля (рисунок 2):

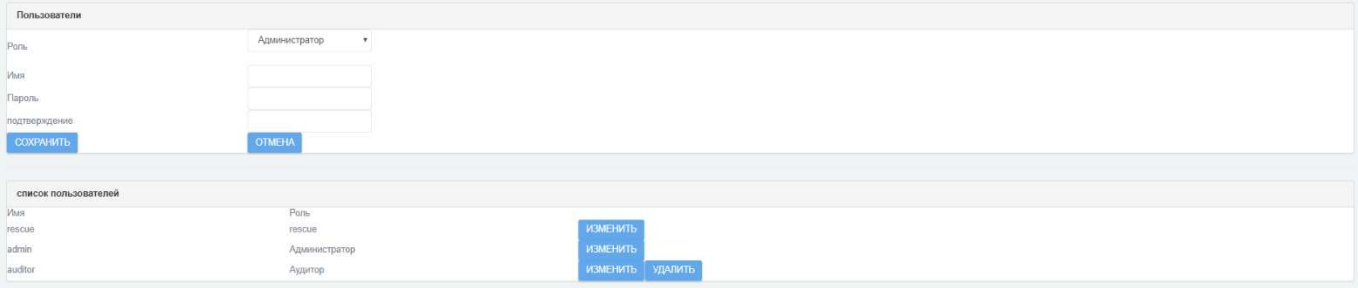


Рисунок 2 - Раздел «Система → Пользователи»

– **«Имя»**;

– **«Пароль»**;

– **«Подтверждение»**.

– нажмите кнопку **«Сохранить»**.

Список пользователей можно посмотреть в секции **«список пользователей»**. При необходимости, можно удалить пользователя, нажав на кнопку «Удалить».

Авторизация аудитора и пользователя выполняется аналогично авторизации администратора (см. раздел 5.2). Для работы с Рубикон-К получите ваш логин и пароль у администратора.

5.4 О программе

После успешного прохождения процедуры авторизации администратор может посмотреть сведения о Рубикон-К, перейдя в меню **«Система → О программе»** (рисунок 3).

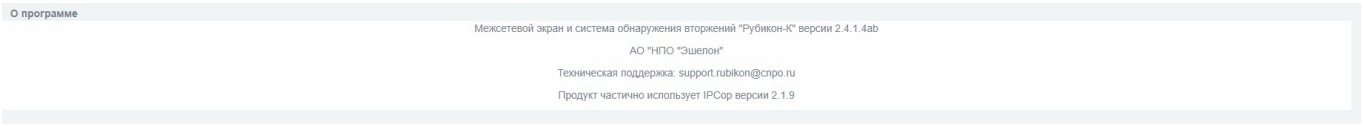


Рисунок 3 - Раздел «Система → О программе»

6 СЕТЕВЫЕ НАСТРОЙКИ

6.1 Общие положения

В зависимости от используемых функций в комплексе «Рубикон-К» предусмотрены следующие типы физических сетевых интерфейсов:

1) **«красный»**: 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. На красном интерфейсе происходит трансляция сетевых адресов по портам, указанным в составе сетевого пакета;

2) **«зеленый»**: сетевой интерфейс, подключаемый к внутренней сети. По умолчанию все пакеты, маршрутизируемые между различными зелеными интерфейсами, не блокируются;

3) **«синий»**: для этого интерфейса включен режим **«белого списка»**, т.е. запрещены как входящие, так и перенаправляемые пакеты от всех адресов, кроме специально разрешенных на странице **«Межсетевой экран → Доступ к синему интерфейсу»**.

4) **«оранжевый»**: 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.

Каждому интерфейсу можно назначить одну из следующих политик (таблица 2).

Таблица 2 - Доступность политики в зависимости от цвета интерфейса

Интерфейс	**Политика**		
	Закрыто	**Полуоткрыто**	**Открыто**
Зеленый	✓	✓	✓
Синий	✓	✓	✓
Оранжевый	✓	×	✓
Красный	✓	×	×

В таблице 3 приведено описание правил, создаваемых по умолчанию при применении каждой из политик:

Таблица 3 - Описание сетевых политик

Тип правила	**Политика**		
	Закрыто	**Полуоткрыто**	**Открыто**
Входящее	Все соединения запрещены	DNS, DHCP, NTP, ICMP, Proxy	DNS, DHCP, NTP, ICMP, Proxy
Перенаправление	Разрешен доступ в сеть	Разрешен доступ в сеть	Разрешен доступ в сеть и из сети
Исходящее	Доступ разрешен	Доступ разрешен	Доступ разрешен

Примечание - На поставляемом Рубикон-К включен сервис DHCP. Если в вашей сети используются статические IP-адреса или уже установлен DHCP сервер, то необходимо отключить его в настройках Рубикон-К.

Примечание - Если при установке новой сетевой карты в аппаратную платформу Рубикон-К не был найден драйвер сетевой карты (или она была установлена позже), то интерфейсы этой карты отобразятся в веб-интерфейсе под именами eth"n", где "n" является номером интерфейса. В случае возникновения подобной ситуации обратитесь в техническую службу поддержки.

6.2 Предназначение цветов интерфейсов

По умолчанию все физические интерфейсы изделия «Рубикон-К» являются зелеными. Для переназначения цветов интерфейсов выполните следующие действия:

– настройте администрирование комплекса «Рубикон-К» на странице **«Межсетевой экран → Настройки межсетевого экрана»** (рисунок 4);

1) по умолчанию первые четыре зеленых интерфейса помечены как административные, т.е. по ним разрешено администрирование Рубикон-К;

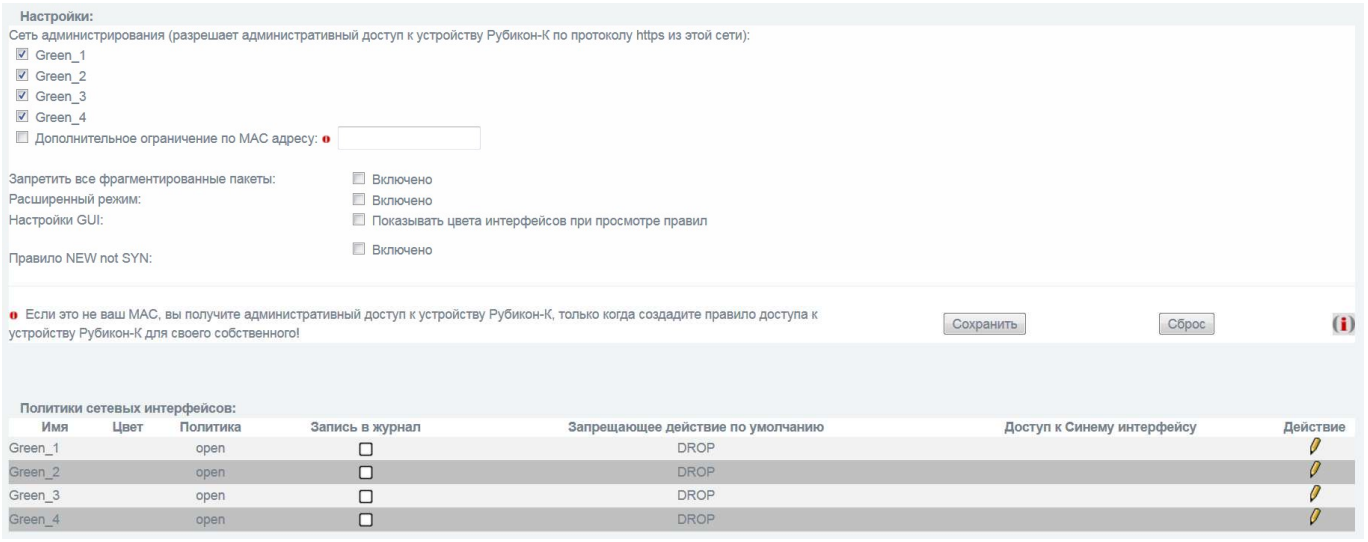


Рисунок 4 - Раздел «Межсетевой экран → Настройки межсетевого экрана»

2) цвет таких интерфейсов изменить нельзя, поэтому перед назначением цветов настройте администрирование.

– назначьте цвета интерфейсов на странице **«Сеть → Настройка адаптеров»** (рисунок 5), выполнив следующее:

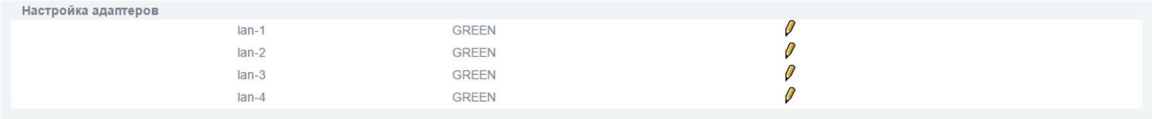


Рисунок 5 - Раздел «Сеть → Настройка адаптеров»

1) напротив нужного интерфейса нажмите кнопку редактирования;

2) выберите цвет интерфейса;

3) нажмите кнопку редактирования, для сохранения настроек;

4) номера интерфейсов внутри цвета (например, GREEN 1, RED 2) назначаются в инкрементивном порядке и не зависят от реальных имен интерфейсов;

5) настройте сетевые адреса для измененных интерфейсов в разделе **«Система → Интерфейсы»** (рисунок 6).

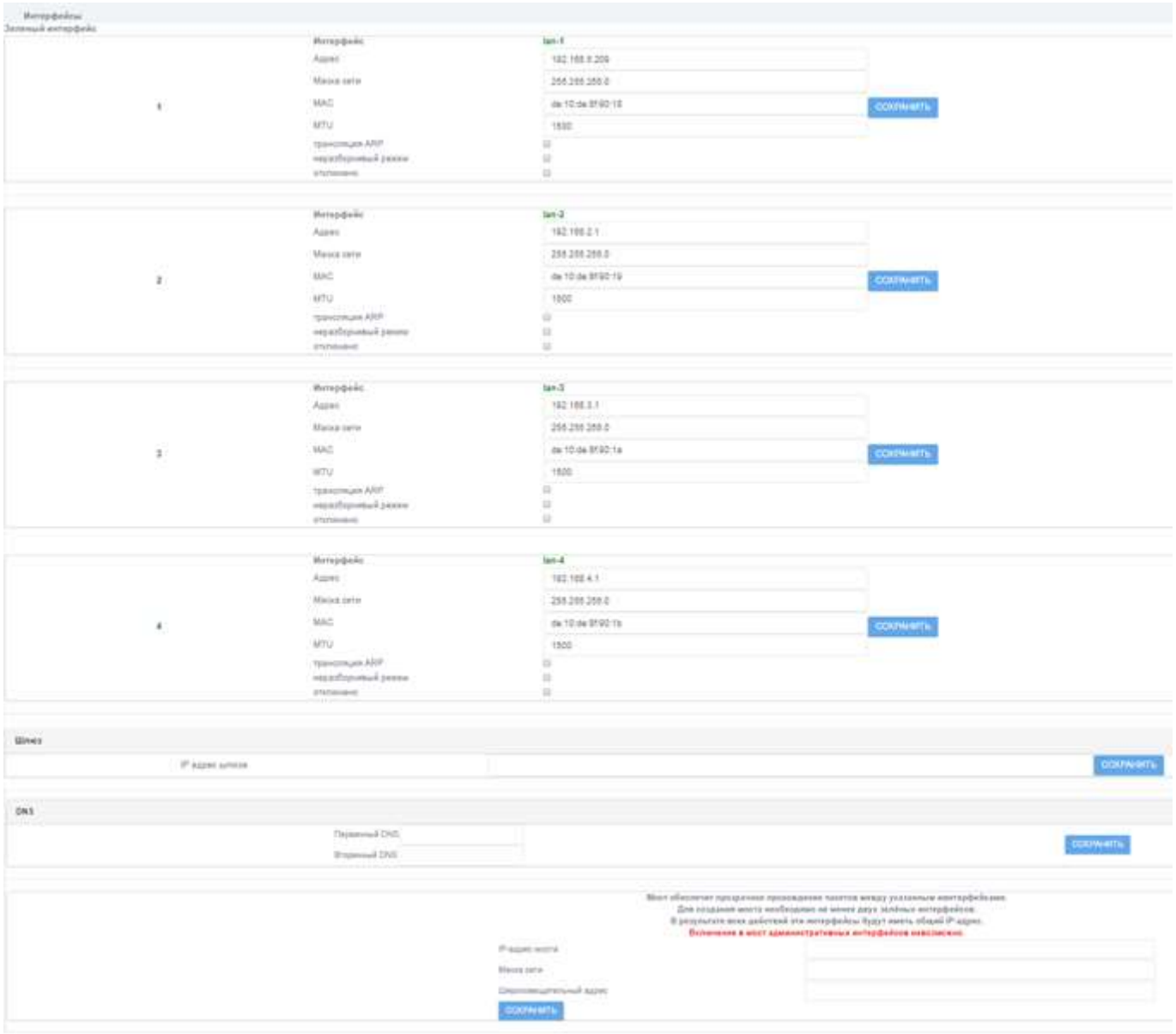


Рисунок 6 - Раздел «Система → Интерфейсы»

6.3 Ограничение трафика

В разделе **«Службы → Ограничение трафика»** установите ограничение скорости для входящих и исходящих соединений (рисунок 7).

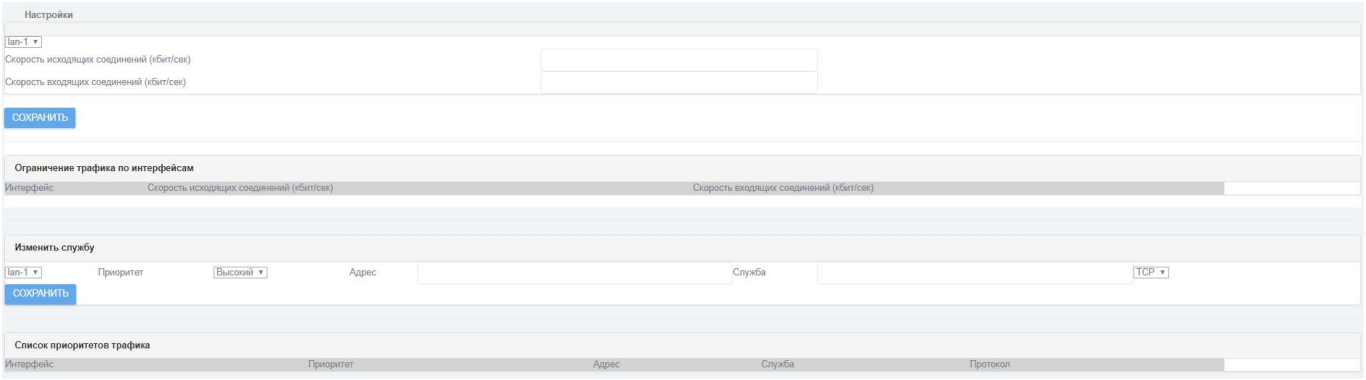


Рисунок 7 - Раздел «Службы → Ограничение трафика»

В секции **«Настройки»** выполните следующие действия:

1) выберите имя интерфейса в выпадающем списке;

2) заполните текстовое поле **«Скорость исходящих соединений (кбит/сек)»**;

3) заполните текстовое поле **«Скорость входящих соединений (кбит/сек)»**;

4) нажмите кнопку **«Сохранить»**.

В секции **«Изменить службу»** настройте приоритеты трафика (рисунок 7), для этого выполните следующие действия:

1) выберите имя интерфейса в выпадающем списке;

2) выберите **«Приоритет»** в выпадающем списке - высокий, средний или низкий;

3) заполните текстовое поле **«Адрес»**;

4) заполните текстовое поле **«Служба»**;

5) в выпадающем списке выберите протокол TCP или UDP;

6) нажмите кнопку **«Сохранить»**.

7 МЕЖСЕТЕВОЙ ЭКРАН

7.1 Общие положения

В Рубикон-К за каждым сетевым интерфейсом закреплена определенная роль или набор особенностей взаимодействия с сетью и другими интерфейсами. Каждая роль или каждый сегмент сети определяется цветом: зеленый, красный, синий и оранжевый. Правила МЭ прикрепляются к имени интерфейса (например, GREEN 1), поэтому после каждой смены ролей интерфейсов (см. 6.2) необходимо перенастраивать правила МЭ в соответствии с текущими параметрами. Подробнее о настройке сетевых интерфейсов рассказано в разделе 6.

7.2 Настройка фильтрации пакетов

Фильтрация пакетов применяется для создания правил прохождения пакетов из зеленой сети в красную, синюю, оранжевую, организации взаимодействия между физическими и виртуальными сетями, а также для настройки административного доступа к Рубикон-К.

Для настройки фильтрации пакетов выполните следующие действия:

1) настройте сетевые интерфейсы;

2) перейдите на страницу настройки: **«Межсетевой экран → Настройки межсетевого экрана»** (рисунок 4);

3) в разделе **«Расширенный режим»** поставьте галочку напротив пункта **«Включено»**;

4) нажмите кнопку **«Сохранить»;**

5) перейдите на страницу **«Межсетевой экран → Службы»**. В данном разделе можно создать свою службу, а можно посмотреть какие существуют службы по умолчанию. Чтобы добавить свою службу для МЭ заполните следующее (рисунок 8):

- в текстовом поле **«Имя службы»** напишите имя службы;
- в текстовом поле **«Порты»** укажите номер порта, инвертируйте при необходимости;

– в выпадающем списке **«Протокол»** выберите протокол, который будет использоваться, инвертируйте при необходимости;

– в выпадающем списке **«Тип ICMP»** выберите тип ICMP;

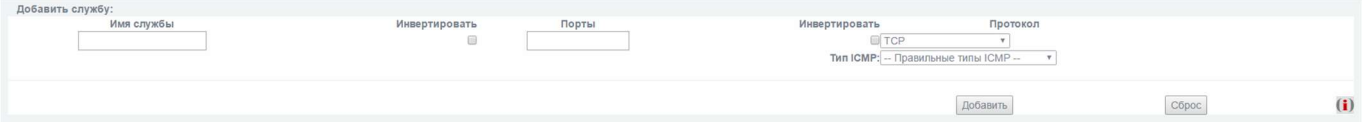


Рисунок 8 - Раздел «Межсетевой экран → Службы»

6) нажмите кнопку **«Добавить»**;

7) перейдите на страницу настройки правил фильтрации **«Межсетевой экран → Правила межсетевого экрана»** (рисунок 9);

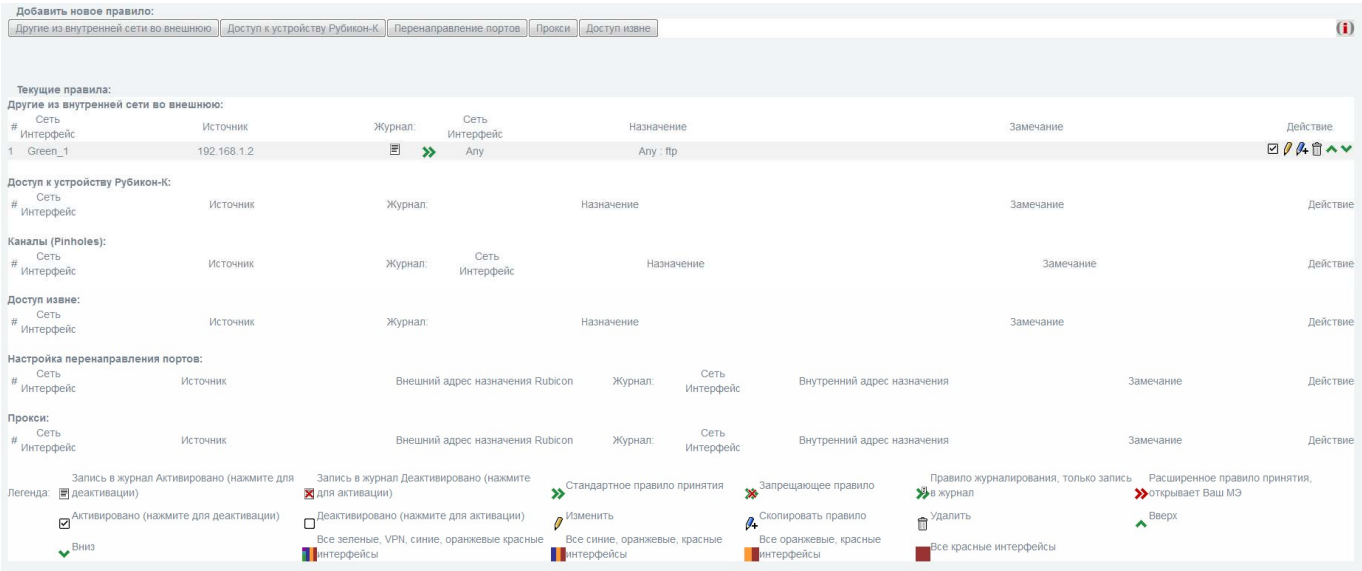


Рисунок 9 - Раздел «Межсетевой экран → Правила межсетевого экрана»

В данном разделе можно увидеть текущие правила. Текущие правила можно изменять, копировать, удалять, перемещать, активировать и деактивировать. Легенда указана внизу раздела.

8) выберите действие **«Другие из внутренней сети во внешнюю»**;

9) создайте правило (см. разделы 7.2.1-7.2.8);

10) перед тем как сохранить и применить правило, нажмите кнопку **«Далее»**, для предварительного просмотра (рисунок 10);

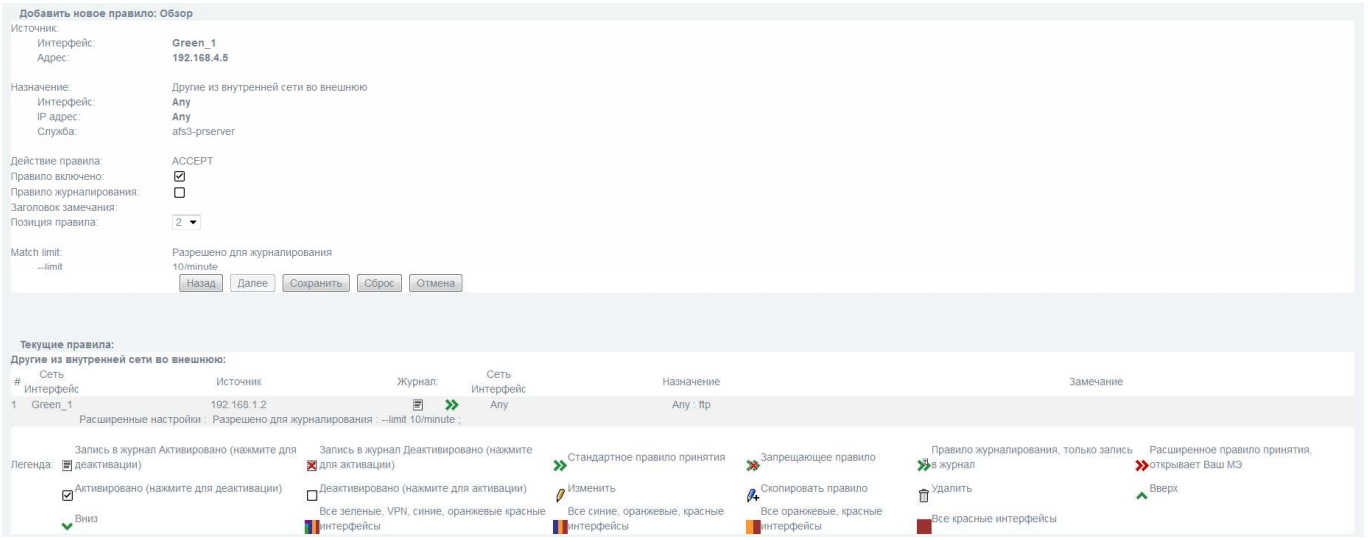


Рисунок 10 - Предварительный просмотр правила

Здесь вы можете сбросить настройки и перейти на предыдущую страницу, нажав кнопку **«Сброс»**, или уйти со страницы интерфейса, нажав кнопку **«Отмена»**.

11) откорректируйте параметры правила при необходимости;

12) нажмите кнопку **«Сохранить»**, чтобы сохранить параметры и включить правила.

7.2.1 Фильтрация по сетевому адресу отправителя

В разделе **«Другие из внутренней сети во внешнюю → Источник»** (рисунок 11):

1) поставьте переключатель в пункт меню **«Формат адреса»**;

2) в выпадающем списке выберите значение **«IP»**;

3) в текстовом поле **«Адрес источника (MAC или IP или сеть)»** укажите IP-адрес отправителя.

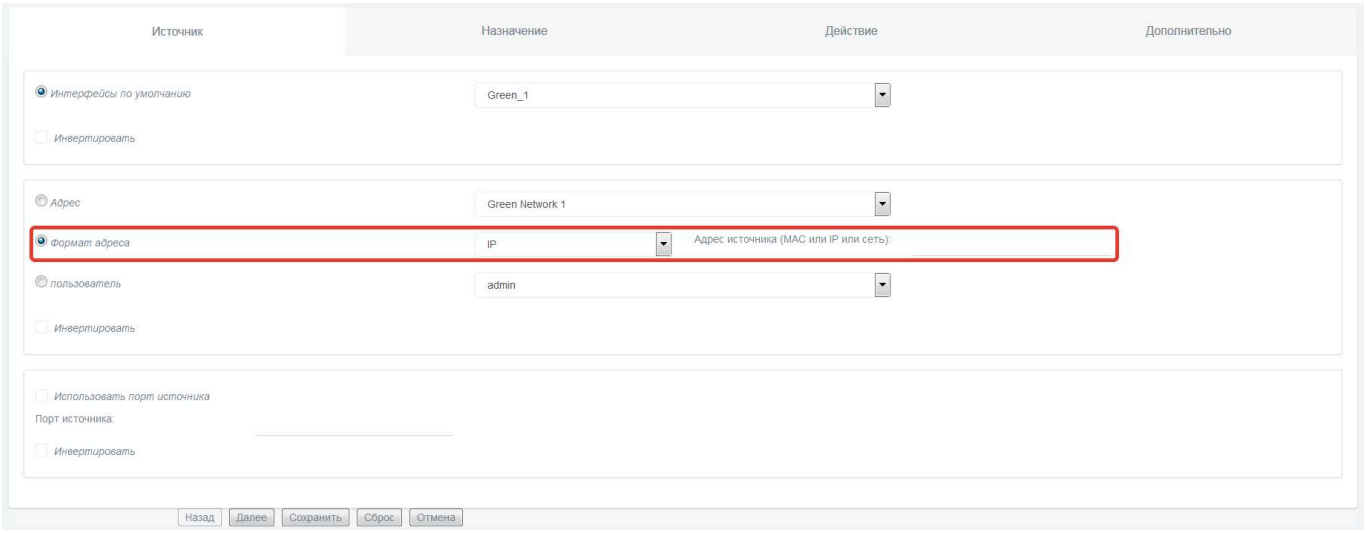


Рисунок 11 - Раздел «Источник»

7.2.2 Фильтрация по сетевому адресу получателя

В разделе **«Другие из внутренней сети во внешнюю → Назначение»** (рисунок 12):

1) поставьте переключатель в пункт меню **«IP или сеть назначения»**;

2) в текстовом поле укажите IP-адрес получателя.

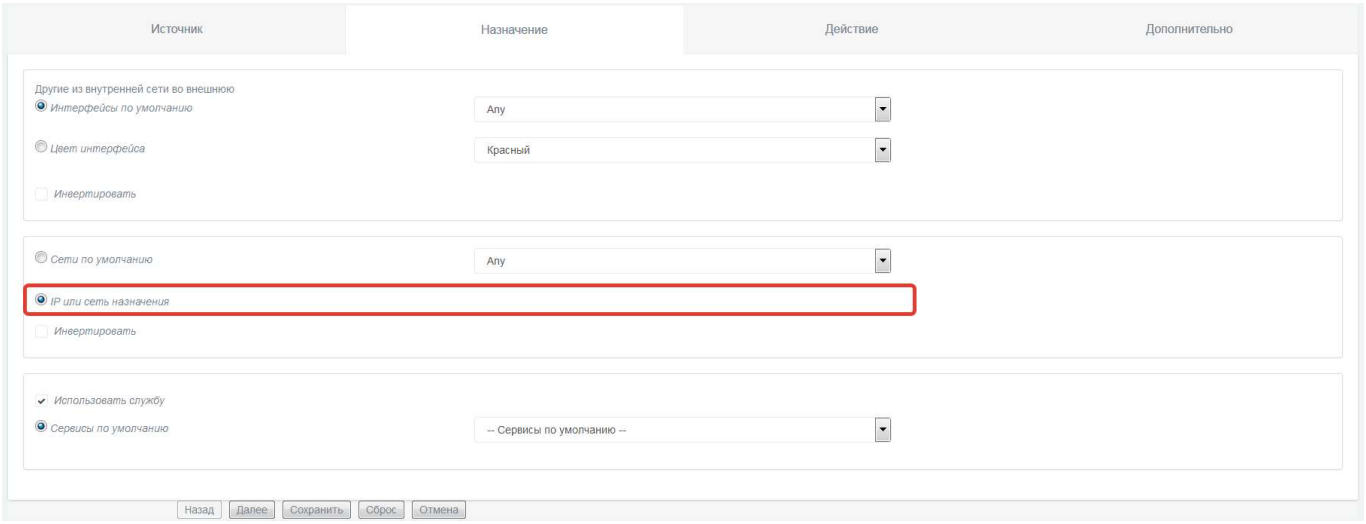


Рисунок 12 - Раздел «Назначение»

7.2.3 Фильтрация по сетевому протоколу, который используется для взаимодействия

В разделе **«Другие из внутренней сети во внешнюю → Назначение»** (рисунок 13):

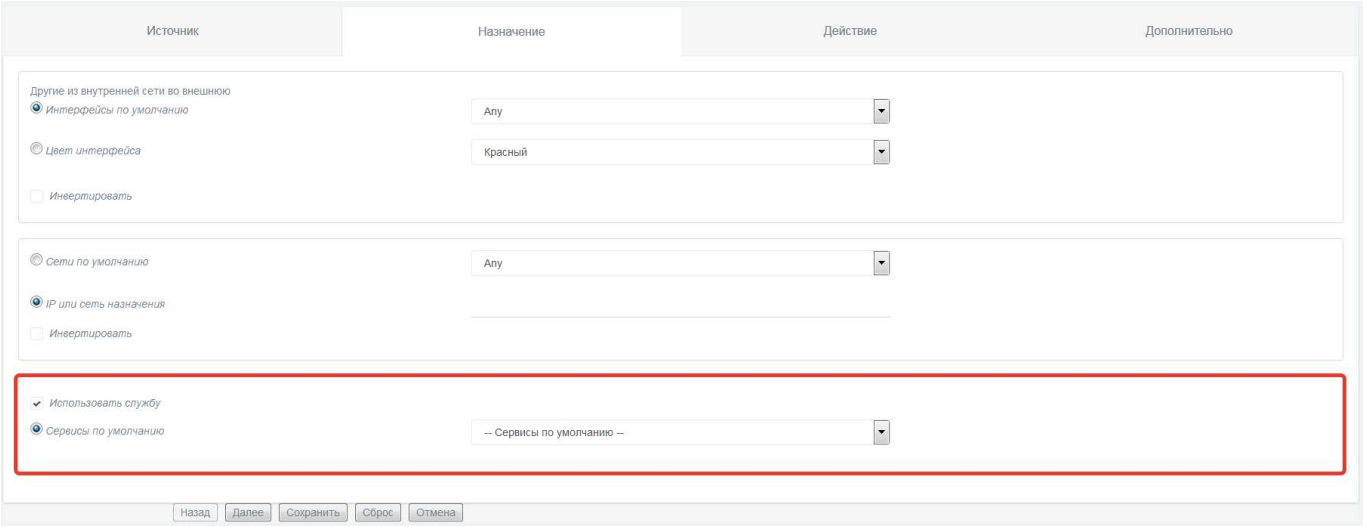


Рисунок 13 - Раздел «Назначение»

1) поставьте галочку напротив пункта **«Использовать службу»**;

2) поставьте переключатель в меню **«Свои сервисы»** или **«Сервисы по умолчанию»** в зависимости от того какую службу вы собираетесь выбрать;

3) в выпадающем списке выберите службу, использующую сетевой протокол, по которому планируется осуществление фильтрации;

Например: выберите службу по умолчанию **Ping**. Служба Ping работает по сетевому протоколу ICMP.

7.2.4 Фильтрация по направлению пакета

1) заполните поля правила в разделе **«Другие из внутренней сети во внешнюю → Источник»** — для входящего пакета (рисунок 11);

2) заполните поля правила в разделе **«Другие из внутренней сети во внешнюю → Назначение»** — для исходящего пакета (рисунок 12).

7.2.5 Фильтрация по транспортному протоколу, который используется для взаимодействия

В разделе **«Другие из внутренней сети во внешнюю → Назначение»** (рисунок 13):

1) поставьте галочку напротив пункта **«Использовать службу»**;

2) поставьте переключатель в меню **«Свои сервисы»** или **«Сервисы по умолчанию»** в зависимости от того какую службу вы собираетесь выбрать;

3) в выпадающем списке выберите службу, использующую транспортный протокол, по которому планируется осуществление фильтрации;

Например: выберите службу по умолчанию **domain**. Служба DNS использует транспортный протокол UDP.

7.2.6 Фильтрация по портам источника и получателя в рамках сеанса (сессии)

– По портам источника — в разделе **«Другие из внутренней сети во внешнюю → Источник»** (рисунок 14):

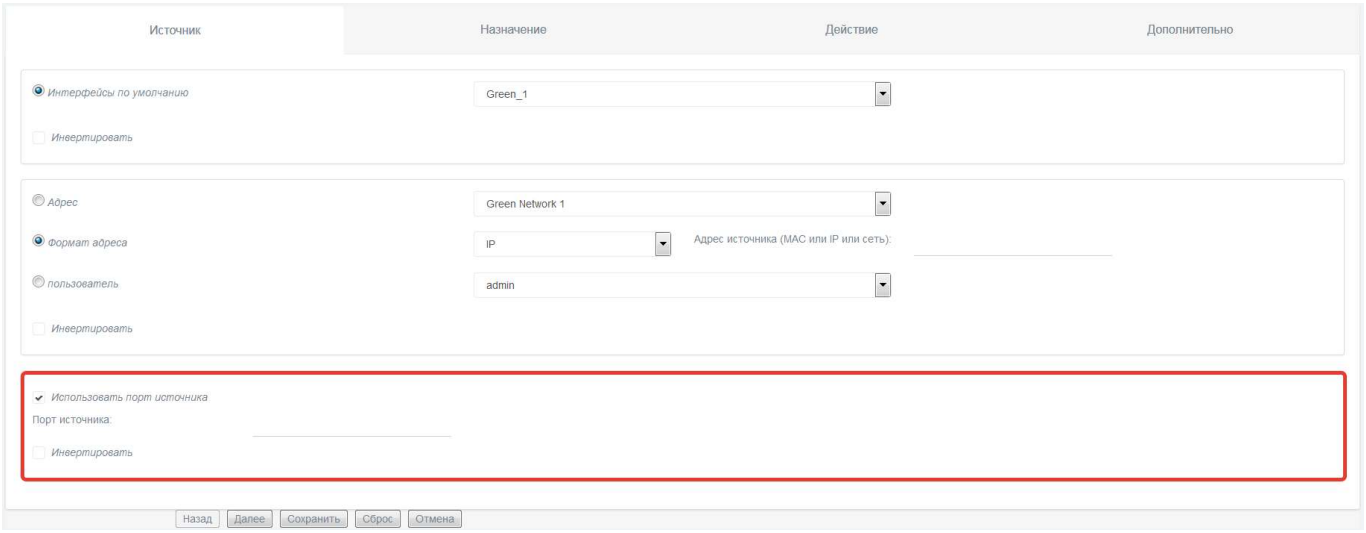


Рисунок 14 - Раздел «Источник»

Данный режим позволяет указывать порт, с которого поступают сетевые пакеты. Применяется в том случае, когда необходимо фильтровать ответные пакеты от сетевых сервисов (http-, ftp- серверы и т.п.), при этом порт назначения может не указываться, так как чаще всего он выбирается произвольно.

1) поставьте галочку напротив пункта **«Использовать порт источника»**;

2) в текстовом поле укажите порт источника, инвертируйте при необходимости.

– По портам назначения — в разделе **«Назначение»** (рисунок 13):

1) поставьте галочку напротив пункта **«Использовать службу»**;

2) поставьте переключатель в меню **«Свои сервисы»** или **«Сервисы по умолчанию»**, в зависимости от того какую службу вы собираетесь выбрать;

3) в выпадающем окне выберите необходимую службу.

Например, выберите службу по умолчанию **https**. Служба HTTPS использует порт 443.

7.2.7 Фильтрация по флагу фрагментации

В разделе **«Другие из внутренней сети во внешнюю → Дополнительно → Фильтрация по маске (4 байта)»** (рисунок 15):

– поставьте галочку напротив пункта **«Включить фильтрацию по битовой маске»**;

– если необходимо фильтровать фрагментированные пакеты:

1) в текстовом поле **«смещение»** укажите: «**7»**;

2) в текстовом поле **«маска»** укажите: **«0xff000000»**;

3) в текстовом поле **«с»** укажите: **«0x00000000»**;

4) в текстовом поле **«по»** укажите: **«0x00000000»**;

– если необходимо фильтровать нефрагментированные пакеты:

1) в текстовом поле **«смещение»** укажите: **«7»**;

2) в текстовом поле **«маска»** укажите: **«0xff000000»**;

3) в текстовом поле **«с»** укажите: **«0x01000000»**;

4) в текстовом поле **«по»** укажите: **«0x01000000»**.

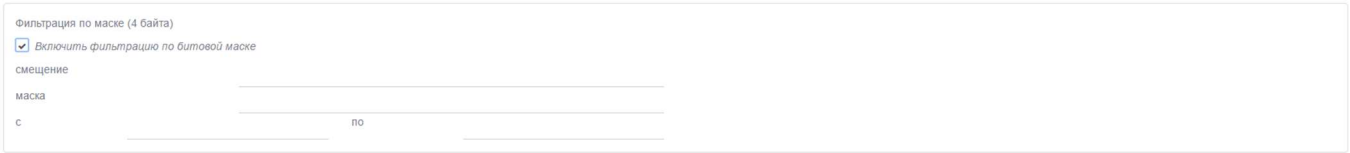


Рисунок 15 - Раздел «Фильтрация по маске» (4 байта)

7.2.8 Фильтрация по интерфейсу, через который проходит пакет

– На уровне сетевого адреса (рисунок 16):

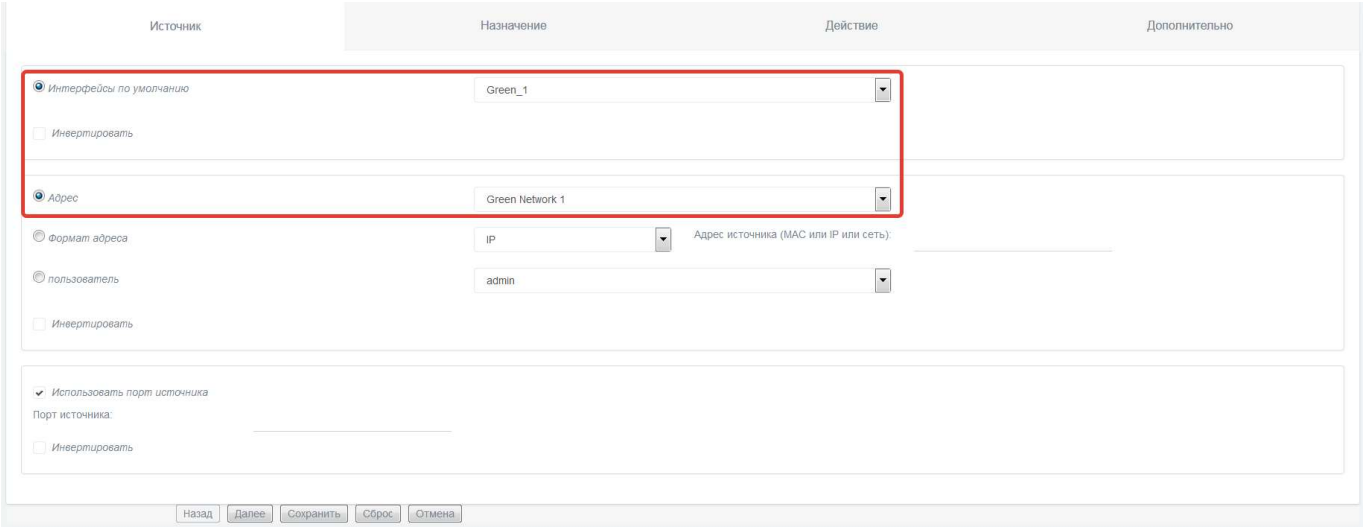


Рисунок 16 - Раздел «Доступ к устройству Рубикон-К → Источник»

1) на странице **«Межсетевой экран → Правила межсетевого экрана»** выберите действие **«Доступ к устройству Рубикон-К»**;

2) в разделе **«Источник»** поставьте переключатель в меню **«Интерфейсы по умолчанию»**;

3) в выпадающем списке выберите значение **«Any»**;

4) поставьте переключатель в меню **«Адрес»**;

5) в выпадающем списке выберите необходимое значение;

6) например, выберите сеть **«Green network 1»**.

– На физическом уровне (рисунок 17):

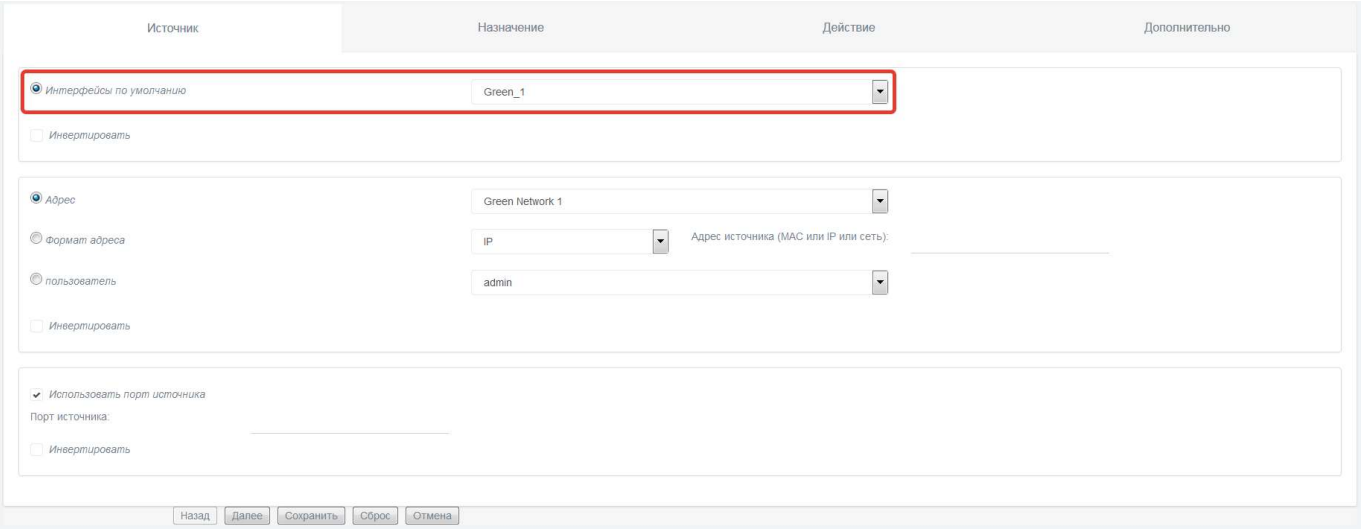


Рисунок 17 - Раздел «Доступ к устройству Рубикон-К → Источник»

1) на странице **«Межсетевой экран → Правила межсетевого экрана»** выберите действие **«Доступ к устройству Рубикон-К»**;

2) в разделе **«Источник»** поставьте переключатель в меню **«Интерфейсы по умолчанию»**;

3) в выпадающем списке выберите необходимое значение;

4) например, выберите интерфейс **«GREEN_1»**.

Повторите действия пунктов 7.2.5-7.2.7.

7.3 Настройка прокси-сервера

Веб-прокси-сервер - это программа, которая делает запросы к веб-страницам от имени других компьютеров в сети. Прокси-сервер кэширует страницы, которые получает из интернета, поэтому если 3 компьютера запрашивают одну страницу, требуется только одна передача из сети Интернет. Если имеется ряд часто используемых веб-сайтов, это поможет сэкономить время на интернет-доступе.

7.3.1 FTP посредничество

Для того чтобы включить функции прокси-сервера в МЭ перейдите в раздел **«Службы → FTP посредник»** (рисунок 18).

– **«enable ftp proxy»** - поставьте соответствующий флажок, чтобы включить функции прокси-сервера в МЭ.

– **«ftp proxy port»** - введите порт, на котором прокси-сервер будет прослушивать запросы.

– **«ftp blocked sequence»** - введите последовательность FTP команд, которая будет блокироваться.

– нажмите кнопку **«Сохранить»**.

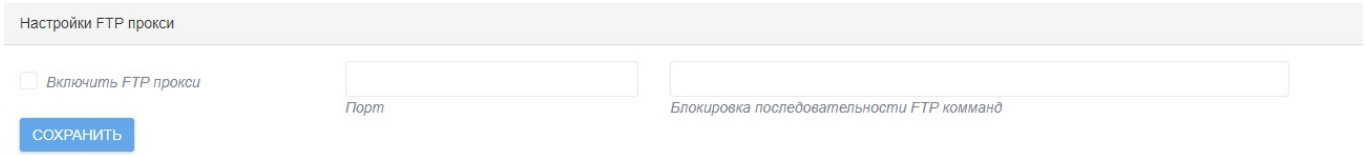


Рисунок 18 - Раздел «Службы → FTP посредник»

7.3.2 Сервисы безопасности FTP

Сервисы безопасности FTP дают возможность осуществлять проверку использования пользователем отдельных команд, их атрибутов безопасности и параметров.

Перейдите в раздел **«Службы → FTP посредник»** (рисунок 19).

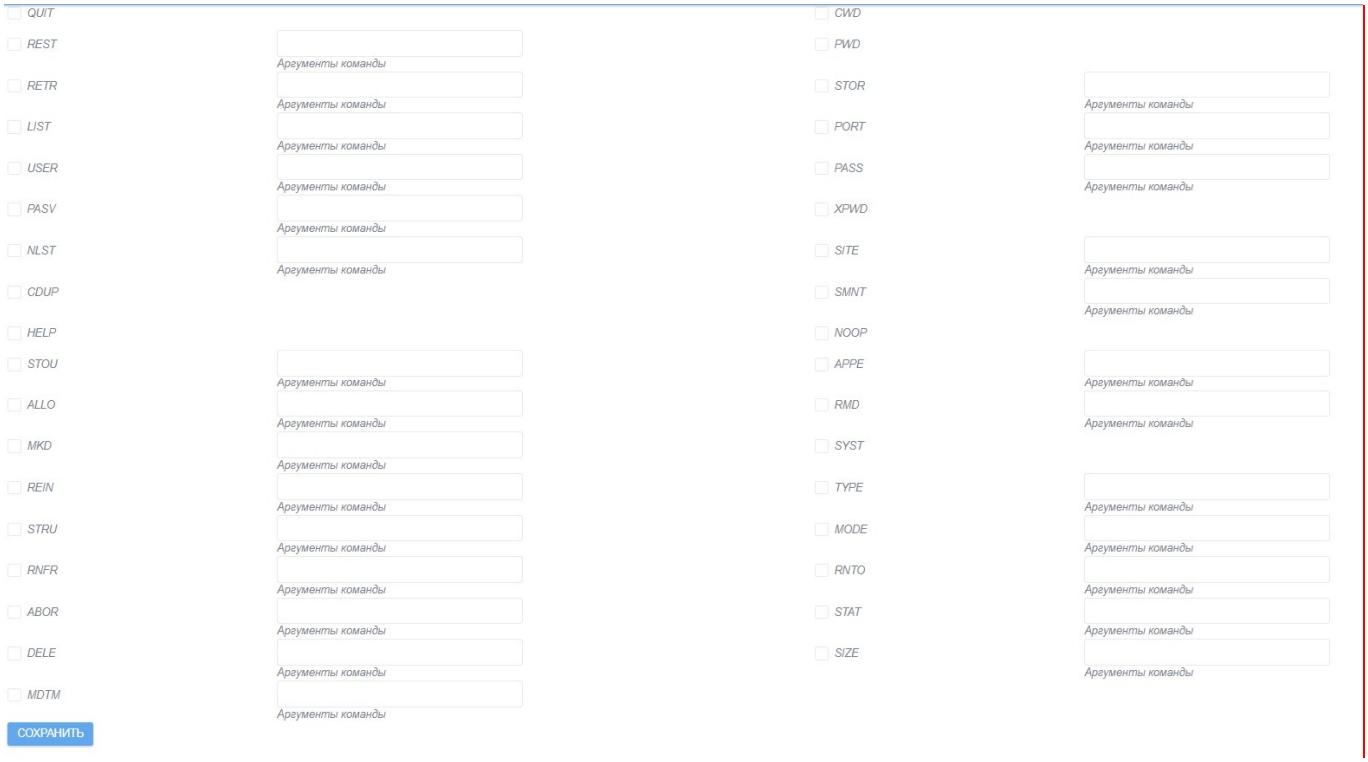


Рисунок 19 - Раздел «Службы → FTP посредник»

– выберите команду из списка;

– в поле **«filtered args» -** укажите параметр, по которому будет происходить фильтрация;

– нажмите кнопку **«Сохранить»**.

7.3.3 Веб-прокси

Перейдите в раздел **«Службы → Прокси»**. Первая строка в данном разделе показывает, запущен или остановлен прокси-сервер (рисунок 20).

Секция **«Настройки»** разделена на три подсекции:

– общие параметры;

– прокси верхнего уровня;

– настройки журналирования.

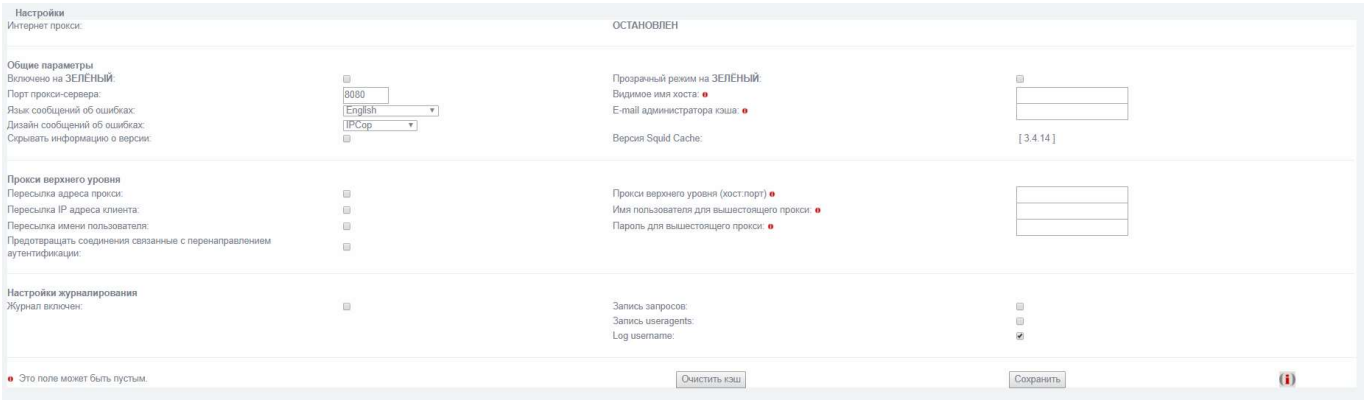


Рисунок 20 - Раздел «Службы → Прокси»

Общие параметры

Здесь вы можете настроить, чтобы прокси-запросы проходили от вашей зеленой (частной) сети и/или синей (беспроводной) сети (если она установлена). Для этого отметьте соответствующие поля (рисунок 21).

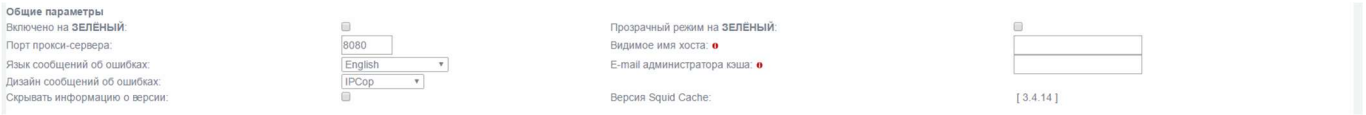


Рисунок 21 - Подсекция «Общие параметры»

– **«Включено на ЗЕЛЕНЫЙ»** поставьте соответствующий флажок, чтобы включить прокси-сервер для прослушивания запросов на выбранном интерфейсе (зеленый или синий). Если прокси-служба отключена, все клиентские запросы будут направлены непосредственно на адрес получателя.

– **«Прозрачный режим на ЗЕЛЕНЫЙ» -** если «прозрачный режим» включен, все запросы на 80 порту будут направлены к прокси-серверу без необходимости специальной настройки клиентов.

– **«Порт прокси-сервера»**. Это порт, на котором прокси-сервер будет прослушивать запросы клиента. По умолчанию 8080. В прозрачном режиме, все клиентские запросы на 80 порту будут автоматически перенаправлены на этот порт.

– **«Видимое имя хоста» -** необязательное поле. Если вы хотите, чтобы клиентам отображалось другое имя в прокси-сообщениях об ошибках сервера, или для прокси-серверов верхнего уровня, то укажите его здесь. Если вы оставите это поле пустым, будет использоваться имя вашего Рубикон-К.

– **«E-mail администратора кэша» -** необязательное поле. Вы можете указать адрес электронной почты, который появляется клиентам в прокси-сообщениях об ошибках сервера. Если оставить его пустым, будет использоваться «веб-мастер».

– **«Язык сообщений об ошибках»**. Вы можете выбрать язык, на котором прокси-сервер будет отображать сообщения об ошибках для клиентов.

– **«Дизайн сообщений об ошибках»**. Вы можете выбрать дизайн, в котором сообщения об ошибках прокси-сервера отображаются на клиентах. Вы можете выбрать между «IPCop» и «Стандартный».

Дизайн «IPCop» включает хороший графический баннер, в то время как «Стандартный» дизайн обычно поставляется с Squid.

Примечание - Если определить «Видимое имя хоста», всегда будет использоваться «Стандартный» дизайн.

– **«Скрывать информацию о версии».** Отметьте этот флажок, чтобы предотвратить отображение версии Squid Cache в сообщениях об ошибках Squid клиентам.

– **«Версия Squid Cache»**. Здесь отображаются установленные версии Squid Cache.

Прокси верхнего уровня

Эти параметры могут потребоваться в цепочке прокси окружения.

Если ваш провайдер требует использовать свой кэш для доступа к интернету, то укажите имя хоста и порт в текстовом поле **«Прокси верхнего уровня»**. Если прокси вашего провайдера требует имя пользователя и пароль, заполните текстовые поля **«Имя пользователя для вышестоящего прокси»** и **«Пароль для вышестоящего прокси»** (рисунок 22).

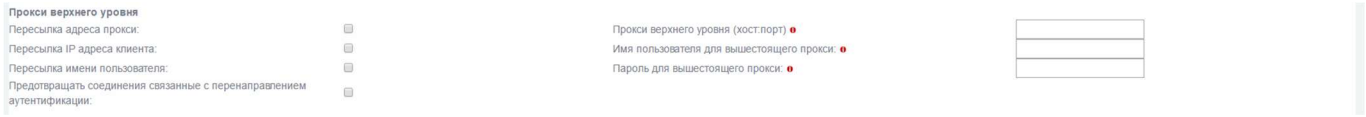


Рисунок 22 - Подсекция «Прокси верхнего уровня»

– **«Пересылка адреса прокси».** Включает HTTP VIA в поле заголовка. Если эта опция включена, эта информация будет добавлена к заголовку http.

Примечание - Если последний прокси в цепочке не удалит это поле, оно будет направлено на узел назначения!

Это поле будет скрыто по умолчанию.

– **«Пересылка IP-адреса клиента»**. Включает HTTP X-FORWARDED-FOR в поле заголовка. Если эта опция включена, внутренний IP-адрес клиента будет добавлен к http-заголовку.

Это может пригодиться для источника ACL или входа на удаленный прокси-сервер.

Примечание - Если последний прокси в цепочке не удалит это поле, оно будет направлено на узел назначения!

Вместо того чтобы переслать «неизвестный», это поле будет полностью скрыто по умолчанию.

– **«Пересылка имени пользователя»**. Если какой-либо тип аутентификации активирован, это поле позволит пересылать логин.

Это может пригодиться для пользователей на основе ACL или входа на удаленный прокси-сервер.

Примечание - Это работает для ACL или ведения журнала, и не работает, если вышестоящий прокси-сервер требует реального входа.

Эта пересылка ограничивается именем пользователя. Пароль не будет передан.

– **«Предотвращать соединения связанные с перенаправлением аутентификации»**. Отключает пересылку Microsoft соединений, ориентированных на проверку подлинности (NTLM и Kerberos).

Настройки журналирования

Рисунок 23 - Подсекция «Настройки журналирования»

– **«Журнал включен»**. Если вы решите включить прокси, то можете также включить журнала веб-посещений, включив опцию «журнал включен». Это позволит прокси-серверу вести журнал системы, который может потребоваться для устранения неполадок (рисунок 23).

Посещения через прокси можно увидеть, проверив прокси-логи веб-страницы.

В журнале также включена поддержка прокси-графиков работы.

– **«Запись запросов»**. Часть URL, содержащих динамические запросы будут удалены по умолчанию перед входом. Если включить опцию «запись запросов» то в журнале будет записан полный URL-адрес.

– **«Запись useragents»**. Включение опции «запись useragents» позволит записывать строку useragent в лог файл /var/log/squid/user_agent.log. Этот параметр журнала используется только для отладки и результаты не отображаются графическим интерфейсом для просмотра журнала.

– **«Log username»**. Включение опции «Log username» позволит записывать строку username в лог файл.

7.3.4 Расширенные настройки

Секция **«Расширенные настройки»** разделена на следующие подсекции:

– управление кэшем;

– порты назначения;

– контроль доступа по адресу;

– классные расширения;

– ограничение по времени;

– лимиты передачи;

– регулирование закачки;

– фильтр MIME типов;

– веб-браузер;

– конфиденциальность;

– redirectors;

– метод аутентификации.

Управление кэшем

Вы можете выбрать, сколько места на диске должно быть использовано для кэширования веб-страниц в разделе **«Управление кэшем»**. Вы можете также установить размер самого маленького объекта в кэш от 0 до 4096 КБ (рисунок 24).

По причинам конфиденциальности, прокси не кэширует страницы, полученные через https или другие страницы, где имя пользователя и пароль передаются через URL-адрес.

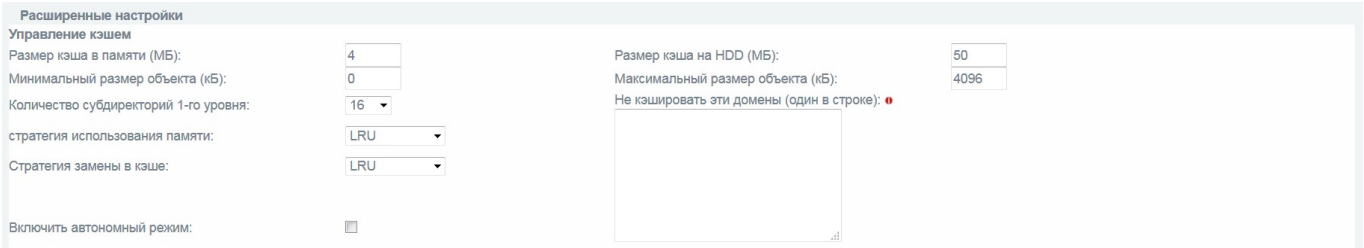


Рисунок 24 - Подсекция «Управление кэшем»

ВНИМАНИЕ! Кэширование может занимать много места на вашем жестком диске. Если использовать большой кэш, то минимальный размер жесткого диска, указанный в документации, будет недостаточно велик.

Чем больше кэш вы выберете, тем больше памяти потребуется прокси-серверу для управления кэшем. Если вы работаете сейчас на компьютере с малым объемом памяти, не выбирайте большой кэш.

– **«Размер кэша в памяти (Мб)»** - это объем физической памяти, используемой для отрицательного кэширования и транзитных объектов. Это значение не должно превышать более 50% от установленной оперативной памяти. Минимальное значение составляет 1 МБ, по умолчанию 2 МБ.

Этот параметр не определяет максимальный размер процесса. Он только ставит ограничения на то, сколько дополнительной оперативной памяти будет использоваться прокси в качестве кэша объектов.

– **«Размер кэша на HDD (Мб)»** - это тот объем дискового пространства в мегабайтах, используемый для кэширования объектов. Значение по умолчанию - 50 Мб. Измените его в соответствии с вашей конфигурацией. Не указывайте здесь весь размер вашего диска. Вместо этого, если вы хотите Squid используйте 80% от вашего диска.

Если вы хотите настроить прокси-сервер без кэширования, выполните следующие действия:

Установите параметры **«Размер кэша в памяти (Мб)»** и **«Размер кэша на HDD (Мб)»** равными **0 Мб**, чтобы полностью отключить кэширование.

– **«Минимальный размер объекта (кБ)»**. Объекты меньше этого размера не будут сохранены на диске. Значение задается в килобайтах и по умолчанию равно **0 Кб**, а это значит, что нет минимального значения.

– **«Максимальный размер объекта (кБ)»**. Объекты больше этого размера не будут сохранены на диске. Значение задается в килобайтах и по умолчанию составляет **4 Кб**. Если вы больше хотите увеличить скорость, чем сохранить пропускную способность, выйдите из этого минимума.

– **«Количество субдиректорий 1-го уровня»**. Значение по умолчанию для кэша жесткого диска субдиректорий 1-го уровня равно 16.

Каждая директория 1-го уровня содержит 256 подкаталогов, поэтому значение 256 директорий 1-го уровня будет использовать в общей сложности 65536 директорий для

кэша жесткого диска. Это значительно замедлит процесс запуска службы прокси, но может ускорить кэширование при определенных условиях.

Примечание - Рекомендуемое значение для 1-го уровня директорий равно 16. Увеличивайте это значение только тогда, когда это необходимо.

– **«Стратегия использования памяти»**. Параметр определяет, какие объекты удаляются из памяти, когда этого требует память. Политикой по умолчанию для замены в памяти является LRU.

Возможно изменение политики:

– **«LRU»**

Оригинальный список Squid, основанный на последней недавно использованной политике (Last Recently Used). Политика LRU хранит недавние ссылки на объекты. Например, он заменяет объекты, которые не использовались долгое время.

– **«heap GDSF»**

(The heap Greedy-Dual Size Frequency) политика оптимизирует объекты по скорости попаданий, сохраняя небольшие популярные объекты в кэше, потому что они имеют больший коэффициент попаданий. Она обеспечивает более низкий уровень совпадения байтов, чем LFUDA, так как она заменяет больше (возможно, популярных) объектов.

– **«heap LFUDA»**

(Least Frequently Used with Dinamic Aging) наименее часто использующиеся объекты с динамическим старением. Эта политика сохраняет популярные объекты в кэше независимо от коэффициента попаданий байтов, за счет скорости так как, один большой, популярный объект позволит предотвратить множество мелких, менее популярных объектов, которые не должны кэшироваться.

– **«heap LRU»**

(Last Recently Used policy implemented using a heap) Последняя недавно использованная политика, с использованием кучи. Работает как LRU, но отличается использованием кучи.

Примечание - При использовании политики замены LFUDA, значение параметра **«Максимальный размер объекта (кБ)»** должно быть больше размера по умолчанию 4096 КБ, чтобы максимизировать потенциальное улучшение скорости попадания байт реализованное LFUDA.

– **«Стратегия замены в кэше»**. Замена параметра политики кэша решает, какие объекты останутся в кэше, а какие объекты будут исключены (заменены), чтобы создать пространство для новых объектов. Политикой по умолчанию для замены кэша является LRU.

– **«Включить автономный режим»**. Включение этой опции позволит отключить проверку кэшированных объектов. Это дает доступ к более кэшированной информации (устаревшие кэшированные версии, с которыми исходный сервер уже соединился).

– **«Не кэшировать эти домены» -** необязательное поле. Список сайтов, запрос которых не может быть удовлетворен из кэша и ответ которых не кэшируется. Другими словами, используйте это, чтобы объекты не кэшировались.

Порты назначения

В этих полях содержатся списки разрешенных стандартных портов для http и зашифрованных SSL портов для https-запросов.

Порты могут быть определены как единый номер порта или как диапазон портов (рисунок 25).

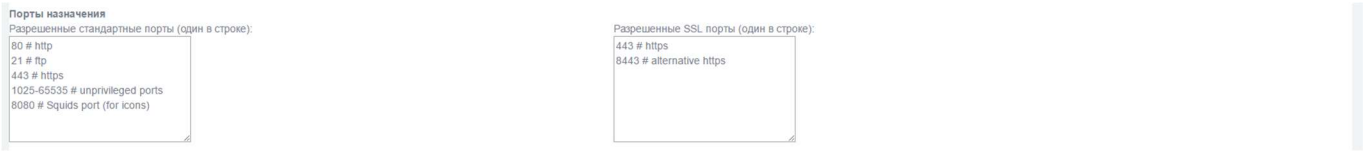


Рисунок 25 - Подсекция «Порты назначения»

Контроль доступа по адресу

Здесь можно контролировать доступ к прокси-серверу на основе сетевого адреса клиента (рисунок 26).

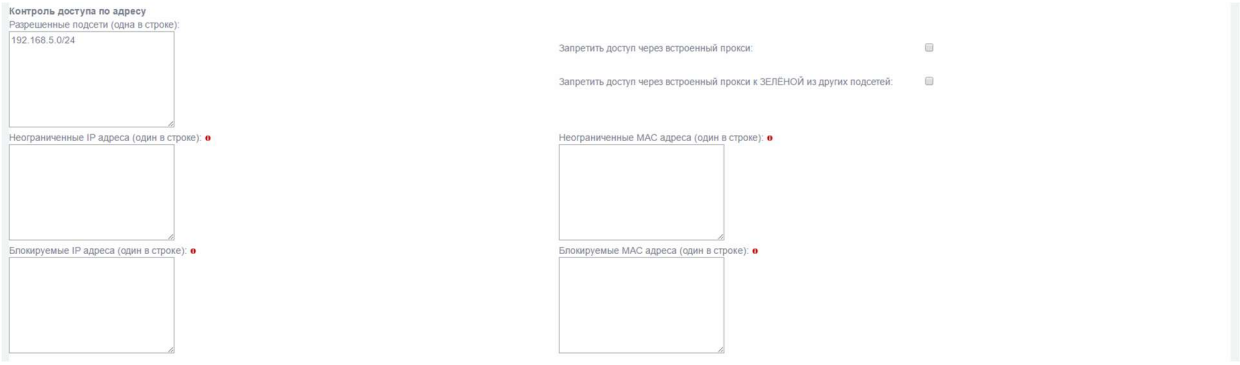


Рисунок 26 - Подсекция «Контроль доступа по адресу»

– **«Разрешенные подсети»**. Для всех перечисленных подсетей разрешен доступ к прокси-серверу. По умолчанию зеленые и синие (если имеются) подсети перечислены здесь.

Вы можете добавить другие подсети, например, подсети за зелеными подсетями в крупных средах, в этот список. Доступ в интернет будет заблокирован для всех подсетей, которые здесь не перечислены.

– **«Запретить доступ через встроенный прокси»**. Этот параметр предотвращает прямой доступ к http через встроенный прокси для локальных веб-серверов, в подсетях определенных выше. Этот выбор переопределяет следующие два параметра, которые управляют доступом по протоколу http к зеленой подсети из синей подсети.

– **«Запретить доступ через встроенный прокси к ЗЕЛЁНОЙ из других подсетей»**. Этот параметр предотвращает прямой http доступ через встроенный прокси веб-сервера к зеленой подсети из любой другой подсети (например, синей).

Например, пока разрешен доступ через встроенный прокси к зеленой и синей подсетям, все запросы, как правило, будут пересылаться на красную подсеть. Но если клиент из синей подсети хочет получить доступ к веб-серверу из зеленой подсети, встроенный прокси-сервер найдет короткий путь между синим и зеленым интерфейсом, независимо от правил МЭ.

Примечание - Для защиты вашего сервера находящегося в зеленой подсети, рекомендуется включить эту опцию и использовать фильтр адресов или ДМЗ при необходимости.

– **«Неограниченные IP-адреса»** - необязательное поле. Для всех клиентских IP-адресов в этом списке будет переопределены следующие ограничения:

1) ограничения времени;

2) предельные размеры для запросов на загрузку;

3) регулирование загрузки;

4) проверка браузера;

5) фильтр MIME типов;

6) аутентификация (требуется по умолчанию для данных адресов, но может быть отключена);

7) одновременный вход одного пользователя на разных ЭВМ (доступно, только если включена проверка подлинности).

– **«Неограниченные MAC-адреса» -** необязательное поле. Для всех MAC-адресов клиентов в этом списке будет переопределены следующие ограничения:

1) ограничения времени;

2) предельные размеры для запросов на загрузку;

3) регулирование загрузки;

4) проверка браузера;

5) фильтр MIME типов;

6) аутентификация (требуется по умолчанию для данных адресов, но может быть отключена)

7) одновременный вход одного пользователя на разных ЭВМ (доступно, только если включена проверка подлинности)

Примечание - Прокси-сервер может определить MAC-адреса клиентов, настроенных для подсетей зеленых, синих или оранжевых интерфейсов.

– **«Блокируемые IP-адреса» -** необязательное поле. Все запросы от клиентов (IP-адресов или подсетей), перечисленные здесь, будут заблокированы.

– **«Блокируемые MAC-адреса» -** необязательное поле. Все запросы от клиентов в этом списке будут заблокированы.

Классные расширения

Классные расширения (ClassRoom Extensions) для прокси-сервера дают возможность делегировать административные задачи, чтобы пользователи без административных прав могли управлять веб-доступом через отдельную страницу (рисунок 27).

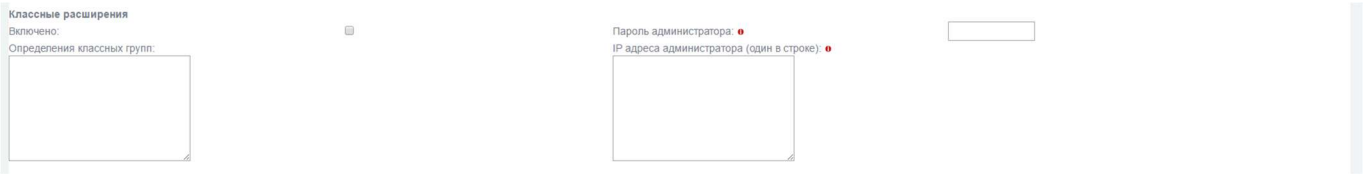


Рисунок 27 - Подсекция «Классные расширения»

– **«Включено»**. Установите этот флажок, чтобы включить административный интерфейс управления веб-доступом.

– **«Пароль администратора»** - необязательное поле. Если этот пароль установлен, введите пароль для управления веб-доступом. Это необязательно, но по соображениям безопасности, либо установите пароль администратора, либо определите IP-адреса администратора.

– **«IP-адреса администратора»** - необязательное поле. Это поле позволяет определить IP-адреса, которые смогут управлять веб-доступом. Это необязательный элемент конфигурации, который может быть использован для повышения безопасности и упрощения управления, если вы не хотите, настраивать пароль администратора.

Высокий уровень безопасности достигается в том случае, если установлен пароль администратора, и IP ограничения, как будет описано ниже в разделе - уровни безопасности.

– **«Определения классных групп»** - определения классных групп вводятся в это поле. Определение классных групп имеют следующий формат:

```
[groupname]
client MAC address or client IP address or IP range or IP subnet
client MAC address or client IP address or IP range or IP subnet
client MAC address or client IP address or IP range or IP subnet
```

Ниже приведены примеры таких 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
```

Каждая группа имеет уникальное имя. Имя группы заключено в квадратные скобки. Это имя будет отображаться в интерфейсе управления веб-доступом.

Каждая группа может иметь неограниченное количество адресов клиентов. Можно использовать смешанные адреса клиента в группе, но каждый адрес должен быть в одной строке. Вот некоторые примеры:

– один хост - MAC-адрес

```
01:23:45:67:89:0A
```

– один хост - IP-адрес

```
192.168.1.11
```

– диапазон хостов

```
192.168.1.21-192.168.1.25
```

– подсеть (обозначение маски подсети)

```
192.168.1.32/255. 255.255.240
```

– подсеть (обозначение CIDR)

```
192.168.1.32/28
```

Уровни безопасности классных расширений:

– **Уровень 1**: Нет пароля, нет ограничения на IP-адреса - нет защиты. Все клиенты могут управлять веб-доступом без каких-либо ограничений. Не рекомендуется для рабочих сред.

Примечание - Используйте первый уровень только для отладки и тестирования!

– **Уровень 2**: Установлен пароль, нет ограничения на IP-адреса - низкий уровень защиты. Все клиенты могут управлять веб-доступом, но требуется пароль, для сохранения изменений. Данный уровень безопасности рекомендуется в среде без специального компьютера администратора.

– **Уровень 3**: Нет пароля, установлены IP ограничения - низкий уровень безопасности. Все перечисленные клиенты могут изменять настройки веб-доступа. Клиенты идентифицируются по их IP-адресу, для сохранения изменений пароль не требуется.

Примечание - Если IP-адрес клиента не указан в списке, интерфейс управления веб-доступом появится в режиме "только для просмотра".

– **Уровень 4**: Установлен пароль и IP ограничения - высокий уровень безопасности. Самый высокий уровень безопасности для интерфейса управления веб-доступом. Только перечисленные клиенты могут изменять параметры, требуется пароль для сохранения изменений.

Примечание - Если IP-адрес клиента не указан в списке, интерфейс управления веб-доступом появится в режиме "только для просмотра".

Ограничения по времени

Эта подсекция определяет время активности веб-прокси. По умолчанию используется, для обеспечения доступа 24 часа в сутки, 7 дней в неделю (рисунок 28).

Рисунок 28 - Подсекция «Ограничения по времени»

Опция **«Разрешить»** разрешает веб-доступ, а опция **«Запретить»** блокирует веб-доступ в пределах выбранного периода времени. От выбора между **«Разрешить»** или **«Запретить»** будет зависеть время действия правила, которое вы хотите применить.

Временные ограничения не будут влиять на следующих клиентов:

– неограниченные IP-адреса;

– неограниченные MAC адреса;

– члены группы **«Расширенный»**, если прокси-сервер использует **«Локальную аутентификацию»**.

Лимиты передачи

Эта подсекция позволяет ввести ограничения на размер каждого скачанного и/или загруженного запроса. Значения приведены в килобайтах (КБ). Вы можете использовать данную подсекцию, чтобы запретить пользователям загружать большие файлы, из-за которых замедлится доступ в интернет для всех остальных пользователей (рисунок 29).

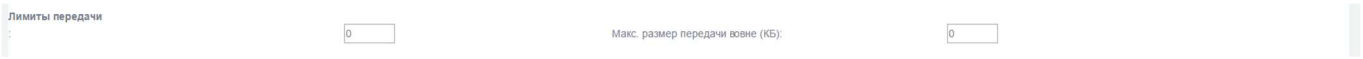


Рисунок 29 - Подсекция «Лимиты передачи»

Установите **«Максимальный размер файла»** и **«Максимальный размер передачи вовне (КБ)»**. По умолчанию стоит **«0»**, чтобы снять все ограничения.

Ограничения загрузки не коснутся следующих клиентов:

– неограниченные IP-адресов;

– неограниченные MAC-адресов;

– члены группы **«Расширенный»**, если прокси-сервер использует **«Локальную аутентификацию»**.

Регулирование закачки

Трафик загрузки может быть не ограничен, или ограничен для зеленого или синего интерфейса и/или хоста на основе типа содержимого (рисунок 30).

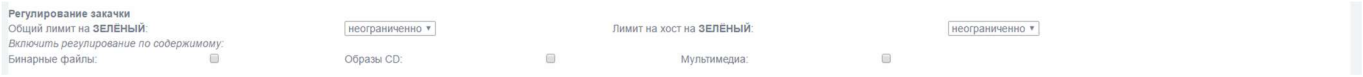


Рисунок 30 - Подсекция «Регулирование закачки»

Регулирование не повлияет на следующих клиентов:

– неограниченные IP-адреса;

– неограниченные MAC-адреса.

Ограничение трафика может быть определено для зеленого или синего интерфейса в качестве общего лимита, и для каждого узла. Используемый трафик для всех хостов будет ограничен общим лимитом.

По умолчанию, регулирование затрагивает все виды трафика, но регулирование может быть ограничено определенными типами контента. Однако это отключает регулирование для других типов контента.

Регулирование контента может быть применено к:

– бинарным файлам: bz2, bin, dmg, exe, sea, tar, tgz, zip и т.д.;

– CD-образам: ccd, cdi, img, iso, raw, tib и т.д.;

– мультимедийным файлам: aiff, avi, divx, mov, mp3, mp4, mpeg, qt и т.д.

Фильтр MIME типов

Фильтр MIME типов может быть настроен на блокирование содержимого в зависимости от его типа.

– **«Включено»**. Если фильтр включен, проверяются все входящие заголовки MIME-типа.

– **«Блокировать эти MIME типы» -** необязательное поле. Если запрошенный MIME тип будет заблокирован, доступ к нему будет запрещен. Таким образом, Вы можете заблокировать контент, независимо от того, какой тип расширения имени файла используется.

Например, добавьте MIME типы в одной строке, если хотите заблокировать скачивание файлов Word:

```
application/msword
```

Или добавьте эти MIME типы, каждый тип в отдельной строке, если хотите заблокировать скачивание MPEG и QuickTime видео файлов:

```
video/mpeg
video/quicktime
```

– **«Не фильтровать следующие направления» -** необязательное поле. Используйте этот список, чтобы избежать фильтрации MIME конкретных адресатов. Это должен быть список, доменов или субдоменов, имена хостов, IP-адреса или URL, каждый на отдельной строке.

Ниже приведены примеры:

```
*.example.net
www.example.net
123.45.67.89
www.example.net/downloads
```

Веб-браузер

– **«Включить проверку браузера»**. Установите этот флажок, если хотите включить проверку браузера.

– **«Разрешенные клиенты для веб-доступа»**. Установите соответствующий флажок / флажки для разрешенных клиентов (рисунок 31).

Рисунок 31 - Подсекция «Веб-браузер»

Конфиденциальность

В данной подсекции можно изменить некоторые поля заголовка http для защиты конфиденциальности (рисунок 32).

Рисунок 32 - Подсекция «Конфиденциальность»

– **«Замена useragent посылаемого внешним сайтам»** - необязательное поле. 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.

С опцией **«замена useragent»** у вас есть возможность переписать эту строку для всех своих клиентов. Для исходящих запросов поле заголовка useragent будет заменено прокси-сервером и передано на внешние сайты вместо исходной строки useragent. Это может быть полезно для защиты конфиденциальности или для обеспечения желаемого уровня совместимости.

– **«Замена referer посылаемого внешним сайтам» -** необязательное поле. 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 адреса. Опция может быть полезна для защиты конфиденциальности.

Примечание - Изменение referer нарушает стандарт http и иногда могут возникнуть трудности. Некоторые сайты блокируют запросы с неверным referer, чтобы защитить себя от так называемого внешнего связывания (deep link) или злоупотребления «кражей» графики с веб-сайта.

Redirectors

Redirectors работают с прокси для фильтрации и перенаправления веб-трафика на основе правил, которые могут включать в себя черные списки, белые списки, временные ограничения и т. д (рисунок 33).

Рисунок 33 - Подсекция «Redirectors»

– **«Включено»**. Установите флажок, чтобы включить перенаправление.

– **«Number of redirector processes»**. Вы можете увеличить или уменьшить количество активных процессов фильтрации. Количество процессов зависит от производительности вашего оборудования, пропускной способности и числа одновременных клиентов. Значением по умолчанию является 5.

– **«Available redirectors»**. Отображает список установленных redirectors, и показывает, какие из них активны. На рисунке 35 показано, что **«URL-filter»** неактивен.

Метод аутентификации

Веб-прокси предлагает несколько методов аутентификации пользователей (рисунок 34).

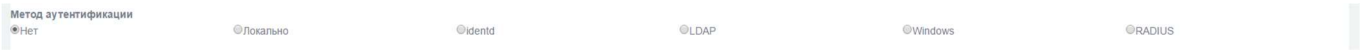


Рисунок 34 - Подсекция «Метод аутентификации»

– **«Нет» (по умолчанию)**. Проверка подлинности отключена. Пользователи не должны авторизовываться, при доступе к веб-сайтам.

– **«Локально»**. Этот метод аутентификации является наиболее оптимальным решением для домашних офисов. Пользователи проходят проверку подлинности для доступа к веб-сайтам, путем введения правильного имени пользователя и пароля.

– **«identd»**. Этот метод аутентификации является наиболее оптимальным решением для сред, где:

- проверка подлинности должна быть «скрытым» процессом, без введения логина и пароля;
- прокси-служба должна работать в прозрачном режиме;
- имя пользователя будет использоваться только для входа, а не для проверки подлинности.

Метод проверки подлинности identd требует identd-сервиса или daemon (программа, работающая в фоновом режиме и выполняющая определённые функции без ведома пользователя) запущенной на клиенте.

– **«LDAP»**. Этот метод аутентификации является наиболее оптимальным решением для средних и крупных сетевых сред. Пользователи будут проходить аутентификацию при входе на веб-сайты, путем введения правильных имени пользователя и пароля. Учетные данные сверяются с внешним сервером с использованием облегченного протокола доступа к каталогам (LDAP).

Проверка подлинности LDAP будет полезна, если у вас уже есть служба каталогов в сети, и вы не хотите сохранять дополнительные учетные записи пользователей и пароли для веб-доступа.

– **«Windows»**. Этот метод аутентификации является наиболее оптимальным решением для небольших и средних сетевых сред. Пользователям нужно будет аутентифицироваться при доступе к веб-сайтам. Учетные данные сверяются с внешним сервером, выступающего в качестве контроллера домена.

– **«RADIUS»**. Этот метод аутентификации является наиболее оптимальным решением для небольших и средних сетевых сред. Пользователям нужно будет аутентифицироваться при доступе к веб-сайтам. Учетные данные сверяются с внешним сервером Radius.

Примечание - При использовании аутентификации и включении в веб-прокси лог-файлов, запрашиваемое имя пользователя будет зарегистрировано в дополнение к URL-адресу. Перед включением лог-файлов при использовании аутентификации, убедитесь, что не нарушаете существующих законов.

Включение взаимодействия с СЗИ

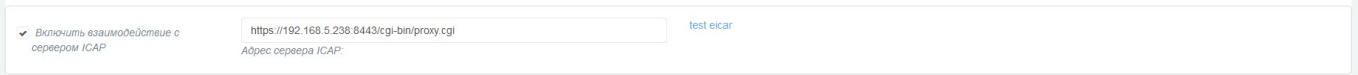


Рисунок 35 - Подсекция «Включение ICAP»

Примечание - Возможность взаимодействия с антивирусом Касперского 5.5 для Proxy Server. Для этого в поле «Адрес сервера ICAP» указывать в формате: icap://addr:port/av/respmod, где addr и port это IP-адрес и порт антивируса.

– **«Включить взаимодействие с сервером ICAP»**. Для того чтобы включить возможность подключения чужого СЗИ, поставьте флажок.

– **«Адрес сервера ICAP»**. В текстовом поле напишите адрес СЗИ. Он будет использован при осуществлении функции прокси МЭ (рисунок 35).

Включение фильтрации по мобильному коду

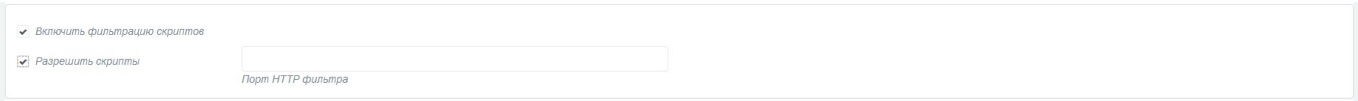


Рисунок 36 - Подсекция «Включение фильтрации скриптов»

– **«Включить фильтрацию скриптов»**. Для того чтобы включить фильтрацию по скрипту, поставьте флажок.

– **«Разрешить скрипты»**. Для того чтобы включить поддержку скриптов, поставьте флажок. В текстовом поле напишите номер порта к которому нужно обращаться (рисунок 36).

7.3.5 Очистить кэш / сохранить

– **«Очистить кэш»**. Вы можете очистить все страницы из кэша прокси-сервера в любой момент нажатием кнопки «очистить кэш».

– **«Сохранить»**. После внесения изменений, нажмите кнопку «Сохранить», чтобы применить их (рисунок 37).

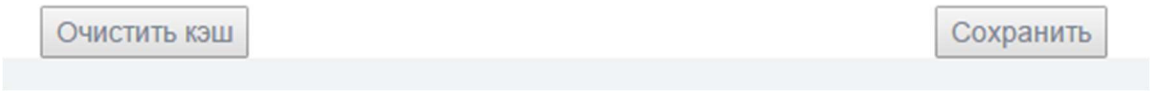


Рисунок 37 - Очистить / сохранить кэш

7.4 Трансляция сетевых адресов

Трансляция сетевых адресов осуществляется автоматически на красном интерфейсе при прохождении сетевого пакета из зеленой подсети. Адрес источника пакета заменяется адресом красного интерфейса Рубикон-К. Изменение трансляции сетевых адресов не предусмотрено.

7.5 Маскирование

Для осуществления замены сетевого адреса на маскирующий адрес (подставной адрес) следующие действия:

– переназначьте цвет маскируемого интерфейса на красный - RED (см. раздел 6.2);

– перейдите в раздел **«Система → Интерфейсы»** (рисунок 38). В настройках красного интерфейса появится новое поле **«mask address»**;

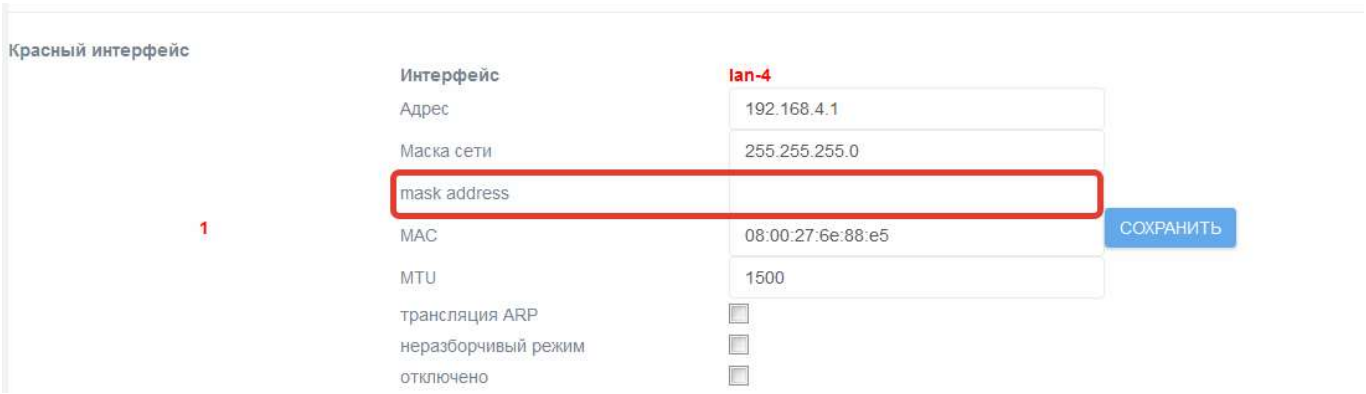


Рисунок 38 - Раздел «Система → Интерфейсы»

– введите маскирующий адрес, заполнив текстовое поле **«mask address»**.

7.6 Трансляция портов

Трансляция портов осуществляется для обеспечения подключения узлов красной подсети к узлам, к которым необходим доступ извне, то есть для организации демилитаризованной зоны.

Для настройки трансляции портов выполните следующие действия:

– настройте сетевые адреса красного и оранжевого или зеленого интерфейса (рисунок 6);

– перейдите на страницу настройки правил фильтрации: **«Межсетевой экран → Правила межсетевого экрана»** (рисунок 9);

– нажмите на кнопку **«Перенаправление портов»**;

– настройте правило фильтрации, заполнив:

1) в разделе **«Источник»** информацию о параметрах источника пакета (адрес, порт) (рисунок 39);

2) в разделе **«Источник»** номер протокола или сервис, который Рубикон-К предоставляет в красную подсеть для доступа к требуемому узлу внутренней подсети (рисунок 39);

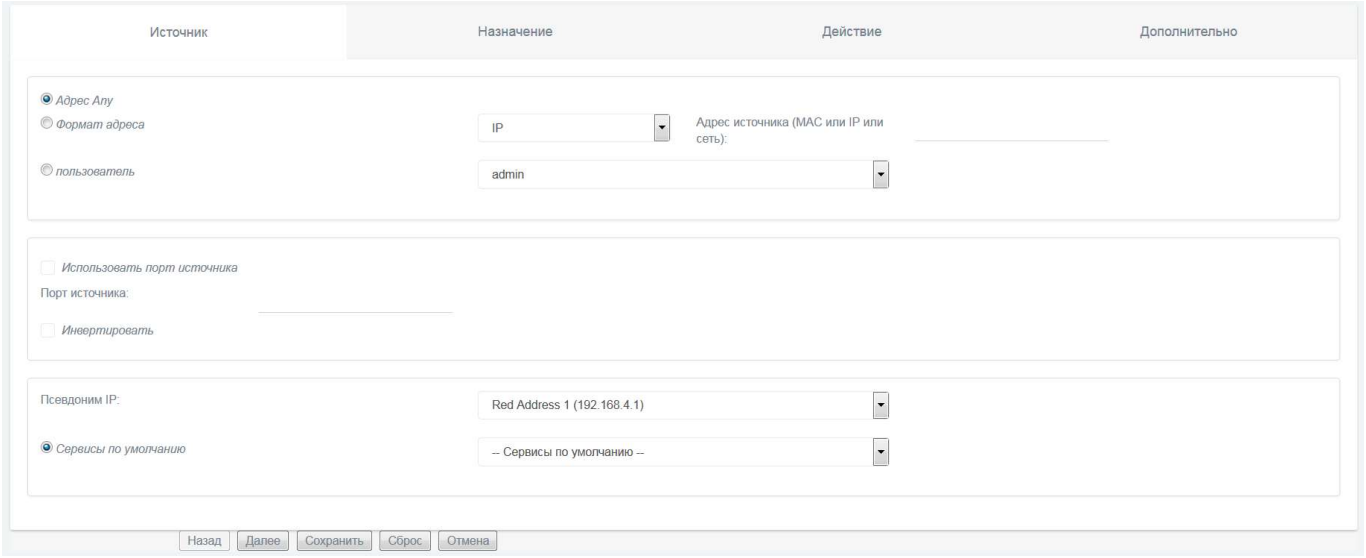


Рисунок 39 - Раздел «Источник»

3) в разделе **«Назначение»** информацию о месте назначения (интерфейс, адрес, порт, предоставляемый конкретным узлом) (рисунок 40);

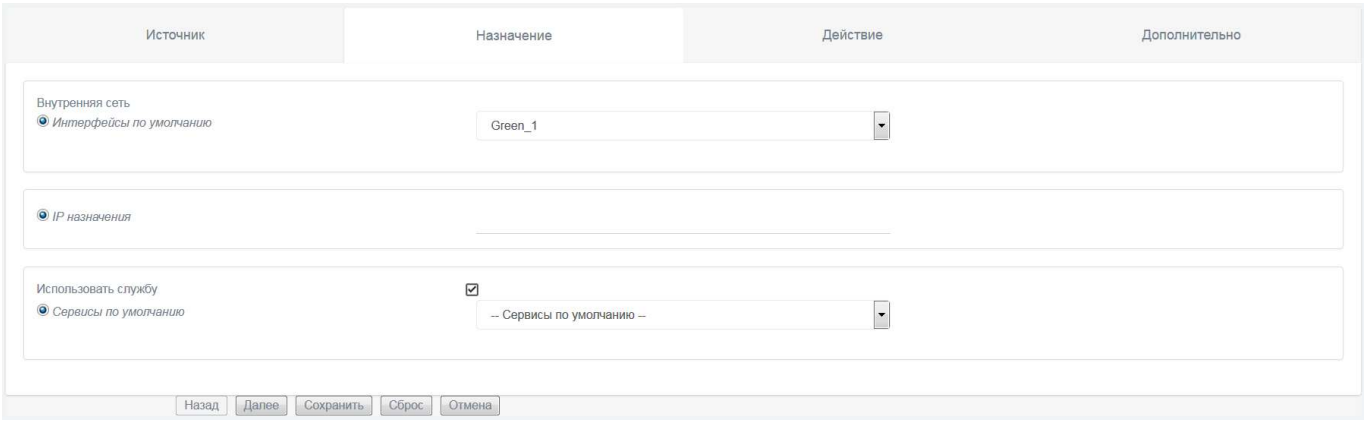


Рисунок 40 - Раздел «Назначение»

4) в разделе **«Действие»** информацию о параметрах фильтруемых пакетов и решении о пропуске или отбрасывании их (рисунок 41);

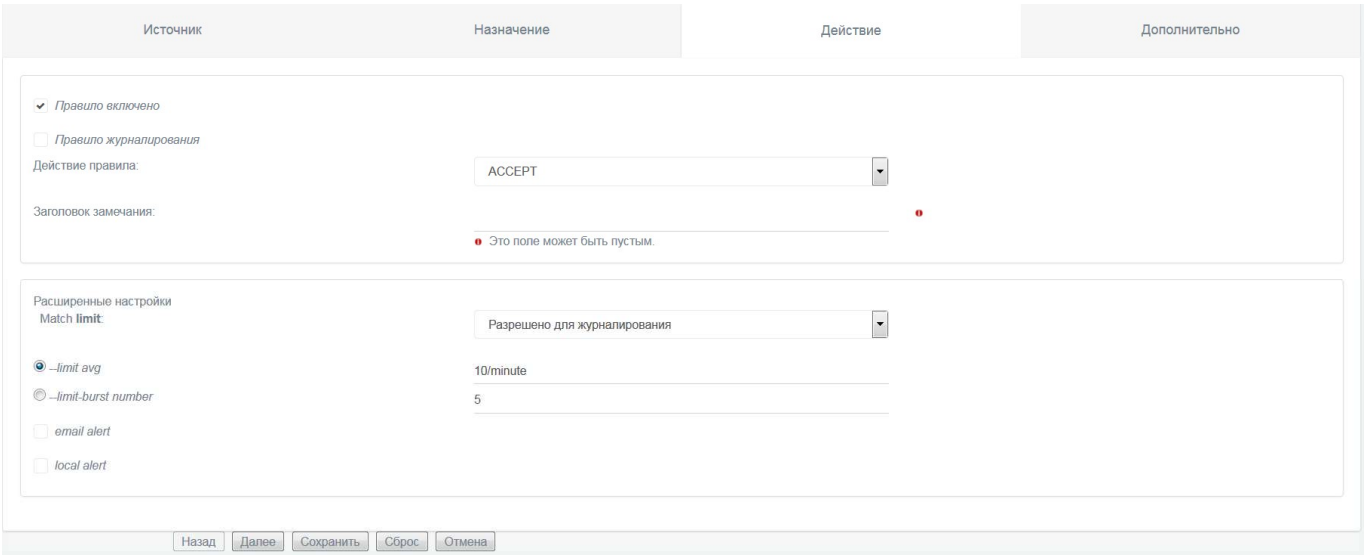


Рисунок 41 - Раздел «Действие»

– выберите необходимое действие для завершения операции по изменению текущего правила:

1) перейдите к просмотру правила нажатием кнопки **«Далее»**;

2) сохраните правило и вернитесь к интерфейсу выбора необходимых действий по настройке правил нажатием кнопки **«Сохранить»**;

3) сбросьте установленные параметры фильтрации нажатием кнопки **«Сброс»**;

4) выйдите из интерфейса изменения правил без сохранения нажатием кнопки **«Отмена»**;

7.7 Таблицы состояний

1) Перейдите на страницу состояний соединения **«Состояние → Соединения»**;

2) В выпадающем списке **«Отображать»** выберите значение **«Состояние»** (рисунок 42) или значение **«Трафик»** (рисунок 43);

3) Нажмите кнопку **«Сохранить»**.

На рисунке 42 отображается таблица состояния всех соединений.

На рисунке 43 отображается таблица с информацией о трафике.

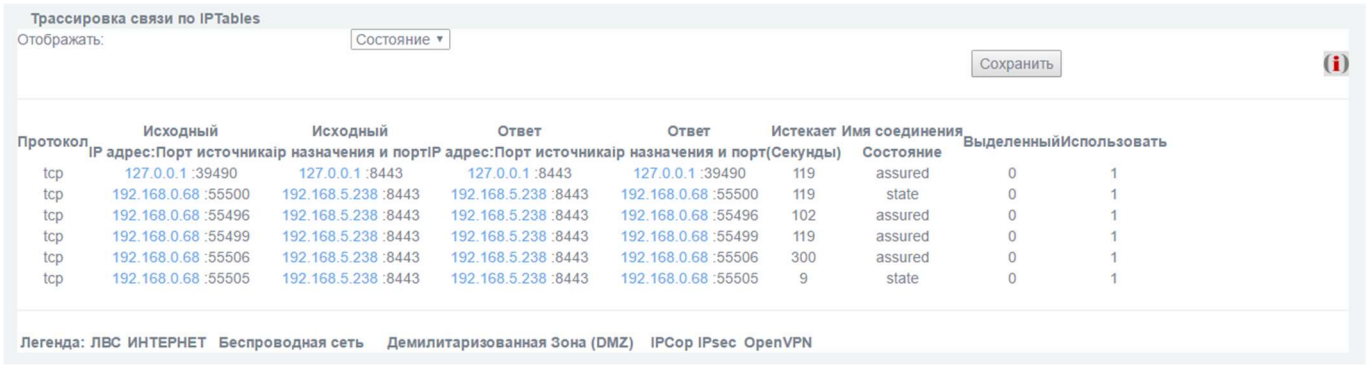


Рисунок 42 - Таблица состояний соединений

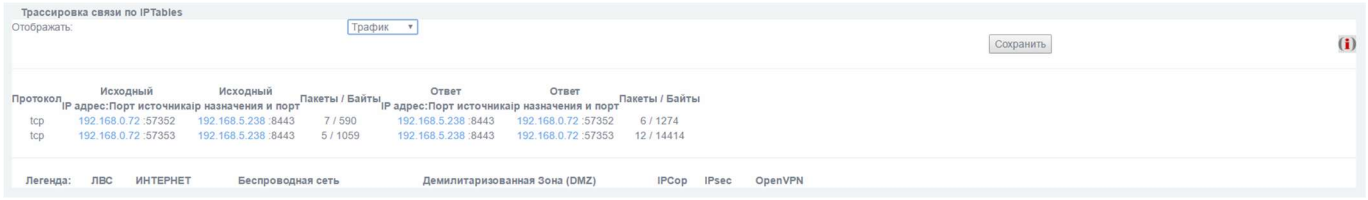


Рисунок 43 - Таблица с информацией о трафике

8 СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

8.1 Интерфейсы, доступные для запуска СОВ

СОВ может быть запущена в качестве отдельного процесса для любого из физических сетевых интерфейсов устройства. Указание о необходимости запуска процесса на том или ином интерфейсе осуществляется выбором соответствующего элемента управления в секции **«Интерфейсы»** на странице установки параметров **«Система обнаружения вторжений → Обнаружение атак»**. Секция **«Интерфейсы»** представлена на рисунке 44.

Рисунок 44 - Раздел «Система обнаружения атак → Обнаружение атак», секция «Интерфейсы»

8.1.1 Запуск на физическом интерфейсе

Для того чтобы подключить СОВ к одному из физических интерфейсов, поставьте отметку напротив его названия в разделе **«Система обнаружения атак → Обнаружение атак»**, секция **«Интерфейсы»** (рисунок 44).

После того как отметка поставлена, сохраните изменения, нажав кнопку **«Сохранить»**. Появится надпись с дальнейшими указаниями (рисунок 45).

Рисунок 45 - Запуск СОВ на физическом интерфейсе

Чтобы применить сохраненные изменения, нажмите кнопку **«Применить»**. Теперь СОВ запущена на выбранном интерфейсе (рисунок 46).

Рисунок 46 - СОВ запущена на интерфейсе Green Snort lan-1

Примечание - Рекомендуется включать СОВ только на внешних интерфейсах, так как работа на всех интерфейсах загружает оперативную память на 300 Мб интерфейс и процессор, что снижает общую производительность Рубикон-К.

8.2 Режимы обнаружения

В Рубикон-К предусмотрено два режима обнаружения вторжений: сигнатурный анализ и эвристический анализ.

8.2.1 Сигнатурный анализ

Режим сигнатурного анализа предполагает наличие базы решающих правил (БРП), которая включает в себя сигнатуры известных атак. Корректная работа данного режима невозможна без актуальной БРП и напрямую зависит от набора правил.

8.2.2 Эвристический анализ

Режим эвристического анализа атак заключается в просмотре сетевого трафика на наличие элементов сканирования портов или узлов сети и выдаче решения о наличии сканирования в сегменте сети.

Для настройки режима эвристического анализа зайдите в раздел **«Система обнаружения вторжений → Настройка обнаружения»**.

Существует два элемента управления (рисунок 47): выбор протокола, и уровень срабатывания. Протокол определяет те сетевые пакеты, которые будут анализироваться. Уровень срабатывания определяет предполагаемую интенсивность сканирования злоумышленником.

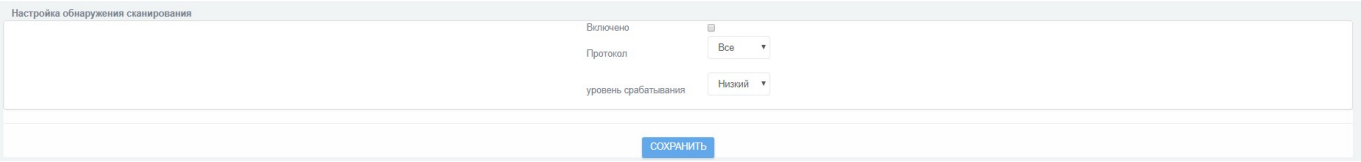


Рисунок 47 - Настройка режима эвристического анализа

Поле «Протокол» может принимать следующие значения:

- Все;
- TCP;
- UDP;
- ICMP;
- протокол IP.

Доступны три уровня срабатывания:

- низкий;
- средний;
- высокий.

СОВ может работать в «прозрачном» режиме, что позволяет Рубикон-К функционировать без нарушения внутренней структуры сети.

8.3 База решающих правил

8.3.1 Загрузка новой базы решающих правил

Для настройки новой БРП загрузите в разделе **«Система обнаружения вторжений** → **Обнаружение атак»** следующие файлы (рисунок 48):

– метка времени в формате tsr: получена от сервера доверенного времени;

– непосредственно набор правил;

– файл УЦ: сертификат, выданный УЦ серверу доверенного времени.

Метка времени состоит из:

– контрольной суммы набора правил;

– времени создания метки;

– ЭП сервера доверенного времени, удостоверяющего целостность описанных выше данных;

– сертификата сервера доверенного времени.

Рисунок 48 — Настройка БРП. Импорт файлов в систему

После того как все файлы выбраны, нажмите кнопку **«Загрузить новый набор правил»**.

Примечание - Если хотя бы один из требуемых файлов не был загружен, после нажатия на кнопку **«Загрузить новый набор правил»** администратор увидит следующее сообщение (рисунок 49):

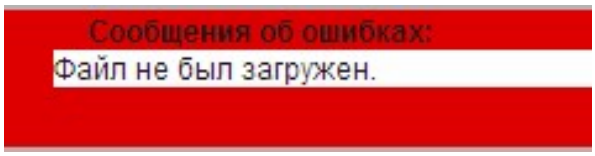


Рисунок 49 - Сообщение об ошибке

После загрузки происходит проверка:

– соответствия контрольной суммы загруженного набора правил контрольной сумме, указанной в метке времени;

– актуальности сертификата сервера доверенного времени, извлекаемого из метки времени.

В случае успешного прохождения проверки с помощью сертификата сервера доверенного времени проверяется ЭП метки времени. Если подпись верна, происходит загрузка правил в хранилище СОВ и удаление временных файлов. Пользователю выводится предложение нажать кнопку **«Применить»**, (рисунок 50), что обновит правила и перезапустит СОВ на выбранных интерфейсах.

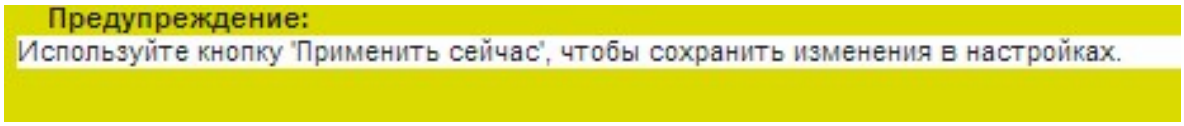


Рисунок 50 - Предложение применить внесенные изменения

После успешного перезапуска, а также по нажатию кнопки **«Прочитать последние записи в журнале установки правил»**, администратор может увидеть информацию, представленную на рисунке 50.

При неуспешной проверке администратор увидит предупреждающее сообщение (рисунок 51):

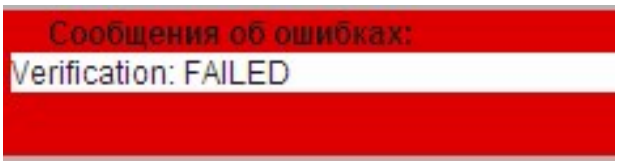


Рисунок 51 - Сообщение об ошибке

Данное сообщение означает что:

– один или более файлов выбраны ошибочно (неверный формат);

– все файлы корректного формата, но контрольная сумма загруженного набора правил не соответствует контрольной сумме, указанной в метке времени;

– сертификат сервера доверенного времени неактуален.

Рисунок 52 - Информация об установленных обновлениях

Справа от кнопки «Применить» отображается дата последнего изменения правил. Также отображаются сведения о результатах проверки метки времени. Результат проверки на рисунке 52 **«done»** означает успешное прохождение проверки. Можно также увидеть сведения о загружаемом наборе правил.

8.3.2 Настройка решающих правил

Включение/отключение решающих правил

Для включения (отключения) срабатывания конкретного решающего правила поставьте отметку напротив его названия в соответствующем контейнере в разделе **«Система обнаружения вторжений → Настройка правил СОВ»**.

Например, на рисунке 53 включены все правила, кроме **«ATTAC_RESPONCES 403 Forbidden».**

Включение/отключение уведомления по электронной почте для каждого правила

Для включения (отключения) уведомления администратора о срабатывании конкретного решающего правила выберите ✉ для включения и ✉ для отключения напротив названия правила в соответствующем контейнере в разделе **«Система обнаружения вторжений → Настройка правил СОВ»**.

Например, на рисунке 53 отключено уведомление обо всех правилах, кроме **«APP-DETECT** Acunetix web vulnerability scanner probe attempt**»**.

.

Рисунок 53 - Настройка решающих правил

9 РЕЗЕРВИРОВАНИЕ

9.1 Горячее резервирование

РУБИКОН-К поддерживает технологию горячего резервирования. Пример, рассматривающий горячее резервирование красного интерфейса WAN, приведен ниже.

Пусть имеется два Рубикон-К, которые подключены в одну внешнюю сеть с основным IP адресом **10.10.10.1** и резервным IP адресом **10.10.10.2**. Основной Рубикон-К имеет IP адрес **192.168.3.1**, а резервный Рубикон-К - **192.168.3.2**. Оба Рубикон-К соединены между собой.

Создайте один общий виртуальный интерфейс, который будет переключаться между Рубикон-К. Для примера это IP адрес **10.10.10.3**.

Для настройки горячего резервирования для данного примера выполните следующие действия:

– в веб-интерфейсе перейдите на страницу: **«Сеть → Функция горячего резервирования»** и нажмите кнопку редактирования нужного интерфейса (рисунок 54);

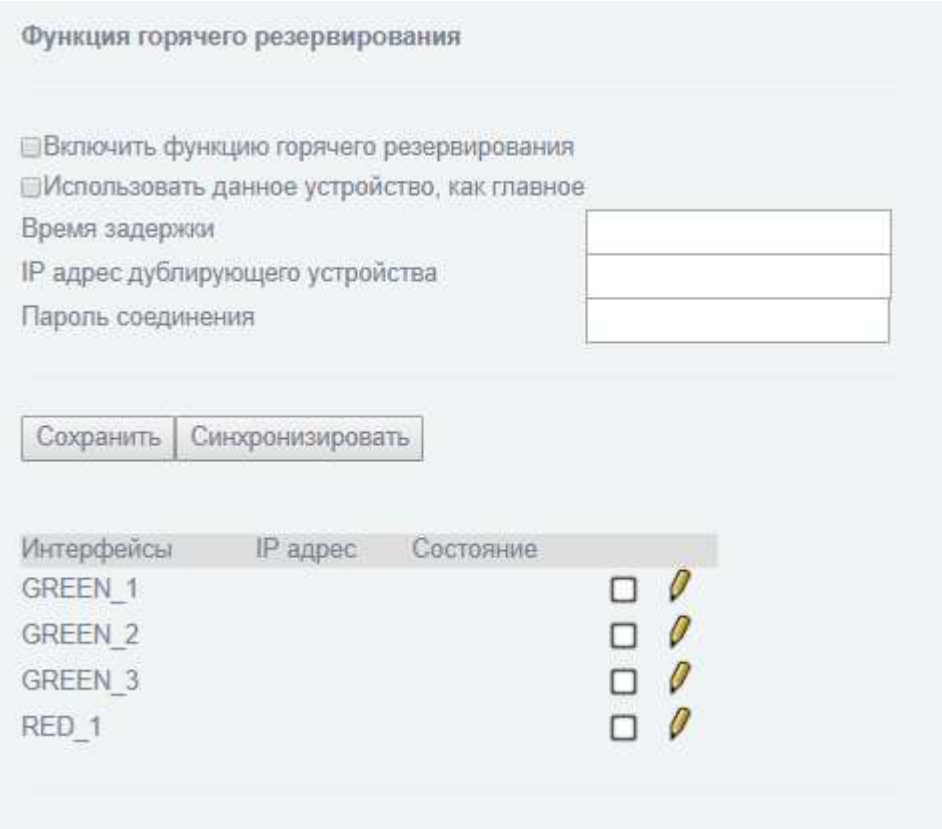


Рисунок 54 - Раздел «Сеть → Функция горячего резервирования»

– укажите общий виртуальный IP адрес и нажмите кнопку **«Сохранить»** (рисунок 55);

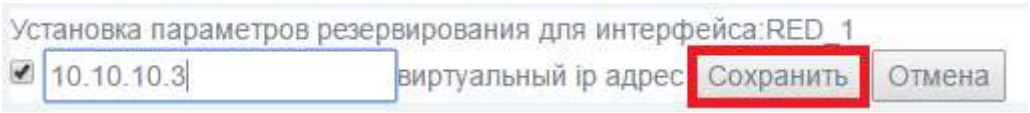


Рисунок 55 - Общий IP адрес

– заполните поля для основного Рубикон-К с указанием необходимых IP адресов, по которым Рубикон-К соединены между собой (рисунок 56)

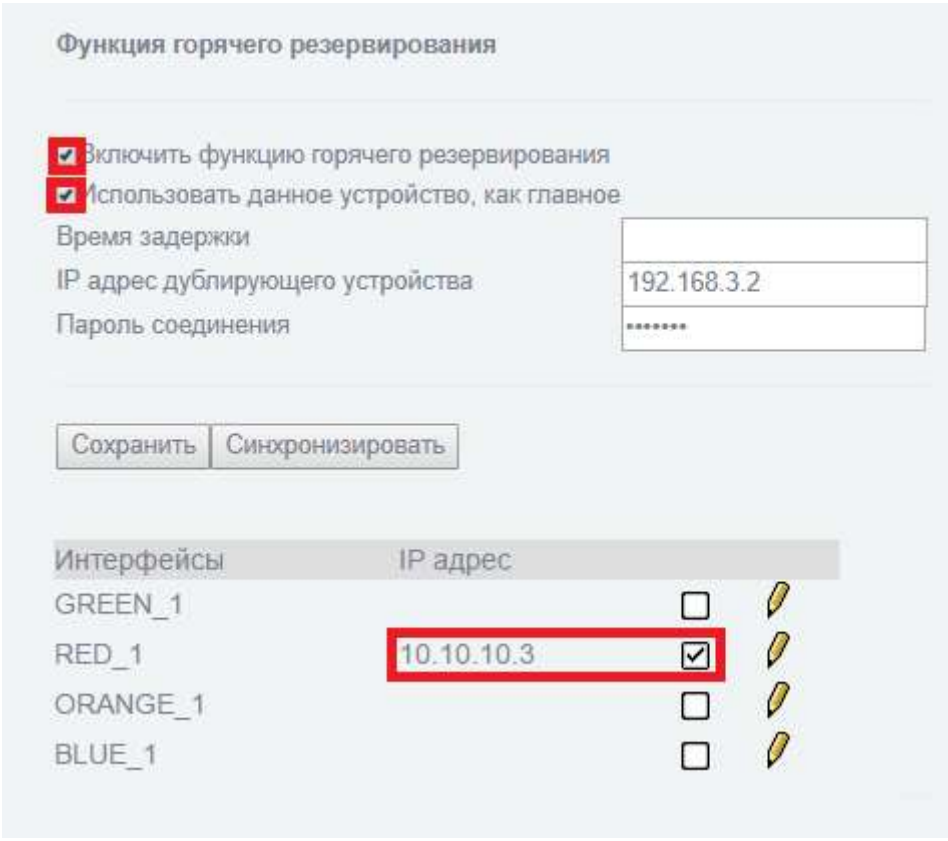


Рисунок 56 - Настройка основного Рубикон-К

– заполните поля для резервного копирования Рубикон-К с указанием необходимых IP адресов, по которым Рубикон-К соединены между собой (рисунок 57);

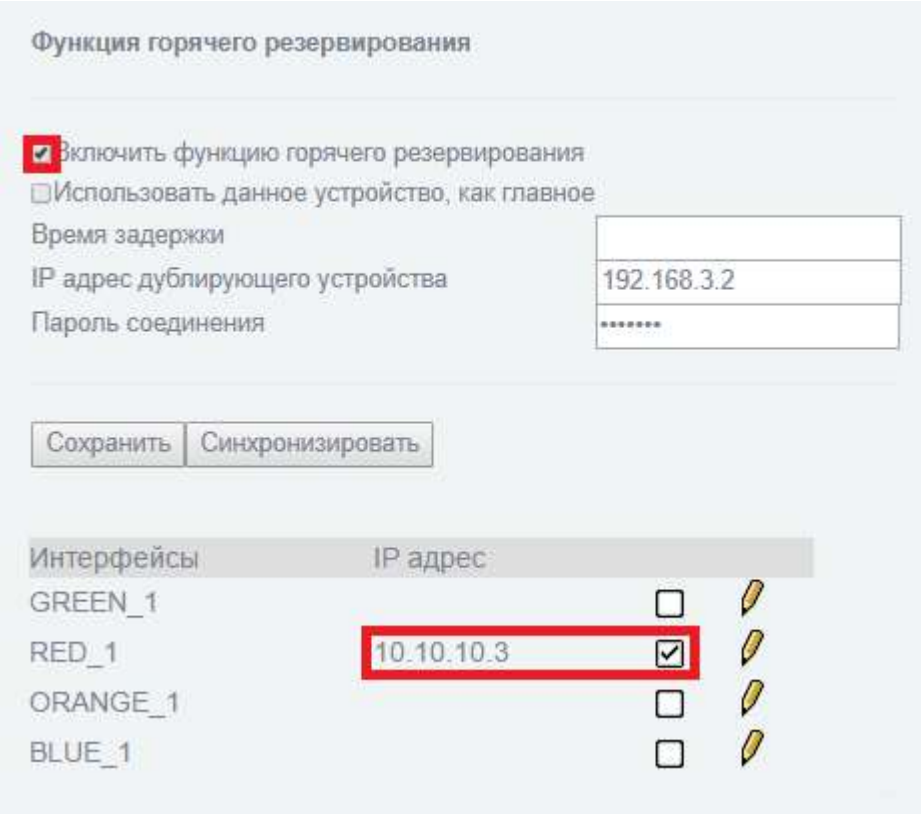


Рисунок 57 - Настройка резервного Рубикон-К

Пароли соединения между основным и резервным Рубикон-К должны совпадать.

Для проверки правильности настройки горячего резервирования зайдите в веб-интерфейсе на страницу **«Состояние → Состояние сети»** и вы увидите данные, аналогичные представленным на рисунке 58.

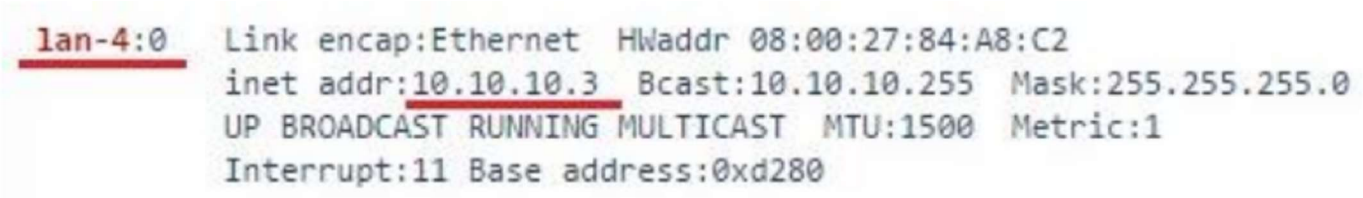


Рисунок 58 - Настройка резервного Рубикон-К

10 ЖУРНАЛ СОБЫТИЙ

10.1 Общие положения

В Рубикон-К есть четыре вида журнала:

1) журнал МЭ;

2) журнал обнаружения атак;

3) журнал обнаружения сканирования;

4) системный протокол - позволяет отслеживать сбои и восстанавливать работу Рубикон-К.

Журнал содержит информацию обо всех действиях, производимых в системе. Регистрируемые события:

- запуск выполнения функций аудита;
- попытка авторизации;
- успешная авторизация;
- неудачная авторизация;
- действия, предпринимаемые в ответ на возможные нарушения безопасности;
- чтение информации из записей аудита;
- параметры, используемые при просмотре;
- все модификации конфигурации аудита, происходящие во время сбора данных аудита;
- разрешения на запрашиваемые информационные потоки;
- все попытки импортировать данные пользователя;
- все попытки экспортировать информацию;
- все модификации режима выполнения функций;
- все модификации значений данных;

- использование функций управления;
- модификация группы пользователей - исполнителей роли;
- каждое использование прав, представленных ролью;
- все модификации значений атрибутов безопасности;
- обнаружение сбоя функций безопасности, если аудит возможен;
- факт возникновения сбоя или прерывания обслуживания;
- возобновление нормальной работы;
- тип сбоя или прерывания обслуживания;
- невозможность возврата к безопасному состоянию после сбоя функций безопасности, если аудит возможен;
- изменения внутреннего представления времени;
- предоставление меток времени;
- выполнение тестирования внешних сущностей и протоколирование результатов тестирования;
- выполнение и результаты самотестирования функций безопасности;
- успешное использование механизмов согласования данных функций безопасности;
- использование механизмов согласования данных функций безопасности;
- идентификация функций безопасности, данные которых интерпретируются;
- обнаружение модифицированных данных функций безопасности;
- любой сбой, обнаруженный функциями безопасности;
- завершение выполнения функций аудита.

Журналы можно хранить локально или отправлять на удаленный сервер (подробнее в разделе 10.2.3).

10.2 Настройка параметров отображения и ведения журналов

Для настройки параметров отображения и ведения журналов перейдите в раздел **«Журналы → Настройки журналирования»**. Откроется страница, представленная на рисунке 59.

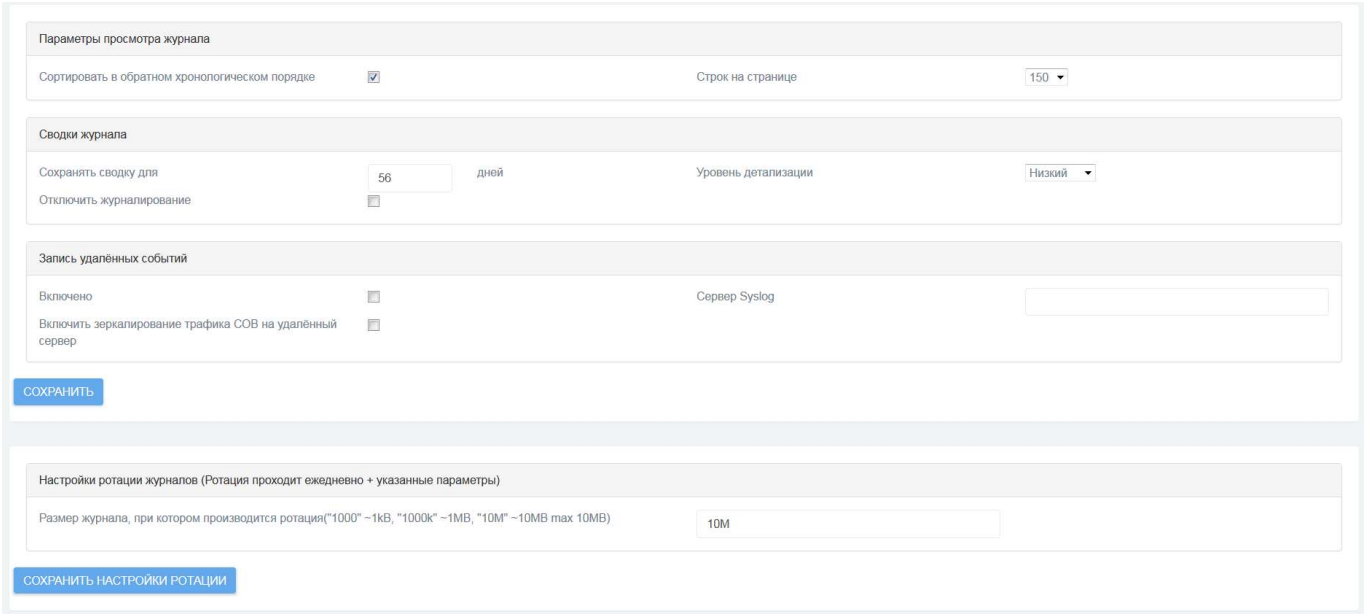


Рисунок 59 — Страница настройки параметров отображения журналов

Для настройки администратору доступны следующие параметры.

10.2.1 Настройки просмотра журнала

Параметр **«Отсортировать 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.

10.2.2 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:

- низкий;
- средний;
- высокий.

Отметка напротив пункта **«Отключить журналирование»** позволяет отключить запись всех системных событий и обнаруженных с помощью Рубикон-К атак, а также отправку записей на удалённый сервер (если эта опция была включена ранее).

10.2.3 Запись удаленных событий

Параметр **«Включено»** предназначен для включения возможности журналирования событий на удаленный сервер.

Строка ввода **«Сервер Syslog»**, предназначена для указания адреса удаленного syslog-сервера.

Параметр **«Включить зеркалирование трафика СОВ на удаленный сервер»** позволяет отправлять трафик СОВ на удаленный сервер.

10.2.4 Настройки ротации журналов

Задайте **«Размер журнала, при котором производится ротация («1000» ~1kB, "1000k" ~1MB, "10M" ~10MB, max 10MB)»** в текстовом поле.

Для сохранения внесенных изменений в настройки параметров отображения и ведения журналов нажмите кнопку **«Сохранить настройки ротации»**.

10.3 Сервер времени

Перейдите в раздел **«Службы → Сервер времени»** (рисунок 60).

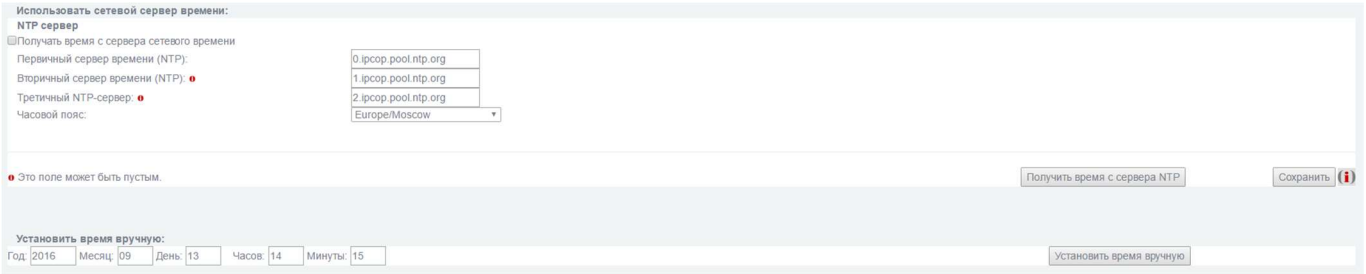


Рисунок 60 - Раздел «Службы → Сервер времени»

В разделе можно указать сервер, который будет передавать временные метки для журналирования, для этого выполните следующие действия:

1) поставьте флажок напротив параметра **«Получать время с сервера сетевого времени»**;

2) заполните текстовое поле **«Первичный сервер времени (NTP)»**;

3) заполните текстовое поле **«Вторичный сервер времени (NTP)»** (необязательное поле);

4) заполните текстовое поле **«Третичный NTP-сервер»**;

5) в выпадающем списке **«Часовой пояс»** выберите город;

6) нажмите кнопку **«Сохранить»**.

Если вы хотите установить время вручную, перейдите в секцию **«Установить время вручную»** (рисунок 60).

10.4 Сводка журнала

Для просмотра общего отчета о работе системы перейдите в раздел **«Журналы → Сводка журнала»**. Страница отображения общего отчета о системе представлена на рисунке 61.

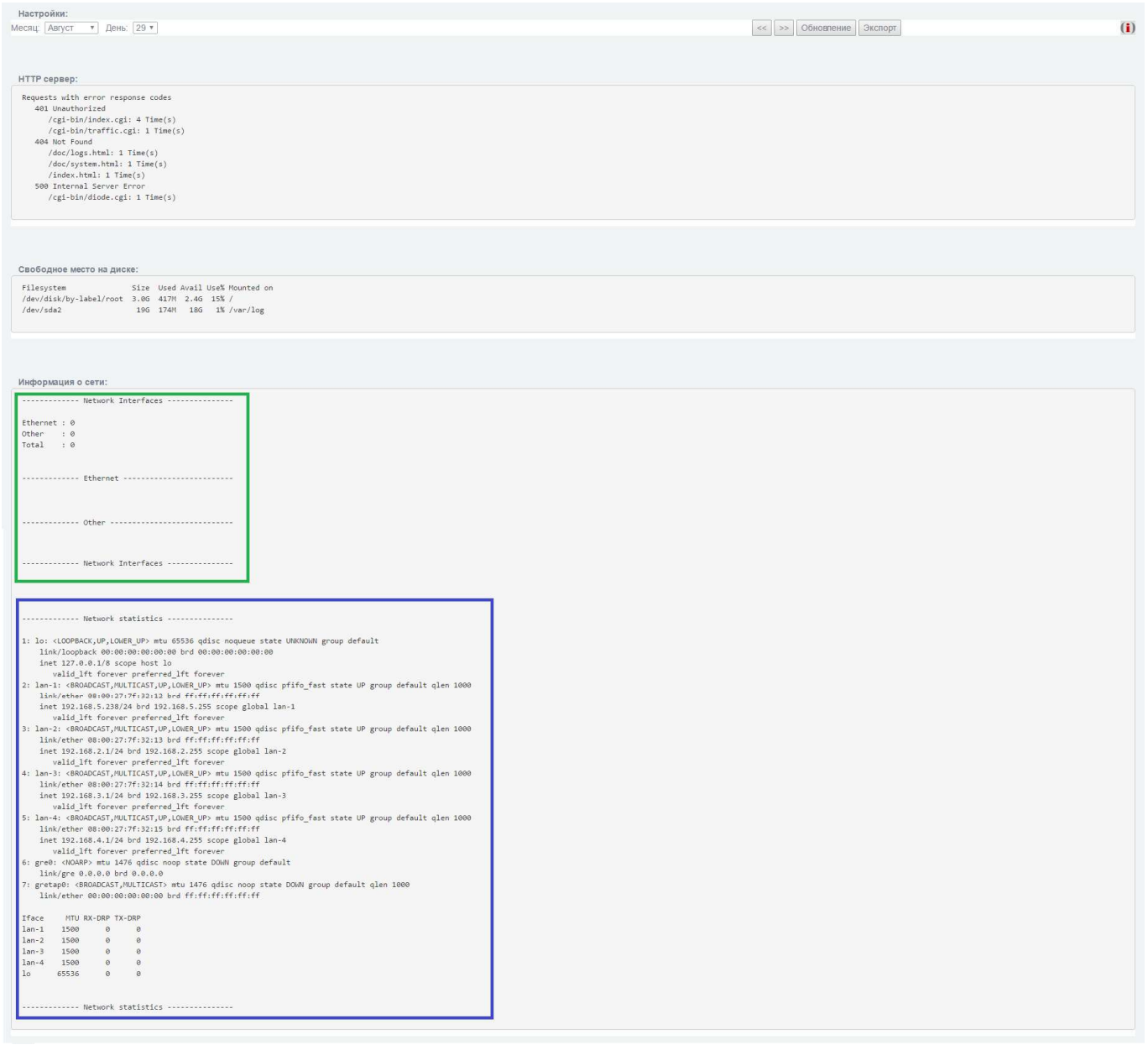


Рисунок 61 - Страница отображения общего отчета о системе

Как видно из рисунка 61, общий отчет о работе Рубикон-К состоит из четырех секций.

10.4.1 Настройки

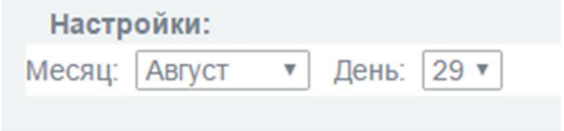


Рисунок 62 - Секция «Настройки»

Администратору предоставляется возможность выбора конкретного дня, за который необходимо просмотреть отчет (рисунок 62).

10.4.2 Информация о сети

Информация в этой секции состоит из двух блоков:

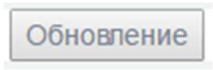
– сведения о сетевых интерфейсах (Network Interfaces): на рисунке 61 выделено в рамку зеленого цвета;

– сведения о конфигурации сетевых интерфейсов (Network Statistics): на рисунке 61 выделено в рамку синего цвета.

На странице общего отчета о работе системы есть ряд кнопок.

предназначена для перехода к странице информации на один день раньше;

предназначена для перехода к странице информации на один день позже;



предназначена для обновления информации для выбранного периода времени;

предназначена для экспорта информации в формате .txt.

10.5 Журнал межсетевого экрана

Чтобы посмотреть журнал межсетевого экрана, перейдите в раздел **«Журналы → Журнал межсетевого экрана»**. Откроется страница, изображенная на рисунке 63.

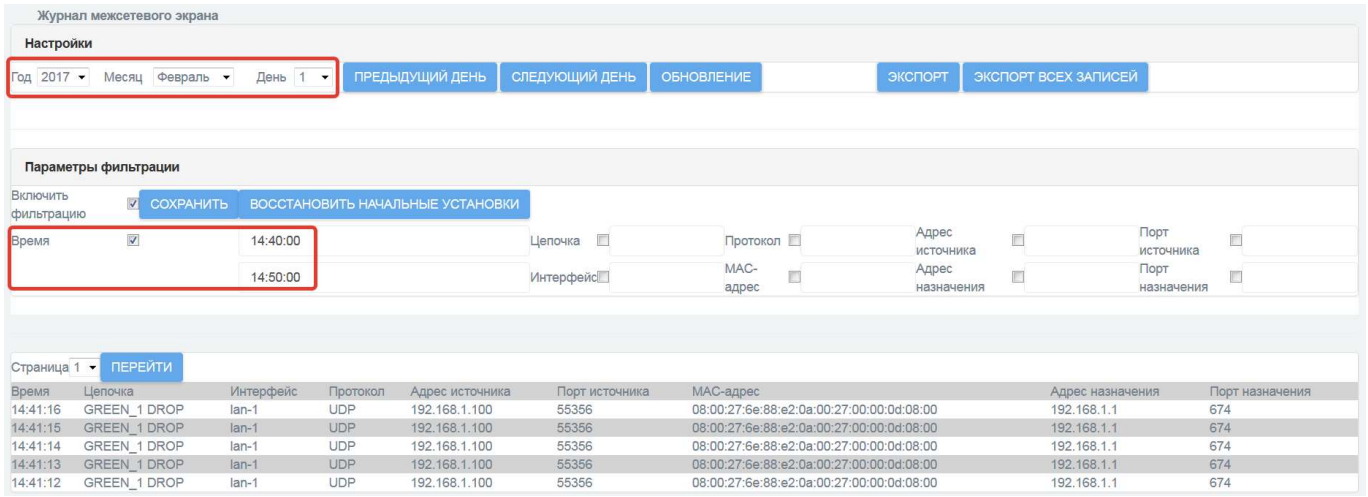


Рисунок 63 - Раздел «Журналы → Журнал межсетевого экрана»

На странице журнала межсетевого экрана предусмотрена возможность выборочного просмотра записей. Для просмотра информации журнала, отсортированной

по какому-либо параметру, включите фильтрацию. Для этого выставите отметку напротив соответствующего пункта и нажмите кнопку **«Сохранить»**.

Загрузить события из журнала можно за период равный одним суткам. Для этого укажите день, месяц и год (рисунок 65).

Возможно ограничить промежуток времени, за который будут отображены события выбранных суток, путем выставления конкретных временных рамок (рисунок 65).

На странице журнала межсетевого экрана есть ряд кнопок.

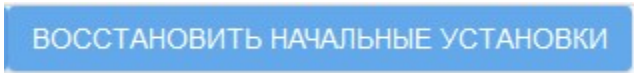
предназначена для перехода к странице информации на один день раньше;

предназначена для перехода к странице информации на один день позже;

предназначена для обновления информации для выбранного периода времени;

предназначена для экспорта информации в формате .txt;

предназначена для экспорта всей информации в формате .zip



предназначена для сброса всех параметров фильтров.

Доступны следующие параметры для настройки фильтрации журнала межсетевого экрана:

- время;
- цепочка;
- интерфейс;
- протокол;
- адрес источника;
- порт источника;
- MAC-адрес;

– адрес назначение;

– порт назначения.

На рисунках 64-66 приведены примеры журналов межсетевого экрана, отсортированных по адресу источника, порту источника и MAC-адресу соответственно.

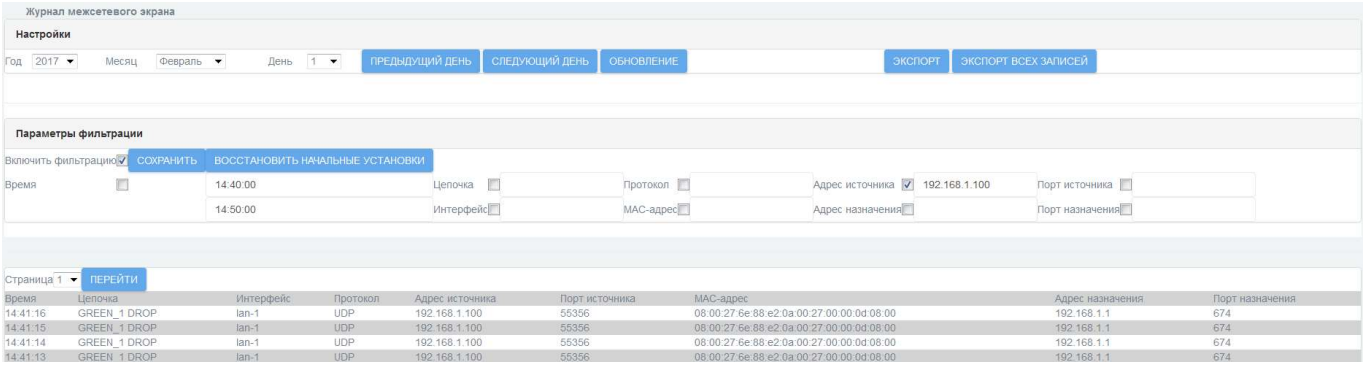


Рисунок 64 - Пример журнала МЭ, фильтр по адресу источника: 192.168.1.100

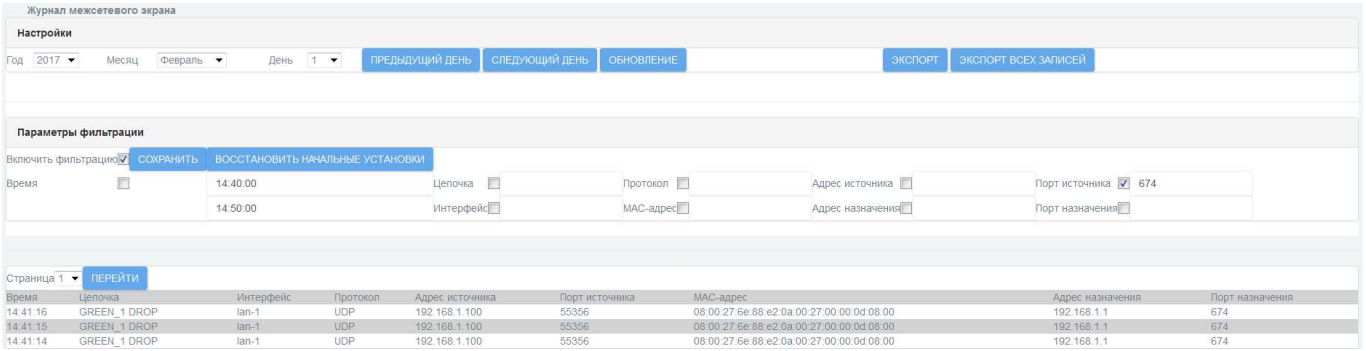


Рисунок 65 - Пример журнала МЭ, фильтр по порту источника: 674

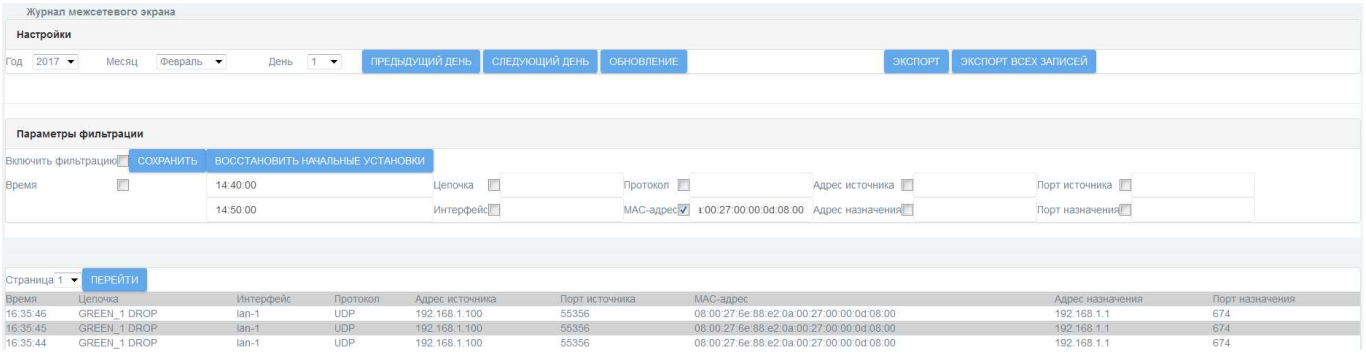


Рисунок 66 - Пример журнала МЭ, фильтр по MAC-адресу:
08:00:27:6e:88:e2:0a:00:27:00:00:0d:08:00

10.6 Журнал обнаружения атак

Чтобы просмотреть журнал обнаруженных атак СОВ, необходимо перейдите в раздел **«Журналы → Журнал обнаружения атак»**. Откроется страница, изображенная на рисунке 67.

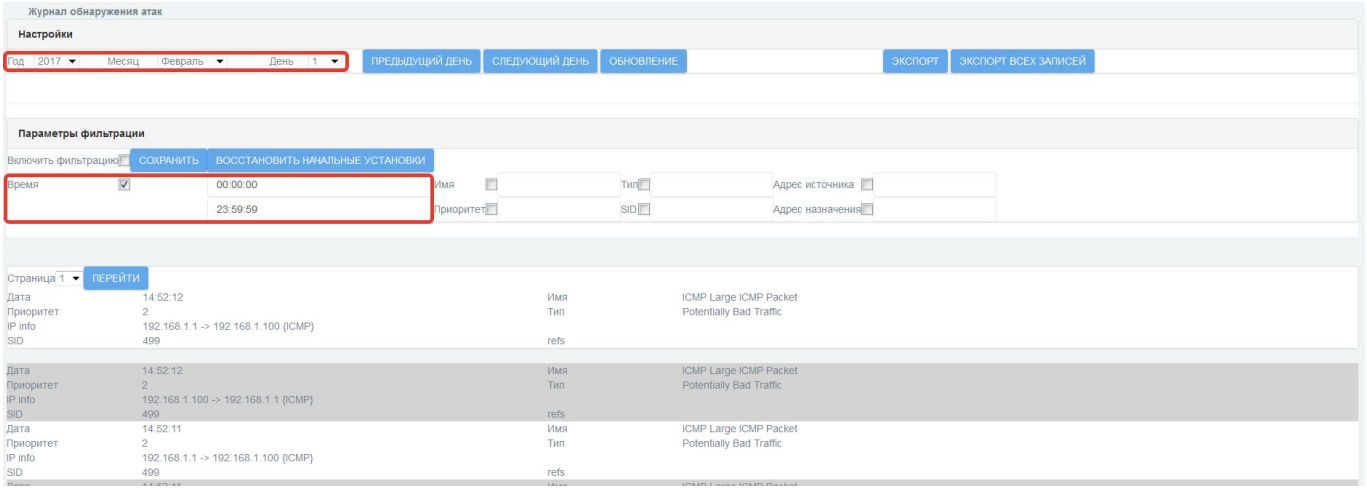


Рисунок 67 - Раздел «Журналы → Журнал обнаружения атак»

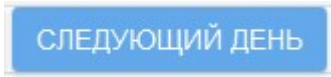
На странице журнала обнаружения атак предусмотрена возможность выборочного просмотра записей. Для просмотра информации журнала, отсортированной по какому-либо параметру, включите фильтрацию. Для этого выставите отметку напротив соответствующего пункта и нажмите кнопку **«Сохранить»**.

Загрузить события из журнала можно за период равный одним суткам. Для этого укажите день, месяц и год (рисунок 69).

Возможно ограничить промежуток времени, за который будут отображены события выбранных суток, путем выставления конкретных временных рамок (рисунок 69).

На странице журнала обнаружения атак есть ряд кнопок.

предназначена для перехода к странице информации на один день раньше;

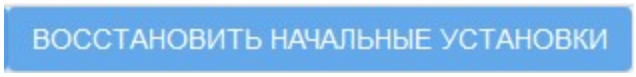


предназначена для перехода к странице информации на один день позже;

предназначена для обновления информации для выбранного периода времени;

предназначена для экспорта информации

в формате .txt;



предназначена для экспорта всей информации в формате .zip

предназначена для сброса всех параметров фильтров.

Доступны следующие параметры для настройки фильтрации журнала обнаружения атак:

- имя;
- приоритет;
- тип;
- SID (Security Identifier);
- адрес источника;
- адрес назначения.

На рисунках 68-70 приведены примеры журналов обнаружения атак, отсортированных по SID, имени и типу соответственно.

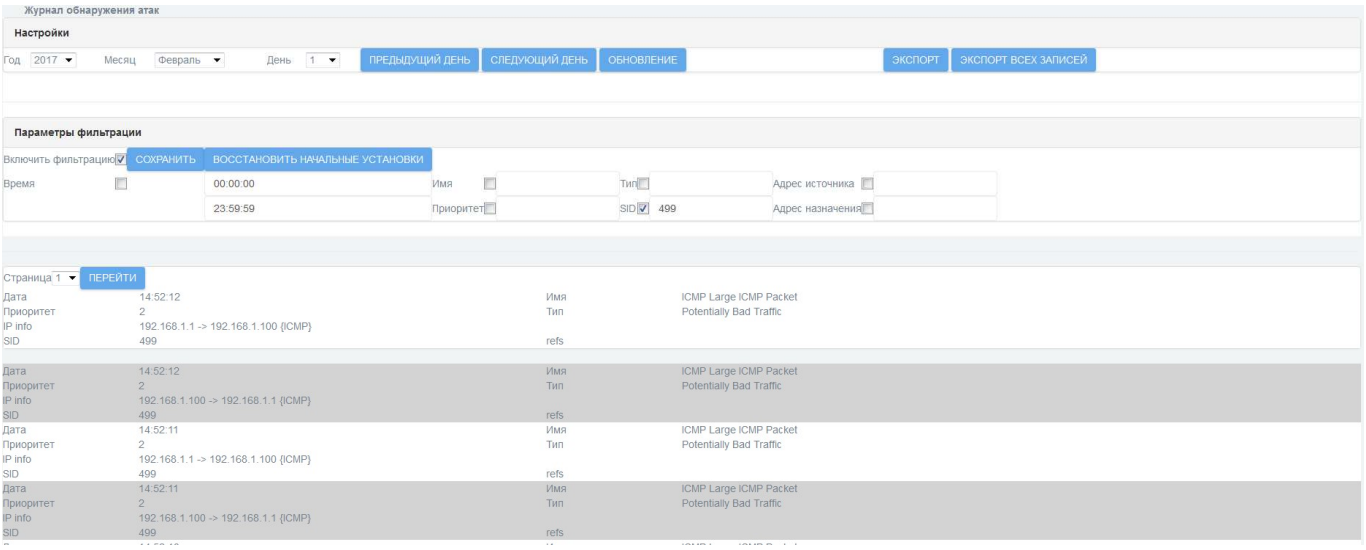


Рисунок 68 — Пример журнала обнаружения атак, фильтр по SID: 499

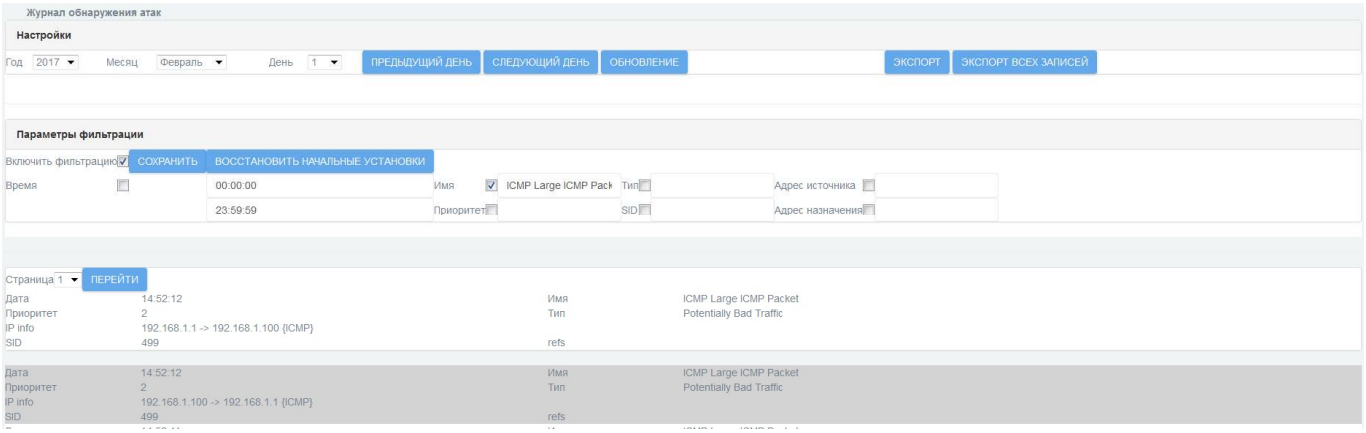


Рисунок 69 — Пример журнала обнаружения атак, фильтр по названию: ICMP Large ICMP Packet

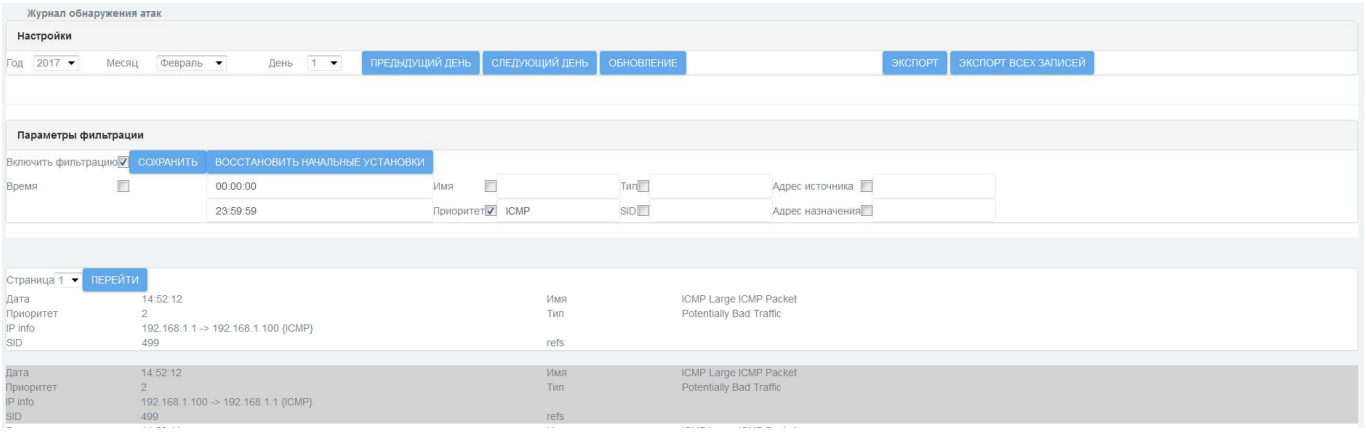


Рисунок 70 — Пример журнала обнаружения атак, фильтр по типу: ICMP

10.7 Системный протокол

Для просмотра системного протокола Рубикон-К перейдите в раздел **«Журналы → Системный протокол»**. Откроется страница, изображенная на рисунке 71.

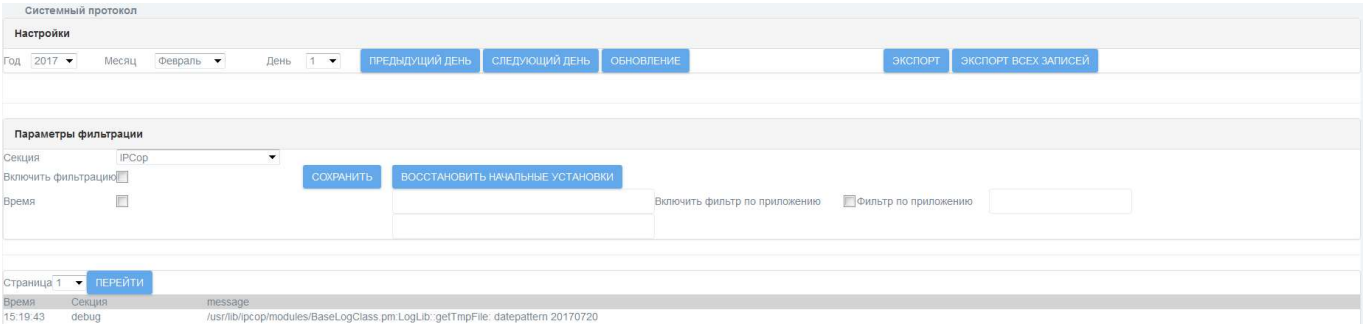
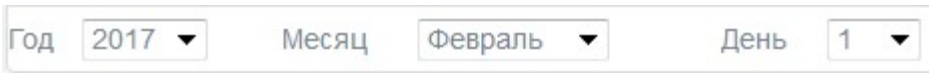


Рисунок 71 - Раздел «Журналы → Системный протокол»

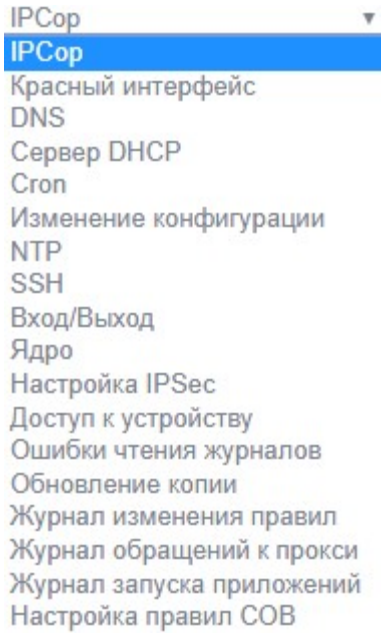
Доступны следующие параметры для настройки фильтрации системного протокола:

По дате:



По времени:

По секции:

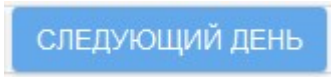


По приложению:

Примечание - Для настройки фильтров по времени и по приложению должны стоять отметки напротив соответствующих пунктов **«Включить фильтр по времени»** и **«Включить фильтр по приложению»**.

На странице системного протокола есть ряд кнопок.

предназначена для перехода к странице информации на один день раньше;

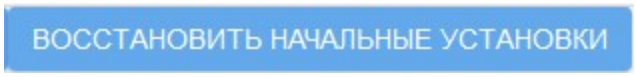


предназначена для перехода к странице информации на один день позже;

предназначена для обновления информации для выбранного периода времени;

предназначена для экспорта информации в формате .txt;

предназначена для экспорта всей информации в формате .zip



предназначена для сброса всех параметров фильтров.

На рисунках 72 и 73 приведены примеры фильтрации системного протокола по секции **«IPCop»** и журналу запуска приложений соответственно.

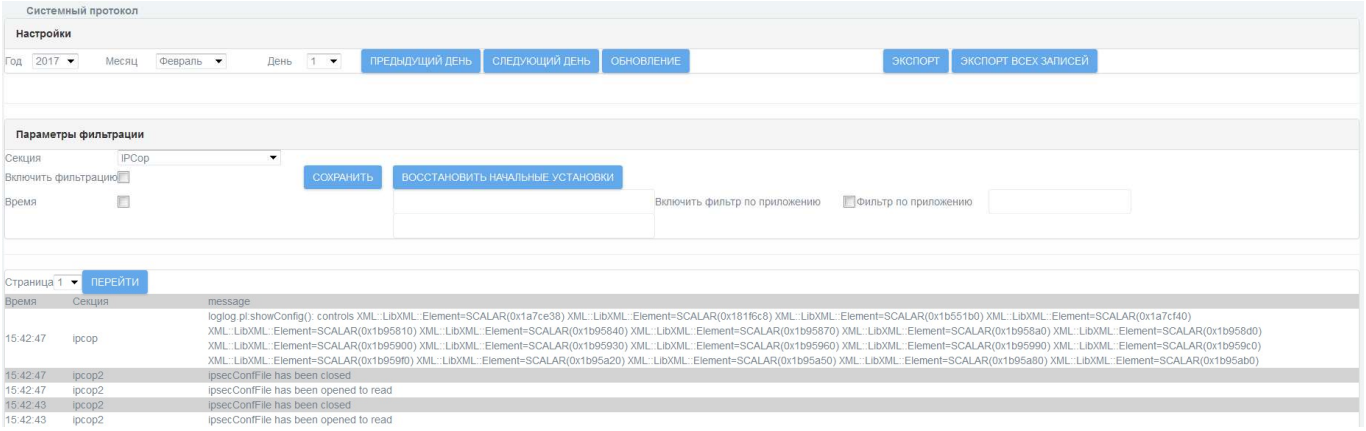


Рисунок 72 — Пример фильтрации системного протокола по секции «IPCop»

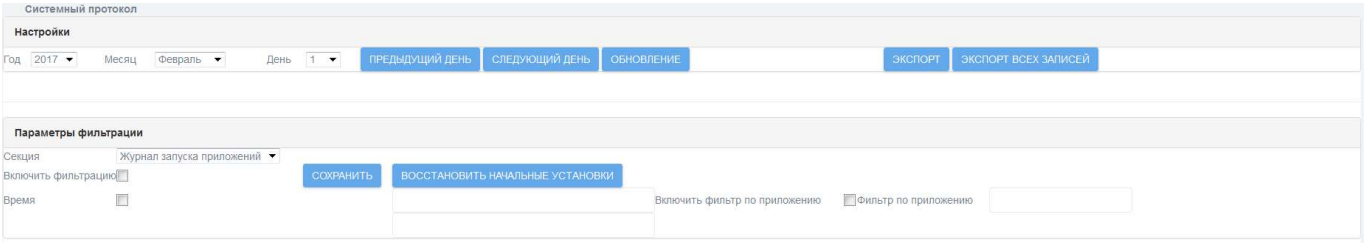


Рисунок 73 — Пример фильтрации системного протокола по секции «Журнал запуска приложений»

10.8 Настройка уведомлений

РУБИКОН-К позволяет настроить уведомление администратора об обнаруженных атаках по электронной почте. Для настройки уведомления по электронной почте перейдите в раздел **«Система** → **Почта»** (рисунок 74).

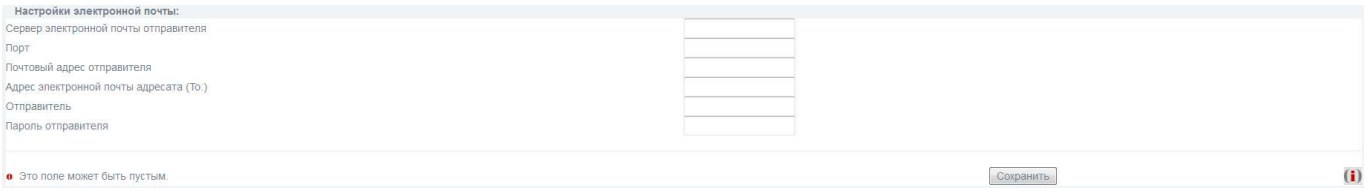


Рисунок 74 - Раздел «Система → Почта»

Для подтверждения правильности внесенной информации нажмите кнопку **«Сохранить»**. После этого, уведомления об обнаруженных атаках будут приходить на электронную почту.

10.9 Настройка языка веб-интерфейса

В настройках Рубикон-К есть возможность выбора языка веб-интерфейса. Для смены языка перейдите в раздел **«Система → Настройки GUI»** (рисунок 75).

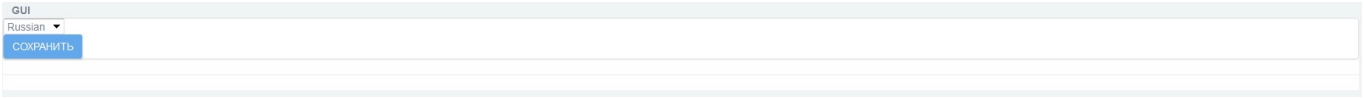


Рисунок 75 - Раздел «Система → Настройки GUI»

Выберите необходимый язык и нажмите кнопку **«Сохранить»**. После этого, язык веб-интерфейса изменится.

11 АВТОМАТИЧЕСКОЕ ВОССТАНОВЛЕНИЕ

11.1 Действия системы в случае сбоя

Вы можете установить действия, которые сделает система в случае выявления сбоя, в зависимости от типа сбоя.

Перейдите в раздел **«Система → Автоматическое восстановление»** (рисунок 76).

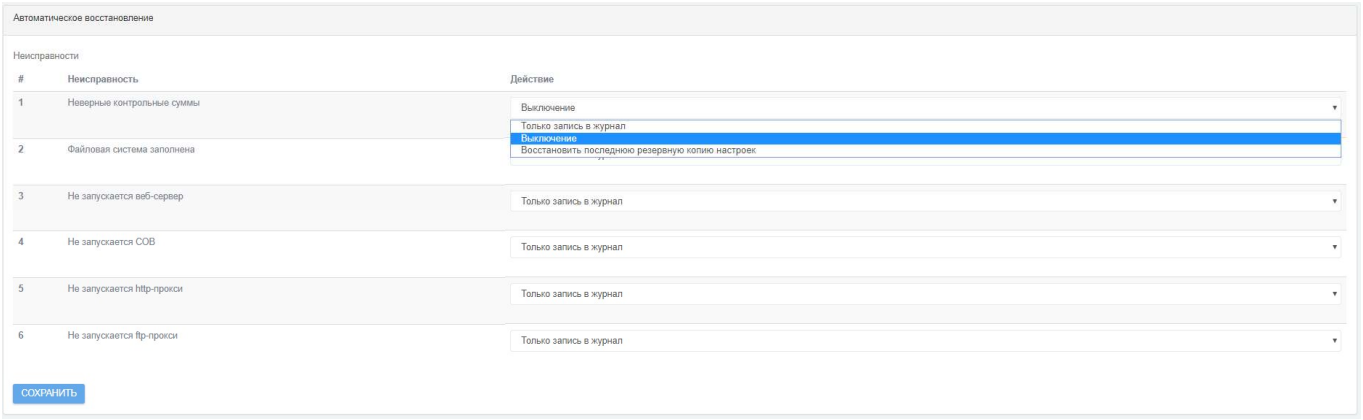


Рисунок 76 - Раздел «Система → Автоматическое восстановление»

В разделе представлено 6 типов сбоя и в выпадающих списках приведены опции восстановления при разных неисправностях:

1) Неверные контрольные суммы:

- Только запись в журнал;
- Выключение;
- Восстановить последнюю резервную копию настроек.

2) Файловая система заполнена:

- Только запись в журнал;
- Выключение;
- Исправить.

3) Не запускается веб-сервер:

- Только запись в журнал;
- Выключение;
- Исправить;

– Восстановить последнюю резервную копию настроек.

4) Не запускается СОВ:

– Только запись в журнал;
– Выключение;
– Исправить;
– Восстановить последнюю резервную копию настроек.

5) Не запускается http-прокси:

– Только запись в журнал;
– Выключение;
– Исправить;
– Восстановить последнюю резервную копию настроек.

6) Не запускается ftp-прокси:

– Только запись в журнал;
– Выключение;
– Исправить;
– Восстановить последнюю резервную копию настроек.

В случае сбоя в журнале аудита регистрируются следующие сообщения (рисунок 77):

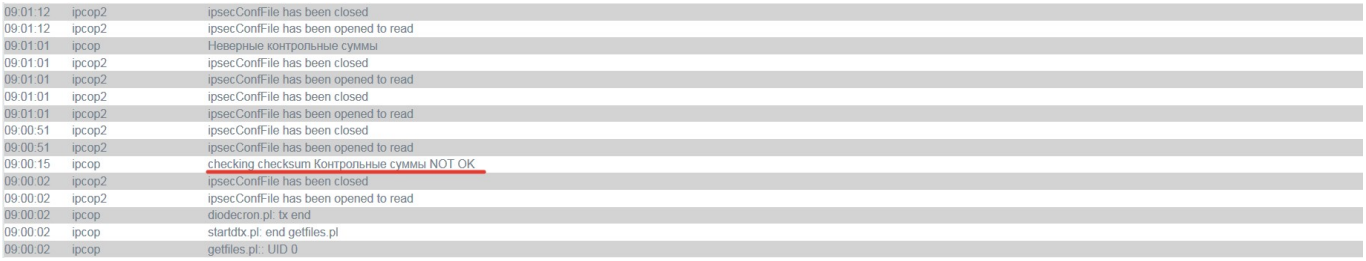


Рисунок 77 - Сообщение от утилиты восстановления

1) «файл конфигурации системы автоматического восстановления не найден» - сообщение появляется при ошибке чтения файла конфигурации утилиты автоматического восстановления;

2) «контрольные суммы NOT OK» - индикация ошибки «неверные контрольные суммы»;

3) «не удалось восстановить конфигурацию из резервной копии» - сообщение появляется при ошибке восстановления из резервной копии (самой новой из имеющихся);

4) «не удалось выключить Рубикон-К» - сообщение появляется при ошибке выключения «Рубикон-К»;

5) «критически мало места на жёстком диске» - индикация ошибки;

6) «не удалось очистить /var/log/archives» - сообщение появляется в случае ошибки действия «Исправить» при неисправности «мало места на ЖД»;

7) «директория /var/log/archive очищена, но места на жёстком диске недостаточно для стабильной работы» - сообщение появляется в случае, если старые логи очищены, но места на диске всё равно мало;

8) «не удалось перезапустить веб-сервер» - сообщение 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»;

13) «ftp-прокси не запущен» - индикация ошибки;

14) «не удалось перезапустить ftp-прокси»;

11.2 Консоль восстановления

Консоль восстановления создана для возможности восстановления системы в случае неработоспособности или отсутствия доступа к веб-интерфейсу. Для того чтобы запустить консоль восстановления выполните следующие действия:

1) войдите в консоль Рубикон-К;
2) введите логин пользователя. По умолчанию **«rescue»**;
3) введите пароль пользователя rescue. По умолчанию **«rescue»**.

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          Send 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 «опцинальные 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-К. 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 ЭВМ.

shutdown — команда выключения ЭВМ.

passwd — команда позволяет сменить пароль для пользователя **rescue**.

rs_web_passwd — команда позволяет сбросить пароль администратора для web-интерфейса Рубикон-К. 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 с логами не доступен для редактирования. При попытке открыть его будет выдана ошибка, говорящая о том, что файл не найден.

12 ПРОВЕРКА ПРОГРАММЫ

12.1 Контроль целостности исполняемых файлов и файлов конфигурации

В Рубикон-К 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.

Для контроля целостности исполняемых файлов и файлов конфигурации зайдите в раздел **«Состояние → Контрольные суммы»** и нажмите кнопку **«Проверить контрольные суммы»**.

При наличии ошибок контрольных сумм исполняемых файлов и файлов конфигурации, результаты проверки будут отображены под надписью **«Ошибки»** (рисунок 78).

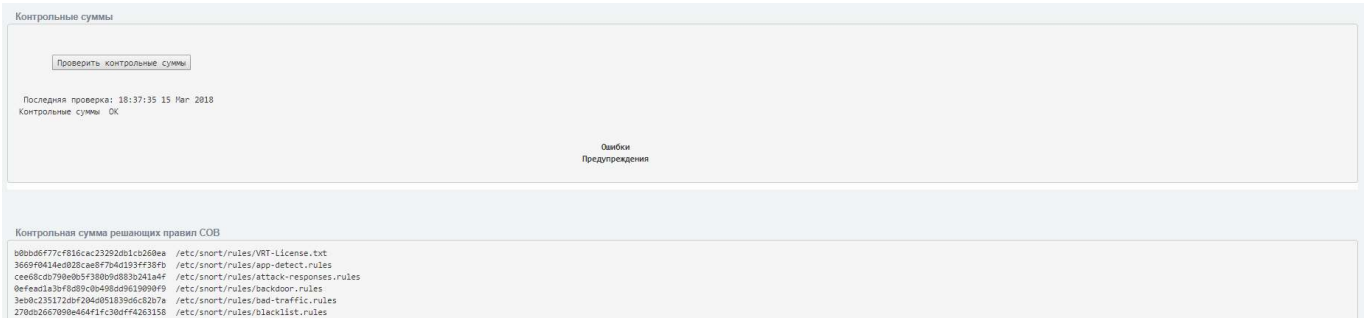


Рисунок 78 - Ошибка верификации контрольных сумм файлов Рубикон-К

12.2 Тестирование САВЗ

Перейдите в раздел **«Службы → Прокси»** (рисунок 79).

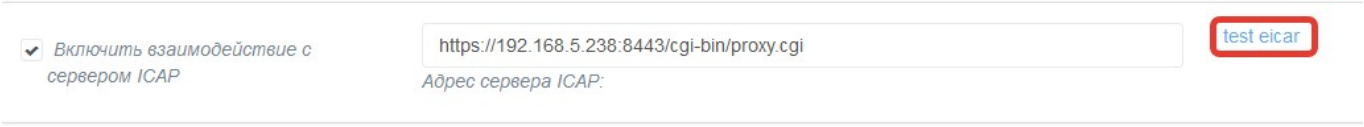


Рисунок 79 - Тестирование САВЗ

Перейдите по ссылке **«test eicar»**. После перехода по ссылке, будет выполнено тестирование САВЗ.

13 ДЕЙСТВИЯ ПОСЛЕ СБОЯ ИЛИ ОШИБКИ

Большинство ошибок можно разделить на два типа:

1) Ошибки конфигурации:

- некорректные сетевые настройки;
- некорректные настройки фильтрации пакетов;
- некорректные правила СОВ.

Чаще всего их можно исправить переконфигурированием Рубикон-К, либо восстановлением из ранее сделанной резервной копии, либо восстановлением с установочного носителя.

2) Ошибки оборудования:

- выход из строя сетевых контроллеров;
- выход из строя дисковых накопителей.

В случае выхода из строя оборудования Рубикон-К эксплуатировать нельзя, оборудование подлежит замене.

Возможны перезагрузки Рубикон-К, вызванные сбоями в питании. При кратковременном сбое Рубикон-К может перезагрузиться самостоятельно, но чаще всего требуется включение вручную. При выключении Рубикон-К сохраняются настройки и состояние сервисов, которые автоматически восстанавливаются после запуска. Однако для контроля ошибок рекомендуется не ранее чем через 30 секунд после запуска вручную проверять состояние запущенных сервисов.

14 ПРОЦЕДУРЫ ОБНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

14.1 Общий порядок поставки обновлений

Доставка обновлений Рубикон-К осуществляется с использованием сетевых протоколов передачи данных (загрузка с сервера АО «Научно-производственное объединение «Эшелон» (далее по тексту Разработчик), параметры сервера обновлений: http://npo-echelon.ru/download/rub_file.php, порт 80.

Разработчик анализирует сообщения о недостатках продукта и потребности пользователей, а затем проектирует, разрабатывает, тестирует и внедряет обновление программного обеспечения Рубикон-К.

Разработчик предоставляет пользователям, оплатившим техническую поддержку, доступ к обновлениям по протоколу HTTPS.

В течение жизненного цикла продукта выпускаются следующие типы выпускаемых обновлений:

- пакет обновления основной версии (Feature Pack) - обновленная основная версия с добавлением новых функциональных возможностей; выпускается раз в год в течение жизни основной версии, является полнофункциональной версией продукта;
- патч (Bugfix) - исправление недостатков продукта в основной версии или пакете обновления, выпускается по мере необходимости;
- пакет модификаций (Service Pack) - дистрибутив, содержащий все патчи, выпущенные за период после последней сертификации или инспекционного контроля. Выпускается в случае накопления большого количества патчей.

14.2 Предоставление обновления покупателям Рубикон-К

Процедура предоставления покупателям Рубикон-К обновлений программного обеспечения Рубикон-К в общем случае выглядит следующим образом:

1) анализ сообщений о недостатках и потребностей пользователей;
2) проектирование и разработка обновления продукта с учетом проведенного анализа;
3) тестирование обновления;
4) оценка влияния обновленного программного обеспечения на функции безопасности Рубикон-К;

5) формирование файла с контрольной суммой обновления;

6) выпуск документа «release notes», содержащего информацию об обновлении, процедур его получения, установки и верификации;

7) выпуск новой версии эксплуатационной документации, если обновление влияет на ФБО Рубикон-К;

8) отгрузка файлов на сервер обновлений;

9) предоставление обновлений клиентам для загрузки.

14.3 Процедуры и меры безопасности при доставке обновлений программного обеспечения Рубикон-К

14.3.1 Оповещение покупателя Рубикон-К об обновлении

Разработчик ведет учет покупателей Рубикон-К. Выполняется регистрация следующей информации: наименование организации, адрес организации, номер знака соответствия, контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование Рубикон-К). Уведомление пользователей о выпуске обновлении программного обеспечения Рубикон-К выполняется с использованием рассылки электронных почтовых сообщений с адреса электронной почты support.rubikon@cnpo.ru. Разработчик направляет документ «release notes» в адрес организаций, оплативших техническую поддержку. Данный документ содержит описание обновления, процедур получения и контроля целостности обновления, процедур тестирования, установки, применения и верификации.

14.3.2 Доставка и контроль целостности обновления программного обеспечения на стороне покупателя Рубикон-К

Обновления программного обеспечения Рубикон-К, успешно прошедшие контроль влияния на безопасность Рубикон-К, публикуются в закрытой части сервера предприятия-производителя. 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 программного обеспечения Рубикон-К публикуется его контрольная сумма. После получение обновления пользователь имеет возможность выполнить контроль его целостности с использованием механизма контрольного суммирования.

14.4 Тестирование обновления программного обеспечения на стороне покупателя Рубикон-К

Обновления программного обеспечения необходимо тестировать на стенде перед их непосредственной установкой. Пример стенда для тестирования (рисунок 80).

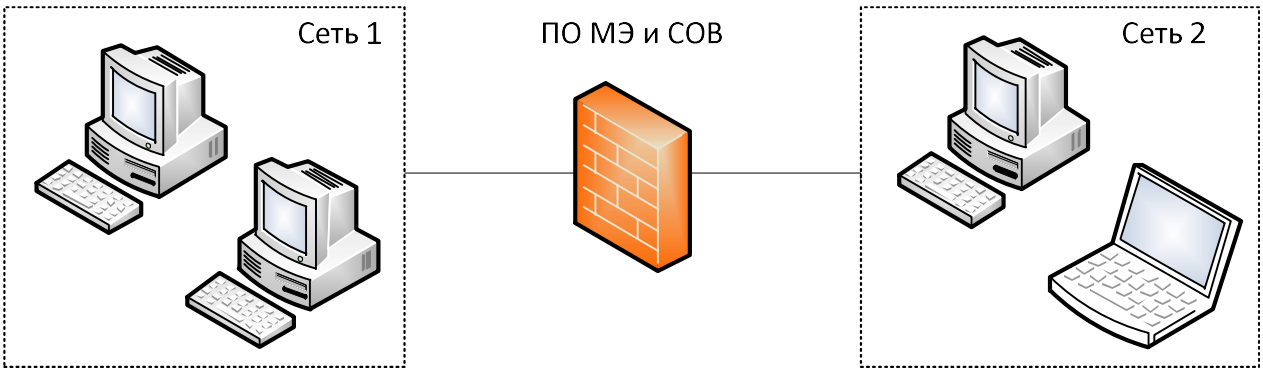


Рисунок 80 - Пример стенда для тестирования обновлений программного обеспечения Рубикон-К

Тестирование обновлений программного обеспечения Рубикон-К включает в себя следующие этапы:

- задание правил фильтрации на Рубикон-К;
- проверка выполнения заданный правил на стенде.

Тестирование считается успешно пройдённым, если заданные правила выполняются в полном объеме.

14.5 Установка и применение обновления программного обеспечения

Обновление программного обеспечения Рубикон-К устанавливается аналогично программному обсечению Рубикон-К. Подробнее процедуры установки и применения программного обеспечения описаны в документе «Межсетевой экран и система обнаружения вторжений «Рубикон-К». НПЕШ.465614.004. Руководство администратора. НПЕШ.465614.004 РА 01.

14.6 Контроль установки обновления

Критерием правильности установки обновления программного обеспечения является доступность веб-интерфейса Рубикон-К и отображение информации о новой версии программы в разделе «О программе».

14.7 Верификация применения обновления

Подробнее процедуры верификации применения обновления программного обеспечения описаны в документе «Межсетевой экран и система обнаружения вторжений «Рубикон-К». НПЕШ.465614.004. Тестовая документация. НПЕШ.465614.004 ТД 01».

14.8 Предоставление обновлений для проведения внешнего контроля

Процедура предоставления внешнего контроля уполномоченной организации:

- уполномоченная организация обращается к Разработчику для предоставления доступа к обновлениям;
- Разработчик предоставляет организации доступ к серверу обновления на оговоренный срок.

Методика тестирования обновлений содержится в документе «Межсетевой экран и система обнаружения вторжений «Рубикон-К». НПЕШ.465614.004. Тестовая документация. НПЕШ.465614.004 ТД 01».

После проведение тестирования должны составляться протоколы и акты испытаний, которые оформляются должны в соответствии с ЕСКД.

14.9 Анализ влияния обновлений на безопасность Рубикон-К

Обновление программного обеспечения Рубикон-К будет влиять на все функции безопасности в связи с тем, что дистрибутив программного обеспечения при наличии новой версии обновляется целиком. В зависимости от типа обновления степень влияния на отдельные функции безопасности различается. Для определения степени влияния необходимо произвести протестировать Рубикон-К согласно методикам, указанным в документе «Межсетевой экран и система обнаружения вторжений «Рубикон-К». НПЕШ.465614.004. Тестовая документация. НПЕШ.465614.004 ТД 01».

При наличии влияния обновления на ЗБ разработчик выпускает новую версию ЗБ.

15 ПРОЦЕДУРЫ ОБНОВЛЕНИЯ БРП

15.1 Общий порядок поставки БРП

Доставка обновлений БРП осуществляется с использованием сетевых протоколов передачи данных (загрузка с сервера АО «Научно-производственное объединение «Эшелон» (далее по тексту Разработчик), параметры сервера обновлений: http://npo-echelon.ru/download/rub_file.php, порт 80.

Разработчик осуществляет проверку, адаптацию обновлений от различных компаний-поставщиков обновлений БРП (далее Поставщик БРП).

Разработчик предоставляет доступ покупателям Рубикон-К к обновленным БРП по протоколу HTTPS.

15.2 Локализация и противодействие новому типу вторжения (атаки)

15.2.1 Фиксация появления нового типа вторжения

Обновление БРП является важным аспектом эффективного функционирования системы обнаружения вторжения.

Поставщики БРП осуществляют постоянный мониторинг появления новых сетевых атак. Обнаруженные атаки локализуются, и на их основе формируется ежемесячное обновление.

Разработчик ежедневно осуществляет загрузку, проверку и анализ обновлений от Поставщиков БРП.

Кроме того, Разработчик независимо от Поставщиков 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.

Существует два механизма, которые используются для обнаружения новых типов вторжений:

исследовательские работы, выполняемые сотрудниками предприятия-производителя (АО «Научно-производственное объединение «Эшелон») сертифицированного Рубикон-К;

акты рекламации, поступающие от пользователей сертифицированного Рубикон-К.

Исследовательские работы предусматривают анализ открытых источников данных сети «Интернет», содержащих сведения об уязвимостях программного обеспечения: cve.mitre.org, osvdb.org, securityfocus.com, secunia.com, securitytracker.com, nvd.nist.gov, cvedetails.com.

При получении акта рекламации выполняется анализ вторжения, описание которого не присутствует в текущей БРП. Выполняются тестовые атаки и исследования на стенде предприятия-разработчика для изучения атаки и формирования ее признаков. По результатам изучения нового типа вторжения устанавливается его актуальность и признаки, которые могут быть использованы для его обнаружения.

15.2.2 Предоставление обновления покупателям Рубикон-К

Процедура предоставления покупателям Рубикон-К обновлений БРП в общем случае выглядит следующим образом:

10) загрузка обновлений с серверов Поставщика БРП, предоставляющих обновления БРП для Разработчика;
11) проверка целостности загруженных обновлений;
12) обработка БРП;
13) тестирование работоспособности СОВ с обновленными правилами;
14) оценка влияния обновленных БРП на функции безопасности СОВ;
15) подготовка к отгрузке обновленных БРП:
    - формирование архива с БРП;
    - формирование файла с контрольной суммой БРП;
    - формирование файла с временной меткой;
16) отгрузка файлов на сервер обновлений;
17) предоставление обновлений БРП клиентам для загрузки.

15.3 Процедуры и меры безопасности при доставке обновлений БРП

15.3.1 Оповещение покупателя Рубикон-К об обновлении

Разработчик с использованием электронных почтовых сообщений направляет в адрес организаций, эксплуатирующих сертифицированный Рубикон-К «Информационный бюллетень», содержащий краткое описание нового типа вторжения и декларацию факта обновления базы решающих правил для обнаружения нового типа вторжения в течение 1

месяца. Разработчик ведет учет списка атак в документе «Описание новых типов вторжений». Для каждого нового типа вторжения указывается следующая информация: идентификатор, дата внесения в перечень, идентификатор документа «Информационный бюллетень», описание атаки и ее признаки, статус (изменение в БРП внесено/не внесено). Момент появления нового типа вторжения фиксируется в документах «Информационный бюллетень» и «Описание новых типов вторжений».

Предприятие-производитель ведет учет покупателей Рубикон-К. Выполняется регистрация следующей информации: наименование организации, адрес организации, номер знака соответствия, контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование Рубикон-К). Уведомление пользователей о выпуске обновлении БРП правил выполняется с использованием рассылки электронных почтовых сообщений.

15.3.2 Доставка и контроль целостности БРП на стороне покупателя Рубикон-К

Обновления БРП, успешно прошедшие контроль влияния на безопасность Рубикон-К, публикуются в закрытой части сервера предприятия-производителя. Доступ пользователей к закрытой части сервера осуществляется с использованием учетной записи и пароля. При публикации обновления БРП публикуется его контрольная сумма. После получение обновления БРП пользователь имеет возможность выполнить контроль его целостности с использованием механизма контрольного суммирования.

15.4 Предоставление обновлений для проведения внешнего контроля

Процедура предоставления внешнего контроля уполномоченной организации:

- уполномоченная организация обращается к Разработчику для предоставления доступа к обновлениям;
- Разработчик предоставляет организации соответствующее ПО для осуществления контроля (ПО СОВ);
- Разработчик предоставляет организации доступ к серверу обновления на оговоренный срок.

Анализ влияния обновления БРП на безопасность Рубикон-К выполняется на стенде Разработчика (рисунок 81).

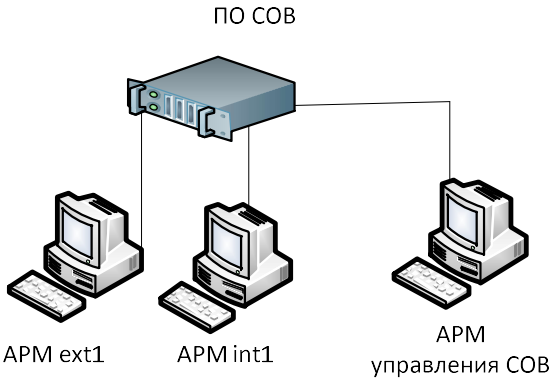


Рисунок 81 - Схема стенда анализа влияния обновления БРП на безопасность Рубикон-К

15.5 Настройки BIOS

Имеется возможность осуществлять управление загрузкой с удаленного АРМ посредством консольного перенаправления. Консольное перенаправление позволяет наблюдать и конфигурировать систему с удаленной терминальной АРМ, перенаправляя клавиатурный ввод и текстовый вывод на последовательный порт.

Базовая система ввода-вывода позволяет перенаправлять консольный ввод/вывод на последовательный порт. Сконфигурировав порт, можно получать удаленный доступ ко всей загрузочной последовательности через COM-порт.

Следующие шаги иллюстрируют, как можно воспользоваться этой функцией:

1) Подключите консольный нуль-модемный кабель одной стороной в консольный порт системы, а другой стороной в последовательный порт удаленного АРМ;

2) Выставите следующие настройки в меню установки BIOS (BIOS Setup Menu): BIOS > Advanced > Remote Access Configuration > Serial Port Mode > [115200, 8, n, 1];

3) Перейти на вкладку «Save & Exit» и сохранить изменения, выбрав «Save Changes and Exit»;

4) Сконфигурируйте последовательный порт на удаленном АРМ. Ниже приведен пример для платформы Windows XP:

a) Нажмите кнопку «Пуск», перейдите в меню Программы> Стандартные> Связь и запустите программу HyperTerminal;

b) Введите имя нового подключения и выберите любую иконку;

c) Нажмите «OK»;

d) Из выпадающего меню «Подключаться через» выберите соответствующий COM-порт на удаленном АРМ и нажмите «ОК»;

e) Установите скорость обмена 115200, «Нет» в выпадающем списке «Управление потоком», 8 бит данных, «Нет» в выпадающем списке «Четность» и 1 стоповый бит.

Для того, чтобы отключить удаленное управление в настройках меню установки BIOS (BIOS Setup Menu), выполнить:

BIOS > Advanced > Console Redirection > [Disabled]

Далее перейти на вкладку «Save & Exit» и сохранить изменения, выбрав «Save Changes and Exit».

Для установки пароля BIOS в настройках меню установки (BIOS Setup Menu), выполнить:

BIOS >Security>Administrator Password и установить пароль.

Далее перейти на вкладку «Save & Exit» и сохранить изменения, выбрав «Save Changes and Exit».